DATA PRIVACY MOVES TO THE HEART OF ENTERPRISE FUNCTIONS

CONTRIBUTING AUTHORS:
ROBERT BOND, PARTNER AND NOTARY PUBLIC, BRISTOWS LLP
JACKI TREVINO, SENIOR CONSULTANT, ADVISORY SERVICES, SAI GLOBAL

The sheer amount of data generated today has made data privacy and protection more vital than ever for enterprises globally.

Far from being a niche issue, data privacy and protection has become integral to successful business operations. Those that don't spend the time, money and effort on risk mitigation could suffer a combination of financial loss, huge fines for issues such as non-compliance, damage to the brand with consumers and clients, and decreased productivity.

Data privacy professionals are responsible for maintaining their company's trust, reputation and confidence when it comes to personal data, and increased media coverage. Coupled with consumers having far more awareness of their rights, makes this more challenging than ever.

In a globalised digital economy, companies are expected to make important data available to consumers 24/7, 365 days a year. A range of sectors such as e-commerce, healthcare, banking, finance and manufacturing are expected to provide data with no downtime, and customers fully expect their personal information to remain secure. Data protection strategies need to meet these expectations, and privacy policies should be tailored accordingly.

In this white paper, UK-based lawyer and internationally renowned data privacy expert Robert Bond, and SAI Global's Senior Consultant, Advisory Services, Jacki Trevino discuss trends in data privacy and protection, the European Union's (EU's) new regulations and best practices in data privacy and security.

A VITAL CORPORATE ASSET

In this environment, data is now viewed as a vital corporate asset. Additionally, the speed at which business is conducted nowadays means responding to cyber incidents as quickly and painlessly as possible is imperative.

Breaches of customer data privacy and stolen or altered data can lead to immeasurable financial losses and much diminished investor confidence. In 2013, US consumer goods chain Target suffered a serious data breach that eroded the public's trust in the brand. Losses totalled USD $252 million through the end of 2015[1].

Cybercriminals violate consumer privacy because it's immensely profitable to do so. There's a growing multibillion-dollar black market for stolen data, and it isn't restricted to basic personal information such as mobile phone and credit card numbers. It also means the security of internet addresses, bank account details and health records are constantly at risk of being breached.

SAFEGUARDING INFORMATION AND ENABLING TRUST

Citizens and customers expect privacy when it comes to their data, and governments and companies alike have a moral responsibility to ensure it remains secure. To this end, an effective data privacy regime will have three main strands:

- Safeguarding information
- Enabling trust
- Protecting data

Data, and data protection, lies at the heart of all modern businesses – big data analytics, outsourced data centres, cloud, managing the use of social media and respecting the rights of staff when using third-party appraisal systems. These considerations are now part of the fabric of everyday life in our 'always-on', 'always-connected' digital economies and communities.

Data protection is also at the heart of any business involved in commercial contracts, corporate restructuring, mergers and acquisitions, personal employee information and reporting.

Recently, renowned whistle-blower Edward Snowden raised awareness of how much data is out there, and how it can be used for good or bad. He also demonstrated how rapidly information spreads and how difficult it is for the traditional gatekeepers, like established media operations and government departments, to contain the spread of information.

With many publicly quoted breaches in the press, when the worst happens, it's not only shareholder value that's damaged, but the business's brand, trust and reputation.

And often enough, the biggest privacy threat is ourselves. Operator error can cause significant privacy breaches and staff need to be highly educated about their treatment of personal information, especially in the workplace.

1. McGinty, K,M 2015 'Target Data Breach Price Tag: $252 Million and Counting', *Mintz Levin*

REGULATION BECOMES PRIMARY DRIVER FOR CHANGE

Possibly the largest single business driver for data protection is the increased regulation occurring worldwide. Governments have finally recognised the importance of protecting electronic communications and stored data, and businesses that don't comply face large fines.

These regulations often define what information must be retained, for how long and under what conditions. Other laws are designed to ensure the privacy of the information in documents, files and databases.

Meanwhile, protecting privacy has become a lot more complicated since we stopped moving data in physical boxes from one place to another. Companies are now putting aside huge sums of money for compliance, having concluded that doing nothing is no longer an option.

EU UPS THE REGULATION ANTE

There isn't much in the way of global uniformity regarding regulation of data privacy and protection, though there are plenty of sector-specific rules in countries such as the US, and most parts of the world have adopted similar laws. The US, however, has no current filing requirements as a processor of personal data, whereas Europe does and Asia is following suit.

Greater global transparency, permission around opt-ins as well as opt-outs are needed, as people want to know what is being done with their data. The EU is leading the way with its General Data Protection Regulation (GDPR) that comes into effect on 25 May 2018.

The GDPR is the most significant development in data protection law for 20 years, and is already being hailed as the 'gold standard' for data protection. The rules will apply not only to organisations inside the EU, but to those that offer goods or services to EU data subjects. The EU-influenced approach is likely to become globally significant to privacy frameworks moving forward, but there still need to be mechanisms that effectively monitor when data flows across borders.

The European approach to privacy is to guide businesses to not just comply with the law but to take an ethical approach to business. With regards to technology, just because something is possible doesn't mean it is desirable; decisions should be made with ethics as well as efficiency in mind.

Via a privacy policy, the GDPR has more requirements around what information organisations need to provide to individuals before processing their data. Individuals will also have enhanced data subject rights including the right to be forgotten (right of erasure), rights to understand profiling by controllers and third-party data processors, and the right to port their data between organisations such as banks and telecom service providers.

Under these regulations, multinationals operating under the EU's jurisdiction face fines of 2% of global revenue for non-compliance, which could include absence of contracts and failure to implement data protection. This rises to a maximum of 4% or €20 million for transferring data from the EU without complying with the law.

There are eight key protection principles of the GDPR. Personal data must be:

- Processed fairly, lawfully and transparently
- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed
- In accordance with the data subject's rights
- Processed in a way that ensures appropriate security of the personal data
- Kept from being transferred to a third country or to an international organisation if the provisions of regulation are not complied with.

Organisations will need to keep a record of their data-processing activities, which must be made available for inspection, while those whose core activities require monitoring individuals for categories such as criminal-related data, will need to appoint a data protection officer.

Organisations, regardless of what jurisdiction they operate in, should take the following steps to prepare for GDPR:

- Assess their exposure to GDPR by carrying out a data-mapping exercise
- Revisit their privacy policy, consent notices and policies and procedures
- Decide whether they need a data protection officer
- Develop a data protection impact assessment
- Put in place procedures to manage use of third-party processors
- Look into suitable cybersecurity insurance
- Review their international data transfer solutions
- Implement and update policies and procedures and training to staff.

Governments, by and large, are realistic about the burden these requirements place on business. Regulators may offer some flexibility around compliance deadlines, but having no plan or rapid reaction taskforce that can handle a data privacy breach is no longer acceptable.

FINDING THE RIGHT DATA PROTECTION SOLUTION

The best data privacy solutions integrate risk management features to assist enterprises in managing risk and are engineered to reduce the risk of data breaches caused by human error throughout the entire data management lifecycle.

They should also contain scalable backup and data recovery features that protect your entire IT infrastructure including systems and apps, regardless of whether they are stored on-site or in the cloud.

Enterprises that use several cloud applications have an added challenge in that their data is often stored in several locations, often without any standardisation. Cloud data loss prevention solutions therefore need to be extensively integrated with every one of your cloud computing service providers as well as your on-site premises across the whole of your company's operations.

Additionally, your employees can only defend your infrastructure against the loss or misuse of personal data if they understand what they're doing, so it's highly advisable to provide them with training that makes them fully aware of their data protection obligations. Look for a provider that also offers good training courses tailored to support your enterprise-wide governance, risk and compliance procedures.

In today's digital economy, data is valuable, which makes it a target for malicious actors and an asset worth protecting. Including data privacy and protection measures in your organisation's risk management regime is simply good sense. It helps your organisation enjoy data's rich benefits – like customer insights, product information and business insights – while mitigating any potential downsides.