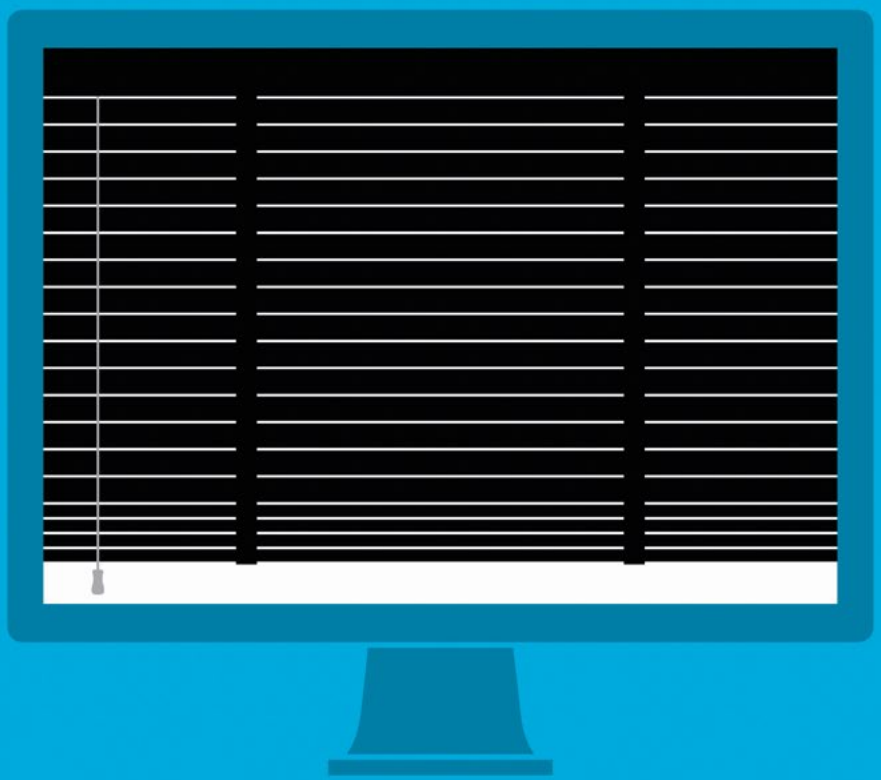

(No) private places

THE ABILITY TO COLLECT, STORE AND SHARE INFORMATION ON INDIVIDUALS HAS NEVER BEEN MORE IMPORTANT TO BUSINESSES, BUT A PATCHWORK OF PRIVACY RULES MAKES FOR A SIGNIFICANT COMPLIANCE BURDEN. DETLEV GABEL AND TIM HICKMAN LOOK AT THE CHALLENGES AHEAD

Legal systems around the world take different approaches to the question of how best to balance the right to privacy with the needs of a modern economy. On the one hand, individuals generally want (and vote for) strong protection of their own privacy. On the other hand, allowing businesses to lawfully use certain information about individuals is increasingly important to global commerce. Striking a fair balance between these competing interests is not an intuitive or straightforward process.

Many countries have no strong laws in this area at all. Of those countries that do have such laws, some (notably the US and Canada) take a 'sectoral' approach, imposing privacy compliance obligations on businesses, based on the nature of their activities. Other countries (notably in the EU, and increasingly in Asia and Latin America) adopt an 'omnibus' approach, imposing essentially the same privacy compliance obligations on all businesses, regardless of their size or the sector in which they operate.

This has meant that international businesses frequently face inconsistent privacy compliance obligations from one country to the next. Even among the EU countries (whose existing privacy laws all stem from a common source – Directive 95/46/EC) national privacy compliance obligations vary significantly. Data-transfer restrictions are much tighter in Germany than in the UK. Data processors need to register with the local Data Protection Authority in Ireland, but not in Spain. Levels of fines for the same infringement may soon be an order of magnitude higher in France than in any other EU country. The relevant privacy laws in the UK only apply to information about living persons, but equivalent laws elsewhere in the EU can extend to deceased persons as well. And so on.

IKON IMAGES

A new sewing kit

The EU institutions, to their credit, have recognised that this patchwork of similar, but not identical, compliance requirements across the EU is unhelpful to anyone who is trying to do business across Europe. In response to this, and a number of other problems, legislators in the EU published a new law, entitled Regulation 2016/679 (the General Data Protection Regulation or GDPR), on 4 May 2016.

It is difficult to overstate the significance of the GDPR from a business perspective.

It is extraordinarily wide-ranging – the rules set out in the GDPR will directly impact every business based in the EU, as well as every business that operates in the EU, even those based abroad. The GDPR is extremely serious – it dramatically increases the maximum fines to the greater of €20m, or 4% of annual worldwide turnover. These figures are deliberately intended to attract board-level attention.

Although the UK is set to leave the EU, it is unlikely that the negotiations of the UK's departure will be completed before enforcement of the GDPR begins on 25 May 2018. Whether the GDPR will continue to apply in the UK after the conclusion of the negotiations remains unclear at this stage.

Perhaps the most ambitious change that the GDPR seeks to achieve is the harmonisation of the data-protection laws of all countries in the EU.

This is no small challenge. First, each country in the EU has its own legal tradition regarding the right to privacy, and national courts with their own case law and precedents on privacy-related issues. Second, each EU country has its own Data Protection Authority, which has its own views on the ways that businesses should be regulated in relation to the use of information about individuals. Third, the EU institutions do not have the power to pass laws in all areas that affect privacy. For example, the EU cannot pass laws regarding employment, national security or freedom of speech – all of which directly intersect with the right to privacy.

Towards a less patchy patchwork

To address these challenges, the GDPR introduces several tools designed to increase the degree of harmonisation within the EU. Most significantly, the legal form that the GDPR takes is known as a 'regulation'. This means that, from the date on which enforcement begins, the GDPR will take effect in each EU country, without the need for national interpretation. The same black-letter law will apply in all 28 EU countries. In theory, this will drastically reduce the number of inconsistent privacy compliance obligations that businesses face across the EU.

But there remains a significant risk that different national Data Protection Authorities might take their own slant on the GDPR, interpreting the black-letter law in light of their own views of how businesses should be regulated, and how the right to privacy should be protected. To address this risk, the GDPR creates a legal mechanism (known as the 'consistency mechanism'), which is designed to ensure that Data Protection Authorities all interpret the law in a consistent manner.

However, it must be acknowledged that the GDPR will not achieve complete harmonisation of privacy laws across the EU. Businesses will continue to face inconsistencies in their privacy obligations from one EU country to the next, because national variations will inevitably persist in some areas. But, there is genuine optimism that the GDPR will mean that businesses face a significantly more consistent set of privacy compliance obligations across the EU.

What should businesses do now?

Having a consistent set of privacy compliance obligations across the EU is really only helpful if businesses understand what those obligations are. Under the GDPR, the obligations are many, and they can be quite technical in nature. Selected examples of particularly important obligations include:

- **Record keeping** – All businesses that are subject to the GDPR will be required to keep detailed records of the ways in which they (and their subcontractors) use information about individuals. This is not a simple task. It requires a thorough understanding of a business's day-to-day operations, and regular reviews to ensure that new business developments and processes are reflected in the records.
- **Appointing a data-protection officer** – Businesses that regularly and systematically monitor individuals, or process sensitive information about individuals on a large scale, must appoint a data-protection officer, who is responsible for data-protection compliance by the relevant business in the EU. A single data-protection officer can be appointed for an entire corporate group, but it is essential to ensure that that person has sufficient powers and resources to fulfil his or her duties.
- **Seventy-two-hour data breach reporting** – The GDPR requires businesses to report data breaches to the relevant Data Protection Authority within 72 hours of detection – an extremely short period of time. The key to meeting this deadline is a decisive allocation of responsibilities, and clear lines of communication. In practice, the person most likely to discover the breach (usually an IT technician), the person to whom it should be reported (usually a member of the legal team), and the person who will make strategic decisions (usually a manager or board member) rarely interact in their ordinary duties. Consequently, it is essential for businesses to ensure that these individuals are used to working together and that they each understand their respective roles and responsibilities, in order to meet this 72-hour deadline.

Although the UK is set to leave the EU, it is unlikely that the negotiations of the UK's departure will be completed before enforcement of the GDPR begins

These examples are illustrative of the significant changes that businesses may need to make, both organisationally and operationally, in order to comply with the GDPR. As enforcement of the GDPR will not begin until 25 May 2018, businesses have a limited window in which to prepare for its impact. It is vital for businesses to ensure that they have set aside enough time, and a sufficient budget, to achieve the necessary changes within this deadline.

Dr Detlev Gabel (left) is a partner in White & Case's Frankfurt office. He specialises in data-protection and technology law

Tim Hickman (right) is a partner in the firm's UK office and advises on all aspects of UK and EU privacy and data-protection law