slaterheelis LLP
SOLICITORS

produced in conjunction with

EUROTEKUK
MANAGED IT SOLUTIONS

A key summary of the General Data Protection Regulation

General Data Protection Regulation

Key summary and what should you be doing now

Introduction

The General Data Protection Regulation ("GDPR") comes into force on 25 May 2018 and will replace the Data Protection Act 1998. Whilst this may seem a long way off, the GDPR makes significant changes to UK data protection law and this note sets out the key areas where it will affect businesses and what businesses can and should be doing now to prepare.

Information Commissioners Office ("ICO") Guidance

As they have done under the current data protection regime, the ICO has published guidance on its website (http:/www.ico.org.uk/for-organisations/data-protection-reform/overview-of-the-GDPR) on preparing for the GDPR and set out what specific guidance they expect to be publishing in 2017 ahead of the coming into force of the GDPR - this note is subject to anything contained in such guidance.

Key Changes

CHANGE	WHAT YOU SHOULD BE DOING NOW
Changes to consent as a legal basis for processing Businesses in the UK have, so far, been able to rely on implied consent under the Data Protection Act but 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 statement. A person is still required to give their explicit consent to process special categories of personal data (things like race, sexual orientation, health etc.).	Whilst the ICO has confirmed that it will be publishing further guidance on consent, at this stage it appears highly unlikely that businesses will be able to continue to rely on implied consent. Businesses that rely on consent as a legal basis for processing personal data will need to review their procedures in detail to ensure that any consent they obtain indicates affirmative agreement from the data subject, rather than a failure to object (the example used in the GDPR is that ticking a blank box will suffice, but failing to un-tick a pre-ticked box will not constitute valid consent). For most businesses this will require a review of existing terms and conditions and privacy policies but it may also require the production of new internal policies setting out how the business intends to comply with this.

CHANGE	WHAT YOU SHOULD BE DOING NOW
Withdrawing consent Data subjects will have the right to withdraw their consent at any time.	It must be as easy to withdraw consent as it is to give it and again businesses should consider their processes for doing this and set them out clearly (in their terms and conditions and privacy policies for example). They should also ensure that they have technological processes and systems in place that would prevent further processing once consent is withdrawn.
The right to be forgotten Individuals will have the right to request that businesses delete their personal data if, for example, the data is no longer necessary for the purpose for which they were collected or the data subject withdraws their consent.	Businesses will need to develop processes and mechanisms setting out how they will implement the right to be forgotten, which may not be straightforward. Businesses should begin evaluating whether they have sufficient technological measures in place to comply with this and if not to look at putting them in place.
Data Protection Officer Businesses will be required to appoint a data protection officer if their processing is a core activity of the business or done on a large scale.	Businesses will need to review and evaluate the level of data processing they undertake and consider appointing a data protection officer with expert knowledge of data protection. This can be an employee or an outside consultant.
Subject access requests Businesses must reply within one month from the date of receipt of a subject access request (down from 40 days under the Data Protection Act) and provide more information than was required under the Data Protection Act. They also will lose the right to charge a £10 administration fee which was often used as a way to delay the start of the period for reply.	Businesses should set out internal policies on how they will respond to subject access requests within the new time scale and how they will search for and provide the additional information required. Having the appropriate technological systems and software in place will help to cut down on the time it takes to comply with a request. The reduction in the timescale and the removal of the fee makes it even more important that staff are able to identify a subject access request when received - it could be made to any member of staff and may not be described as a subject access request.

CHANGE	WHAT YOU SHOULD BE DOING NOW
Data portability Data subjects have the right to obtain a copy of their personal data from a business in a "commonly used" and "machine-readable" format and have the right to transmit that data to another business. They can request the information be transmitted directly from one business to another (where technically feasible).	Businesses that process large volumes of personal data should consider how they will give effect to this and ensure that they have or will have appropriate technological measures in place to do this including protecting the data while in transit using up-to-date encryption and device control software.
Risk-based approach to compliance Under the GDPR, businesses bear responsibility for assessing the degree of risk that their processing poses to data subjects and this is reflected in a number of areas such as: • the new accountability principle and requirement for data controllers to maintain appropriate documentation; • privacy by design and default; • privacy impact assessments; • data security requirements and the appointment of a data protection officer in certain circumstances.	As this is a significant change that may require implementing new procedures by businesses, businesses should start preparing now. The ICO has published a 12-step guide (https:www.ico.gov.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf) which recommends that businesses: • start to brief management on the GDPR and how it affects their business; • review and document the personal data they hold, recording in each case where it came from and with whom it is shared; • consider the legal basis relied upon for the various types of processing that they carry out and document this; • review privacy policies and start to make any changes to comply with the GDPR. Ensuring that encryption methods, intrusion prevention and detection and device control measures are in place and up-to-date will help to show that a business has undertaken an appropriate risk analysis.
Notification Businesses will be required to notify the ICO of all data breaches without undue delay (and where possible within 72 hours). If this is not possible, businesses will have to justify the delay to the ICO by way of a "reasoned justification".	Businesses will need to develop (and follow) a data breach response plan and procedure enabling them to react quickly. Complying with the notification obligations are likely to entail an administrative burden so getting a good response plan together and introducing breach detection software will help streamline the process and minimise costs.
Increased fines Currently, fines under the Data Protection Act are relatively low (the maximum fine is £500,000). The GDPR will significantly increase the maximum fines as follows: • **up to 2% of annual worldwide turnover or 10 million euros** (whichever is the greater) for breaches 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 or 20 million euros** (whichever is the greater) for breaches relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers.	Whereas businesses may have considered data protection issues to be relatively low risk and not placed compliance high on their list of priorities as a result, they will need to look at this again given the high level of fines that can be imposed under the GDPR. Businesses should start engaging with the process of getting GDPR compliant by getting the right policies in place and updating their technological systems where necessary.

CHANGE	WHAT YOU SHOULD BE DOING NOW
Privacy by design and default Businesses will be required to implement data protection by *design* (i.e. when creating new products, services or carrying out any new data processing activities) and by *default* (i.e. to ensure that by default only personal data necessary for each specific purpose is used).	Businesses should look to implement technical and organisational measures to ensure that they take data protection requirements into account from the creation of any new technology, product or service and keep those measures up-to-date. Businesses should also start to plan this into future product cycles.
Privacy impact assessments Businesses will be required to perform data protection impact assessments before any processing that uses new technologies which is likely to result in a high risk to data subjects takes place.	Conduct data protection impact assessments where appropriate, in particular consider the ICO's Privacy Impact Assessments Code.
Dealing with EU citizens Non-EU businesses will be subject to the GDPR if they either: • offer goods or services to data subjects in the EU; or • monitor the behaviour of data subjects that takes place within the EU The Government has indicated that they expect to keep the GDPR applicable in UK law post-Brexit. Even if this changes, you may still be required to comply with the GDPR if your business undertakes either of the above.	At this stage UK Businesses do not have to do anything additional to what is set out in this note, though they should be aware of the territorial scope of the GDPR.

Conclusion

Compliance with the GDPR is likely to require organisation-wide changes for many businesses to ensure that personal data is processed in compliance with the GDPR's requirements. Such changes may include redesigning systems that process personal data, purchasing new systems, and/or renegotiating contracts with third party data processors. Businesses should therefore understand 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 sufficient time or resources to do so.

For advice on the legal issues in this note please contact Slater Heelis. For advice on the systems and technological aspects of this note please contact Eurotek UK.

slaterheelis LLP
SOLICITORS

intouch@slaterheelis.co.uk
0161 969 3131
slaterheelis.co.uk

@SlaterHeelisLaw /slaterheelis

EUROTEKUK
MANAGED IT SOLUTIONS

security@eurotekuk.co.uk
0161 660 2745
eurotekuk.co.uk

@eurotekuk /Eurotek-UK-