THE COMING CONSUMER DATA WARS

NEW EUROPEAN DATA PROTECTION REGULATIONS WILL CHANGE MORE THAN MOST COMPANIES EXPECT

Thierry Mennesson

When companies come looking for permission to use their European customers' data after the General Data Protection Regulation (GDPR) takes effect on May 25, 2018, the answer may well be no. In a recent survey of 1,500 British consumers, our company discovered that as many as half said they were already leaning toward reclaiming their information.

That gives companies less than 12 months to figure out what it will take to get customers to say yes – as well as to figure out procedures and safeguards to assist consumers with accessing, editing, exporting, and deleting any or all of their personal data. And neither job will be easy.

The GDPR complicates business models for both European and US companies. While President Donald Trump removed requirements in April for internet service providers to obtain permission from customers before sharing personal data, the GDPR will still force US companies to deal with the new data rules if they want to do business in the EU – a juggling act that could prove expensive.

But the greater challenge ahead may lie in the anticipated consumer data wars that will arise between the companies that customers trust enough to compile their personal data and the companies forced to let their data go. In this environment, the "haves" will be able to keep customizing and improving their offerings to EU citizens using more data than they ever dreamed accessible. At the other end of the spectrum, new products and services sold by the "have-nots" will likely emerge slowly – or worse, miss the mark entirely because of the lack of insight into evolving customer needs and tastes.

ENTICING CONSUMERS TO TRANSFER THEIR DATA

With the GDPR, companies will be able to access data from both rivals and players outside their industry by enticing consumers to transfer their information. One way this could be accomplished is by offering better prices and services to customers who park their personal data with them. Traditional barriers to entry based on data collected over decades will be demolished, enabling small and nimble tech-based competitors that gain consumers' trust to grow into giants. The good news is that companies can get ahead of this inevitable shake-up by thinking and acting more like consumer-data champions. To keep customers' trust, most enterprises will strengthen safeguards against security breaches. Companies will likely add a chief data protection officer to their executive ranks and hire data protection managers, as stipulated in the new law, to oversee the huge number of procedures and processes the law will spawn, including technologies to capture unambiguous consent for personal data use.

The GDPR complicates business models for both European and US companies

GROWING MARKET SHARE AND ENHANCING PERSONALIZATION

While there will be headaches in getting the technicalities right, GDPR gives companies the opportunity to grow their data-market share and enhance their customer experiences. By consolidating and using all the data at their disposal, including potentially from competitors and other industries, companies will be able to increase the level of personalization in existing product lines, as well as create new ones. For example, European banks' retail fees have been under pressure, and some banks are exploring how GDPR could

EXHIBIT 1: NEW EUROPEAN DATA PRIVACY REGULATIONS

Five steps that companies must take to achieve sustainable GDPR compliance

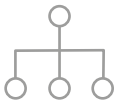
1 MOBILIZATION

Appointment of Data Protection Officer

Privacy impact assessments

Assignment of accountability for data management

Creation of program structures to implement change



2 MAPPING

Creation of centralized data registry

Centralization of consent handling

Monitoring of usage against consent

Review of subject access and breach reporting procedures

3 INTEGRATION

Integration of existing systems with centralized data registry

Redesign of customer interface to capture consent

Creation of a factual audit trail

4 CONNECTIVITY

Creation of customer portal to allow customer to amend the consent given and access their own data

Integration with third-party data sources

Integration with third-party service providers

5 RELIANCE

Fostering of a market for "input" data services (such as collection, storage, classification, verification, and analysis) and "output" data services (such as credit rating, KYC, and AML)

Outsourcing of data management to third parties

Source: Oliver Wyman analysis

offer them the opportunity to charge fees for new types of advice and services.

Here's how this might work: Your bank currently has a limited view of your life through your bill payments. It knows you pay a certain amount to your electricity provider, for example, but that's it. With the new regulations, your bank will be able to tap into the data behind that bill when you agree to share your personal data with it – it will be able to see when you use electricity and for what purpose. As a result, your bank could begin to act as an electricity broker of sorts, potentially promoting a competitor utility's cheaper or better services. Banks could charge clients a small fee for this service and also collect a referral fee from the companies that they promote.

PROVIDING A "DIGITAL SAFE" FOR GUARDING DATA

Some companies may even become the go-to store for managing individuals' data for them. GDPR empowers EU citizens to move all the data they have at their various providers (for instance, Amazon, Vodafone, and so on) to one place – say, a "data safe" provided by a bank – and ask the other providers to erase their data. By providing a digital passport of sorts, companies could help people securely store their personal data and limit its access to businesses they trust.

Companies managing people's data could dominate the marketplace by suggesting where and how customers might want to shop, what they might want to buy, and how they should pay. After reaching a critical scale,

a company could even negotiate bulk deals on behalf of its customers for hotels or mobile phone services, for example.

Some may assume that these new-fangled data-management companies will be digital startups. But the new law could just as easily propel traditional companies with more solid customer relationships to the front of the pack.

Keeping consumers' data safe is about to become even more costly. But it is also going to become more critical. And companies caught unprepared by GDPR may lose the privilege of keeping consumers' data – period. The solution lies not in focusing on how to do the minimum required, but in devising ways to use the law to forge new business lines that will change the economics of consumer-data privacy protection. Those that embrace the future under the new law may find themselves with access to unclaimed digital territory.

Thierry Mennesson is a Paris-based partner in the Digital and Financial Services practices.

This article first appeared in MIT Sloan Management Review.