The GDPR (General Data Protection Regulation); four simple letters are causing more than a few Canadian companies to lose sleep. Yet while Europe’s new regulation will surely hold organizations more accountable for their management of EU citizen-related data, the regulation also presents opportunities for those who can rise above their initial adjustment pains to become market leaders in data protection and privacy.

But first, a GDPR primer
Approved by the European Parliament in April 2016, the GDPR will replace the current 1995 Data Protection Directive as of 25 May 2018. When it does, the regulation will extend the scope of the EU’s data protection and privacy law to any entity collecting, managing, or processing data culled from EU residents. Moreover, it will hold those same organizations responsible for ensuring their third-party vendors and partners are complying with GDPR’s rules as well, less either party face financial penalties up to 4 percent of worldwide turnover.

The journey to compliance
The expectations set out by the GDPR are not likely to catch all companies off-guard. North American players in highly regulated sectors, such as banking and health care, have already adjusted to evolving data protection measures (e.g. the Personal Information Protection and Electronic Documents Act and the Gramm-Leach-Bliley Act), and the anticipated arrival of mandatory breach reporting laws in Canada starting November 1st has motivated many to take preemptive measures.

What the GDPR is doing, however, is pushing companies to truly take stock of their data and begin laying a foundation for an ongoing – and proactive – data risk management strategy.

Designing that strategy begins with tackling key questions both within the boardroom and among all relevant stakeholders with a vested interest in leveraging their data assets, including:
- Do we collect EU data from individuals residing in the EU?
- Do we employ anyone in the EU?
- What about our partners/vendors? Do they collect, process or store data from the EU?
- Do we target EU individuals by offering them products and services, or by monitoring them online? Do we track their cookies and online behaviour? If so, where is our risk exposure?

If the answer is “yes” to any of the above questions, the next move is to pinpoint where your EU-related data lives. This step entails a data-mapping exercise to gain a clear and comprehensive understanding of where your data lives within the organization, how it is being collected, for what purpose, and how it is being used to fuel business objectives.

Bias in the Numbers
The calls for data protection and privacy measures have never been stronger. In addition to countless stories of data leaks and privacy breaches, consumers are becoming more aware of the risks posed by poor or inappropriate use of their sensitive data.

Taken out of context or collected improperly, and the results of ‘Big Data’ can lead companies to make decisions that have negative consequences on their consumers or even staff. Think negative credit scoring, denial of employment, higher insurance premiums, or inability to receive service due to incorrect inferences or conclusions made based on their personal data, and one can understand why initiatives like the GDPR are gaining ground.
The importance of data-mapping and achieving this level of clarity is articulated in Article 30 of the GDPR, which emphasizes: “Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities [and] each processor and, where applicable, the processor’s representative shall maintain a record of all categories of processing activities carried out on behalf of a controller.”

Third-party risk
No organization works in isolation. The journey to GDPR compliance requires a heightened level of due diligence around vendor selection and management. It is important to remember that both controller and processors will be held accountable moving forward and, because of this, both will be required to demonstrate compliance or provide sufficient guarantees they have implemented risk intelligent approaches and appropriate safeguards to meet the GDPR’s data protection and privacy standards.

In short, the GDPR brings with it a shift in accountability. In advance of May 2018, all organizations will be obligated to review their agreements with suppliers and data processors and take measures to ensure everyone within the data ecosystem network is protecting the “crown jewels.”

Taking a right-sized approach
There are no boxes to check when preparing for the GDPR – no “one and done” tasks to delegate to a Chief Security Officer. This initiative, at its core, is a call for organizations to embrace a proactive risk management approach, which means embedding the processes, tools, and – most importantly – a culture that places ongoing data protection and privacy as a critical priority.

The need for this risk-based approach is echoed throughout the GDPR; specifically in Article 32, which reads: “Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.”

Translation? Becoming GDPR compliant is not a “set it and forget it” obligation. There is no right-sized strategy for achieving 100% compliance. An organization’s approach will depend on its unique risk exposures, its current data security controls, and the specific actions it needs to take to remedy its identified gaps and data security weaknesses. The right approach will be defined by an organizational, enterprise-wide review with input from across all functions, including privacy champions within the business who must be engaged throughout the compliance journey.

Document, document, document
The importance of documentation cannot be understated. One of the fundamental differences between the GDPR and the past Data Protection Directive or existing privacy laws is the ongoing need to test and provide proof of compliance.

Fortunately, the regulation recognizes privacy seals and certifications and external third party reviews or audits. Here is where Privacy by Design Certification programs can provide a neutral, expert assessment, identifying gaps and areas for improvement, and recommending solutions.

Remember, there is no room for empty promises and assumptions under the GDPR. To be compliant means proving it – a due diligence defense to demonstrate good faith steps toward compliance to comply with all 99 articles of the regulation, and to do so both consistently and accurately.

All hands on deck
Data, as it is often said, is both an asset and liability. While it can drive invaluable market insights and enable companies to target their customers in a meaningful way, failure to protect that information can cause financial, reputational, or legal penalties.

Upholding data security and privacy is a duty that does not belong to any one person or a single department. It is a multi-faceted issue that demands input and engagement from executive management, IT, security, business, legal, and frontline professionals. True, it can be a challenge to unite internal teams in amending processes, systems, and enterprise culture. However, this enterprise-wide approach is essential to becoming a responsible and trustworthy data collector.

A ticking clock
The time to act is now. Rather than view the GDPR as a compliance burden, organizations can leverage the regulation as a guide to becoming a data management leader to earn and retain trust with their customers. After all, the GDPR is not just about privacy, it is about promoting good data governance and accountability – attributes that will become key market differentiators as more and more consumers wake up to the risks of the digital age.