BNY MELLON | PERSHING

Navigating the new regulatory paradigm for privacy

DATA MANAGEMENT FOR TODAY'S (AND TOMORROW'S) ADVISOR

Data protection, privacy and disclosure are sometimes nothing more than business buzzwords. But more often they represent a deep, enduring trend as technological advancements intersect with an increased vigilance regarding the use and ownership of personal information. Recent high-profile data breaches involving Facebook, Cambridge Analytica and Google (to name just a few) are shining an even brighter spotlight on issues like transparency and data protection.

No industry is immune from this changing landscape – certainly not financial services, with its rigorous regulatory oversight, dependency on data collection and inherent reliance on third-party data providers, digital record-keeping and vendor management.

Major regulatory reforms like the European Union's General Data Protection Regulations (GDPR), introduced in May 2018, or the California Consumer Privacy Act (CCPA) may not seem to impact advisors outside of Europe and California, but such advisors would be wise to become familiar with them. Not only are GDPR and CCPA harbingers of sweeping data-related reform to come, but they may also affect advisors who are based beyond the current regulatory jurisdictions.

Defining personal information

It's well documented that the primary objective of GDPR is to protect the privacy rights of individuals by standardizing and restricting how organizations collect and process personal

data. The onus falls squarely on the shoulders of such organizations (or "data collectors," as characterized in GDPR terms) to own the data management lifecycle. The CCPA provides consumers with certain rights regarding how organizations collect, sell or otherwise share their personal information.

What is involved in meeting all of these enhanced data management responsibilities? The task includes:

The initial data collection

Disclosures to the consumers

Storing and securing of information

Processing and transferring information

Data anonymization or aggregation

Disposal and deletion of unneeded information

Over the years, authorities have cast a wider net regarding what is considered personal information, and individuals now have a greater ability to access and control what personal information businesses are holding. For instance, Facebook now allows users to download all of their data, see which advertisers have uploaded their information to a contact list, and control how the service manages any location data it has collected from their mobile devices. In other words, consumers are more empowered than ever before and this trend is poised to continue.

For organizations that breach any of their data management requirements, the levying of potentially severe fines and penalties has dramatically increased as new privacy laws take effect. Regulators hold more influence now and are doing more as well, so American advisors should care about client privacy and data management. When the European Union rolled out GDPR, many data collectors in America examined their businesses and concluded that they don't have any direct exposure because they are not targeting services to residents in the European Economic Area (EEA). In fact, many American businesses may not have complied with GDPR, or even made an attempt, because they weren't prospecting and working with European residents.

But laws like GDPR and CCPA are "extra-territorial." They are not concerned with the location of the organization itself as a business entity that's processing sensitive personal information. They are concerned, however, with the residency of the individuals whose information is in question. So it's a matter of California residents' information being processed anywhere in the world, or EEA residents' information in Europe being processed anywhere in the world. If one of your clients moves to Europe or California, for example, then GDPR or the CCPA will apply and you'll need to comply with the new privacy laws in those regions.

Evolution of regulatory stringency

GDPR has become the de facto baseline for data management compliance, but it's not as simple as saying that complying with GDPR means you're complying with similar laws around the world. It simply means if you comply with GDPR, you've got the highest possible baseline. We have specific laws in America, such as the Gramm-Leach-Bliley Act and Regulation S-P, that require financial institutions to divulge their practices regarding personal information sharing and protection.

Nonetheless, the Gramm-Leach-Bliley Act does not address issues pertaining to modern technology. Under the old framework, there was "nonpublic personal information" (NPPI), such as an individual's name, address or Social Security Number. With new laws coming into play, there's a more fulsome definition of personal information that extends beyond NPPI to include geolocation information, IP addresses, email addresses and even any biometric information you might be collecting. These are some of the important considerations when laws like the CCPA start to encompass other categories of information within the definition of personal information.

For instance, consumers these days have come to expect the greatest convenience when executing a range of online financial transactions, whether they're using a laptop, tablet, mobile phone or other device. Security measures like facial recognition, biometrics, scanning, fingerprinting and eye scanning are now common, but remember that it's all considered personal information and comes with additional data management requirements. If you were collecting disparate pieces of information to create a profile and make business decisions vis-à-vis a client, it might also be viewed as personal information under various laws.

Although Europe is further along when it comes to consumer access to personal information, CCPA is helping Americans take a step forward. In mid-2020, California residents will be able to ask businesses to reveal what personal information they've collected, and those businesses will need to provide their response within a regulatory timeframe. Under these rules, businesses will be obligated to inform California residents about what specific categories of information they have gathered and whether that information has been sold or shared to anyone else.

Bear in mind, third parties provide services being offered to investors. These companies can range from marketing companies, to all types of service providers, including those involved in statement generation or firms supplying an investment model to investors. The new laws are putting more onus on the business to understand and map the lifecycle of that data – in a clear, consolidated inventory – to prove that they know where the data is going, how it's being used, how long it's being retained and ultimately how it's deleted.

Your opportunity to differentiate

Given the potential for severe fines and penalties for non-compliance, advisors should work with their lawyers to develop a defensible position on how they're handling data within the information lifecycle, especially in the event of security failures and breaches. All states have breach reporting requirements, but now CCPA is raising the bar and giving consumers/investors the right to take action. In fact, they can litigate, so there's an extra incentive for advisors and their firms to implement a locked-down process for knowing what information they're collecting, where it's being stored and how it's stored (e.g., file cabinets, systems applications, collaboration tools or even in emails). If you have employees who exchange HR information via email, you need to be aware of that because, whether it's through regulatory inquiry or an investor request, you're obliged to be in a position to provide a replay of the information you have stored.

Your ability to competently respond to those requests may increase the trust that you build with employees, investors and regulators alike. Other potential benefits of strong adherence to privacy legislation are financial, such as avoiding loss of revenue, litigation costs and remediation costs. Another benefit is the effective management of reputational risk. It often takes considerable time and effort to build a reputation, but you may lose it in the blink of an eye. You can avoid damage to your brand by keeping sensitive information secure and reducing your exposure to data breaches. A strong reputation for proficient data management can bolster client relationships. It can also be a valuable differentiator for your practice that can help sway client sentiment in your favor and become a tipping point for prospects trying to decide with whom to conduct their business.

Compliance is paramount because it helps you properly steward your clients' assets, and your reputation and personal brand are at stake as well. When you're compliant on data management issues, you avoid making negative media headlines and drawing regulatory scrutiny, whereas competitors may find themselves front and center if something goes awry and they are heavily penalized for a data breach. You can certainly do without this form of publicity, notably in the social media era of instant worldwide communication and judgement. It can be onerous to monitor, interpret and comply with privacy demands. Already a challenge for larger firms, smaller firms may find complexity and costs daunting. A RegTech strategy – using technology to help firms solve for regulatory and compliance issues – can be instrumental in helping firms of all sizes scale to regulatory demands and comply with new and existing regulations in an efficient, responsive manner.

Advisor best practices

When providing consultative services to our clients at Pershing, we discuss creating or refining a risk-based privacy program that considers all the aspects of data collection, and then taking those key concepts and trying to apply them broadly to a comprehensive data management process. Don't take a "wait and see" approach – you can gain a meaningful competitive advantage by being proactive rather than passive.

We don't recommend trying to comply only with current elements of a given state law, because you should be forward-looking. Instead of focusing on developing a program to comply with California law today, for instance, consider potential new laws in other states/jurisdictions and what nuances these laws may feature, including having different exemptions or different definitions of personal information.

> "Look at your privacy program and information security holistically to uncover common denominators across all laws (or potential laws). It's important to start with this perspective, then work to improve and mature your overall privacy program accordingly."
>
> *-Troy Guinn-Bailey*
> *Vice President, Privacy Compliance Officer at Pershing*

We typically advise our clients to set up a program that broadly applies and has the capacity to create a defensible position in the event of legal action. In addition to collaborating with your firm's legal counsel, try engaging experts who understand complex and evolving privacy regulations. Adopting a cross-functional approach involves performing a thorough analysis of your business and pulling in people from different areas of the organization, such as sales and marketing, data management, information security, compliance, executives and audit personnel, partnering with them from the start to ensure a holistic approach.

These professional functions play a critical role in testing and remediating issues. Together they can offer a robust perspective on the entire business and your data, helping you understand how you process data, whether you have a legal basis for retaining that data, and what is done with the data when you no longer have a contractual or regulatory basis for holding onto it. There could also be practices taking place within the firm that are bespoke and may warrant additional documentation and tailored oversight, and you wouldn't have been aware of them had you not consulted subject matter experts from around the firm to shed light on certain practices.

Be informed, be ready

Pershing is committed to educating advisors on the potential (and often significant) impact of industry regulations, helping them not only to prepare for regulatory change but to seize the opportunity as well. Our global team of experts has the resources and support capabilities to help advisors and their firms manage risk, achieve greater efficiency and drive growth – all while satisfying progressively stringent industry compliance requirements.

To help advisors and their firms navigate the ever-evolving landscape of data management and regulatory reform, we offer a robust educational program, including regulatory and compliance webcasts on various important topics that our legal and compliance teams

conduct roughly once a month. For instance, we may explore privacy regulation, provide a recap of CCPA, discuss upcoming regulatory change or take a look at data privacy laws across the globe. We also provide high-level overviews and FAQs through our marketing center that goes out through our NetX360® tool.

Tips for advisors in smaller firms

Because advisors in smaller firms lack the robust infrastructure, specialized resources and programs of larger organizations, they may need to be more hands-on with regulatory compliance.

1. Privacy notices represent your policies and procedures. Make sure they're up to date and accurately reflect your practices.
2. If you're part of an affiliate and transfer sensitive information internally, disclose it in the privacy notice. Review and address individual rights processing because it's a fairly new concept.
3. When working with third parties, either those that supply data or those you may share data with, such as vendors or data processors, ensure contract language about data handling is fully compliant.
4. Examine how you exchange files with third parties to see if these files contain too much personal information for the task at hand.
5. If you transfer information outside America, disclose it and have the appropriate contracts and data protection safeguards in place.
6. Evaluate your firm's information security protocols to ensure they are current and have appropriate access and entitlement controls.

With our training and awareness materials, our goal is to provide clients with crucial updates and analysis of regulatory change. "We also share best practices among advisors and their firms," says Ken Shatzer, Vice President, Privacy Compliance at Pershing. "We have a constant finger on the pulse of the industry and are regularly involved in industry conversations about data protection and information security, and maintain a wide network of peers, clients and industry trade groups like the Securities Industry and Financial Markets Association to assist with benchmarking."

We conduct calls with our clients' compliance and operations personnel, so in addition to providing consultation services, we can also benchmark by discussing what actions we're taking relative to what our clients are doing.

The industry will inevitably continue to evolve, and data privacy issues and regulations will expand in scope. Advisors and their firms must stay at the forefront of this evolution and be ready to implement new policies, procedures and programs to keep pace. GDPR and the CCPA are just the tips of the regulatory iceberg, as we expect new laws to be implemented in the near future – not only around the world but also in our backyard as more states unveil their own reforms and the potential remains for a blanket federal privacy law.