BRIEFING NOTE

Governance

The General Data Protection Regulation (GDPR)

Introduction

This briefing note looks to summarise the main points held within the GDPR but, as can be seen, this still results in an overview which is not very brief.

The General Data Protection Regulation (GDPR) is an EU law which comes into force on 25th May 2018. The UK government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Most headlines seem to concentrate on the maximum fines for infringement, subject access requests and the "right to be forgotten". However, the GDPR is much more than these headline grabbers.

The GDPR will introduce a common Data Protection policy across the whole of the EU and will apply to any organisation that holds data on EU citizens no matter where they are based.

Appendix A provides the key differences between the Data Protection Act and the GDPR, as supplied by the Scheme Advisory Board.

Who does the GDPR apply to?

The GDPR apples to 'Controllers' and 'Processors', which have broadly similar definitions as those under the Data Protection Act 1998 (DPA). For clarity:

Data Controller - determines the purpose and means of processing the personal data (i.e. the Scheme Manager)

Data Processor - processes the personal data on behalf of the Controller (e.g. Kier)

The GDPR will lead to significantly more legal liability to Processors if they are responsible for a breach (under the DPA the responsibility was with the Controller). This does not mean that the Controller is relieved of any obligation where a Processor is involved – the GDPR places further obligations on the Controller to ensure their contracts with Processors comply with its requirements.

What Information does the GDPR apply to?

Personal Data

Although the GDPR definition is more detailed (e.g. an IP address will be seen as personal data), for most organisations keeping member/employee information the change to the definition will make little practical difference. If the data you hold currently falls within the scope of the DPA it will also be covered by the GDPR.

The GDPR applies to both automated personal data and to manual filing systems that are accessible according to specific criteria. This is a wider definition than under the DPA and could include chronologically ordered sets of manual records containing personal data (e.g. one-off payments held in a paper ledger).

Sensitive Personal Data

The GDPR refers to this type of data as "special categories of personal data". Again, these are broadly the same as under the DPA but with some minor changes. For example, this now covers genetic and biometric data if it is used to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but extra safeguards apply to its processing.

Principles

These are similar to those under the DPA, but with additional detail and a new accountability requirement being attached. There are no principles relating to individuals rights nor for transferring personal details overseas; these are specifically addressed in separate articles (contained within Chapter III and Chapter V of the GDPR respectively).

The accountability principle is the most significant addition. The GDPR will require you to show how you comply with the principles (e.g. documenting decisions you take about processing activity).

Key Areas to Consider

Lawful Processing

For processing to be lawful under the GDPR, you need to identify a legal basis before you can process personal data. These are often referred to as the "conditions for processing" under the DPA.

It is important that you determine your legal basis for processing personal data and document this.

This becomes more of an issue under the GDPR because your legal basis for processing has an effect on individuals' rights. For example, if you rely on someone's consent to process their data, they will generally have stronger rights, for example, to have their data deleted.

Consent

As a general point it is recommend that reliance on consent as a justification for processing of data by Scheme Managers should be avoided where another lawful basis for processing can be relied on. This is because consent has to be freely given and individuals have to be free to withdraw consent at any time. If consent is withdrawn, the Scheme Manager would then have to cease processing the data concerned and this is unlikely to be practical in many cases.

Article 6 of the GDPR provides that the processing of personal data is lawful only if:

(i) the data subject (i.e. the member or beneficiary) has given their consent to the processing of their personal data;
(ii) processing is necessary for the performance of a contract to which the data subject is a party or to take steps to enter into a contract at the request of the data subject;
(iii) processing is necessary for compliance with a legal obligation on the Controller;
(iv) processing is necessary to protect the vital interests of an individual;
(v) processing is necessary for the performance of a task carried out in the public interest; and/or
(vi) processing is necessary for the purpose of a legitimate interest.

Although Trustees of private sector schemes typically rely on point (vi) (i.e. they need to hold and process personal data to fulfil the purposes of the pension trust) this does not apply to processing carried out by public authorities.

Individual member consent[1] for the processing of personal data to carry out basic administration of the Public Sector Schemes should also not be relied on.

Due to Public Sector Schemes being required to comply with the relevant Pension Regulation, point (iii) (i.e. processing is necessary for compliance with a legal obligation) would be the basis that Scheme Managers could rely on (legal advice may be required to confirm this is the case).

Special Categories of Personal Data

Generally, under Article 9 of the GDPR, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing 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 is prohibited subject to a number of exceptions.

Two of these exceptions are explicit consent or that the processing is necessary for carrying out obligations under employment, social security or social protection law (including pensions), or a collective agreement pursuant to Member State Law (i.e. the Pension Scheme Regulations).

[1] Individual member consent will be required when processing medical data for ill health benefits.

There is therefore a strong argument that the processing by a Scheme Manager of special categories of member personal data will not require specific consent, on the basis that it is necessary to perform obligations under social protection law.

However, in relation to health data, because consent is needed under the Access to Medical Reports Act 1988 it is recommended that explicit member consent is sought when dealing with ill health early retirement applications.

Children's Personal Data

The processing of personal data in relation to children is required under the Pension Scheme Regulations and therefore, where survivor benefits are payable to the child of a member, such processing would be lawful processing of personal data and the child's consent would not be needed.

It should be noted that the GDPR contains provisions that are intended to enhance the protection of children's personal data, in particular in relation to privacy notices for children where services are offered directly to a child. It is not believed that consent will be needed if a beneficiary is a child. However, if privacy notices are provided to children then they would need to be drafted as simply as possible so that children are able to understand them.

Guidance from the Information Commissioner's Office (ICO) is expected in relation to the processing of children's data.

Member Data Where There Is No Longer a Liability

Under the GDPR, personal data should not be longer than necessary and therefore there is a requirement on the Data Controller to establish time limits for erasure or periodic review. However, as has been seen in the ongoing GMP reconciliation process, and in tracing lost pensions, there could be a requirement for specific member data to be retained even after that member no longer holds benefits in that scheme.

Due to pensions being very long term liabilities, there is an argument that it can be justified to keep data for ex-members indefinitely. However, given the data should be held only for as long as is needed, and only essential data should be retained, this will require a decision about what is really needed. For example, after a member has transferred out it may be felt unnecessary to retain the salary and service data that was used to calculate the transfer value or their bank account details. Where it is possible to "fillet" the retained data to the bare essentials this would be helpful to comply with the GDPR, though this non-essential data may still exist within back-up data.

We expect market practice to develop over time and this will be kept under review. Further, the use of approved codes of practice and certification mechanisms are endorsed by the GDPR. Whilst no such codes or certification schemes have currently been published or approved it is expected that they will be produced in due course and this may include codes of practice on the retention of data.

Individual Rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for individuals:

1. to be informed - emphasises transparency over how personal data is used
2. of access[2] - similar to existing rights under DPA, though the £10 access fee is removed[3]
3. to rectification[1] - correct any inaccuracies or missing information)
4. to erasure (also known as right to be forgotten) – deletion, or removal, of personal data where there is no compelling reason to hold it
5. to restrict processing - e.g. accuracy is being contested
6. to data portability – provision of data in a structured, commonly used and machine readable form
7. to object - individuals must be informed of their right to object "at the point of first communication" and in any privacy notice)
8. in relation to automated decision making and profiling – to safeguard against the risk that a potentially damaging decision is taken without human intervention

Accountability and Governance

These provisions within the GDPR complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

It is expected that comprehensive but proportionate governance measures are put in place. Good practice tools, such as privacy impact assessments and privacy by design, are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

You **must**:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection

[2] To be provided without undue delay, and within one month from receipt of request. This can be extended by further two months if request is complex or numerous. Explanation for the extension must be provided within the initial one month timeframe
[3] A 'reasonable fee' can be charged, based on the admin cost of providing the information, when a request is manifestly unfounded or excessive, particularly if it is repetitive.

policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- As a Public Body, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default.
- Use data protection impact assessments where appropriate.

Data Protection Officer (DPO)

As a Public Body, the GDPR requires that you appoint a DPO.

The role of DPO should be a standalone function in order to avoid any conflict of interest. In other words, the data protection officer should not also have responsibility for an authority's use of personal data.

Once appointed, the DPO should open communications with Kier to ensure any relevant processes are understood and any additional requirements can be agreed and documented.

Legal Entity Has More Than One Role

The Data Controller can, potentially, have more than one role in respect of employee/scheme member personal data. If this is the case, there should be documented protocols in place to show the different circumstances in which the entity is processing personal data. It would also need to be careful to ensure that where it holds personal data that it has obtained in one capacity, that it does not inadvertently use that data to perform its other roles.

What do I need to record?

You must maintain internal records of processing activities. You must record the following information. There are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

Name and details of your organisation (and where applicable, of other Controllers, your representative and data protection officer).

- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

Data protection by design and by default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Under the DPA, privacy by design has always been an implicit requirement of the principles – e.g. relevance and non-excessiveness - that the ICO has consistently championed. The ICO has published guidance in this area.

The Article 29 Working Party has published guidelines and FAQs on lead supervisory authorities ‧. These are intended to assist in identifying which is the lead supervisory authority when a Controller or Processor is carrying out cross-border processing of personal data.
The Working Party is inviting comments on these documents up to 15 February 2017.

Data protection impact assessments

What is a data protection impact assessment?

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

While not a legal requirement under the DPA, the ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach.

When do I need to conduct a DPIA?

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.
- large scale processing of special categories of data or personal data relation to criminal convictions or offences.
  This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.
- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the Controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.

- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Breach notification

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

What is a personal data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

What breaches need to be notified to the relevant supervisory authority?

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

When do individuals have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

A ‘high risk’ means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What information must a breach notification contain?

- The nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify a breach?

A notifiable breach has to be reported to the relevant supervisory authority **within 72 hours of the organisation becoming aware of it.** The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

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

What should I do to prepare for breach reporting?

You should make sure that your staff understands what constitutes a data breach, and that this is more than a loss of personal data.

You should ensure that you have an internal breach reporting procedure is in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.

In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Transfer of data

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

It is not envisioned that Scheme data administered by Kier would be transferred outside the EU. Any changes to the storage of data will be discussed with each scheme prior to any transfer.

Appendix A

Overview of Key Changes

The General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED) will both apply from 25 May 2018. The Regulation will directly replace many of the provisions of our own data protection legislation (the Data Protection Act 1998 (DPA) in the UK). Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), however there are new elements and enhancements so there is a need to implement some new procedures and do some existing procedures differently. The LED applies directly to those UK bodies processing personal data for law enforcement purposes, which will include the Home Office.

The Data Protection Principles, as set out in the DPA, remain but they have been condensed into six, as opposed to eight, principles. Article 5 of the Regulation states that personal data shall be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Under the GDPR the supervisory authority has a number of new powers (for the UK the supervisory authority for GDPR is the ICO). This includes an increase in the upper limit for fines from up to £500,000 or 1% of annual turnover to an upper limit of 20 million euro or 4% of global annual turnover, whichever is higher (for some infringements and an upper limit of 10 million euro or 2% of global annual turnover for others). In addition an ability to issue warnings, carry out audits, require specific remediation (financial compensation), order erasure of data and suspend data transfers to a third county. Their powers extend to the right to enter premises for the purposes of monitoring compliance. Importantly some of these powers can be applied to Data Processors and Controllers, see table below for further information.

So what does this means in practice? You will need to continue to manage and protect information as you do now, whilst also implementing some new procedures. You need to ensure you are aware of the changes that may affect your business areas outlined in the below table.

The DPA says	The GDPR/ LED says	Suggested Action Plan
Subject access requests must be responded to within 40 calendar days	Respond to SARs electronically and in a commonly used format within one month [the Cross Government view is that this equates to 30 calendar days and (in effect) 20 working days], extendable by a further two months (conditions apply), providing some additional information such as the data retention periods and the right to have inaccurate data corrected.	Update policy/guidance/ procedures. Plan how requests will be handled within new timescales identify how/what additional information must be provided. Continue to manage customer SARS through the Subject Access Request Unit, seeking to respond within new timescales and manage all staff requests through KIMU. Continue to provide data electronically.
Organisations are permitted to charge a reasonable fee for data requests.	Personal data requests will be free. Organisations can charge a reasonable fee or refuse a request if requests become manifestly unfounded or excessive. Fee must be proportionate to the cost of administration.	Update policy/ guidance/ procedures, to include different grounds for refusing to comply with a SAR (manifestly unfounded or excessive requests can be charged for or refused).
Data subjects have a right to be informed: • what data is held on them • the purpose it is being processed for • who it may be shared with	Inform data subjects of the legal basis for processing their data. To include: • who the Data Controller is • how their data will be held • data retention periods • who data will be shared with • how to gain access to it • the right to complain to the ICO if they think data is handled incorrectly	Review and update all privacy and fair processing notices

The DPA says	The GDPR/ LED says	Suggested Action Plan
Data breach reporting is only mandatory if the breach is covered by the Privacy and Electronic Communications Regulations 2011 and is noted as an advisory step for organisations outside of the PECR.	All data breaches where it is likely to result in a risk to the rights and freedoms of individuals must be notified by the Data Controller (Home Office) to the relevant supervisory authority (in most instances the ICO) within 72 hours. Any delay to this timeframe must be communicated to the ICO. If the data breach is likely to result in a high risk to an individuals' rights and freedoms the data subject must also be informed without undue delay (some exceptions apply).	Appoint a DPO with a supporting office to act as a point of contact for the reporting of breaches to the ICO [to be confirmed]. The DPO will be supported by a DPP network who will be the first point of escalation for business areas. Breach reporting instructions to be included within policy and guidance. Determine what constitutes high risk.
Under the current legislation there is no need for any business to have a dedicated DPO	A DPO is mandatory for any business or organisation with more than 250 employees The DPO should report to the highest management level of the Controller or Processor.	HO will recruit a DPO at SCS level with office support function
There is no requirement for an organisation to remove all data they hold on an individual	An individual will have the 'Right to erasure' (with all information being permanently deleted) – which comprises all data including web records and portability (provide the personal data in a structured, commonly used and machine readable form).	Only applies to data obtained by data subject consent; if the majority of data collected by the organisation is not done by customer consent, these obligations will not apply to much of the data the organisation holds.

The DPA says	The GDPR/ LED says	Suggested Action Plan
Privacy Impact Assessments (PIA) are not a legal requirement under DPA but has always been 'championed' by the ICO	Data Protection Impact Assessments (DPIA) will be mandatory and must be carried out when there's a high risk to the individuals freedoms, and in particular should be undertaken prior to commencing processing of personal data on new technologies DPIAs help an organisation to ensure they meet an individual's expectation of privacy.	The DST will be replaced with a DPIA and will be required for all instances of all data processing (not restricted to sharing) where the privacy of an individual or individuals is potentially impacted. Ensure DPIAs considered for all changes, new projects and integral to Change Management
Data collection does not necessarily require an opt-in under the current Data Protection Act	Consent is key. Individuals must actively opt-in whenever data is collected and there must be clear privacy notices. Notices must be concise, transparent, with consent able to be withdrawn at any time	To review all instances where customer consent is the legal basis for processing
Liability for data breaches remains with the Data Controller where they use a third party to act as a Data Processor (under a legally binding contract).	The GDPR places new legal obligation on Data Processors including a requirement to maintain records of personal data and processing activities. Data Processors have significantly more liability in the event of a data breach. Liability can fall to any party unless one can prove that it is not in any way responsible A Controller may seek redress from a Processor. As a Data Controller, GDPR places further obligations on you to ensure your contracts and processes comply with the GDPR.	Identifying existing contracts, working with commercial to review and ensure compliance. Ensure that it is clear regarding the use of data and who the Data Controller/Processor is.

The DPA says	The GDPR/ LED says	Suggested Action Plan
Under the DPA there is no special protection for children's personal data.	Special protection for children's personal data, particularly in the context of commercial internet services (e.g. social networking). If an organisation offers online services to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. At age 16 a child can give their own consent (although this may be lowered to a minimum of 13 in the UK).	Continue to operate our safeguarding procedures. Ensure privacy notices are written in language that children will understand.
Every Data Controller must lodge a formal notification document with the ICO outlining how personal data will be processed by that Controller.	The current system of notification under the DPA will be replaced by a requirement for Data Controllers to keep their own record in relation to all the personal data they process; this must include; details of the purpose of processing; recipients; transfers to third countries; time limits for erasure and a general description of the technical and organisational measures in place to protect personal data.	Establish this document as a result of the data mapping exercise and identify a central resource within the organisation to manage and maintain it.

LED only changes

The DPA Says	The LED says	Suggested Action Plan
No logging requirement under the DPA. This relates to the ability of the Data Controller to maintain an audit of how personal data is being processed, including gathered, accessed, shared, stored and destroyed.	Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged so that this identification can be used to establish the justification for the processing operations. Logs should solely be used for verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.	Identify all the systems processing personal data, analysing existing logging capacity, identifying gaps and mitigating risks. Priority will be given to business critical systems.