The joys of data hygiene Europe’s tough new data-protection law

Complying will be hard for businesses, but it will bring benefits too

Print edition | Business

Apr 5th 2018

BOOK clubs usually meet to discuss literature. But members of DataKind, a group of volunteers that helps charities use data to improve their services, are gathering in London to study a legal text. The General Data Protection Regulation (GDPR), set to come into effect on May 25th, is arguably the most complex piece of regulation the European Union (EU) has ever produced. A thick print-out includes its 99 articles and 173 preliminary comments. Gianfranco Cecconi, a data scientist leading discussions, is poring over a lengthy section he has annotated in red pencil.

After years of deliberation on how best to protect personal data, the EU is imposing a set of tough rules. These are designed to improve how data are stored and used by giving more control to individuals over their information and by obliging companies to handle what data they have more carefully. Recent revelations that Cambridge Analytica acquired data on Facebook users in underhand, and possibly illegal, ways has underscored the need to tighten lax regimes. On April 4th Facebook raised its estimate of the number of people involved from 50m to 87m and admitted that many more may have had their details scraped from its website.

Mr Cecconi is not alone in trying to get to grips with the GDPR. The tentacles of the

new regulations reach far beyond Europe. It applies to businesses and other organisations around the world if they collect or process the personal data of EU residents.

Unsurprisingly, there are many complaints from companies about the law's complexities and the bureaucratic burden it will impose. Critics also argue that the GDPR will stymie innovation in Europe: for instance, by making it more difficult for firms to develop artificial-intelligence services, for which data are the main input. When firms launch a new offering, they may have to ask people again whether they can use their information even if they have already stored it (although the GDPR allows for use of data for scientific and statistical purposes without further consent in some cases).

Yet amid the gripes, there are also positive noises. "The text is actually quite easy to read and it makes organisations like ours aware of the data they hold," says Mr Cecconi of Datakind. "It has helped us to put our data house in order," agrees Daniel Ross, a lawyer at Allscripts, an American firm that helps hospitals and doctors manage electronic health records. The unexpected welcome stems from the fact that the GDPR is "two-faced", in the words of Viktor Mayer-Schönberger of Oxford University. It imposes costs but also structure.

The new law was mostly written by privacy-conscious Germans. Consent to collect and process personal data now has to be "unambiguous" and for "specific" purposes, meaning that catch-all clauses hidden in seldom-read terms and conditions, such as "your data will be used to improve our services", will no longer be sufficient. "Data subjects" can demand a copy of the data held on them ("data portability"), ask for information to be corrected ("right to rectification"), and also request it to be deleted ("right to be forgotten").

The GDPR is prescriptive about what organisations have to do to comply. They have to appoint a "data-protection officer" (DPO), an ombudsman who reports directly to top management and cannot be penalised for doing his job. They also have to draw up detailed "data-protection impact assessments", describing how personal data are processed. And they have to put well-defined processes in place to govern the protection of personal data and to notify authorities within 72 hours if there is a breach. Companies that persistently ignore these rules face stiff fines of up to €20m ($25m) or 4% of global annual sales, whichever is greater.

As a result the GDPR ensures that all organisations which collect and keep data will take their use (and abuse) much more seriously. Take the fines. Under the GDPR's predecessor, an EU directive dating from 1995, fines were negligible. The upshot was that firms gave data protection little attention and few resources. But the risk of hefty penalties has raised privacy to a board-level matter. "We have support from the top down," says Susan Bandi, who is in charge of data security and privacy at Monsanto, an agrochemicals company.

The GDPR obliges organisations to create an inventory of the personal data they hold. With digital storage becoming ever cheaper, companies often keep hundreds of databases, many of which are long forgotten. To comply with the new regulation, firms have to think harder about "data hygiene", explains Ms Bandi: what type do they have, what are the risks in keeping the data, how do they have to protect them and, not least, do they really need to keep them?

Mastercard, for instance, has built portals for card holders to check what data are

being kept. Efforts of this sort have made the company “more mindful” about how it treats personal data, says JoAnn Stonier, Mastercard’s chief data officer. Such mindfulness will spread. Firms have to make sure that businesses from which they receive personal data, and ones to which they send such information, are also in compliance. The idea is that the GDPR should become self-policing.

As the requirements for handling personal data become more testing, many organisations will increasingly outsource the task. According to Richard Hogg, IBM’s “GDPR evangelist”, they will eventually “run their business without even touching such information at all.” IBM uses artificial intelligence to sift through a firm’s contracts with business partners to find any privacy clauses that need upgrading. Teaming up with Mastercard, IBM also recently set up a data trust called Truata that offers to manage, analyse and protect data on behalf of other companies.

Many of Microsoft’s products also come with data-protection features. Azure, its computing cloud, offers tools that help firms with data-subject requests. To get there will take some time, but the GDPR is clearly speeding up the construction of a global “privacy infrastructure”, in the words of Peter Swire of Alston & Bird, a law firm. The big questions are how far and fast this infrastructure will extend.

So far, of the many companies that need to comply, nearly 60% are not ready, according to some estimates. In some cases, cluelessness is the cause. Many smaller firms, says Liz Brandt of Ctrl-Shift, a privacy consultancy, do not have the resources to organise themselves, at least not in the time European lawmakers have given them. Others are simply content to wait and see what transpires.

Indeed, the eventual impact of the GDPR will largely depend on how regulators and courts interpret the requirements. “The legislation is four to five times more complicated than existing law,” says Eduardo Ustaran of Hogan Lovells, a law firm. “We’ll probably spend the next 20 years figuring out what it means to be compliant.” Mr Cecconi’s optimism may fade if his book club is meeting to analyse the GDPR’s text for years to come.

This article appeared in the Business section of the print edition under the headline "The joys of data hygiene"

Print edition | Business

Apr 5th 2018