Get Ready to Go Beyond GDPR

September 2018

Having met the core requirements of the General Data Protection Regulation (GDPR), organizations are now seeing the downstream effects of ongoing compliance and realize there's more to do

TABLE OF CONTENTS

Executive Summary

Having met the core requirements of the General Data Protection Regulation (GDPR), organizations are now seeing the downstream effects of ongoing compliance and realize there's more to do. Cultural change that balances intentional security and privacy by design is required across the organization. It must also be championed from the top at scale. Having external partners to support the transformation will increase the likelihood of success and ensure effective privacy protection, no matter what legislation is in force.

Privacy has been the new normal for nearly two decades, but the General Data Protection Regulation (GDPR) raises the stakes for safeguarding Personally Identifiable Information (PII). It's here to stay and will likely evolve over time and be joined by additional regulatory frameworks.

Understanding that GDPR will change over time is as critical as having met the core requirements of the European's privacy legislation by the deadline. It provides impetus for embedding privacy in the culture of the organization, so it can stay ahead of the curve as additional compliance obligations arise.

While you've likely taken the obvious steps needed to satisfy GDPR requirements, compliance is a state of being, not an end goal. With any legislation, there's bound to be occasional surprises and changes, no matter how well you're prepared. Some less obvious tasks are likely to present themselves. If GDPR is the new normal, it's time to think about how you can make privacy part of your organization's culture rather than just a periodic exercise that checks off boxes from a list.

This means being intentional about compliance, whether it's GDPR or other regulatory frameworks. Otherwise, you're always going to be playing catch-up, which puts your organization at risk. Robust information security practices can go a long way to supporting compliance, but they don't mean you're automatically compliant or guarantee privacy of PII.

With regulatory pressures increasing, compliance is table stakes. You need to go beyond the bare minimum so you're not only ready for GDPR today and tomorrow, but what it will be two years from now and beyond. Embracing privacy by design with embedded security across your organization will enable you to navigate an ever-changing regulatory landscape, so you can more easily adapt to GDPR changes as well as any new privacy legislation that comes along.

Meeting Core GDPR Requirements

GDPR went into full effect May 25, 2018 after a two-year grace period. Like the Y2K deadline, organizations had a heads-up to prepare. But the similarities end there. GDPR compliance is a long-term exercise in maintaining data privacy, not just implementing some code.

Data Privacy

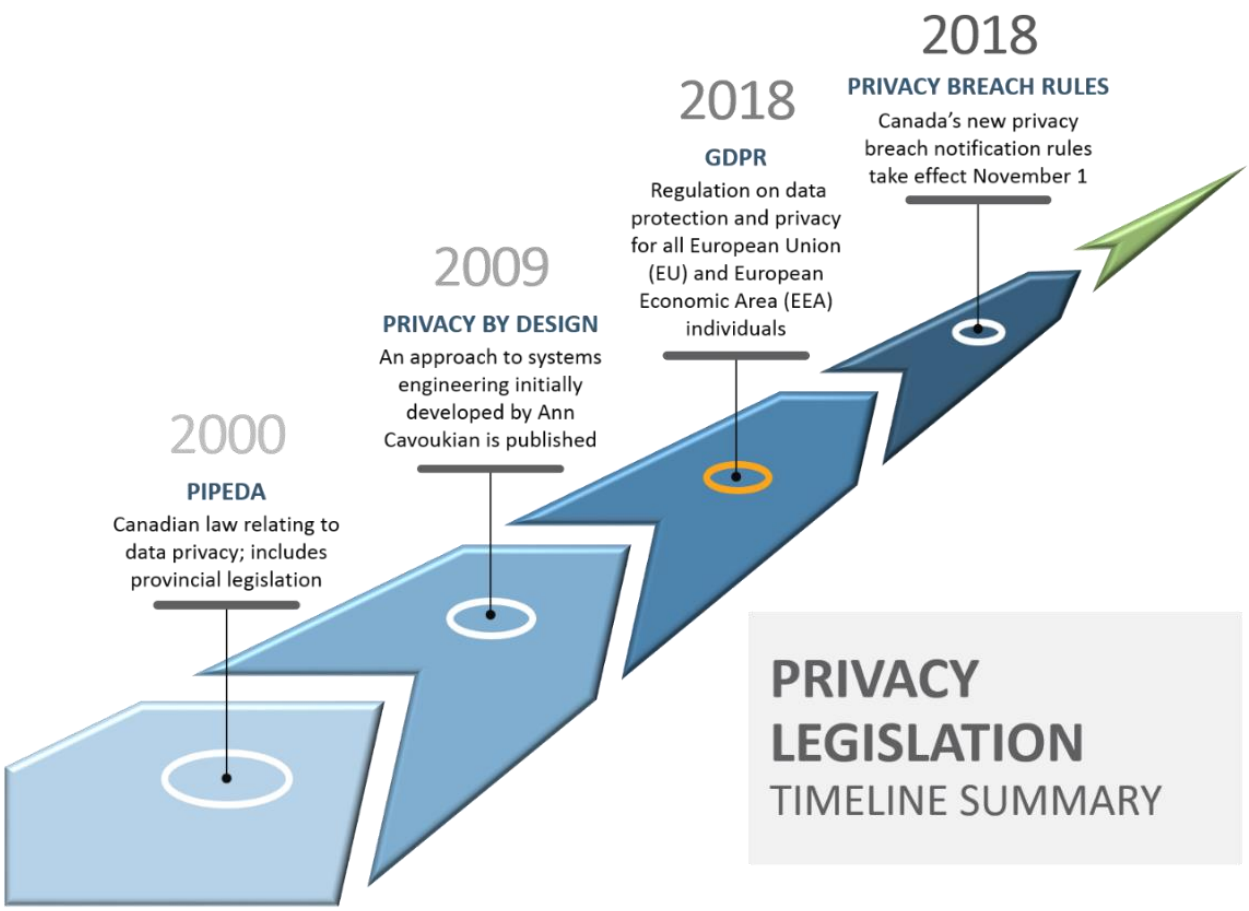
This legislation was jointly enacted by the European Parliament, the Council of the European Union (EU), and the European Commission to strengthen and unify data protection for all individuals within the EU, while securing personal data exported from the EU. What makes GDPR different from previous legislation, including Canada's own Personal Information Protection and Electronic Documents Act (PIPEDA), is that privacy is now driven by citizenship, not geography.

GDPR Compliance is a long-term exercise in maintaining data privacy; that privacy is now driven by citizenship

PIPEDA might have been good for exercising your data privacy compliance muscles, but it didn't automatically mean you were GDPR compliant—you had to figure out if you were in scope by looking at whether you were collecting and storing PII about European citizens. It not only cemented privacy as being an ongoing operational concern but gave you a more stringent set of rules to play by.

Some of GDPR's requirements were clear from the outset. It distinguishes itself with its penalties for non-compliance. An EU organization caught not compliant is subject to fines of up to four percent of a parent company's annual revenue to a maximum of EU20 million. Aside from the hefty price tag for non-compliance, there were other new rules to follow.

Under GDPR, a breach notification must be done almost immediately. The Province of Alberta already had a provision for breach notification under its own legislation, and breach notification is being made part of PIPEDA. From the outset, GDPR required that an organization suffering a breach posing a risk to individuals must notify the relevant Data Protection Authority within 72 hours, and affected individuals without undue delay.



The Right to be Forgotten

The breach notification amplifies GDPR's protection of the citizen, as does another key element of the legislation—the "right to be forgotten."

As an organization, you must get consent from individuals to use their PII, use it only for what it's intended for, and renew consent if the purpose changes—going well beyond the consent required by Canada's Anti-Spam Legislation (CASL). Most of all, the data subject can choose to withdraw that consent, meaning any PII must be destroyed immediately. That puts the onus on you to understand the complete lifecycle of your data, from onboarding to where the data is stored to proper removal of that data.

You must get consent from individuals to use their Personally Identifiable Information, use it only for what it's intended for, and renew consent if the purpose changes—going well beyond the consent required by Canada's Anti-Spam Legislation (CASL)

In theory, deleting PII seems straightforward. In practice, there are many variables depending on the size of the organization and the number of applications that handle an individual's data—many of which operate in their own siloes. A financial services organization, for example, sells different products to the same person—mortgages, retirement savings, investments, insurance and lines of credit. In some cases, these lines of business are mandated to be completely separate by other regulatory frameworks. This can lead to duplicate records, so in practice, the request to be forgotten may not be fully implemented.

And that's just within one organization. Even if you're a smaller company, you may know who all your customers are and where data is stored, but what about business partners and services providers? Most technology providers may have an idea where data is stored, but backups for redundancy generally imply broad distribution across different countries or regions.

Data Protection Officer (DPO)

Finally, GDPR is mandating a critical job posting for organizations if they are a public authority, engage in large-scale systematic monitoring, or engage in large-scale processing of sensitive personal data—that of a Data Protection Officer (DPO), a role regulated businesses were likely to have in place prior to GDPR.

Even if you don't fall into those categories, you may still want to have a person or an integrated team that has the skillsets necessary who can be the point of contact with the Data Protection Authority, as well as retain legal counsel that is up to speed on GDPR.

At its essence, GDPR is all about people having a right to know what data of theirs you have and where it's stored, and then giving you permission to use that data. For large organizations with millions of customers—banking and insurance, for example—it's a lot of data. And it may not be where you think it is. It's one of the less obvious pressures created by GDPR, which is why there's more to do beyond the initial compliance deadline.

Uncovering Lesser Known GDPR Pressures

Having met the core requirements of GDPR, you're now living and breathing the new normal. You're seeing the downstream effects of ongoing compliance and realize there's more to do. Cultural change is required across the organization, and GDPR seeps into your business processes at every turn.

Data Transmission

Now it's clear how important it is to not only know where your data is stored, but how it is transmitted. Exchange of data between countries and regions may not be direct. If you're an international banking organization, for instance, your sensitive business information about customers may not go directly from your Canadian office to your office in Europe—a "friendly jurisdiction" so to speak. Internet traffic can be routed indirectly before it gets to its destination, even though it's pretty much instantaneous. Private data may in fact end up traversing an "unfriendly jurisdiction" and for a nanosecond, it's at greater risk. It's just enough time for a data leak that will make you non-compliant with GDPR, which brings us to another less obvious nuance of the legislation.

Private data may in fact end up traversing an "unfriendly jurisdiction" and for a nanosecond, it's at greater risk

While May 25, 2018 was the deadline meet the core compliance goals, it's assumed that all the standards, practices, procedures and activities will pass GDPR muster. But the legislation is not a reporting regime. You didn't have to report by the deadline that you did in fact have all your ducks in a row. But if you did have a data leak—perhaps in an aforementioned unfriendly jurisdiction—not only could it result in litigation, but the DPA could decide to audit all your activities. If you're not fully compliant, there are serious consequences.

Passing an audit means thinking about how an individual's data is going to be used in a business process. You must think about every customer engagement, particularly when you onboard them, to ensure you have the necessary consent to use their data. But you also must be able to articulate clearly how you will use their information and anticipate how that might evolve over time. People responsible for clients are now playing a role in in compliance—they need to understand how client data is used, transmitted and stored. An employee should instinctively know how to delete all relevant data when a customer asks to be forgotten.

Data Collection

This brings us to a GDPR nuance that may seem counter-intuitive in an era where companies look to amass as much information about their customers as possible to better serve them and sell them more products: Do you really need to collect the data you're collecting? Once you've committed to storing data, you're on the hook if it's compromised. So, the new normal of privacy suggests that perhaps you should only collect information you really need to deliver a product or service to your customer.

Do you really need to collect the data you're collecting?

If you must collect information about your customers, GDPR calls "pseudonymization" out several times as a useful tool to protect PII. The legislation describes pseudonymization as the "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately." With pseudonymization, customer data is broken down so identifiers that could link it to an individual are no longer linked to the other data, making the person unidentifiable unless the data is re-linked.

Data Retention

But regardless of how much data you collect, GDPR also requires you to revisit your data retention policies. Depending on your industry, you're required to hold on to people-generated information—medical records, for example. This means GDPR affects your records management capabilities and best practices. How long do you keep data? How long do you need to keep it? If an individual withdraws consent, you have your answer, but otherwise, you need to balance the benefits of holding on to information with the risk of having it fall into the wrong hands. And no matter what, your records management process must support secure disposal of data.

Your records management process must support secure disposal of data

Data disposal is not just relegated to digital, either. Certain industries are still rather paper-minded – legal and medical offices tend to be full of paper files. Withdrawing consent doesn't just mean someone has to hit "delete" on a keyboard, it may also mean a visit to the paper shredder after tracking down multiple file folders in different offices.

Protecting the Privacy of Citizens; not just Customers

Much of the chatter around GDPR preparation has been about protecting customer data. But it's important to remember the goal of the legislation is to protect the privacy of European citizens, and citizens are more than customers. They're also patients, charitable donors, taxpayers, investors and stakeholders, among others. Your GDPR efforts should encompass more than just the people you sell products and services to.

A data breach doesn't just threaten the privacy of your customers, but anyone involved with your organization

For example, if you're a financial services organization with operations worldwide, there's a good chance you have an office in Europe. And most certainly, you will hire some local people. When you onboard employees, you're going to collect some personal information about them, and that data is going to be in scope of GDPR. Similarly, if you hire a European citizen at your Canadian head office, you need to be compliant. When you think beyond customers, it becomes clear how expansive the scope of GDPR really is. A data breach doesn't just threaten the privacy of your customers, but anyone involved with your organization.

Compliance Requires Cultural Change

Understanding the ramifications of a data breach with GDPR scope brings with it another less obvious requirement, but one that is essential. Compliance requires a culture change in your organization. Getting ready for the initial deadline required certain skills and roles, both new and existing. There were plenty of hours put in by IT folks and the legal department. But in the new normal, compliance becomes everyone's job, and that's a huge shift because data privacy is not the first thing an employee thinks about when they go about their day. They assume IT is keeping company data secure, and hence, keeping PII private.

The challenge, however, is that someone onboarding a new customer is not necessarily thinking about that person's privacy. They're thinking about how they're going to best serve that customer and maximize revenue from the new relationship. However, GDPR is further adding to the tension that exists in most organizations—balancing information security with the need to get things done as quickly as possible. The idea that security should be embedded in applications and business processes isn't new, but GDPR amplifies the need to significant strengthen the privacy aspects.

If you are to make security and privacy part of everyone's thinking, the culture shift must be driven from the top. In addition to executive buy-in—and from your board of directors—you need to have a champion of privacy. This is an additional hat your DPO could wear, or a Chief Privacy Officer. It's not enough to have someone spearhead initial GDPR compliance and be responsible for keeping boxes ticked off. You need someone who can lead that culture shift over the long haul.

Balancing Security & Privacy

Driving a culture of security and privacy throughout the organization doesn't happen overnight. Under GDPR, it becomes an ongoing necessity.

Information security, however, is generally seen as the responsibility of the IT team—most users take for granted that the applications and data they're interacting with everyday have been adequately safeguarded. Further, many organizations assume good security ensures privacy, which in turn means they're compliant, whether it's with GDPR or any other regulation governing their industry.

Security by Design

Good security must be by design. Information Security is everyone's business. That means driving it into everybody's thinking. However, privacy is dependent on good security. But turn it around, and good privacy doesn't automatically mean you have good security. Security and privacy must be done together, and that means breaking down siloes, so they can enable each other.

It's about knowing what data you have, where it's stored, what it's being used for and how it flows through the organization

Traditionally, information security was all about keeping good data in and threats to data out. But thanks to mobile devices, distributed offices and remote workers, there's no longer a clear perimeter to secure. But unlike security, which was about protecting data and information, privacy goes further. It's about knowing what data you have, where it's stored, what it's being used for and how it flows through the organization, regardless of the technology and format.

This is why breaking down siloes is essential to GDPR compliance—security and privacy can and must co-exist, and both must be embedded in the culture of the organization so that people can deliver business processes effectively. Security is being thought of earlier when developers build applications and operating systems. It's no longer something that gets tacked on afterward. Meanwhile artificial intelligence and machine learning is enabling more proactive security in large part because it's no longer feasible to just rely on people to keep up with the ever-increasing threat landscape. Maintaining privacy needs to follow suit and become more automatic.

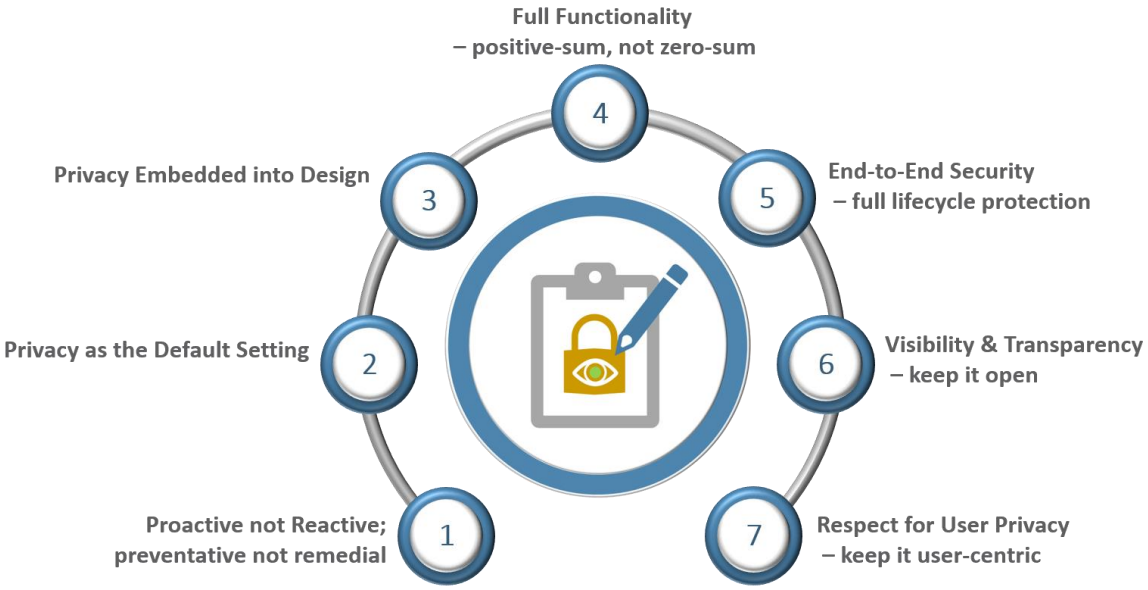
Security by design also means opening a dialogue with various aspects of the organization, so that thinking about security becomes more distributed. That's how it can begin to intersect privacy and support GDPR compliance. Breaking down siloes enables privacy requirements to inform security design, requirements and operations, so it doesn't violate any privacy, but rather, maximizes it. Ultimately, security and privacy are distinct, but equal, and they must work effectively together.

Embracing Privacy by Design

There's a healthy tension that should take place between security and privacy. If you have two people worrying about different things that are connected, they're likely to come up with a better solution by working together. Just as security is becoming more and more embedded in applications and business processes, GDPR provides increased impetus for privacy by design. Marrying the two is critical to making the culture shift necessary for navigating the new normal.

Privacy by design long predates GDPR, and it's been helpful for ongoing PIPEDA compliance. Coined in the 1990s by then Information and Privacy Commissioner of Ontario Ann Cavoukian, the intent of privacy by design was to address the ever-growing and systemic effects of information and communication technologies, and of large-scale networked data systems.

7 Principles of Privacy by Design



Applied to GDPR, it means thinking about privacy first, not after the fact, so it's apt the first of the seven foundational principles of privacy by design is that it's not reactive. Just as good security is about being preventative rather remedial, privacy by design aims to proactive and prevent infractions from ever occurring—this speaks to the culture change that needs to take place and the need for employees to think about privacy as execute their daily tasks. As GDPR raises the bar for privacy, the culture of the organization must be one of attentiveness to privacy and adaptability.

The second principle builds on that idea: privacy is the default setting. Privacy by design means personal data is automatically protected in any business process or IT system, and an individual's privacy remains intact without them having to take any action, in alignment with the intent of GDPR. This is further supported by the third principle: Privacy is embedded into the design and architecture of IT systems and business practices rather than be added later as an afterthought.

As you can see, privacy by design already dovetails with security by design, and the fourth principle illustrates how the two must work together: Good security doesn't have to create barriers. Privacy by design is not meant to be a zero-sum game. The aim is to provide full functionality that accommodates all legitimate interests and objectives—again, privacy can inform security requirements—and create "win-win" scenarios. Per Cavoukian's fifth privacy by design principle, security is end to end, protecting data throughout its lifecycle, once again anticipating the new normal that is GDPR compliance. The goal of privacy by design's sixth principle is to assure all stakeholders that everything is operating with transparency and can pass third-party verification, no matter the business practice or technology involved. Following this principle would enable an organization to skillfully handle a GDPR audit.

Privacy by design's final principle also echoes GDPR's aim to protect the privacy interests of the citizen by emphasizing the importance of the data subject. It requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Intentional Security & Privacy

Embracing privacy by design can help you create a culture that marries security and privacy, so they broaden to encompass a user-centric perspective. But if you don't change the culture, you won't help people understand why things must be different. Changing technology is relatively easy—transforming a culture is a big challenge, particularly in large organizations with many moving parts, especially when everyone is focused on the daily tasks of serving customers and growing business.

However, if you can make security and privacy intentional, it positions you to not only be compliant with GDPR, but to navigate any changes as it evolves and whatever comes next. But this must be done at scale across the organization—one small group of security and privacy professionals led by the most dedicated internal champion won't be able to do it themselves.

Nurturing a "By Design" Culture for Ongoing Compliance

Altering the culture of organizations, especially large ones, is no mean feat regardless of what that goal is. Much like digital transformation, the many moving parts of GDPR compliance touch on many areas of your business, including operations, legal and IT, so there is a strong case to be made for having a champion—perhaps your Chief Privacy Officer or Chief Data Officer—who can drive a culture of privacy by design from the top.

You should assess the level to which privacy and security are done "by design"

Your starting point should be taking stock of your current GDPR status and ability to comply. Having met the initial obligations, you should assess the level to which privacy and security are done "by design." This will require to affirm that you understand what PII is being collected, how it's transmitted and stored, and what it's being used for. You must also be certain you have a process to fully delete PII when a data subject revokes consent. And all this requires the participation of every employee who might collect and interact with the said data for the culture shift to take place.

Given the scope of ongoing GDPR compliance and depending on your available internal resources, it may make sense to seek outside help. One obvious area for outsourcing is the DPO, as you may not require one full-time or have someone such as a Chief Security Officer or Chief Privacy Officer who can liaise with an outsourced resource effectively. In addition, a "DPO-as-a-Service" model can leverage experience from other engagements, including tools and expertise that will support the culture change GDPR requires.

Whether you solicit one partner or multiple partners to support your compliance efforts, remember that they must able to contribute to the culture shift you need to foster and maintain over the long haul. Compliance under GDPR and any other privacy framework is a long-term activity, so you need to think about your partnerships that way too.

Compliance Means Avoiding Complacency

The emergence of GDPR has reinforced how protecting PII, whether it's that of customers, employees, stakeholders, donors or patients, has become intertwined with business processes and day-to-day operations.

Even if you've been successful at prioritizing privacy since the inception of PIPEDA and rose to meet the immediate challenges of GDPR, there's always a danger of becoming complacent about compliance. It's not enough to keep on top of the regulations and how they exist today, but how they might evolve over time. How you do business may change as well, thanks to new competitors, disruptors and transformative technologies, which means you may need to reorient your compliance activities.

It's not enough to keep on top of the regulations and how they exist today, but how they might evolve over time

Being compliant under GDPR, PIPEDA and what comes next is a state of being, one that presents changes and surprises. Embracing privacy by design and imbuing it in your culture will enable you to conduct business in such a way that PII is protected automatically.

IT Infrastructure & Operations Delivery Experts

Email: AdvisoryServices@coreio.com

Main: 905-264-8520

Toll-free: 1-844-261-5803

100 Simcoe Street, Suite 115
Toronto, ON
M5H 3L2