In a digital world, data emerges as a critical business asset, that must be carefully managed and accounted for. Around the world, new and emerging data privacy regulations seek to control how companies store, manage and distribute personal data. While individual jurisdictions may have their own specific requirements and nuances, there are many common themes across data privacy regulations. Companies with an international or global presence can harness the power of modern technologies to adopt a global view of data privacy.

**Why data privacy matters**

Although data privacy is a concern of all companies, it is particularly relevant for banks who collect and process large volumes of data. In most jurisdictions, regulatory compliance is complex and will require business processes and systems to be reviewed and potentially adapted. Additionally, privacy regulations allow for compliance infringements to be enforced with fines. In some cases, the regulation may also allow for private right of action.

All companies will approach compliance differently, but it can be a complex undertaking. Here’s a closer look at what all financial institutions should consider when making preparations for data privacy compliance.
The complexity of consent

Under almost all data protection programs, consent cannot be implied; it must be obtained in writing (or a digital equivalent). Valid consent must be obtained in advance and for a stated purpose. Accurate record keeping is crucial to demonstrate consent, which may be withdrawn at any time.

For the first time in many jurisdictions, banks need to justify why they are storing data. This may conflict with the data maximization advice of regulators who universally encourage banks to store large volumes of customer data to assess risk, and/or prevent money laundering or financial crime. Customer data that has been acquired for one purpose (for example, KYC) cannot be used for another, like marketing.

Banks must understand their data map to define exactly where private data starts, what the data is used for and where the process ends, and complete it before obtaining consent. Technology that automates data mapping can reduce the time taken to complete from months to weeks, boost efficiency and improve accuracy.

Data sharing and open banking

Many are preparing for a new era of open banking and data sharing between banks and third parties. Prior customer consent is a prerequisite in all open banking initiatives, but nuances may apply in specific jurisdictions. Banks must ensure data sharing procedures are robust and that corrections can be made with minimal effort.

For many large banks, this will require a review of existing processes and procedures with some incremental work to extend existing data protection principles. But for smaller banks, or those with third-party processing arrangements, determining exactly where data resides and for what purpose can be a significant undertaking.

In most cases, banks need a data protection impact assessment (DPIA), which documents all data processing activities that might pose a regulatory risk to individuals, along with measures, safeguards and mitigation mechanisms implemented. The DPIA methodology provides a practical snapshot of the organization’s regulatory status.

Conducting a DPIA manually is a huge undertaking that requires continual investment and commitment. Tasks-orientated automation tools have been successfully deployed for other global data privacy regulations to manage the controller documentation and identify gaps or SLA shortfalls.
Turning data protection into opportunity

Despite the challenges that come with implementing robust data protection and privacy measures, it can bring new opportunity. Banks can leverage it to reinforce customer relationships, nurture deeper engagement and cultivate loyalty.

Data compliance also fosters a bank culture of privacy and a new way of looking at customer data, employee data and personal data from institutional clients. By segregating data according to its purpose, it can be used in a more contextually relevant and compliant manner.

The right technology takes the complexity out of data privacy

FIS’ Data Privacy Suite is designed to improve automation, data mapping and gap analysis. These solutions are continually tested in some of the world’s toughest regulatory environments, can be deployed in as little as three months and may deliver a return on investment in less than six months.

To learn more about how FIS’ holistic technologies can help you turn the data privacy challenge into an opportunity, click here or contact getinfo@fisglobal.com.