

Embrace Data Ethics as an Essential Part of Business Strategy



Not just a matter of regulatory compliance, highly regulated industries and others that are not must consider embracing data ethics as a component of their overall business strategy.

The Data Ethics Problem

According to Deloitte, 9.7 billion data records have been lost or stolen worldwide since 2013. And since it went into effect in 2018, more than 95,000 complaints have been filed relating to the EU's GDPR statute.

Despite advances, legislation is not keeping up with the ethical issues raised by the large volume and variety of data collected. Those issues are bound to impact data-heavy businesses where it hurts, the bottom line.

Indeed, considering today's data-savvy consumers, expanding data regulations and the revenue impacts of poor policy, a comprehensive data ethics strategy supported by robust [data governance tools](#) should not be optional.

Data-Savvy Consumers

Building customer satisfaction and trust provide ample motivation for creating a data ethics strategy. In the modern business landscape, and a world where data breaches continually grab headlines, the conclusion is inescapable.

As data-driven technologies expand, e.g. AI, you can expect the demands for ethical data practices to also increase.



Since the implementation of GDPR in 2018, the marketing privacy landscape has evolved greatly. Experts refer to a major global shift in power to consumers. Sooner or later, B2C marketing leaders will struggle to maintain access to the volumes of consumer data they consume for marketing and advertising programs.

Before the pandemic, experts had forecast a 300% increase in data-related class action lawsuits for 2020.

In addition to evolving privacy concerns, consumers are adopting more anti-surveillance and privacy products. Marketers stand to lose access to a wide variety of data, from IP addresses and device IDs to facial and location data as a result.

Regulatory Fines and Costly Breaches

In a previous post, we looked at current [International and U.S. Data Protection Legislation](#). And fines recently levied against Facebook and Google indicate the seriousness of regulators. Google's recent record GDPR fine by the French data privacy enforcement agency totaled \$57 million, many times larger than previous penalties.

Even without large regulatory fines, the cost of inadequate data governance is high.

IBM's annual "Cost of a Data Breach" report found that the *loss of business* represents the largest cost of a data breach to an organization. It also found that a data breach costs a business an average of \$8.6 million in the U.S. Interestingly, 70% of survey respondents said that remote work would increase the cost of a data breach.

Revenue Impacts

In addition to the damage done by data breaches, more people grow skeptical of how their personal data is handled. Many are influenced by the prevalence of personal data-related stories in the news.

Thus, organizations can leverage an excellent data governance record to establish data ethics as a component of their brand strategy.

Once the province of data innovators like Amazon and Netflix, big data collection, optimization and governance now appears on everyone's radar. Organizations need competitive differentiators. A positive enterprise data governance customer experience potentially provides a good one.

On the other hand, brands will suffer reputation damage if they fail to correct shadowy data practices and weak data ethics. Even in areas that regulations don't cover, consumers demand ethical behavior.

Privacy practices that make it difficult to opt out or push users to consent to broad data sharing will be called out, resulting in brand damage and employee discontent.

The direct cost of non-compliance seems high. But consider the loss of revenue the business will suffer by alienating customers with questionable privacy practices or overreaching surveillance data. Adopting responsible data ethics standards pays off.



Data Ethics Principles

In establishing a data ethics strategy, what are the data ethics principles organizations should consider? You may want to start by asking questions like: What is required? Should we do this? And what could go wrong?

Then consider the following principles:

Transparency – This includes what data is being collected, how it is used, disclosed, and deleted. How algorithms work should be explained and whether you're dealing with a bot or a person.

Accountability – Accountability requires clarity about who authorizes data collection and who sets and enforces the standards. Include the integrity of data sources, identifying and evaluating risks, and the consequences of developing new data sources and uses.

Privacy – Laws around the globe acknowledge privacy rights in our names and likeness, relationships, personal information, and property. Other [privacy issues include data security](#) and knowing who has data about us and how it's used.

Accuracy – Data should be accurate and kept up to date with ways to correct and delete it in place. Data should also be handled and shared carefully to ensure its accuracy is maintained.

Bias – Look to prevent discrimination from being introduced into decisions from biased algorithms or the underlying data.

Look to the Data Experts

As countries and states add to the legal requirements and organizations consider the revenue impacts and adapt to please data-savvy consumers, data ethics strategies stand to grow in importance and visibility.

Messaging Architects encourages every company to begin the journey of creating a viable data ethics strategy by adopting a set of data ethics principles to follow. As always, our experts stand ready to assist with data ethics, [information governance](#) and [regulatory compliance initiatives](#).