Understanding ethical considerations in data management and what it takes to achieve a high standard of ethics in the organisation by Ben Crew of FTI Technology.

Business and ethics are becoming increasingly interdependent—not only because of regulatory pressures, but because more and more organisations are recognising that ethical behavior is not just the right thing to do, but a must. Investors and the general public are demanding more transparency, more accountability and overall higher standards in corporate conduct. Global Investor Insights research from FTI Consulting found that, “82 per cent of institutional investors believed a company’s value increased 20 per cent or more when it had a positive rating,” across environmental, social and governance factors.

As we now live in a largely digital-first world, ethical principles no longer apply only to an organisation’s physical, environmental, social and financial impacts on society. Ethics must now also be considered in the context of data management and data privacy. Certainly, organisations around the world have been forced in recent years to strengthen information governance, privacy and security controls in response to emerging legal and regulatory obligations, but sound data management is now about more than that. It is also about protecting and shepherding data in a way that builds trust and values each data subject as a person with fundamental rights.

So, how do information governance professionals and data privacy officers do this? How do they move from a discipline focused on what they are allowed to do, to one that focuses on what they should be doing? What are the key ethical considerations we need to address when building policies and programs? And what business benefits can we achieve when we take steps to enhance data subject rights beyond regulatory requirements?

Below are several key considerations that address these questions and support the implementation of ethics in data management.
» Transparency, in policy and purpose. Many data protection regulations require organisations to transparently communicate their privacy policies and intentions for how personal data will be used and to obtain consent for collecting and storing personal data. Often, companies check the box for compliance by publishing a detailed privacy policy, but most of those policies are excessively long and laden with legalese—meaning that few, if any, data subjects are actually able to fully decipher to what they are consenting. This is a prime example of practices that are compliant but do not necessarily meet high ethical standards. True transparency is publishing consent and use notices that are as brief as possible, specific, written in plain language and free from clauses and loopholes that undermine privacy.

» Reasonable use of data. Organisations are hungry for data and ready to leverage it for an array of purposes, including sales, marketing, competitive intelligence, product development, customer service and more. As valuable as customer data is, it is important to remember that the organisation does not own personal information, the data subject does. Therefore, data should only be used in ways that uphold, rather than exploit, privacy rights. This means ensuring that legal mechanisms are in place for data processing and use, continually asking why data is being sold, shared, stored, etc., and adhering to reasonable purpose limitations. More, when sensitive data is being collected, processed, stored and shared, it must be done so with strong protections and security controls to mitigate the risk of breach.

» Awareness of the data universe. With social media and the digital nature of day-to-day life, the boundaries of privacy have been blurred. It can be difficult for legal, compliance and privacy teams to determine what data is classified as personal vs. publicly available data and how different categories of information are flowing throughout their organisation. This is where data mapping comes in. In order to fulfill legal, regulatory and ethical data protection obligations, an organisation must know what data it has, where it is and how it moves between systems and stakeholders. Data maps are also integral to effective response in the event of a data breach. The data map enables the team to determine what systems were exposed, what data resided in those systems, who had access, which data subjects were impacted, etc.—details that are essential to breach investigation, notification and remediation.

» Education among stakeholders. Continually managing and enforcing privacy policies and data use across a large enterprise is a massive undertaking. Various stakeholders will inevitably want to implement new products, services, functions and other business operations involving data that may be subject to privacy obligations—and every time a new use is proposed, the purpose of that use must be questioned against legal, regulatory and ethical considerations. If those requirements are met, privacy notices and workflows must then be revised. Meeting the scope and scale of this level of enforcement requires extensive and ongoing education throughout the organisation. Employees must understand the laws that govern data management and use, and the potential repercussions when sensitive and personal data is mishandled, so that they consistently consult with legal and privacy teams before kicking off a new data-driven initiative. Ultimately, achieving and maintaining a high standard of ethics requires a cultural shift that comes from the top. With trust and transparency woven into the fabric of the corporate culture, organisations will be better equipped to reduce the risk of a breach, respond to regulatory inquiries, maintain competitive advantage and extract value from their data.

As valuable as customer data is, it is important to remember that the organisation does not own personal information, the data subject does. Therefore, data should only be used in ways that uphold, rather than exploit, privacy rights.”


Text by:
BEN CREW, senior director, FTI Technology