Thorntons

The General Data Protection Regulation: A Comparative View of Key Issues

The EU General Data Protection Regulation ("GDPR") was approved by the European Parliament in April 2016. As a regulation, it is directly applicable without the need for domestic legislation and it is due to be applicable in all member states from 25th May 2018. It shall effectively repeal the current data protection regime under the Data Protection Act 1998 ("DPA") and introduce a new framework regulating the processing of personal data.

Its purpose is multi-faceted. For individual citizens, it aims to strengthen European citizens' rights in relation to how their personal data are processed. For organisations it aims to provide support by doing away with the fragmented approach currently held across Europe and replace it with a more harmonised regime.

While it is a significant reform in the area of data protection, not all of the current practices will completely disappear. GDPR, in many respects, builds on the current position rather than completely eradicating it. This article provides a comparative view of the current vs. future data protection regime focusing on key issues.

Issue	DPA	GDPR	Comment
Definition of 'Personal Data'	*"personal data"* means data which relate to a living individual who can be identified— (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.	"personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	The definition of personal data is largely the same under GDPR as it is under the DPA: on a basic level it continues to mean any information which can be used to identify an individual. The definition in the GDPR has however been clarified and now specifically covers ID numbers, physical and physiological indicators, and IP addresses. Organisations currently caught by DPA ought to assume they will be caught by GDPR also.
Definition of 'Sensitive Personal Data'	*"sensitive personal data"* means personal data consisting of information as to— (a) the racial or ethnic origin of the data subject,	GDPR uses the term "special categories of personal data" meaning personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs,	Despite the new name, this class of data is largely similar in substance to the DPA. The inclusion of genetic data (data that relates to the inherited or acquired genetic

	(b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.	or trade union membership. This term also includes personal data that consists of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.	characteristics of a natural person and which gives unique information about that person) and biometric data (personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person (e.g. data arising from fingerprints) where used to identify an individual is new. Please note that it is not intended that photographs will necessarily be considered a special category of data, albeit they may be where e.g. used as part of a biometric passport.
Accountability	Did not expressly exist under the DPA.	GDPR introduces a new obligation on Data Controllers to be able to demonstrate compliance with the six data processing principles contained in Article 5 of GDPR (e.g. data shall be processed fairly and lawfully, limited purposes, data minimisation, accuracy, kept for no longer than necessary, kept secure etc.).	It will not be enough to comply with GDPR; Data Controllers need to be able to demonstrate that they comply. Compliance with GDPR will need to be embedded throughout the organisation. In practice this is likely to have an impact on the governance of the organisation. What this looks like in practice will depend on each organisation however it is likely to lead to consideration of the following: • regular staff training sessions;

			• compliance with GDPR's record keeping obligations; • ensuring appropriate organisational and technological measures are in place to ensure security and integrity of data; • execution of privacy impact assessments when rolling out new projects; • undertaking appropriate due diligence on suppliers; • ensuring appropriate internal policies are in place and these are implemented e.g. internal privacy policies, security breach policy, on-boarding new suppliers policy; • ensuring supplier and other contracts and privacy policies address data protection appropriately; and • undertaking regular internal audits.
Fines	The ICO can serve monetary penalty notices for contraventions of the DPA up to a max of £500,000.	The GDPR will have a two tier penalty system: • **Greater of 2% of annual global turnover or €10M** – to cover e.g. failing to obtain parental consent for children; failure to adopt appropriate technical and organisational measures designed around systems and which achieve certain default positions; failure to put in place specific contractual terms with data processors; failure to notify a breach to supervisory authority; failure	The maximum fines that can be imposed are significantly higher than the current system, quickly promoting data protection to a board level issue. Notably processors will be caught by GDPR and can also receive fines, which is not currently the case. With a view to minimising risk, organisations ought to undertake a gap analysis/audit of their current data protection compliance and if necessary,

		to appoint a Data Protection Officer (if applicable); • **Greater of 4% of annual global turnover of €20M** – to cover failing to comply with the six data processing principles; infringing data subjects' rights; failure to comply with a limitation order from e.g. ICO etc.	implement measures to bring compliance up to GDPR standard.
Reporting Security Breaches	No absolute statutory requirement to report security breaches to ICO.	Controllers must report a personal security breach to the ICO without delay and at the latest, within 72 hours of becoming aware of it if it presents a risk to the rights and freedoms of the data subjects. Processors must report a personal security breach to the data controller without undue delay.	In the event of a personal security breach, it is imperative that organisations can take steps to mitigate the loss or damage to the data subjects and also the organisation itself. It is good practice for organisations to consider putting in place a plan now to deal with security breaches, to include, identification of staff members responsible for notifying the ICO.
Data Protection Officers (DPO)	No legal requirement for organisations to appoint a DPO in the UK.	Organisations will require to appoint a DPO if they fall into one of the following categories: • public authority (except from courts acting in their judicial capacity) e.g. a University or Local Council; • an organisation whose core activities involve data processing which require regular and systematic monitoring of data subjects on a large scale e.g. insurance companies; • an organisation whose core activities	Organisations which do not fall into any of the named categories can choose to voluntarily appoint a DPO. However it seems unlikely that organisations will do so as even voluntarily appointed DPOs will have to adhere to the DPO's obligations under GDPR. If an organisation decides that it is not necessary to appoint a DPO, it is recommended to keep a record of its internal analysis used when determining whether a DPO is necessary or not. This

		consist of processing special categories of data or personal data relating to criminal convictions and offences, on a large scale; or • the Member State in which they are based requires it e.g. Poland. GDPR sets out a minimum set of tasks attributed to the DPO. These include (a) informing and advising the organisation and employees of GDPR and associated laws; (b) monitoring compliance with the GDPR and associated laws and the organisation's policies and procedures, assigning responsibilities within the organisation and training staff involved in processing and audits; (c) provide advice regarding data protection impact assessments and monitor performance; (d) liaise with supervisory authority e.g. ICO; and (e) to act as the contact point for the supervisory authority on issues relating to processing.	record could be useful in the event the decision not to appoint a DPO is ever challenged. The role is designed to be a senior role with the ability and freedom to act independently with direct access to highest levels of management. Given the seniority of the role, the level of knowledge required and the amount of organisations that will need to appoint one, there may be a shortage of suitable candidates in the short to medium term. Accordingly HR teams may wish to start thinking about how to fill this role well ahead of the 25th May 2018 deadline. Failure to appoint a DPO could lead to a fine of the greater of 2% of annual worldwide or €10M.
'Legitimate Interests' and relying on this to justify processing personal data.	Organisations can legitimise processing personal data if this is necessary for legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice	GDPR provides for a similar 'legitimate interest' basis to process personal data as is currently available under the DPA, except that this will not be available to public authorities in the performance of their tasks. Note:- the term 'public authority' is not defined under GDPR. Until	Once arguably a 'catch all' processing basis will be under much more scrutiny going forward. Organisations wishing to rely on legitimate interests to justify processing personal data need to establish and be able to

	to the rights and freedoms or legitimate interests of the data subject	clarified it is suggested that organisations currently defined as public authorities under the DPA assume they will continue to be referred as such under GDPR.	demonstrate what this legitimate interest is. Appropriate records ought to be kept in this regard and this 'interest' ought to be evaluated on an evolving basis to ensure it continues to justify processing personal data. Such records ought to assist if ever called upon by the ICO on this point. In addition, organisations ought to communicate to data subjects by appropriate means typically within the privacy statement what the legitimate interest is. Public authorities ought to review the basis upon which it is processing personal data. Where it is relying on the legitimate interest basis, it is recommended that they seek to identify whether processing can be justified under a different basis.
Consent	EU Data Protection Directive (which DPA implements) defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." Individuals ought also be given information on the type of information being collected, why the information is being processed	GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" Going forward, there must be some form of clear affirmative action to signify	Relying on consent obtained prior to GDPR will continue to be a valid basis upon which to process data post-GDPR, provided such consent meets the requirements of GDPR. Organisations should review the basis upon which consent was obtained against GDPR requirements and consider whether fresh consent needs to be obtained or alternatively, identify whether processing

	and any other aspect which affects them. Opt-out or deemed consent such as unticking a box is permissible under certain circumstances.	consent – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. GDPR emphasises that consent must be freely given – it is therefore important that it is separate from other terms and conditions. The ICO recommends that organisations ensure that its consent mechanisms are specific, granular, clear, prominent, opt-in, documented and easily withdrawn. Some key things to think about are: • **Unbundled**: consent should not generally be a precondition of signing up to a service, particularly in relation to obtaining consent for marketing. • **Active opt-in**: pre-ticked opt-in boxes are invalid. • **Granular**: provide options to consent to different types of processing. • **Named**: name your organisation and any third parties who will be relying on consent. • **Ability to withdraw**: tell people they have the right to withdraw their consent at any time, and how to do this. Provide an easy and quick way for people to exercise this right.	can be legitimised by other means.

Data Processors	"Data Processors" means any person who processes the data on behalf of the data controller (other than an employee of the data controller). Data processors are not directly subject to the DPA and no enforcement powers can be used against them.	Data processors are now included in the scope of the GDPR and will now have direct statutory obligations to comply with. Key issues processors ought to be aware of are: • potentially exposed to enforcement action e.g. fines; • can be held to account by the data subjects directly e.g. compensation; • may require to appoint a DPO if appropriate (see above); • will have new record keeping obligations; • will need to ensure its contracts comply with GDPR mandatory clause requirements; • need customer consent prior to engaging sub-processors; • must implement appropriate organisational and security measures to ensure security and integrity of data.	This is a key change for those currently acting as data processors who until GDPR largely escaped legal responsibility for processing personal data. Processors ought to start preparing for GDPR now and evaluate and address the additional risk and cost GDPR may present to their organisation.
Extra Territorial Scope	The DPA as it stands only applies to organisations processing data in the UK.	The GDPR will apply across the whole of the EU. Will also effect organisations operating out with EU if they offer goods and services to, or monitor, EU citizens.	This extra-territorial reach will help to prevent any gaps in the protection of EU citizens' personal data. Non-EU organisations caught by GDPR ought to address any areas of non-compliance ahead of May 2018. Likewise EU based data processors/controllers should consider approaching any suppliers they use outwith the EU with a view to discussing

			how the necessary steps can be taken to ensure the relationship complies with GDPR e.g. by updating any processing contract.
Rights of Data Subjects	Data subjects generally have the following rights under the DPA: • The right of access to a copy of the information comprised in their personal data; • The right to object to processing that is likely to cause or is causing damage or distress; • The right to prevent processing for direct marketing; • A right to object to decisions being taken by automated means; • The right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and • The right to claim compensation for damages caused by a breach of the Act.	GDPR largely retains the rights data subject currently enjoy. It does go further however by strengthening the current right to object to processing and by introducing a new 'right to be forgotten' and the right to data portability'. Potentially these could be significant.	Data subjects have increased rights over how their data are used under the GDPR. They are not always absolute rights and it is unlikely to be straightforward for organisations to determine how they should respond to such requests. We recommend that organisations consider putting in place back end policies and procedures to deal with requests from data subjects to ensure these can be done in an efficient and cost-effective manner.
Children	The current DPA does not directly deal with children specifically apart from a general provision in s. 66 that the age of consent of a child is dependent on their capacity when under the age of 16, but that children of 12 years and above will be presumed to be of sufficient age and maturity.	GDPR has introduced specific protection with regard to the processing of data of children, who are identified as "vulnerable individuals" deserving of "specific protection". Broadly, GDPR will impact the processing of children's data by the following means: • **Parental Consent for Online**	Organisations ought to review the basis upon which they process children's data and identify if they are valid under GDPR. In particular, organisations will need to be alert to the varying ages of consent if their customers are located in more than one Member State. GDPR in this regard may also present

		Service: if your organisation targets online services at children and the processing condition relied upon is consent then, following GDPR, such consent will only be valid if the child is at least 16 years old or if younger, consent is provided by someone who has parental responsibility over that child. Member States have some discretion in relation to the age a person is considered to be a child in so far as they may lower it provided it is not lowered beyond 13 years. It has been reported that the UK shall lower the age of consent to 13 years. • **Privacy Notices:** privacy notices and information directed at children must be written in clear and plain language that they can easily understand. • **Profiling and Automated Decision Making:** GDPR contains restrictions on decisions based solely on automated processing and profiling if the decisions significantly affect the data subject. One restriction is that such measures should not be used when concerning children.	certain practical difficulties for organisations in terms of how they verify that consent is given or authorised by someone with parental responsibility as opposed to a child pretending to be the parent. It is easy to identify circumstances where relying on online consent to process data relating to a child from someone with parental responsibility could be open to challenge. Organisations should also be aware that Member States, the EDPB and the Commission are encouraged to create codes of conduct in relation to the personal data of children. This may result in additional requirements being imposed following the implementation of such codes.
Privacy Notices	In order to comply with the fairness processing principle, organisations collecting information must have a method	GDPR builds on DPA in this regard in terms of the information that must be supplied to data subjects. The manner in which these	Organisations ought to review their privacy notices and update these to comply with GDPR standards as required and also how

	of informing individuals who they are, the purposes of gathering/processing the information, and any further information that is necessary in the circumstances. The ICO recommends under the DPA this is done by a privacy notice, but that is not compulsory if the data controller can evidence compliance with the fairness principle in other ways.	notices are communicated must also be considered to ensure they are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.	these ought to be communicated. The EU Commission may introduce the use of standardised icons to ease understandings and we await clarification on this.

Thorntons

Whitehall House 33 Yeaman Shore Dundee DD1 4BJ

Tel 01382 229111
www.thorntons-law.co.uk/GDPR