General Data Protection Regulation: key provisions and what businesses should be doing now

by Bridget Treacy, Hunton & Williams LLP

Practice notes | **Maintained** | European Union, UK, United Kingdom

An at-a-glance guide to the key provisions of the General Data Protection Regulation (GDPR), how it will affect businesses and what businesses can be doing now to prepare for the new European data protection regime.

Note: UK data protection law will change on 25 May 2018, when the EU General Data Protection Regulation takes effect, replacing the Data Protection Act 1998. See *EU General Data Protection Regulation toolkit* for information on the new Regulation and Practical Law's updating policy.

Scope of this note

The current EU data protection regime is based on the *Data Protection Directive (95/46/EC)* that was introduced in 1995. Since then, there have been significant advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information. In addition, the various EU member states have taken divergent approaches to implementing the Data Protection Directive, creating compliance difficulties for many businesses. The EU's legislative bodies, national data protection authorities and EU member states have spent considerable time over the last four years preparing an updated and more harmonised data protection law *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, more commonly known as the General Data Protection Regulation (GDPR), was published in the Official Journal of the European Union on 4 May 2016 and EU organisations will have to comply with its provisions by 25 May 2018 (see *Legal update, General Data Protection Regulation to apply from May 2018*).

This note focuses on the application of the GDPR to businesses and what they should be doing now to prepare. While much of it will also apply to the public sector, it does not address any of the provisions in the GDPR that are specific to public sector organisations. Nor does it address *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* (Directive for the police and criminal justice sector), which forms part of the EU data protection reform package and comes into force on 5 May 2016. EU member states must transpose it into national law by 6 May 2018.

In the light of the UK's decision to leave the EU, for further information on the implications of Brexit on the GDPR see *Brexit and the GDPR*.

Impact of the GDPR on businesses and what they should be doing now: key concepts

Steve Wood, Head of Policy Delivery at the Information Commissioner's Office (ICO), in his blog post "A data dozen to prepare for reform" of 14 March 2016, explained that:

> "Many of the principles in the new legislation are much the same as those in the current Data Protection Act. If you are complying properly with the current law, then you have a strong starting point to build from. But there are important new elements, and some things will need to be done differently."

(see *Legal update, ICO publishes guidance on GDPR preparation*). Please note that the ICO has since updated its 12 step guide to mark one year to go until the GDPR (see *Legal update, ICO warns businesses to prepare with one year to go until the GDPR*).

The ICO has published guidance on preparing for the GDPR and the specific guidance organisations can expect to see in 2017 (see *Legal update, ICO updates GDPR Overview*) and the Article 29 Working Party (WP29).has published its action plan for 2017 (see *Legal update, Article 29 Working Party adopts GDPR Action Plan 2017*).

Key concepts table: key

✔	This change is broadly positive for most businesses
✘	This change is broadly negative for most businesses
=	This change is broadly neutral for most businesses

Some concepts will change

The GDPR will introduce **several new concepts and approaches**, the most significant of which are outlined in the table below. The GDPR is also designed to be more future-proof and forward-looking than the Data Protection Directive, and as technology-agnostic as possible.

Some concepts will stay the same

Many of the existing core concepts under the Data Protection Directive will remain unchanged. For example, the concepts of personal data, data controllers, and data processors are broadly similar in both the Data Protection Directive and the GDPR. These issues are not addressed further below.

Multiple drafts

As with any EU legislation, multiple drafts of the GDPR were created and edited before the final text. The major drafts are:

- **The Commission Text.** The Commission published the first draft of the GDPR on 25 January 2012 (see *Legal update, European Commission proposes new data protection framework*).
- **The Parliament Text.** The Parliament adopted a series of proposed amendments to the Commission Text on 12 March 2014 (see *Legal update, European Parliament vote approves draft Data Protection Regulation*).
- **The Council Text.** The Council proposed further amendments in its own Text, released on 15 June 2015 (see *Legal update, Council agrees common approach on proposed Data Protection Regulation*).
- **The Compromise Text.** The Council of the European Union and the Parliament agreed a compromise text in December 2015 (see *Legal update, EU data protection reform package agreed*), which the Council and the Parliament subsequently formally adopted (see *Legal updates, Council formally adopts EU data protection reform package* and *EU Parliament approves data protection reform package*).

Key concepts and changes	Effect on businesses	What businesses should be doing now
Greater harmonisation. The GDPR introduces a single legal framework that applies across all EU member states. This means that businesses will face **a more consistent set of data protection compliance** obligations from one EU member state to the next. For further information, see *Practice note, Overview of EU General Data Protection Regulation: History and background.* For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: history and background* and, particularly *General Provisions: material scope*.	✔	Greater harmonisation is broadly likely to be a positive change. However, the GDPR is still likely to require significant changes for many businesses, and many of these changes will require substantial lead time. It is therefore important for businesses to plan ahead. Member states will have some flexibility over decisions, for example, the age at which online service providers must verify that parental consent has been given before providing the service can be set at 13 to 16 years of age (see *Legal updates, Government calls for views on General Data Protection Regulation derogations* and *ICO responds to government consultation on GDPR national law derogations*). Businesses should start to consider how they will verify a young person's age and obtain parental or guardian consent and put systems in place.

Expanded territorial scope. Non-EU data controllers and data processors will be subject to the GDPR if they either: • Offer goods or services to data subjects in the EU irrespective of whether payment is received. • Monitor data subjects' behaviour insofar as their behaviour takes place within the EU. This means that **many non-EU businesses** that were not required to comply with the Data Protection Directive **will be required to comply with the GDPR**. This is not an entirely new concept and reflects similar developments in EU case law, for example, the ECJ considered the scope of "establishment" in *Weltimmo [2015] EUECJ C-230/14 (01 October 2015)*. On 1 October 2015, the Hungarian data protection authority sought to fine Weltimmo, a Slovakian-registered online property company that advertised properties in Hungary, for breaches of the Data Protection Directive. On referral, the ECJ interpreted the meaning of "establishment" broadly in the context of an online business, and ruled that the data protection law of a member state may apply to a data controller even when it is registered in another member state, if, in relation to its data processing activities, there is "any real and effective activity, even a minimal one, exercised through stable arrangements" in the other member state. The ECJ also held that where a complaint is made to a national supervisory authority (SA), and it determines that the law of another member state applies, it may only exercise its intervention powers within its own territory and cannot impose a penalty on a data controller which is not established in its territory. It should instead request the SA of the member state whose law is applicable, to act. For further information see *Legal update, ECJ rules on "establishment" in a member state for online business processing data* and *Article, EU data protection: ECJ extends the long arm of the law*. For further information see *Practice note, Overview of EU General Data Protection Regulation: Territorial scope* and *Obligations on data controllers and data processors*. For background analysis during the	✘	Businesses established outside the EU that are not subject to the Data Protection Directive should consider whether any of their entities are subject to the GDPR. If so, such a business should review the compliance obligations of its affected entities under the GDPR.

Increased enforcement powers. Currently, fines under national law vary, and are comparatively low (for example, the UK maximum fine is £500,000). The GDPR will significantly increase the maximum fines and SAs will be able to impose fines on data controllers and data processors on a two-tier basis, as follows: • Up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default. • Up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers. The investigative powers of SAs include a power to carry out audits, as well as to require information to be provided, and to obtain access to premises (in accordance with local law requirements). For further information, see *Practice note, EU General Data Protection Regulation, enforcement, sanctions and remedies*. For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: enforcement, sanctions and remedies.*		Businesses that had previously regarded non-compliance with EU data protection law as a low-risk issue will be forced to re-evaluate their positions in the light of the substantial new fines, increased SA enforcement powers and grounds for seeking judicial remedies under the GDPR. The WP29 intends to publish guidance on administrative fines.

Consent, as a legal basis for processing, will be harder to obtain. The Data Protection Directive distinguished between ordinary consent (for non-sensitive personal data) and explicit consent (for sensitive personal data). The GDPR requires a very high standard of consent, which must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic or oral) statement. An individual's explicit consent is still required to process special categories of personal data. Businesses must be able to demonstrate that the data subject gave their consent to the processing and they will bear the burden of proof that consent was validly obtained. When the processing has multiple purposes, the data subject should give their consent to each of the processing purposes. The data subject shall have the right to withdraw their consent at any time. The execution of a contract or the provision of a service cannot be conditional on consent to processing or use of data that is not necessary for the execution of the contract or the provision of the service. Data controllers cannot rely on consent as a legal basis for processing if there is a "clear imbalance" between the parties (for example, the employer and employee relationship) as consent is presumed not to be freely given. For further information see *Practice note, Overview of EU General Data Protection Regulation: Consent requirements*. For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: definitions: consent* and *principles and lawfulness of processing: legal grounds for processing*.		Businesses in the UK have, so far, been able to rely on implied consent. Although the Council deleted the requirement for consent to be "explicit", the bar is still set very high. As businesses must be able to demonstrate that an individual gave their consent to the processing, it is unclear, without formal regulatory guidance, how far they can continue to rely on an individual's implied consent. The ICO has published draft guidance on consent which addresses the use of implied consent (see *Legal update, ICO publishes draft guidance on consent in General Data Protection Regulation*). Businesses that rely on consent, as a legal basis for processing personal data, will need to carefully review their existing practices to ensure that any consent they obtain indicates affirmative agreement from the data subject (opt in) (for example, ticking a blank box). Mere acquiescence (for example, failing to un-tick a pre-ticked box) does not constitute valid consent under the GDPR. Businesses must also consider how they will discharge the evidential burden of demonstrating that consent has been obtained. Businesses must ensure that an individual can withdraw their consent at any time. It must be as easy to withdraw consent as to give it. Changes to consent mechanisms will require careful review, and may take time to implement. The WP29 is aiming to publish guidance on consent.

The risk-based approach to compliance. The GDPR adopts a risk-based approach to compliance, under which businesses bear responsibility for assessing the degree of risk that their processing activities pose to data subjects. This can be seen in several of the provisions, for example, the new accountability principle and requirement for data controllers to maintain documentation, privacy by design and default, privacy impact assessments, data security requirements and the appointment of a data protection officer in certain circumstances. **Low-risk processing activities may face a reduced compliance burden**. For further information see *Practice note, Overview of EU General Data Protection Regulation: Obligations of data controllers and data processors*. For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: obligations of controllers and processors*.	✔	As this may involve substantial changes to existing compliance strategies and arrangements businesses should start their preparation now. The ICO has published a helpful 12-step guide to assist businesses (see *Legal update, ICO publishes guidance on GDPR preparation*), which recommends that businesses: • Create awareness among the senior decision makers in the business. • Audit and document the personal data they hold, recording where it came from and who it is shared with. • Review the legal basis for the various types of processing that they carry out and document this. • Review privacy notices and put in place a plan for making any changes to comply with the GDPR (see *Legal update, ICO publishes updated privacy notices code of practice with GDPR compliance element*). • The WP29 has published guidelines on data protection officers and draft guidelines on privacy impact assessments (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*) and is aiming to publish guidelines on transparency.

The "one-stop shop". Under the Data Protection Directive, each SA may exercise authority over businesses operating on its territory. Under the GDPR, a business will be able to deal with a single SA as its "**lead supervisory authority**" across the EU. Where a controller or processor has more than one establishment in the EU, the GDPR anticipates that they will have a main establishment, and work with the SA for the main establishment where cross-border processing is involved ("**lead SA**"). The lead SA will be responsible for all regulation of cross-border processing activities carried out by that controller or processor. The lead SA must work with all other "concerned SAs". All concerned SAs have a say in decisions on enforcement relating to cross-border processing activities. If the concerned SAs cannot agree on a decision, the matter is referred to the European Data Protection Board (EDPB), which has a range of powers to ensure the consistent application of the GDPR across the EU, including the power to make the final decision in enforcement cases (the **consistency mechanism**). Purely local cases will continue to be handled by the SA for the local jurisdiction. The WP29 has finalised its understanding of the modalities of the future SA cooperation system and it has agreed position papers on mutual assistance, the one-stop-shop and joint operations, and SAs will test these in 2017. For further information see *Practice note, EU General Data Protection Regulation: Enforcement, sanctions and remedies*: For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: obligations of controllers and processors*.		For businesses that only operate within a single EU member state, and only process the personal data of data subjects residing in that member state, interaction with the local SA under the GDPR will be similar to interaction with the local SA under the Data Protection Directive. Multi-nationals and businesses that operate in more than one EU member state will see a substantial change, as the one-stop shop will mean that they predominantly interact with a single SA as their "lead authority" (rather than multiple SAs). The ICO recommends that businesses should start to determine which SA will be their lead authority. The WP29 has published guidelines for identifying a controller or a processor's lead SA (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*). Recent ECJ decisions have emphasised the independence of SAs and their competence to enforce data protection law where the data controller is "established" in their member state or the subject substantially affects individuals in its member state: • *Schrems v Data Protection Commissioner (Case C-362/14, 23 September 2015)* (see *Legal update, ECJ rules that the US Safe Harbor arrangement is invalid*). • *Weltimmo* (see *Expanded territorial scope*, above and *Legal update, ECJ rules on "establishment" in a member state for online business processing data*).

Privacy by design and by default, privacy impact assessments, prior consultation and standardised icons. **Mandatory privacy by design and default**. Having regard to the state of the art and the cost of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk to individuals, businesses will be required to implement data protection **by design** (for example, when creating new products, services or other data processing activities) and **by default** (for example, data minimisation), at the time of the determination of the means for processing and at the time of the processing itself. **Mandatory privacy impact assessments**. Businesses will be required to perform **data protection impact assessments** (PIAs) before carrying any processing that uses new technologies (and taking into account the nature, scope, context and purposes of the processing) that is likely to result in a high risk to data subjects, takes place. In particular, PIAs will be required for: • A systematic and extensive evaluation of personal aspects by automated processing, including profiling, and on which decisions are based that produce legal effects concerning the data subject or significantly affect the data subject. • Processing of special categories of personal data or data relating to criminal convictions and offences on a large scale. • A systematic monitoring of a publicly accessible area on a large scale. The SA will publish a list of the kind of processing operations that require a PIA. Data controllers can carry out a single assessment to address a similar set of similar processing operations that present similar high risks. **Mandatory prior consultation**. In addition, where a PIA indicates that the processing would result in a high risk to individuals, the business must consult, before any processing taking place, with the SA. In addition, standardised icons to indicate important features of the relevant data processing activities in a simplified format may be prescribed by delegated acts.	✘	In particular, the GDPR will require businesses to implement technical and organisational measures (such as pseudonymisation) to ensure that the requirements of the GDPR are met. Businesses must both: • Take data protection requirements into account from the inception of any new technology, product or service that involves the processing of personal data, with an ongoing requirement to keep those measures up-to-date. • Conduct data protection impact assessments where appropriate. These steps will need to be planned into future product cycles. The ICO has published version 2 of its paper on Big Data about which it says "While this is not a guidance document on the GDPR, it does discuss GDPR provisions that are relevant to big data and machine learning" (see *Legal update, ICO publishes paper on big data, artificial intelligence, machine learning and data protection with GDPR compliance element*). The ICO's Privacy Impact Assessments code of practice, provides helpful guidance on when and how to implement PIAs (see *Legal update, ICO publishes privacy impact code of practice*). The WP29 has published draft guidelines for consultation on PIAs (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*).

Registrations. Instead of registering with an SA, the GDPR will require businesses to **maintain detailed documentation** recording their processing activities and the GDPR specifies the information this record must contain. Data processors must keep a record of the categories of processing activities they carry out on behalf of a controller. The GDPR specifies what this record must contain. These obligations do not apply to an organisation employing fewer than 250 people unless the processing is likely to result in high risk to individuals, the processing is not occasional or the processing includes sensitive personal data. In addition, in certain circumstances, controllers or processors are required to **appoint a data protection officer**. For further information see *Practice note, Overview of EU General Data Protection Regulation: obligations of data controllers and data processors.* For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: obligations of controllers and processors*.	=	Businesses should: • Review their existing compliance programmes, and ensure that those programmes are updated and expanded as necessary to comply with the GDPR. • Ensure that they have clear records of all of their data processing activities, and that such records are available to be provided to SAs on request. • Appoint a data protection officer (particularly, where it is mandatory to do so) with expert knowledge of data protection. Businesses should be aware that if an employee is appointed as the data protection officer, that employee may have protected employment status in some EU member states. • The WP29 has published guidelines on data protection officers (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*). • Section 111 of the UK's Digital Economy Act 2017 provides for the repeal of the notification regime. The government is working on an alternative funding model for the ICO based on fees from data controllers. Section 108 of the Act provides that "the Secretary of State may by regulations require data controllers to pay charges of an amount specified in the regulations to the Information Commissioner". This provision will be brought into force by statutory instrument (see *Legal update, Digital Economy Act published: data protection implications*).

New obligations of data processors. The GDPR introduces **direct compliance obligations for processors**. Whereas under the Data Protection Directive processors generally are not subject to fines or other penalties, under the GDPR processors may be liable to pay fines of **up to 4% of annual worldwide turnover of the preceding financial year** or **20 million euros**, whichever is greater. For more information see *Practice note, Overview of EU General Data Protection Regulation: obligations on data controllers and data processors*. For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: obligations on controllers and processors*.		The GDPR is likely to substantially impact both processors and controllers that engage processors, in the following ways: • The increased compliance obligations and penalties for processors are likely to result in an increase in the cost of data processing services. • Negotiating data processing agreements may become more difficult, as processors will have a greater interest in ensuring that the scope of the controller's instructions is clear. • Some processors may wish to review their existing data processing agreements, to ensure that they have met their own compliance obligations under the GDPR. Data controllers should identify their processor agreements early on so that they can review and amend them as necessary. These changes are likely to require time to implement (see *Practical Law's in-house blog, GDPR: first lines of attack on the new data processor compliance obligations*). The ICO is aiming to publish guidance on contracts and liability early in 2017 (see *Legal update, ICO updates GDPR Overview*).

Strict data breach notification rules. The GDPR requires businesses to notify, the SA of all data breaches without undue delay and where feasible within **72 hours** unless the data breach is unlikely to result in a risk to the individuals. If this is not possible it will have to justify the delay to the SA by way of a "reasoned justification". If the breach is likely to result in high risk to the individuals, the GDPR, requires businesses to inform data subjects "without undue delay", unless an exception applies. Data processors must notify the data controller. For further information see *Practice note, Overview of EU General Data Protection: Data security* and *Data security breach*. For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: obligations of controllers and processors*.		Businesses will need to develop and implement a data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach. Complying with the data breach reporting obligations in the GDPR will also entail a significant administrative burden for businesses, which may increase costs. On the other hand, the harmonisation of the data breach reporting obligation will allow businesses operating across multiple EU member states to have one pan-EU data breach response plan. Although *Practice note, Data security and data security breaches*, is based on the Data Protection Directive, it provides a helpful starting point. The WP29 is aiming to publish guidance documents on notification of personal data breaches.
Pseudonymisation. The GDPR introduces a new concept of "pseudonymiseation" (that is, the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual, without additional information). Pseudonymous data will still be treated as personal data, but possibly subject to **fewer restrictions on processing**, if the risk of harm is low. It requires that the "key" necessary to identify data subjects from the coded data is kept separately, and is subject to technical and organisational security measures to prevent inadvertent re-identification of the coded data. For further information see *Practice note, Overview of EU General Data Protection Regulation: GDPR: definitions*. For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up, definitions*.		Currently, SAs have differing approaches to anonymisation and pseudonymisation, and the criteria for determining whether data are truly anonymised or pseudonymised. Compliance with these divergent guidelines is often difficult for businesses that process anonymous or pseudonymous data in multiple EU member states. EU-wide guidelines are expected to be produced, unifying the current disparate approaches. Businesses should keep this issue under review.

Binding Corporate Rules (BCRs). BCRs are agreements used to lawfully transfer personal data out of the European Economic Area (EEA). The GDPR **formally recognises BCRs**. They will still require SA approval, but the approval process should become **less onerous than the current system**. BCRs are available to both controllers and processors. However, in relation to the ECJ's recent judgment (*Schrems v Data Protection Commissioner*), declaring the Commission's Decision on EU-US Safe Harbor invalid, the UK's Information Commissioner has confirmed that: > "the terms of the judgment inevitably cast some doubt on the future of these other mechanisms [standard contractual clauses and BCRs], given that data transferred under them is also liable to be accessed by intelligence services whether in the US or elsewhere" (*ICO Blog, 27 October 2015*). On 25 May 2016 the Irish Data Protection Commissioner (DPC) confirmed it was seeking a declaratory judgment from the Irish High Court on the validity of standard contractual clauses (SCCs), and a referral of the issue to the ECJ. The US government and other interest groups have joined the proceedings (see *Legal updates, Irish DPC intends to refer standard contractual clauses to ECJ* and *US government and interested groups seek to join Irish case on EU standard contractual clauses*). The European Commission has published Commission implementing decisions amending its Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries and amending its adequacy decisions on non-EU "whitelisted" countries. The amendments strengthen SAs' powers in relation to SCCs and white-listed countries. but it remains to be seen what effect the amendments will have on the ongoing challenge of the validity of SCCs (see *Legal update, Amendments to Standard Contractual Clauses and "white-listed" country decisions published in OJ*).	Unclear	The GDPR introduces a slightly broader range of mechanisms to transfer personal data out of the EEA, including approved codes of conduct and certification mechanisms. The WP29 is aiming to publish guidance on certification. It also formally recognises BCRs as a lawful data transfer mechanism (whereas the Data Protection Directive does not). The GDPR also makes it easier for businesses to obtain approval from DPAs of their BCRs. Pre *Schrems*, the view was that once the GDPR applies, it is likely that there will be an increase in the number of businesses that seek to implement BCRs. However, it is difficult to assess the effect on businesses as the impact of the ECJ's judgment on standard contractual clauses and BCRs is still being analysed. For further information, see: • *Legal update, ECJ rules that EU-US Safe Harbor arrangement is invalid*. • *Legal update, Article 29 Working Party publishes statement in aftermath of Safe Harbor invalidity ruling*. • *Article, The Future of EU-US data transfers – Reactions to the Schrems decision on the EU-US Safe Harbor* *ICO blog: The US Safe Harbor - breached but perhaps not destroyed! (27 October 2015)*. Businesses should review their procedures and legal basis for transferring personal data outside of the EEA and keep this under review, particularly as the validity of transfer mechanisms continues to be examined by the ECJ. The fines for breach of the data transfer restrictions under GDPR fall into the higher tier for failure to comply with the requirements. An additional complication is the effect of UK's decision to leave the EU (see *BREXIT and the GDPR*). The WP29 is planning to publish guidance on international data transfers and the ICO is planning to publish a paper on its international strategy.

The right to erasure ("right be forgotten"). Individuals will have the **right to request that businesses delete their personal data** in certain circumstances (for example, the data are no longer necessary for the purpose for which they were collected or the data subject withdraws their consent). It remains unclear precisely how this will work in practice. In May 2014 in *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, 13 May 2014*, on a referral from a Spanish court, the ECJ explored the existence and scope of the right to be forgotten and ruled that an individual has a right to rectification, erasure or blocking of that information, and a right to object to the processing of the information in certain circumstances. For further information see *Legal update, ECJ confirms right to have search engine results removed where they affect privacy rights*. For further information see *Practice note, Overview of EU General Data Protection Regulation: rectification and erasure*. For background analysis during the legislative process see *Practice note, EU General Data Protection Regulation noter-up: rights of the data subject*.		In general, the rights of data subjects are expanded under the GDPR. As a result, businesses will need to devote additional time and resources to ensuring that these issues are appropriately addressed. In particular, businesses should consider how they will give effect to the right to erasure (right to be forgotten), as deletion of personal data is not always straightforward. As a result of the *Google Spain* decision, many businesses may already be doing this. For further guidance see: • *Checklist, removal of links from search engines*. • *Legal update, Article 29 Working Party issues guidelines on implementing the ECJ's decision in Google Spain*. • *ICO blog: Has the search result ruling stopped the internet working? (2 November 2015)*.

The right to object to profiling. In certain circumstances, individuals will have the right to object to their personal data being processed (which includes profiling). **Profiling**" is defined broadly and includes most forms of online tracking and behavioural advertising, making it harder for businesses to use data for these activities. The fact of profiling must be disclosed to the data subject, and a PIA is required. For further information see *Practice note, Overview of EU's General Data Protection Regulation: measures based on profiling*. For analysis of the legislative process see *Practice note, EU General Data Protection Regulation noter-up: rights of the data subject*.	✘	The impact of these restrictions on a given business will largely depend on how frequently that business engages in profiling activities. For those businesses for which profiling is a rare or occasional activity, it may simply be easier to cease such activities than to comply with the GDPR. Businesses that regularly engage in profiling activities (for example, in the advertising, marketing or social media context) will need to consider how best to implement appropriate consent mechanisms to continue these activities. Businesses should watch for further guidance, and should keep this issue under review. The ICO has published a discussion paper on profiling which sought feedback by 28 April 2017 (see *Legal update, ICO publishes discussion paper for feedback*) . The WP29, and possibly the European Data Protection Board, are expected to provide guidance on profiling.
The right to data portability. Data subjects have **a new right to obtain a copy of their personal data from the data controller in a commonly used and machine-readable format** and have the right to transmit those data to another controller (for example, an online service provider). In exercising their right, the data subject can request the information be transmitted directly from one controller to another, where technically feasible. For further information see *Practice note, Overview of EU General Data Protection Regulation: Rights of data subject.* For analysis of the legislative process see *Practice note, EU General Data Protection Regulation noter-up: rights of the data subject*.	✘	All businesses should keep this issue under review. Businesses that process large volumes of personal data (for example, social media businesses, insurance companies, banks) should consider how they will give effect to these rights. Many new-to-market online businesses may welcome this new development as a way to improve competition in the sector while established providers will view it in less beneficial terms. The WP29 has published guidelines on data portability (see *Legal update, Article 29 Working Party publishes GDPR guidelines on DPIAs for consultation and adopts final guidelines on DPOs, data portability and lead supervisory authority*).

Data subject access requests Business must reply within one month from the date of receipt of the request and provide more information than was required under the Data Protection Directive. For further information see *Practice note, Overview of EU General Data Protection Regulation: Data subject access*. For analysis of the legislative process see *Practice note, EU General Data Protection Regulation noter-up: rights of the data subject*.	✘	Businesses should plan how they will respond to data subject access requests within the new time scale and how they will provide the additional information required.

BREXIT and the GDPR

In the light of the UK's decision, on 23 June 2016, to leave the EU, many businesses were left wondering whether to comply with the GDPR. The widely held view was that the UK would still wish to be considered an "adequate" jurisdiction for data protection to enable trading with the EU (see *Practice note, Cross-border transfers: Adequate level of protection*.).

Shortly after the result of the referendum, the UK's Data Protection Minister at the Department for Culture Media & Sport (DCMS) published a statement explaining that if the UK remains within the Single Market, EU rules on personal data might continue to apply fully in the UK, but in other scenarios, all EU rules might be replaced with national ones. The Minister's view on the importance of consistency in data sharing across national borders aligns with that of the ICO (see *Legal update, ICO publishes statement on GDPR following Brexit vote*) and this will be particularly important for multi-national businesses. The Minster commented, "One thing we can say with reasonable confidence is that if any country wishes to share data with EU Member States, or for it to handle EU citizens' data, they will need to be assessed as providing an adequate level of data protection. This will be a major consideration in the UK's negotiations going forward" (see *Legal update, DCMS view on Brexit, the GDPR and EU-US Privacy Shield*).

In November 2016, the government confirmed that the UK will adopt the GDPR (see *Legal update, Government confirms UK will opt in to GDPR in May 2018*). In February 2017, at an EU Home Affairs Sub-Committee meeting, the Minister of State for Digital and Culture, Matthew Hancock MP, answered questions on the EU data protection package and the post-Brexit UK data protection landscape. He reiterated that the UK will implement the GDPR to secure unimpeded data flows between the UK and the EU, particularly to underpin free trade. The Minister would not be drawn on whether the UK would seek an EU "adequacy" decision in Brexit negotiations nor speculate on what alternative arrangements might arise, as negotiations have yet to commence. The Minister said that to ensure that duplication or inconsistencies with the GDPR will not arise when it becomes directly applicable on 25 May 2018, UK legislation will be brought forward in the next parliamentary session to repeal parts of the DPA, in particular, its enforcement provisions (see *Legal updates, Minister discusses EU data protection package, Brexit and EU-US data transfers*). As the first step towards this, the government published its call for views on the derogations (see *Legal updates, Government calls for views on General Data Protection Regulation derogations* and *ICO responds to government consultation on GDPR national law derogations*).

Those responsible for an organisation's compliance with data protection legislation may encounter difficulty gaining management or board level support as major investment may be required to change systems and processes.

However, with fines for non-compliance, set to escalate to the greater of 4% of annual worldwide turnover or EUR 20 million for breach of the data protection principles, failing to comply with the conditions for consent, data subjects' rights and international data transfers this should provide a good starting point for discussions around senior management buy-in.

For further information see *Article, BREXIT and the implications for data protection* .(please note that this article is currently under review)

On balance, will the GDPR be good news or bad news for businesses?

The GDPR has the potential to introduce positive changes for many businesses. It is designed to increase the harmonisation of national data protection laws across the EU while, at the same time, addressing new technological developments. The GDPR 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. Businesses may also benefit from the "one-stop shop", which will permit them to deal primarily with a single SA. However, there remain areas in which there will continue to be material differences from one member state to another affecting data protection compliance requirements (including issues of national security, journalism, freedom of speech, employment law, professional secrecy laws and laws on the interception of communications).

Compliance with the GDPR is likely to require organisation-wide changes for many businesses, to ensure that personal data are processed in compliance with the GDPR's requirements. Such changes may include redesigning systems that process personal data, renegotiating contracts with third party data processors and restructuring cross-border data transfer arrangements. Businesses should therefore consider that these changes may require a significant amount of time to implement, and plan ahead. Failure to do so could mean that businesses are left with new requirements to implement, without having set aside appropriate resources necessary to achieve compliance.

The GDPR also has implications for other areas of European data protection law, for example:

- The European Commission launched a consultation on the E-Privacy Directive, which compliments the Data Protection Directive. This is, in part, to ensure consistency of the provisions of the E-Privacy Directive with the GDPR. The consultation closed on 5 July 2016 (see *Legal update, European Commission consults on E-Privacy Directive*). The ICO responded to the consultation (see *Legal update, ICO publishes response to European Commission consultation on E-privacy Directive*) and the Article 29 Working Party and the European Data Protection Supervisor both published their opinions (see *Legal updates, Article 29 Working Party publishes opinion on review of E-Privacy Directive* and *EDPS publishes opinion on review of E-Privacy Directive*); all three agreed on many aspects as to how the E-Privacy Directive should be reformed. In January 2017, the European Commission published its draft E-Privacy Regulation which will be directly applicable in member states and should assist businesses as they will only have to comply with one set of e-privacy rules, rather than varying rules in member states (see *Legal updates, European Commission publishes draft E-Privacy Regulation* and *EDPS issues opinion on proposed E-Privacy Regulation*). The aim is to finalise the new law by 25 May 2018, so that it coincides with the GDPR.
- The European Court of Justice's decision in *Schrems v Data Protection Commissioner*, which invalidated the European Commission's adequacy decision on the EU-US Safe Harbor, has created uncertainty for EU data controllers that transfer personal data to the United States (*Legal update, ECJ rules that safe harbor arrangement is invalid*). The EU and the US agreed on a replacement, the EU-US Privacy Shield adequacy decision (see *Legal update, European Commission adopts EU-US Privacy Shield adequacy decision*) and in a subsequent statement, the WP29 welcomed the development but anticipates that the first joint annual review will be key to assessing the robustness and efficiency of the Privacy Shield, the outcome of which may also

impact on other transfer mechanisms such as BCRs and SCCs. As this is the first adequacy decision to be drafted since the European Parliament formally adopted the GDPR, it does not reflect many of the improvements that the GDPR offers to individuals and, in the light of that, the WP29 recommends that a review of the EU-US adequacy decision (as well as adequacy decisions issued for other third countries), take place shortly after the GDPR applies on 25 May 2018. However, in November 2016, privacy advocacy groups Digital Rights Ireland and La Quadrature du Net filed actions for annulment of the adequacy decision (see *Legal update, Two privacy advocacy groups challenge Privacy Shield at EU General Court*). The UK government has since applied to intervene in the Digital Rights Ireland challenge to declare it inadmissible and is considering doing the same in relation to La Quadrature du Net. In April 2017, due to various concerns MEPs called for an assessment of the Privacy Shield (see *Legal update, MEPs pass non-legislative resolution on the Privacy Shield calling for proper assessment*). For further information see *Practice note, Cross-border transfers of personal data*.

Further reading

- *EU General Data Protection Regulation, toolkit.*
- *Legislation tracker, Personal data protection reform package*.
- *Practice note, EU General Data Protection Regulation: regulatory guidance*.
- *Practice note, Drafting for Brexit: Brexit clauses*.

END OF DOCUMENT

