WHITE PAPER

Thinking Beyond GDPR – Data Management To Get Better Answers For Your Business

Anette Bergendorff and Mark Perrett

09.18 / EB10249 / ALL INDUSTRIES / WHITE PAPER

teradata.

Table of Contents

GDPR and Beyond

In the run-up to the implementation of the General Data Protection Regulation (GDPR), many consumers were bombarded with endless emails from organisations, highlighting new privacy policies or desperately seeking continued consent to be contacted for marketing purposes. As many commentators pointed out, some of these contacts were actually not compliant, either with the spirit or the letter of the regulation.

What seems to have happened in many organisations is what typically happens when new regulatory requirements, particularly those which feature data as one of their major underlying domains, are introduced. Companies identify the minimum standard of technical compliance that they need to demonstrate to the various regulators and then look for the least disruptive way of meeting that minimum standard.

Teradata's position is that this is perhaps acceptable in a scramble to ensure legal compliance, but in today's digital world, where data underpins the viability of your business, levels of ambition and resulting standards should be a lot higher.

Why GDPR

According to surveys, more than 90% of Europeans say they want the same data protection rights across the EU, regardless of where their data is processed. With GDPR, the EU commissioners' intentions are to making Europe fit for the digital age, by updating existing privacy regulations for the protection of personal data "as a default".

The regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business, by clarifying rules for companies and public bodies in the digital single market. With this statement let us think about one example of events or behaviour that the commissioner might have had in mind to want Europe to become 'fit for the digital age'.

Is it transparent to your customer how you processed their data?

Is the data only processed for the purpose that consent was given?

Is data minimised to what is absolutely necessary? (i.e. No unnecessary duplicates)

Have you removed inaccurate data?

Have you enforced storage limitations on data? (i.e. Don't keep data longer than you're allowed)

Is data appropriately secured? Including with 3rd parties?

Let's look at the financial services industry – specifically the giant FinTechs – and the people segments of 'unbanked' or 'under-banked'. Under-banked are people who do not use banking services much, maybe (at a maximum) use a regular debit card and withdraw money, but no other services around. Unbanked are those who do not have a bank at all. Being unbanked does not mean they don't have money, don't want to buy a car or an apartment or go on holiday trips.

The reason why FinTech has grown so fast, and become a leader in many areas, is because the market is so complex and there are so many different kinds of people on the market – it has forced FinTech companies to create services for everyone and learn how to handle all audiences.

The easiest group of customers, when today's banks were originally founded, was the traditional consumer – people who have salary accounts, credit cards, loans, buy insurance and do normal banking. These are the people banks were giving the normal low interest rates and charging quite high fees to. Here is where the world-leading FinTechs are smart, thinking that this segment of consumers is already crowded – so why not instead go after the unbanked or under-banked, which the incumbents aren't really paying much attention to?

There is one problem though, there are millions of people who come with no data, for example in countries such as China and India. They haven't been in the system, so there is no historic traditional data like: salary, purchase transactions, bills and loan payments. They've never been served because the banks don't know them. How are banks going to approve a loan, or how can an insurance company give them health coverage if there's no data? So, they need to look to alternative data sources.

The digital age referred to by the European commissioner, is one where applying and getting a loan happens solely through a web page. The loan provider will say: "We're sorry, but we don't have enough information about you, but we really would like to help you – so we need to know a bit more about you. Please consent to following data sources by opting in."

The loan provider then goes in a needlessly automated manner and collects information from mobile data, social media data, e-commerce data, etc. These unconventional data sources will now, with well thought-out artificial intelligence (AI) scoring algorithms, act as a new type of basis for approving a loan or not. Somewhat scary, since people might, in the future, be valuated or 'scored' based on other things than just their financial strengths or weaknesses.

So, if the FinTechs paved the way in how to view customers with untraditional banking data, the traditional banks are, of course, close behind wanting to do the same interacting with external data providers to get even more data about their customers. This is where GDPR comes into play and it performs on the consumers' side of the digital playing field.

What's Your Level of Ambition?

The fundamental point about GDPR is that it was conceived as a consumer protection device, to protect individuals from the negative impacts of having their personal data used inappropriately or disclosed thoughtlessly. It therefore represents the formalisation of a previously implicit contract between organisations and individuals, which at its core essentially should mean "if you share some of your data with us, we'll use that data to our mutual benefit". Most consumers understand this implicit contract, but have probably struggled in the past to understand the balance of benefit between the organisation and themselves – this is what drives individuals to remove marketing consent, for example.

Again, looking at the current digital economy, it is clear that past hype around "big data" and current hype around "AI" places high quality, auditable data at the heart of most organisation's ambitions for the future. In financial services, communications, retail, manufacturing, indeed virtually every industry, the future is being painted as "excelling in analytics".

GDPR should also provide a vehicle for organisations to fund investment in the fundamental foundations of the coming revolution. AI will not generate business transformation if the underlying data is of poor quality, low volume or unrepresentative of the whole business.

57% of customers will stop doing business with a company that has broken their trust

66% of respondents to a customer trust survey view personal data as valuable and are willing to share it with companies in exchange for some form of value

45% of respondents are willing to share personal data if a company asks up front and makes clear how the data will be used

Data taken from Customer Trust Index with Teradata

Therefore, it is suggested that of the example ambitions cited below, forward-thinking organisations should (of course) be focusing towards the ultimate goal of transforming their business. Teradata would suggest that being fully compliant with the spirit of GDPR is the only way to achieve this transformation.

When approaching GDPR and setting up the initial analysis and project, Teradata's suggestion is to decide the level of ambition before allocating resources and budget. Many companies settle for achieving the first level while others often look to the regulation to see how it can help them find new ways of operating the business.

1. Minimum: only to be able to stay in business = compliant
2. Manage to meet the current or next business plan and goals, as well as metrics
3. Finding new opportunities and revenue
4. Lastly taking a leap, becoming something different, transforming the business

Formulating these plans is in effect developing a data strategy or an analytics strategy. All mature organisations have a strategic plan, a marketing plan, a sales strategy and most will have detailed IT plans designed to support these strategies. Understanding and deciding on the role and function of data in organisations is equally important as the

CASE STUDY

Large European Bank

7 MONTHS 4 WEEKS

A large European bank spent seven months manually documenting the end-to-end data lineage from source systems through to report production for a regulatory process. It identified that data passed through five databases before they ran out of time.

Automating the approach: In just four weeks Teradata published source-to-target data lineage that identified how the business process accessed data from 74 databases on multiple platforms (Teradata, MS SQL Server/SSIS, Oracle, into Excel) with data finally going back to Teradata for reporting.

Outcome: Verified accuracy of data lineage, redirected users to accurate data, removed >30% of data not needed and reduced ongoing costs.

move to digital continues. Fundamental questions would include the value of both individual data and a statement of value exchange with customers: “if you share this data with us, we’ll give you this in exchange.” To give an example, one of the authors of this paper was once offered £5 for his TripAdvisor username by an international credit card company. Great idea, but that valuation was frankly insulting.

Historic levels of marketing consent, often running below 50% of the customer base, would also suggest that lack of access to data could even represent an operational risk for many businesses. To mitigate mishaps like the TripAdvisor example companies need to have a data strategy, which sooner than later will find its way into the boardrooms because data is the core asset for revenue in almost every business. Having an implicit or explicit value of data to the business but also to the customer is likewise highly desirable, but in practice rarely achieved, even when considered.

The Customer Owns Their Data

If the protection of their information is guaranteed, many people will gladly trade their data for benefits, such as better health management or autonomous driving with fewer road deaths. The benefits of such data analysis are high, comprehensible and clear.

People don’t want to pass on their personal data unrestrictedly and uncontrollably to companies, which then derive the sole benefit from it. Unlimited access to location and contact data in exchange for Wi-Fi at the airport? That’s a bad deal for customers.

But it is equally clear that progress today is first and foremost digital progress – and without data there can be no digitalization. Businesses and consumers alike depend on access to data. How’s that going to work together?

We need a new deal for the management of data. A new balance between organisations and individuals. Personal information for personal use. Public data, sensor data or aggregated and anonymised data for many important purposes. This is fair and will not harm strong sustainable business models.

Those companies that are prepared will recognise clear-cut benefits; consumers will be more likely to trust an organisation that looks after their personal data. The best companies will keep their customer data private. There will be a competitive advantage in being ethical. Teradata has developed the Customer Trust Index to focus attention on this aspect of data management but also to try to provide an objective and comparable way to assess just how well companies are doing in adhering to the spirit of GDPR legislation – because Teradata believes in taking the concept of ‘Privacy by Design’ a step further to ‘Trust By Design’.

Knowledge is Power

Companies need a full and working overview of the flow of their personal data, end-to-end. Understanding and becoming compliant with GDPR relies on knowledge of where private data is held, how it is secured, who has access to it and when and where it moves. For any business that wants to hold or process privileged information, proving that they aren't vulnerable to potential privacy breaches is essential. Know your private data, and your right to hold it, in detail.

Gathering this type of information cannot be done manually – degrees of automation are required and Teradata offers a number of approaches suitable for large organisations to track data lineage and provenance.

In large enterprises, excel sheet documentation will not be enough. For smaller enterprises, inexpensive solutions to data management outweigh the financial and reputational consequences of being irresponsible with your customers' data. Which then comes back again to the reality that we're sitting on so much data, and it raises the questions: how much data do we want to surface? Are data subjects or citizens ready to understand what we have? And are they able to make decisions based on that? Hopefully this generation of more ethically-minded engineers or data scientists will start thinking in that way as well.

Teradata's position is that how an organisation chooses to orchestrate analytics should first and foremost be driven by the desired business outcomes. These will vary by industry and by business, depending on ambition and maturity, but may include a prioritisation of revenue growth, improved customer experience or dramatic increases in operational efficiencies. However, implementing the most appropriate information architecture is then the next priority.

A Question of Architecture

Data protection is not just a regulatory issue. Good data protection is also a question of the underlying technology, which can reflect the legal requirements. With the GDPR, many organisations must meet technical regulatory and analytical requirements.

For example, are you set to make data anonymous wherever possible, encrypt only sensitive data starting with your data lake or the old databases with structured data? Whichever area you've decided to begin with, make sure you start by finding where various kinds of data is stored within the company.

Having knowledge about your data and being aware of how to protect personal data in every way is defined as 'data protection by design and default'. Which basically is about knowing what data do you collect by default and what do you pass on by default? What happens when you start turning things off and who takes on the responsibility to turn things on again. That's a default.

In times of GDPR, leveraging a comprehensive data architecture proves to be an advantage; organisations can clearly determine where data is located and to what degree of detail. This allows them to delete the data if necessary and assign the access rights as appropriate. Baking in the functional requirements for compliance with GDPR, at the point of specifying that architecture is critical. It is for this reason that Teradata has a consulting role described as "Ecosystem Architect". Our consulting services take a holistic view to the development of both a technical and a functional architecture, which ensures that considerations of data lineage, quality validation and auditable exploitation are embedded in the design.

What Does Teradata Offer

Teradata is uniquely positioned to help organisations design for the future. Our consulting methodology begins with understanding your desired business outcomes. We have a vision for the future of your industry and a clear understanding of the choices that need to be made to support your specific focus – we employ senior business specialists from all major industry sectors who have delivered value both as practitioners and also as consultants.

We can review your current analytical capabilities across a range of dimensions, including architecture, technology, tools, people and process. We develop analytical roadmaps for our clients, which ensure that individual initiatives are implementable at scale. Our end-to-end view, from data source to business outcome, ensures that the requirements for GDPR are considered at every stage and that appropriate decisions are taken to ensure the right balance of compliance against business value.

If you believe you have met the minimum requirements of GDPR successfully, but have a vision for doing more, contact us for an introductory discussion. We have proven expertise in delivering analytics strategies, information ecosystem architecture and ensuring that genuine business value is delivered from your information assets. We have automated tools to help track data through the organisation from point of acquisition to operational usage. We also have happy customers who we've helped realise the value of data and who are already reaping multi-million dollar benefits from transforming their organisations to be data-centric, whilst at the same time keeping their customer's data safe.

Examples of how we've helped our customers include:

- Automated assessment of data lineage. In one client, we discovered that a process the client thought comprised some seven data sources in fact utilised over seventy sources – an oversight that could have had profound implications from a GDPR compliance perspective. We discovered this in four weeks after a failed seven month (manual) project that the client undertook themselves.
- Database encryption services, to support information security and protection of personally identifiable information (PII).
- Data anonymisation by using synthetic data, GPUs and deep learning.
- CDPs/CDVs (customer data platforms/customer data vaults) – integrating customer data cross storage locations within companies.
- Data portability capabilities to adhere to one of the subject access requests (SARs) of GDPR.
- Consent management database to store and keep track of all consent from different front-ends.
- Forensic analysis of existing data warehouses, identifying in some cases huge duplication of data sets (in one case, hundreds of instances of essentially the same customer data set).
- Outlining the company's data strategy to reflect the business model and other operative strategies.

17095 Via Del Campo, San Diego, CA 92127 Teradata.com