GUIDANCE NOTE

General Data Protection Regulation ("GDPR")

December 2017

1. What is GDPR?

The General Data Protection Regulation ("GDPR") is a European regulation designed to strengthen and unify data protection for all individuals within the European Union ("EU").

Despite the UK's current intention to leave the EU in 2019, the new law comes into force on 25th May 2018 so will affect all UK organisations. Until that time the Data Protection Act 1998 ("DPA") and associated legislation will continue to apply.

There is a lot of information circulating about GDPR some of which is helpful and some of which is a little misleading. This Guidance note aims to provide factual detail relating to GDPR requirements and provide links to useful resources as GDPR continues its passage through the UK legislature.

2. Where to go for information?

Firstly, don't believe all publications and information available. We would suggest, in addition to raising any queries with us, that reference is made to the information available and published by the Information Commissioners Office ("ICO"), the UK Regulator for data protection matters.

The CEO of the ICO has a blog which is useful in separating facts from hype. The following are useful starting points for information:-

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/institute-of-directors-digital-summit/

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/institute-of-directors-digital-summit/

The notable point from the text of the CEO's speech to the Institute of Directors is the comment that the ICO views fines as a last resort and that the ICO considers its remit to guide, advise and educate organisations on how to comply with the law.

3. GDPR is not yet finalised

GDPR will replace the Data Protection Act 1998, together with the Privacy and Electronic Communications Regulations.

As at the time of writing the UK Government is still debating various elements of the GDPR including how it will be enforced on a practical basis. For example, one of the key elements of the processing of personal information is the "legitimate interest" grounds on which parties can process personal information, which is outlined in more detail below.

The effect of this is that whilst arrangements and planning should be taking place, organisations cannot have everything in place until the legislative process is complete and organisations should keep up to date with guidance from the ICO. We would recommend that organisations prepare on a belt and braces approach and adjust that approach as guidance is released and the legislation is finalised.

4. Key Principles of GDPR

The purpose of GDPR is to encourage best practice in the processing of personal data. A significant addition to what organisations may be doing under the current data protection regime is that GDPR adds more accountability into the regime.

Whilst organisations may comply with GDPR they need to be able to show and demonstrate how the organisation complies.

This means decisions must be documented and organisations must have policies on how personal data will be processed.

Under GDPR, personal data shall be:-

- Processed lawfully, fairly and in a transparent manner;
- Collected for a specified, explicit and legitimate purpose (and not further processed in a manner incompatible with those purposes)
- Adequate and limited to what is necessary;
- Accurate with reasonable steps taken to try and ensure this;
- Kept secure.

5. What is Personal Data? Has this changed?

The definition of "personal data" in GDPR is more expansive than under the DPA but the view from the ICO is that in reality there ought to be little practical difference. Broadly speaking and as a rule of thumb, if you can identity any individual for data relating to their personal life, their family, or their business/professional life, it is classed as personal data.

Examples would include:-

- Name with a home address;
- Online profile with a name and the company the person works for;
- A corporate email address;
- HR records;

- Customer lists and contact details;
- IP addresses.

Sensitive Personal Data is classed as "special category personal data" and covers information on a person's health; sexual orientation, genetic or biometric data. This kind of data is handled more strictly than provisions relating to sensitive personal data under the DPA.

- **Data Controller and Data Processor**

As with the DPA, GDPR retains "data controllers" and "data processors". The data controller determines how and why personal data is processed and the data processor acts on the controllers behalf.

- **Data Protection Officer**

It is not compulsory under GDPR to appoint a Data Protection Officer unless the organisation:-

- Carries out large scale systemic monitoring of individuals (e.g. online behaviour tracking);
- Carries out large scale processing of special categories of data or data relating to criminal convictions and offences;
- Is a Public authority (except for Courts acting in a judicial capacity).

Whilst it may not be compulsory to appoint a Data Protection Officer, it is prudent that organisations look at the various elements within the organisation and appoint someone to oversee the protection of data within departments as part of the ability for an organisation to be able to demonstrate compliance.

GDPR needs to be seen as organisation wide, from senior management to every member of staff so that data protection becomes embedded within the organisation. Awareness and buy in to the principles of GDPR are key parts of compliance and it has to be an ongoing process.

- **Individual Rights**

There are 8 GDPR rights that need to be understood and considered. Rights for individuals under GDPR are far stronger than under DPA. GDPR creates new rights and strengthens existing DPA rights.

- *The right to be informed*

  An individual needs to be provided with "fair processing information" and this would typically be through a privacy notice and must clearly and transparently set out how personal data is used.

  Any privacy notice must be published and be accessible, and in easy to understand language. Internal procedures should provide information as to how employees are expected to process personal data. The information that ought to be included in a privacy notice is determined by how data is obtained. The ICO have produced a useful table:

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

- *The right to access*

This is similar to rights under the DPA and organisations should be prepared to provide the following:-

i. Confirmation that their data is being processed;
ii. Access to their personal data;
iii. Other supplementary information.

Access requests should be answered without delay and the right to charge £10 has gone, but a reasonable fee can be charged if requests are excessive, unreasonable, or repetitive.

- *The right to rectification*

Individuals have the right to request personal data is rectified if it is inaccurate or incomplete. Such requests need to be responded to within a month, or two if complex. If incorrect information has been shared with third parties, they need to be notified of the rectification as soon as possible.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

- *The right to erasure/to be forgotten*

Broadly, the right is to enable an individual to request deletion/removal of personal data where there is no compelling reason for its continued processing.

Consideration will need to be given as to the circumstances when an individual requests that data is erased. There may be times when the request can be fulfilled, but there may be times when the request cannot be fulfilled.

Where personal data cannot be deleted, organisations should consider whether other ways are possible to satisfy the request, i.e. ensure that the data is restricted for processing.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

- *The right to restrict processing*

As with the DPA, individuals have a right to block or suppress processing. When processing is restricted, organisations can store personal data but not process it.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

- *The Rights to Data Portability*

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the movement, copying, transferring of personal data easily from one IT environment to another in a safe and secure way without hindrance to the usability of the data.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

- *Right to Object*

Individuals have a right to object to processing that organisations undertake. The right to object should be in the privacy notice and at the point of first communication. This right must be "explicitly brought to their attention and presented clearly and separately from any other information".

Importantly if an organisation processes personal data for direct marketing purposes and an individual objects, the processing must stop as soon as the objection is received. No exceptions. No grounds for refusal.

If personal data is processed for legitimate interests and an individual objects, the processing must stop unless there can be demonstrated compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

- *Rights related to automated decision making and profiling*

This right stems from the expansion of digital technologies where significant amounts of "behind the scenes" processing may take place, such as trawling social media and websites to create datasets detailing an individual's behaviour.

Automated decision making should not take place in the case of children. Where it takes place in the case of an adult, procedures need to be in place where the individual can obtain human intervention with a view to being able to get an explanation of the processing being undertaken and information to be able to challenge the process.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

- **How to make GDPR manageable?**

The starting point is to try to understand what data the organisation has and what the organisation does with it. If individuals have been tasked and appointed with responsibility within the organisation for GDPR compliance, it is worth undertaking an audit to identify data held across the various elements of the organisation, e.g. sales, marketing, HR etc. The following should be considered:-

- What personal data is held? Is it necessary to collect that data?
- Does any personal data qualify as sensitive/special category personal data?
- How the organisation collects data?
- Does the organisation have consent for processing the data? Was the consent acquired in a GDPR compliant manner?
- Where is data held and how secure is it?
- What measures are in place to prevent data breaches?
- How long the data will be held? Is the data such that there is a specific timescale for holding it?
- Is data shared with third parties?

- **Data Security and Third Parties**

Data Security should be high on the list when conducting a data audit. Once an organisation has assessed the data it has, it needs to assess how secure it is. Data breaches, especially sensitive data breaches or breaches involving financial details can cause significant stress to individuals. Organisations should try to identify weaknesses in their organisation, whether it be how individual employees access data, or engagements with third party suppliers.

The ICO has significant guidance on Data Security

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

Special consideration ought to be given to data held on minors, i.e. children under 16. Children under the age of 16 cannot give consent under GDPR, although the UK is looking at lowering this to 13. As such, consideration ought to be given where data is held on individuals under the age of 16 as to whether age verification systems ought to be added to systems that capture information. If the organisation is likely to receive or request information which may come from a minor (however ultimately defined) consideration should be given to mechanisms for obtaining a parent or guardian's consent as processing the data would then be permitted under GDPR.

As part of the data audit and security review it should be clear as to what arrangements are in place with third parties, whether employees, suppliers, customers or any other party. Those people and organisations that have data shared with them ought to be part of the GDPR planning. Once identified consideration needs to then be given as to the capacity in which the organisation handles the data, i.e. whether as data processor or data controller.

From there effective liaison needs to be undertaken with the third parties to ensure that they understand their obligations and the organisation's needs to understand how their processes impact on the data protection policy.

- **What is the lawful basis for the processing under GDPR?**

Once the audit has been undertaken, decisions can be taken as to how data held is to be used and processed and consideration given to how future personal data is collected, processed and, if appropriate, stored.

A lot of focus on GDPR has focussed on the concepts of consent. Consent is ***one*** of the grounds under which personal data can be processed.

Again the ICO has published lengthy guidance on consent as part of a consultation exercise.

https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

GDPR sets higher standards than DPA in relation to consent. Consent is not a new concept and was present under the DPA but mechanisms for consent will need to be more robust under GDPR. It may be, depending on the data being processed, that a more granular method of opting in to the processing (whether for marketing purposes or otherwise) is required. The retention of records of consent, and the provision of a simple, and easy to access method of being able to withdraw consent should be considered.

Any consent must be:-

- Freely given;
- Specific for a particular purpose;
- Fully informed.

Additionally there must be an indication signifying agreement, which must involve the individual undertaking a clear affirmative action and any agreement must also be unambiguous.

An update to the ICO's guidance is due in the near future.

In addition to consent, there are 5 (five) other ways in which data may be processed and comply with GDPR. These are:-

- Contract – the data subject has entered into a contract;
- Compliance – i.e. data needs to be processed to comply with a legal obligation;
- Vital Interests – i.e. data can be processed if required to protect someone's life
- Public Test – i.e. data processed for the public interest; and
- Legitimate Interests – i.e. if there is a genuine and legitimate reasons for processing the data – including for commercial gain.

It is likely that organisations may well seek to rely on the "legitimate interests" limb. GDPR recognises that there may be good reason to process data without consent – including for commercial gain – but if this is relied on the issues of fairness, transparency and accountability still apply.

Legitimate Interests is, at the time of this note, still being debated by Government and so the precise extent of this element of compliance is still unclear. However, the view expressed by the ICO is that it is likely that most UK organisations are likely to use this, particularly in relation to processing personal data for marketing purposes.

In terms of the processes that organisations tend to employ under DPA, i.e. a tick in a "marketing box" as overarching consent for marketing to business to consumer (B2C) and business to business (B2B) these will need to be reviewed and different mechanisms put in place for B2C and B2B. Overarching consent is not be permissible under GDPR.

Existing consents ought to be reviewed to ensure that they check the GDPR standards. If they do, no further action is necessary.

- **Breaches**

A personal data breach under GDPR means a breach of security leading to:-

- Destruction of;
- Loss of;
- Alteration of;
- Unauthorised disclosure of;
- Or access to

personal data.

Under GDPR, notification needs to be made to the relevant supervisory authority, which in instances where organisations elect the UK to be lead regulator would be the ICO, within 72 hours where a loss of customer details leaves individuals open to identity theft. However, certain breaches may not meet this threshold and each instance must be judged on its own facts. GDPR does recognise that it may not be possible to fully investigate matters in that timeframe and information can be provided on a phased basis.

Specific information needs to be included as part of any notification.

Failing to notify a breach when required to do so can result in a significant fine of up to 10 million Euros or 2 per cent of global turnover.

It is important for organisations to have in place robust internal reporting procedures and protection against breaches. Organisations should also have in place an environment where breaches can be reported given the potential fines for breach and tight timescales for notification, where required.

- **Data Protection by Design and Default**

Under GDPR there is an express requirement that privacy is built into an organisation's systems from the start – not simply bolted on to the existing policies. In some instances, an organisation will have to a have in place a Data Privacy Impact Assessment in place.

- **European Organisations**

For organisations that operate in more than one EU member state, a lead data protection supervisory authority needs to be chosen. Once chosen it should be documented it and the Data Protection Officers should be are aware of it and what it does.

If the organisation operates in more than one EU member state, the lead authority is the one in the state where your main establishment is. The main establishment is the location where the organisations central administration in the EU is, or else the location where decisions about the purposes and means of processing are taken and implemented. This is only relevant where the organisation carries out cross-border processing.

General

The principles set out in this Guidance discussed above are not intended to be prescriptive and it is the responsibility of each individual organisation to ensure that it has, and can prove that it has, adequate procedures in place that are proportionate to the level of risk faced by its business.

The comments in this Guidance Note are of a general nature only. Full advice should be sought on any specific problems or issues.

ASHTON BOND GIGG
DECEMBER 2017