A concise guide to the key provisions of the General Data Protection Regulation (GDPR)

Kemp Jones Solicitors LLP
12 Basepoint Business Centre
Aviation Business Park
Enterprise Close
Christchurch
Dorset BH23 6NX

Tel: 01202 651294
Email: raynerjones@kempjones.co.uk

TABLE OF CONTENTS

Page

A concise guide to the key provisions of the General Data Protection Regulation (GDPR)

In this guide we focus on how the GDPR will affect businesses and what businesses can be doing now to prepare for the new regime.

Scope of this note

The current EU data protection regime is based on a Data Protection Directive that was introduced in 1995.

Since then, there have been major advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information.

In addition, EU member states have taken different approaches to implementing the Data Protection Directive, creating compliance difficulties for many businesses.

GDPR is an updated and more harmonised data protection law.

Businesses will have to comply with its provisions by 25 May 2018

Please see the section below - Brexit and the GDPR – for a summary of the implications of Brexit on the new regime.

We also touch briefly on the issue of Encryption – earlier this year the ICO issued new guidance on the use of encryption software to protect the security of personal data – please see **Encryption** below

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

Steve Wood, Head of Policy Delivery at the Information Commissioner's Office (ICO), in his blog "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."

The ICO has published guidance on preparing for the GDPR, details of the GDPR guidance that organisations can expect to receive and when, and an overview.

Some concepts will stay the same

Some 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.

Some concepts will change

However, the GDPR will introduce **several new concepts and approaches**, the most significant of which are outlined in the table below.

Key concepts and changes	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.	Overall, the GDPR is still likely to require significant changes for many businesses, and many of these changes will require substantial lead time. 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. Businesses could now 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; or Monitor data subjects' behaviour 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.	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 NDPAs (the ICO in the UK) will be able to impose fines on data controllers and data processors on a two-tier basis, as follows:	This is a major change. Businesses that had previously regarded non-compliance with EU data protection law as a low-risk issue must now re-evaluate their position and start to see data protection in a completely different light - as a very high-risk issue

Key concepts and changes	What businesses should be doing now
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 NDPAs include a power to carry out audits, as well as to require information to be provided, and to obtain access to premises	
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). An individual's explicit consent is still required for sensitive personal data. However, the GDPR requires a very high standard of consent – in all cases - 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 statement. 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	Businesses in the UK have, so far, been able to rely on implied consent. The bar is now set very high. As businesses must be able to demonstrate that an individual gave their consent to the processing, it is unclear, at the moment, how far they can continue to rely on an individual's implied consent. 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 (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 be able to demonstrate that consent

Key concepts and changes	What businesses should be doing now
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.	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 consideration, and may take time to implement.
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. Low-risk processing activities may face a reduced compliance burden.	As this may involve substantial changes to existing compliance arrangements businesses should start their preparations now. The ICO has published a helpful 12-step guide to assist businesses, 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.
The "one-stop shop" Under the Data Protection Directive, each NDPA may exercise authority over businesses operating in its territory.	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

Key concepts and changes	What businesses should be doing now
Under the GDPR, a business will be able to deal with a single NDPA 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 NDPA 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 NDPA for the local jurisdiction.	local NDPA under the GDPR will be similar to interaction with the local NDPA 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 NDPA as their "lead authority" (rather than multiple NDPAs). The ICO recommends that businesses should start to determine which NDPA will be their lead authority.
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	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

Key concepts and changes	What businesses should be doing now
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 out 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. 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 NDPA 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 NDPA. In addition, standardised icons to indicate important features of the relevant data processing activities in a simplified format may be prescribed by delegated acts.	ongoing requirement to keep those measures up-to-date; and Conduct data protection impact assessments where appropriate. These steps will need to be planned into future product cycles. The Information Commissioner's Privacy Impact Assessments code of practice, provides helpful guidance on when and how to implement PIAs

Key concepts and changes	What businesses should be doing now
Registrations Instead of registering with an NDPA, the GDPR will require businesses to maintain detailed documentation recording their processing activities. 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.	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 NDPAs 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.
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.	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.

Key concepts and changes	What businesses should be doing now
	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.
Strict data breach notification rules The GDPR requires businesses to notify the NDPA 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 NDPA 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.	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.
Pseudonymisation The GDPR introduces a new concept of "pseudonymisation" (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 reidentification of the coded data.	Currently, national DPAs 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.

Key concepts and changes	What businesses should be doing now
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 NDPA 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, and a referral of the issue to the ECJ	The GDPR introduces a slightly broader range of mechanisms to transfer personal data out of the EEA. 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. 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.
The right to erasure ("right to 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 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

Key concepts and changes	What businesses should be doing now
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.	of personal data is not always straightforward. As a result of the *Google Spain* decision, many businesses may already be doing this.
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.	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. The European Data Protection Board is expected to provide further guidance on profiling. Businesses should watch for further guidance, and should keep this issue under review.
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).	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.

Key concepts and changes	What businesses should be doing now
In exercising their right, the data subject can request the information be transmitted directly from one controller to another, where technically feasible.	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.
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.	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

Many businesses may be considering what approach to take in the light of the UK's decision, on 23 June 2016, to leave the EU.

The widely held view is that the UK would still wish to be considered an "adequate" jurisdiction for data protection to enable trade with the EU

The UK's Data Protection Minister at the Department for Culture Media & Sport 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 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"*.

The ICO will be speaking with government to discuss the implications of the referendum and to present its view that, given the growing digital economy, reform of the UK's data protection regime remains necessary.

It is still too early to say what form the UK's data protection law will take but, the ICO has been clear throughout that organisations should continue to prepare for and comply with the GDPR now, rather than lose valuable compliance preparation time.

Those responsible for an organisation's compliance with data protection legislation may encounter difficulty gaining management or board level support for this approach, 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.

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 DPA.

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).

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.

Encryption

The ICO has published new guidance on the use of encryption software to protect the security of personal data.

The Data Protection Act 1998 (DPA) does not specifically state that organisations must encrypt personal data.

However, the seventh data protection principle requires organisations to take appropriate technical and organisational measures to keep the personal data they hold secure.

Peter Brown, a Senior Technology Officer at the ICO, has stated in a blog, *"Encryption, being a widely available technology with a relatively low cost of implementation, is one such measure. The ICO takes the view that regulatory action may follow in cases where a lack of encryption has led to a loss of data. A significant number of the monetary penalties we have issued since 2010 relate to the failure to use encryption correctly as a technical security measure. Where data is not appropriately secured, loss, theft or inappropriate access is much more likely to occur. On top of the fines, data controllers risk significant damage to their reputation if they do not store personal data securely."*

The guidance features several scenarios designed to help organisations consider when and how they should encrypt personal data.

For example, transferring personal data by CD, DVD or USB, sending personal data by email or fax, or storing personal data on devices such as laptops, mobile phones, back-up media, databases or file servers

As regards collecting data, if personal data is in any way sensitive or otherwise poses a risk to individuals (for example because it includes credit card numbers), collection would only be sufficiently secure with the use of a secure, encryption-based transmission system.

This data should also be held on a server properly secured by encryption or similar techniques.

This Note incorporates material by Bridget Treacy of Hunton & Williams LLP originally published on Practical Law™ and is reproduced with the permission of Thomson Reuters™