Willis Towers Watson

HUNTON& WILLIAMS

Technical Insight

Proposed changes to EU data protection legislation

On 14 April 2016 the European Parliament voted to adopt new data protection law for Europe, the **General Data Protection Regulation.** Data protection law will be significantly tightened, and individuals' rights (including to bring claims) will be strengthened. Fines will rise to as much as 4% of global turnover for breach of the law, including data breach. The Regulation is due to take effect in 2018, and will impact all business sectors. Organisations should start now to assess how the Regulation will change their current data protection compliance obligations.

Background

Until the mid-1990s, the data protection laws of EU member states were largely unharmonised. This meant that businesses operating in the EU faced different compliance obligations depending upon national legal requirements.

In 1995 the EU introduced Directive 95/46/EC which created a broadly consistent set of data protection laws for the EU. The directive (like any EU directive) needed to be transposed into the national laws of member states. Consequently, although the general principles of data protection law are similar across the EU, there remain differences between the laws of each member state and so businesses continue to face conflicting requirements. Furthermore, the various EU member states have taken divergent approaches to implementing the directive, creating compliance difficulties for many businesses.

Since 1995, there has been significant advancement in information technology and fundamental changes to the ways in which individuals and organisations communicate and share information. Data in itself has become an increasingly valuable asset for many businesses. The volume of data routinely collected and used by organisations greatly exceeds what could only have been imagined in 1995.

The explosive growth of social networking and big data analytics (among other things) highlighted the fact that the existing law is outdated and that a new approach to data protection is required, leading to the European Commission publishing its first draft of the Regulation in 2012.

The key changes

Challenging for businesses

- Increased enforcement powers
- New obligations of data processors
- Expanded territorial scope
- Consent, as a legal basis for processing, will be harder to obtain
- Privacy by design and by default
- Strict data breach notification rules
- The 'right to be forgotten'
- The right to object to profiling
- The right to data portability

Positive for businesses

- Greater harmonisation
- Risk-based approach to compliance
- The 'one-stop shop'
- 'Pseudonymisation'
- Binding corporate rules

Further detail on these changes overleaf.

The purpose of the new regulation

The purpose of the Regulation is to further harmonise national data protection laws across the EU, strengthen the obligations on those who use personal data, and enhance individuals' rights. At the same time, new technological developments are taken into account.

The Regulation will be directly applicable across the EU, without the need for national implementation. Businesses are likely to face fewer national variations in their data protection compliance obligations. However, there remain areas in which there will continue to be differences from one member state to another.

The key changes – in detail

Changes that could be challenging for businesses

Increased enforcement powers

The Regulation will significantly increase the maximum fine for breaching data protection law to €20 million, or 2 – 4% of annual worldwide turnover, whichever is greater. This is a significant change from the current fines, which vary from country to country, but are comparatively low (e.g. the UK maximum fine is £500,000).

New obligations of data processors

The Regulation imposes obligations directly on data processors who will also be subject to enforcement action. Processors will be subject to fines of up to the same levels as controllers if they breach their obligations. Currently, processors are generally not subject to fines or other penalties.

Expanded territorial scope

The changes mean that non-EU businesses will be subject to the Regulation if they: (i) offer goods or services to data subjects in the EU; or (ii) monitor data subjects' behaviour in the EU. Many non-EU businesses that were not previously required to comply will now be brought into scope.

Consent, as a legal basis for processing, will be harder to obtain

Consent must be freely given, specific, informed and unambiguous, and demonstrated either by a statement or a clear affirmative action. The controller must be able to demonstrate that consent has been obtained, and consent must be capable of being withdrawn at any time. Specific restrictions apply to children's consent.

Privacy by design and by default

Businesses will be required to implement data protection by design (e.g. when creating new products, services or other data processing activities) and by default (e.g. data minimisation). Businesses will also be required to perform data protection impact assessments to identify and address privacy risks in new products.

Strict data breach notification rules

The Regulation will require businesses to notify data breaches within 72 hours where there is risk to affected individuals. If the data controller cannot do this, it will have to justify the delay to the Supervisory Authority (SA). If the breach has the potential for serious harm, data subjects must be notified without undue delay.

The 'right to be forgotten'

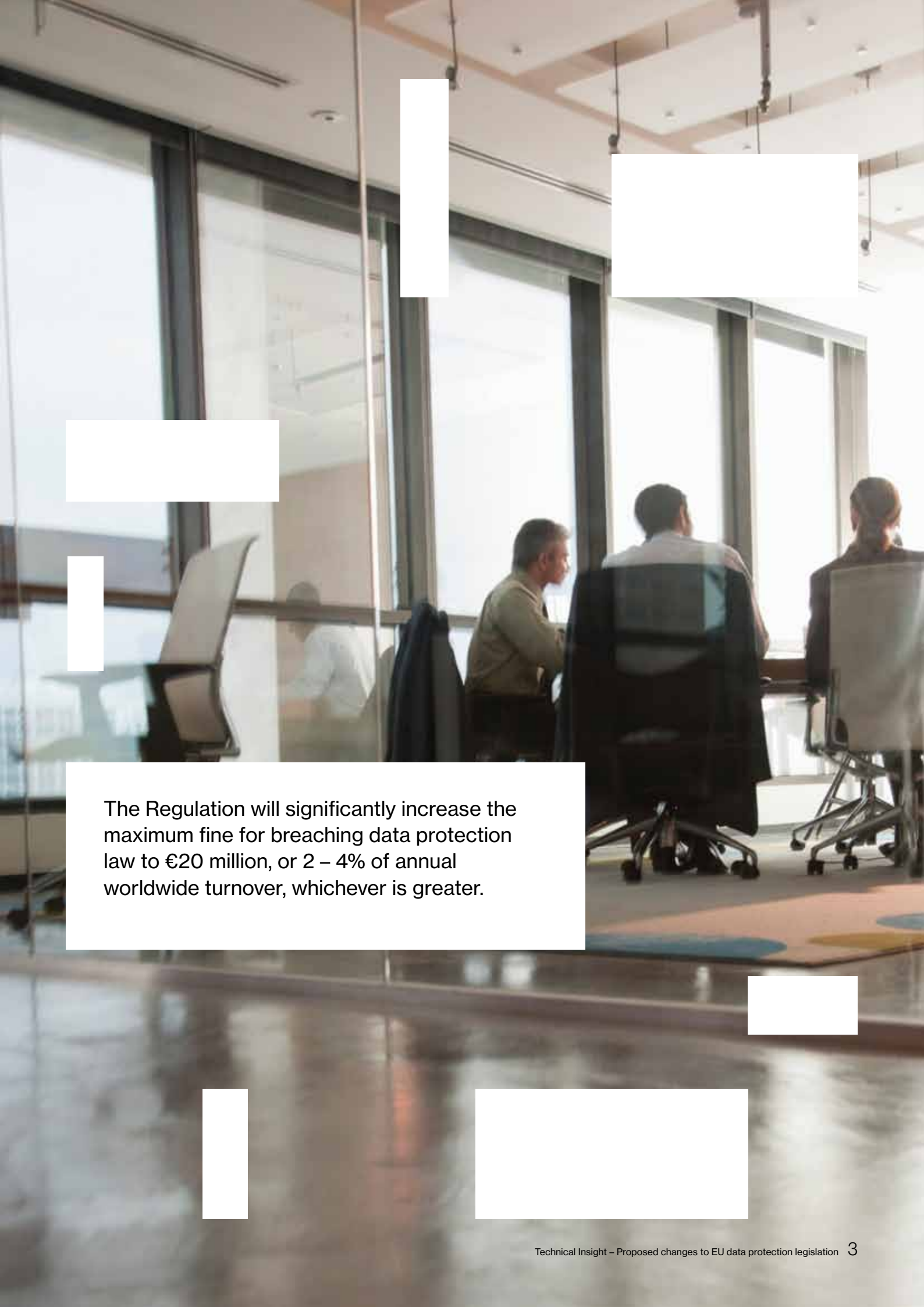
Individuals will have an expanded right to request that businesses delete their personal data in certain circumstances (e.g. the data is no longer necessary for the purpose for which it was collected).

The right to object to profiling

Under the Regulation, individuals will have the right not to be subjected to profiling that 'significantly' affects them. 'Profiling' includes most forms of online tracking and behavioural advertising, making it harder for businesses to use data for these activities.

The right to data portability

The Regulation will give data subjects the right to obtain a copy of their personal data from the data controller in a commonly used format. This will, in theory, enable data subjects to have their data transmitted directly from one service provider to another seamlessly.



The Regulation will significantly increase the maximum fine for breaching data protection law to €20 million, or 2 – 4% of annual worldwide turnover, whichever is greater.

Neutral changes for businesses

There are also some elements of the Regulation which, on balance, would have a neutral impact on most businesses but are still worthy of note – for example registrations. Instead of registering with a SA, businesses will be required to maintain a detailed inventory recording their processing activities. Many will be required to appoint a data protection officer.

Changes that could be positive for businesses

Greater harmonisation

The Regulation will introduce a single legal framework that applies across all EU member states. This means that the issue of member states implementing the existing requirements differently will (to a large extent) fall away so that businesses will face a more consistent set of data protection compliance obligations across EU member states.

Risk-based approach to compliance

Under the Regulation, businesses will be responsible for assessing the degree of risk that their processing activities pose to data subjects, and for implementing appropriate measures to ensure compliance. Low-risk processing activities may face a reduced compliance burden.

The 'one-stop-shop'

Under the new regulation, a business with operations across the EU will be able to deal with the SA in the jurisdiction of its main establishment, as 'lead authority'. This will not prevent other SA's from taking enforcement action, but will encourage closer working relationships with lead SAs.

'Pseudonymisation'

The Regulation introduces a concept of 'pseudonymised data' (i.e. data that can no longer be attributed to a specific individual, such as key-coded data). Pseudonymous data will still amount to personal data, but may be subject to fewer restrictions on processing, provided that the risk of harm is low.

Binding Corporate Rules (BCRs)

BCRs are agreements used to lawfully transfer personal data out of the European Economic Area (EEA). The Regulation will formally recognise BCRs. They will still require SA approval, but the approval process should become less onerous than under the current system.

Areas remaining unharmonised

Although the Regulation increases the harmonisation of data protection law across the EU, some existing core concepts will remain largely unchanged – for example, the concepts of personal data, data controllers and data processors which are broadly similar in both the existing directive and the Regulation.

In addition, there will still be areas under the new regulation where the applicable requirements vary among member states (as some categories of information fall outside of the EU's legislative remit). These include:

National security

Data processed for the purposes of the national security of a member state is exempt from the Regulation as member states have different approaches to national security. Each member state will continue to take its own approach as to what data processing activities are deemed necessary for national security.

Journalism and freedom of speech

The concepts of 'journalism' and 'freedom of expression' will continue to vary from one member state to another.

Employment law

Member states may continue to adopt their own rules regarding the processing of personal data in an employment context.

Professional secrecy laws

Some member states have laws on professional secrecy that prevent the processing of certain data, even where the Regulation would otherwise permit that processing.

Laws on interception of communications

Member states have interception laws under the E-Privacy Directive, which are not uniform across the EU.

International Insight: Privacy Shield

The EU-US Privacy Shield ("Privacy Shield") is a proposed agreement between the EU and U.S. Announced in February 2016, it is currently being considered by the European Commission and European Parliament. If adopted, it will provide a framework for EU-U.S. transfers of personal data, replacing the Safe Harbor framework which was declared invalid in October 2015 by the Court of Justice for the EU in the case of *Schrems v Data Protection Commissioner*.

Like the previous Safe Harbor regime, the Privacy Shield will require self-certifying companies to comply with a set of core privacy principles:

- **Notice:** informing individuals about the Privacy Shield, their rights under it, and how their data is processed.
- **Choice:** allowing individuals to object to the disclosure of their information to third parties or the use of their data for materially different purposes, and opting out of direct marketing.
- **Security:** requiring security measures appropriate to the nature of the data and the proposed processing. These obligations must be flowed on to sub-processors.
- **Data integrity and purpose limitation:** limiting data to what is relevant, and keeping it accurate, complete and current.
- **Access:** allowing individuals to access their data without giving a reason and to arrange for the correction, amendment or deletion of their data where it is inaccurate or has been processed in violation of Privacy Shield.
- **Accountability and onward transfer:** limiting the onward transfer of personal data to specified purposes on the basis of a contract that provides the same level of protection as guaranteed under the Privacy Shield.
- **Recourse, enforcement and liability:** putting in place robust mechanisms to ensure compliance with the Privacy Shield, and independent and free redress mechanisms capable of providing effective remedies.

Securing redress for EU citizens whose data are processed by U.S. companies was fundamental to the agreement of a replacement for Safe Harbor and the Privacy Shield provides several avenues for redress. Regulation of the Privacy Shield will be more proactive than under Safe Harbor. U.S. companies that rely on the Privacy Shield will be required to self-certify on an annual basis. Their adherence will be reviewed proactively by the Department of Commerce, which will monitor and actively verify that each company's privacy policies meet the requirements of the Shield, and that companies remain compliant with the privacy rules they put in place.

Current Status

The Privacy Shield is not yet in force. There is a strong appetite on both sides of the Atlantic for an agreement that will enable companies to transfer personal data with greater ease. On 13 April 2016, European Data Protection Authorities (known as the Article 29 Working Party or "WP29") recognised the Privacy Shield is an improvement to the now invalid Safe Harbor, but highlighted several shortcomings challenging whether the Privacy Shield affords European citizens essentially equivalent safeguards when their data are processed in the U.S. The shortcomings concern data retention, purpose limitation, onward transfers, and the complexity of rights of redress. WP29 also remains concerned about national security guarantees.

The Opinion of WP29 is merely advisory and the European Commission could still proceed with the current draft of the Privacy Shield, but it is clear that some individual regulators within WP29 feel strongly that it is not adequate. It is not yet clear what course the Commission will take, or what legal challenges may be made. For now, data transfers to the U.S. may still take place under the existing data transfer mechanisms, EU Model Clauses or Binding Corporate Rules.

What happens next?

The EU Parliament voted to adopt the Regulation on 14 April 2016. Once published in the Official Journal, there will be a two year implementation period, with the Regulation coming into force in 2018.

Data protection will become as significant a compliance risk for organisations as antitrust issues, with significant regulatory sanctions. Under the Regulation, data protection will no longer be an area in which businesses can afford to take casual risks.

The Regulation is likely to require company- wide changes for many businesses. Organisations should start to consider the impact of those changes now, and begin to work towards compliance. It is already clear that some changes will take time to embed within businesses, and others may require significant change to existing processes. As a first step, businesses need to take stock of their existing data assets and compliance profile, and then systematically assess how the Regulation will impact existing compliance. For most organisations, this will be a sizeable project. Organisations in the UK, which until now have enjoyed a light touch data protection regime, arguably will have the most to do to prepare for data protection under a harmonised regime.

Contact

For more information on the EU data protection legislation changes and how they may impact your business please contact:

Fredrik Motzfeldt

T +44 (0)20 3124 7962
E fredrik.motzfeldt@willistowerswatson.com

Darryl Brophy

T +44 14 7322 3819
E darryl.brophy@willistowerswatson.com

Glyn Thoms

T +44 (0)20 3124 8673
E glyn.thoms@willistowerswatson.com

Bridget Treacy

T +44(0)20 220 5731
E btreacy@hunton.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

About Hunton & Williams

Hunton & Williams' is an international law firm, and its Global Privacy and Cybersecurity practice is consistently ranked in "Band 1" by *Chambers and Partners*. Hunton & Williams has many years' experience assisting multinational companies with all aspects of privacy and cybersecurity.

FP2034/15594/04/16