HEWITSONS

THE NEW GENERAL DATA PROTECTION REGULATION

Introduction

The General Data Protection regulation (the 'GDPR') will introduce a number of changes, including an expanded territorial reach of its provisions, increased rights for data subjects and a re-balancing of the liability and risk attributed between data controllers and data processors.

Whilst the Data Protection Directive had to be enacted through UK legislation to take effect, the GDPR will apply directly and immediately from 25th May 2018. It is strongly recommended that organisations, both data controllers and data processors, prepare well in advance for the forthcoming changes.

Much of the Data Protection Act 1998 (enacting the EU Data Protection Directive 95/46/EC) carries over into the spirit and wording of the GDPR. In the following table we set out a summary of the principal changes and new obligations affecting data processors. The table highlights key issues to be considered by 'processors' before carrying out data processing activities under the new regime.

The impact of Brexit

Article 50 has now been triggered and the formal process of the UK's exit from the European Union set in motion. Nonetheless, the timing of the GDPR means that it will come into effect well before the UK's eventual exit from the EU, the latter due to take place in March 2019. The GDPR will apply in this timeframe and potentially beyond, with the UK likely to transpose a great deal of European legislation directly into domestic law. Additionally, whether the GDPR is brought into UK law or not, non-EEA (European Economic Area) organisations, including those in the UK and elsewhere, will still be caught by the GDPR if they offer goods and services to companies in the EU or monitor the behaviour of EU data subjects.

Issues	The GDPR	Comments
Definition of "processor" In general terms, a "processor" is any entity or individual (other than an employee of a controller) that processes personal data on the controller's behalf.	In summary, a "processor" is an entity that processes personal data on behalf of the "controller".	The concept of a "processor" is essentially unchanged under the GDPR. Any entity that is a data processor under current data protection law will almost certainly continue to be a processor under the GDPR. The GDPR will impose specific obligations on processors and there is an increased risk of legal liability if a processor is responsible for a data breach (these are key differences compared to current data protection law).

Issues	The GDPR	Comments
Territorial Scope The processing of personal data may take place in the EU or outside of the EU.	The GDPR will apply to the processing of personal data by a processor not established in the EU where the processing activities relate to: ■ the offering of goods and services to data subjects in the EU; or ■ the monitoring of the behaviour of data subjects in the EU.	Under the GDPR the focus will be on the subject matter of the data processing activities rather than where the processing is taking place or where the processor is based.
Appointment of processors Organisations that act as data controllers often appoint service providers to process personal data on their behalf. EU data protection law imposes certain requirements on organisations that wish to do so.	A controller that wishes to appoint a processor must only use processors that provide sufficient guarantees to implement appropriate technical and organisational measures, so that processing will meet the requirements of the GDPR and ensure the protection of the rights of data subjects. The controller must appoint the processor in the form of a binding written agreement, which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. In particular, the processor must: ■ only act on the controller's documented instructions; ■ ensure that all personnel who process the relevant data are subject to appropriate confidentiality obligations; ■ take all measures to ensure the security of the personal data that it processes; ■ abide by the rules regarding appointment of sub-processors; ■ implement measures to assist the controller in complying with the rights of data subjects; ■ assist the controller in its dealings with data protection authorities and data subjects; ■ at the controller's choice, either return or destroy the personal data at the end of the relationship (except as required by EU or Member State law); and ■ make available to the controller all information necessary to demonstrate compliance with the GDPR.	The GDPR refers to significant new requirements that must be included in all data processing agreements. The GDPR does not contain transitional arrangements, so existing data processing agreements are also affected and may need to be re-negotiated to ensure that they meet the requirements of the GDPR. The negotiation of data processing agreements (existing and new) is likely to be more complex in the future given the wider range of issues to be considered under the GDPR.

Issues	The GDPR	Comments
Direct legal obligations Legal compliance obligations for processors as well as controllers.	The GDPR will apply to the processing of personal data by a controller or a processor that falls within the scope of the GDPR (regardless of whether the relevant processing takes place in the EU or not).	Current data protection law only imposes direct compliance obligations on controllers (with processors generally only having contractual obligations, not direct legal compliance obligations). The GDPR will impose legal compliance obligations directly on controllers and processors.
Conflicts between the controller's instructions and EU law	The processor must act in accordance with the controller's instructions. If the processor believes that the controller's instructions conflict with the requirements of the GDPR or any other applicable EU laws, the processor must immediately inform the controller.	The GDPR provides a sensible solution, requiring the processor to inform the controller that it cannot comply with the controller's instructions where those instructions conflict with applicable law. It is then for the controller to issue revised instructions that are consistent with applicable law.
Appointment of sub‑processors Processors may only appoint sub-processors with the permission of the controller.	The processor must not appoint another processor without the prior written authorisation of the controller. Where the controller agrees to the appointment of a sub-processor, the same obligations set out in the contract between the controller and the processor must be imposed on that sub‑processor.	The processor will have to pay careful attention to the terms of any contract which it enters into with a sub-processor to ensure that all of the relevant obligations 'flow down' to the sub-processor. If the sub-processor fails to fulfil such obligations, the processor will remain fully liable to the controller for the performance of the processor's obligations to the controller.
Processor's obligation of confidentiality	Processors must ensure that the personal data that they process is kept confidential. The contract between the controller and the processor must require the processor to ensure that all persons authorised to process the personal data are under an appropriate obligation of confidentiality.	Data processors are already under this obligation to ensure confidentiality of personal data, so there is likely to be little practical change for processors in this regard.
Compliance with the controller's instructions	Processors (and any sub-processors) must not process personal data, except in accordance with the instructions of the controller (unless required to do so by EU law or the national laws of a Member State).	The relationship between the controller and processor is based on the principle that the processor will only process data in accordance with the controller's instructions. The GDPR preserves the position under current data protection law.
Failure to comply with the controller's instructions	Where a processor, in breach of the GDPR, determines the purposes and means of any processing activity, that processor will be considered to be a controller in respect of that processing activity.	If a processor makes its own decisions in respect of personal data, rather than following the controller's instructions, that processor will become a controller, and be subject to the full compliance obligations of a controller in relation to that processing.

Issues	The GDPR	Comments
Records of processing activities	Each processor must maintain a record of all processing activities carried out on behalf of a controller. This record must contain: ■ the name and contact details of each controller on behalf of which the processor is acting, of any other processors and any data protection officers; ■ the categories of processing carried out on behalf of each controller; ■ information regarding cross-border data transfers; and ■ a general description of the technical and organisational security measures implemented in respect of the processed data. The record must be in writing, which includes in electronic form.	An organisation acting as a processor will (unless exempt) be subject to this new obligation of maintaining a record of its processing activities, and will be required to make the record available to supervisory authorities on request. This obligation could require significant investment by processors in record-keeping functions. However, the record keeping obligation will not apply to an organisation employing fewer than 250 persons, but there are exceptions to this.
Cooperation with supervisory authorities Supervisory authorities are responsible for implementing and regulating EU data protection law.	Processors are required to cooperate, on request, with supervisory authorities in the performance of their tasks.	The GDPR will fundamentally change the obligations of processors in this regard. Data processors currently have no direct interaction with the data protection authorities under EU data protection law, but under the GDPR they will be obliged to interact with and assist supervisory authorities.
Security of processing EU data protection law obliges processors to ensure the security of personal data that they process.	Processors must implement appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access. Depending on the nature of the processing, these measures may include: ■ the pseudonymisation and encryption of personal data; ■ the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; ■ the ability to restore the availability and access to personal data in the event of a physical or technical incident; and	Current data protection law requires data controllers to contractually impose data security requirements on data processors. The GDPR will impose these requirements directly upon processors, and expose processors to fines, penalties and compensation claims for failure to satisfy those requirements. Consequently, the level of risk faced by processors under the GDPR will be significantly increased. No codes of conduct or data protection certification mechanisms are yet in place.

Issues	The GDPR	Comments
	■ a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational security measures. Adherence to an approved code of conduct or an approved certification mechanism may provide evidence that the processor has met these obligations.	
Notification of personal data breaches	The processor must notify the controller without undue delay after becoming aware of any personal data breach.	This will be a new obligation for data processors. The obligation to notify 'without undue delay' will probably require clarification in the agreement with the controller, as the corresponding obligation on the controller is to notify the relevant supervisory authority not later than 72 hours after having become aware of the breach.
Appointment of a data protection officer (DPO) In certain circumstances, EU data protection law requires a person to be formally appointed to the role of DPO in order to oversee an organisation's data protection compliance.	A processor will be required to designate a DPO where: ■ the processing is carried out by a public authority (but not the courts); ■ the core activities of the controller consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or ■ the core activities of the controller consist of processing on a large scale of certain 'special categories of data' and personal data relating to criminal convictions and offences.	Even if not required to appoint a DPO, the GDPR does envisage that a processor may wish to designate a DPO. Whilst having a DPO in place may be an additional expense, over the long-term the appointment of a DPO may help to reduce the risk of non-compliance with the GDPR. A person designated as a DPO may be a member of staff, or may be appointed as such under a service contract. The GDPR contains additional provisions regarding the position of the DPO and the tasks which he or she will undertake.
Restrictions on Cross-Border Data Transfers EU data protection law restricts the transfer of personal data to third countries unless the transfer is to a country which ensures an adequate level of protection, a lawful transfer mechanism exists, or an exemption or derogation applies.	Under the GDPR, the obligations regarding cross-border data transfers will apply directly to processors.	Processors should already be complying with the rules regarding cross-border data transfers (on the basis of the instructions issued by the relevant data controller). However, the possibility of direct liability for processors (as well as contractual liability of processors to controllers) creates a new category of risk for processors that engage in such transfers.

Issues	The GDPR	Comments
Liability of processors EU data protection law recognises the possibility that processors may be liable for breaches of their legal or contractual obligations.	Any data subject who has suffered damage as a result of an infringement of the GDPR will have a right to receive compensation directly from a processor for the damage suffered. A processor will be liable for the damage caused by its processing activities only where it has: ■ not complied with obligations under the GDPR that are specifically directed to processors; or ■ acted outside or contrary to lawful instructions of the controller.	a result of breach or non-compliance with the GDPR will be a new risk. Processors should check their existing insurance policies and/or speak to their insurance brokers to determine the extent to which possible claims would (or would not) be covered. A processor will be exempt from liability if it proves that it was not in any way responsible for the event giving rise to the damage. If the damage is caused by both the processor and a controller, each of them will be held liable for the entire damage. This is to ensure effective compensation of the data subject.
Administrative fines Infringements of the GDPR may result in substantial fines	A supervisory authority may impose fines, depending on a whole range of factors, regarding the infringement in question. For some infringements, the fine can be up to EUR 10,000,000 (or 2% of worldwide annual turnover, if higher) whilst for others the fine can be up to EUR 20,000,000 (or 4% of worldwide annual turnover, if higher).	The potential amount of these fines is not insubstantial and should provide a sufficient incentive for processors to ensure compliance with their obligations under the GDPR.

Bill Thatcher

Partner
Cambridge
01223 461155
billthatcher@hewitsons.com

Valerie Lambert

Partner
Cambridge
01223 447427
valerielambert@hewitsons.com