TEXT BY GAVIN BLAIR

# Looking out for the common netizen

## The EU's General Data Protection Regulation comes into force

When Facebook CEO Mark Zuckerberg testified before the US Congress last month about his company's dubious handling of users' personal information, he was pressed on whether he would extend the protections of the European Union's General Data Protection Regulation (GDPR) to users globally. His responses did not reassure people outside the EU.

However, for those in the EU, the new regulations will come into effect on 25 May. They will update the previous directive of 1995, a time before multinationals were making billions from leveraging data online. The GDPR strengthens rights individuals have over the way their data is treated; tightens rules on how companies can collect, store and process personal information; and significantly increases penalties for companies that fail to comply with the new regime.

Another crucial aim of the GDPR is to harmonise data protection across the EU.

"In the past, at the EU level, there was only the directive ... a kind of guideline that had to be implemented into national law by the member states," explains Ulrich Kirchhoff, a lawyer at Tokyo's Arqis Foreign Law Office, who has been advising companies in Japan on the new landscape. "But since the directive only provided a certain framework, the regulations varied to a certain extent between member states."

As a result, one of the main problem areas has been cross-border enforcement.

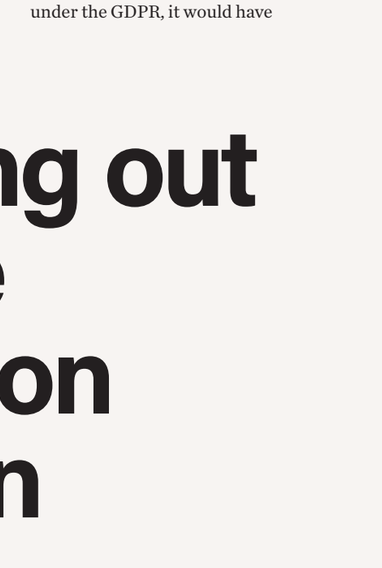
"If you live in Austria or Germany and provided your data to a company headquartered in Ireland, and there was an issue with how they treated your data ... where do you make your claim?" says Kirchhoff. "It will be much easier under the new regulations; you will be able to enforce your rights as a data subject in your own country."

As with many new laws governing areas as complex as this, exactly how some aspects are to be interpreted has yet to be clarified. There will undoubtedly be consequences for companies doing cross-border business, which could be an EU resident buying a product from a website in Japan.

The GDPR's expanded territorial jurisdiction is probably the most significant change to the regulatory environment, potentially affecting companies no matter where they are located. The GDPR will not only apply to the processing of personal data in the EU but also where the processing activities are related to offering goods or services — even when free of charge — to EU residents from abroad.

For a Japanese e-commerce company, for example, to come under the GDPR, it would have to actively be marketing its services to customers residing in the EU, such as by allowing payment in euros or having European languages on its website.

What is less clear, however, is a situation where a Japanese company, or a foreign company operating in Japan, collects data from Japanese individuals and then transfers it to a server in the EU. If it is processed in the EU, then does the legal basis for obtaining the personal data in Japan — not currently considered "safe" in terms of data protection — serve to justify its processing in the EU and a subsequent transfer back to Japan?




According to a European Commission official, "the EU and Japan are currently working on reciprocal adequacy decisions which would be of great benefit for our companies." This would result in Japan being treated "like an EU member state for the purpose of data transfers."

Another complex issue, albeit a more familiar one, is the right to be forgotten. Formally known as "the right to erasure" in the GDPR, the issue has attracted attention since a European court in 2014 ordered Google to allow EU citizens to have some information about them removed from its search results. The US tech giant has since received more than 650,000 requests to remove certain websites from its results.

The GDPR details, clarifies and broadens the scope of the right to be forgotten, making it a fundamental right of data subjects, as well as requiring data controllers to enable individuals to exercise that right. It also clarifies the exceptions to the rule, including freedom of expression and information, legal obligation compliance, public interest and scientific or historic research.

Another change surrounds the issue of consent. The mere ticking of a box on a website or form will no longer give companies blanket permission to do what they will with personal data.

According to Dr Tobias Schiebe, a lawyer at Arqis with a specialisation in HR compliance and labour law, the approaches to obtaining consent from employees in Japan and Europe are very different, something that is being solidified under the GDPR.

"In Europe, under the GDPR ... consent can only serve in exceptional cases as a valid and reliable legal basis for processing of employees' data," explains Schiebe. "[This is] due to the fact that it is often arguable whether consent can be freely given ... due to the subordinate–superior relationship between employee and employer."

Other rights that will be strengthened in favour of individuals under the GDPR include those related to privacy, the right to be notified of a data breach within 72 hours of a company becoming aware of it, the right of access to any stored personal information and the ability to receive and transfer that data elsewhere.

**The GDPR strengthens the rights individuals have over the way their data is treated**

On the companies' side, the requirements for data protection officers (DPOs) will be bolstered, with their roles and responsibilities clearly defined and expanded. DPOs must now report directly to the highest level of management and not carry out any other tasks in the company that could result in conflicts of interest.

Laws are usually only as effective as the sanctions behind them and penalties have also been increased under the GDPR. Companies in breach of the new regulations can be fined up to €20 million, or 4% of annual global turnover, whichever is greater. That is surely more than enough to grab Mr. Zuckerberg's attention. ●