TRUATA.

Don't believe the hype:

Data Privacy Myths are a Ticking Time Bomb

The extent to which a business analyses and acts upon its data can have a massive impact on its bottom line and ability to stay competitive in the marketplace.

For businesses large and small, this presents a conundrum: how can we use data to our advantage, while maintaining consumer trust and complying with data protection laws?

Dr. Maurice Coyle
Chief Data Scientist at Truata

It may be that the sheer volume of hype around GDPR and ensuing torrent of online 'guidance' has overwhelmed and confused businesses. But however it happened, many businesses now fall into one of two equally unfortunate camps. Either they fail to make the most of their data, which is a valuable asset that could drive their business forward, or they run the risk of reputational damage and incurring fines or other sanctions for breaching data laws.

The result?

The worst of all worlds – companies are not realising the full value of their data while consumers don't trust those very same companies to handle their data responsibly.

Even worse, popular myths surrounding the GDPR mean some well-intentioned companies who are attempting to respect the data rights of their customers are operating under a false sense of security and may come under regulatory scrutiny. This is terrible – both for brand value and for business.

But it doesn't have to be this way. If businesses get a grip on the facts of GDPR rather than the myths, and realise that it's perfectly possible to crunch data and still comply with the law, they can put data and analytics to best use and greatly enhance performance. Even better, they can do this without fear of regulators and their punitive powers, or of alienating their customers by being accused of abusing their trust.

The risks of using personal data

A key requirement for analytics is historical data, but identifiable personal data is tightly controlled under GDPR. Not only must businesses have a legal basis such as consent from the data's owner to process it, they must make sure that any consent received is for a specific purpose. And they may need to obtain fresh consent for each new purpose with separate legal bases required for analysing data and targeting customers, for example. Consent as a legal basis is not necessarily a good fit for analytic purposes because of these constraints.

This is every bit as challenging as it sounds and consent rates below five per cent are not unusual, leaving many companies with seriously patchy or incomplete data sets. The size of data sets available for analyisis is reducing with an adverse effect on accuracy.

The outcome?

The outcome for businesses is often poor. Not only is a huge percentage of data missing, there is also an inherent bias between data owners who give consent for processing and those who do not. This, combined with a shorter data horizon caused by strict data retention periods under GDPR, generates an inevitable adverse impact on data analytics.

Genuine anonymization is the key

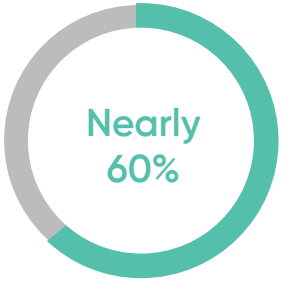
Analytics conducted using truly anonymized data is not subject to privacy laws. But the bar has been raised on what is considered anonymized.

To achieve "true anonymization", businesses need the right expertise and data-handling infrastructure. Beyond that, there are plenty of myths around the anonymization of data which also need to be navigated.

What are the myths?

The first myth is that encryption is anonymization. Businesses that analyse and archive encrypted data often believe they are complying with GDPR, but this is not the case. Encryption does not equal anonymization because it is possible to reverse it. Encrypted data is still personal data and therefore the full requirements of GDPR apply. Advances in cybercrime mean criminals are getting better at decrypting data, for example through brute force attacks and various ways to compromise decryption keys – these render sensitive data unprotected. So while encryption does enhance privacy, it is a security mechanism and cannot be considered as anonymization.

In a similar way, in-house anonymization often fails to meet the requirements of GDPR, particularly when the original data source is not deleted. Removing identifiable elements from the data set is not enough, when the original (identifiable) data remains in the hands of the original controller of that personal data and in fact data must be aggregated to the point where event-level detail no longer exists in order to meet the threshold for anonymization. This has been echoed by data protection authorities, with the Irish and Dutch DPAs both publishing opinions that if anonymized and original data sets are maintained by the same controller, the data is considered pseudonymised/ personal data and subject to the provisions of the GDPR.



of consumers are uneasy with companies using their personal data for analytics*

Addressing the problem

However, businesses can address this problem if they de-identify their data and then transfer that data set to a third party with the expertise and infrastructure to become a controller of the data and further anonymize the data in accordance with the law (while also taking on responsibility for compliance with GDPR in respect of that data).

Companies can then work safely on complete sets of anonymized data to gain all the benefits and insights advanced analytics can provide.

* Truata 'Customer State of Mind' Survey 2019

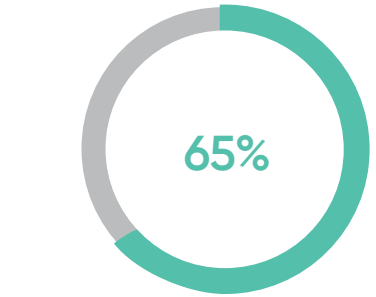
Buyer beware

A clear message

From all of this, a clear message emerges. The need to drive value from data analytics is here to stay. But so are privacy laws, such as the GDPR – because they're driven by consumer concerns triggered by the ongoing need for companies to drive value from data. Business reputations and performance rely heavily on the ability of companies to leverage the maximum value of both, to use analytics to drive performance and trustworthiness (including with respect to data privacy) to reassure customers, add brand value and stay on the right side of the law.

The difficulty for businesses

It is very difficult for businesses to achieve all this using in-house resources alone. They have enough challenges to deal with – this isn't another one they need to add to their already-full plates. Finding a trustworthy partner to handle their anonymization instead, enabling them to then focus on serving their customers, including through the use of that anonymized data, will pay off handsomely for companies. Those companies will benefit from better analytics, greatly reduced liability and a commercial edge – the actual trust of their customers - that may be the envy of their sector.



of consumers say they are more likely to be loyal to a company if they trust them to use their personal data appropriately.

Find out more at truata.com

* Truata 'Customer State of Mind' Survey 2019