Data protection and information privacy are defining characteristics of the digital age. To date, 107 countries have put legislation in place to secure the protection and privacy of data. The European Union was an early adopter, with the General Data Protection Regulation (GDPR) in force since May 2018. Other countries have followed with their own data privacy regulations and 2020 is set to be a momentous year for data privacy and protection across the globe.

In the United States this year, the California Consumer Privacy Act (CCPA) was enacted, and new data protection legislation will soon come into force in Brazil and Thailand. Countries like India and South Korea are also joining the movement for stricter data protection laws. While every jurisdiction sets out from a unique position, the common direction is toward the international harmonization of consumer data privacy and protection. Similarly, it makes practical sense for international organizations that are subject to new data privacy laws to adopt a holistic view of data protection to replace disjointed compliance projects in individual jurisdictions.

**Major changes, big penalties**
In nearly all cases, new legislation represents a seismic change in data privacy regulation. Companies that collect personal data must first obtain provable consent from the individual (data subject). Failure to comply can mean massive fines, often based on global turnover and other sanctions, including imprisonment of personnel.
The elements of data privacy all banks must know

1. **Personal data defined.** Most data protection legislation offers a broad definition of personal data related to an identified or identifiable person. Data may be isolated or aggregated, so virtually any data may be included. Personal data held must be documented, along with the source and with whom it is shared. The regulations may call for an information audit across an organization, or within specific business areas. If any data is found to be inaccurate and has been shared, the third party must be informed so that records can be corrected.

2. **Valid consent required.** Consumer consent is a fundamental feature of many data privacy regulations around the world. Where consent is required, the burden of proof resides with the controller. Consent must be obtained in advance and must be free, unequivocal, and provided for a specific purpose. The consumer’s consent must be provided in writing or by other means that prove the data subject’s intent. In many countries, it is deemed that consent has been withheld in the absence of consent. Further, consent may be revoked at any time.

3. **Privacy by design is key.** All services, products and systems must be designed to guarantee privacy and data protection rights. The general principles of data protection should by default be the most protective; it is the decision of data subjects to make them flexible if they wish. Data privacy related to a service or product is taken into account at the point of delivery and from the inception of the product concept.

4. **Designate a data protection officer.** In many jurisdictions, organizations involved in the large-scale processing of data will need to appoint a data protection officer (DPO). The DPO is responsible for data privacy compliance and the management of data subject requests.

5. **Data record processing is critical.** All personal data processing activities must be recorded for the duration of the data subject life cycle. Data controllers must record which types of personal data are collected, why and for how long data will be retained.

6. **Don’t neglect data portability and erasure.** Individuals have the right to request copies of personal data held by data controllers; it must be available in a usable, readable and transferable format. Similarly, individuals can request the erasure of their data provided there is no legal or contractual reason to retain it.

7. **Conduct a privacy impact assessment.** A privacy impact assessment (PIA) tool enables an organization to identify and fix problems at an early stage and reduces associated costs and damage that might otherwise occur. Following the success of GDPR, some data privacy laws specify conditions under which a PIA will always be required, like when new technology is deployed or a profiling operation significantly affects data subjects.
Focus on how to boost efficiency, reduce costs and mitigate risk

In most cases, data controllers and processors must take action to achieve and maintain good data protection and governance to meet the compliance deadlines. Although data protection is complex, an experienced partner can help you mitigate risk, accelerate progress and adapt more efficiently and cost-effectively.

FIS has helped many of the world’s top financial institutions implement technical solutions that offer a solution to the data rights challenge. We adopt a holistic range of modern technologies, including robotic process automation and artificial intelligence that are infrastructure agnostic and non-invasive.

Our 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 return on investment in less than six.

To learn more about how we can help you overcome the data privacy challenge, click here or contact us at getinfo@fisglobal.com.