Hogan Lovells

The General Data Protection Regulation (GDPR): action plan for pension scheme trustees

July 2017 (revised March 2018) Pension briefing

HIGHLIGHTS

The European General Data Protection Regulation (GDPR) will apply directly in the UK from 25 May 2018, and will make some fundamental changes to the current requirements surrounding data protection. Key areas of change include:

- the information which must be contained in privacy notices (notices stating the use to which an individual's personal data may be put);
- what must be done when seeking individuals' consent to the processing of their data;
- requirements around data subject access requests (when individuals can demand to see the personal data being held about them); and
- accountability and the sanctions for failure to comply.

Complying with GDPR is expected to be obligatory, regardless of the outcome of the UK's Brexit negotiations.

This note explains what trustees should do to prepare for GDPR and sets out practical steps to ensure their scheme is GDPR-ready.

INTRODUCTION

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018. As a Regulation (rather than a European Directive) it will immediately apply throughout the European Union.

The government has indicated that the requirements of GDPR will continue to apply in the UK following Brexit. The Queen's Speech, given on 21 June 2017, announced that a new Data Protection Bill will replace the current Data Protection Act 1998 (DPA98) and will implement the requirements of GDPR. Details of the current requirements under the DPA98 are set out in regulations. The extent to which these requirements will be replicated in secondary legislation under the new Data Protection Bill is not yet known.

WHAT SHOULD TRUSTEES DO NOW?

A pension scheme trustee will usually be a "data controller", responsible for ensuring compliance with data protection legislation, including the new requirements under GDPR.

In preparing for GDPR, trustees should prioritise four key areas:

- updating privacy notices;
- record keeping and accountability;
- dealing with third party processors; and
- preparing for breaches.

A summary of recommended action points for trustees is included at the end of this note, with the key action points highlighted in red.

Trustees may find it helpful to discuss GDPR and cyber-security issues with the sponsoring employer. In many cases, tying in with what the employer is doing, and making use of the employer's IT support, will result in lower overall costs.

Trustees should also ensure that they and their pension team have appropriate training to understand their responsibilities under GDPR, including how they will respond to any data breach (please see below).

What is data?

There are three broad categories of data for the purposes of the GDPR.

- **Personal data**: any information relating to an identifiable natural person. An "identifier" for this purpose includes their name, identification number, location data, online identifier; or other factors (such as genetic or social factors) which are specific to that person's identity. Some personal data is treated as "**special categories**" of data (currently known as "**sensitive personal data**"), with additional requirements applicable to its processing. Examples of special categories of data are:

- data revealing racial or ethnic origin;
- health data; and
- information concerning an individual's sex life or sexual orientation.

- **Anonymous data**: information which is not related to an identifiable person, and which is outside the scope of GDPR.
- **Pseudonymous data**: a new category of data, which does not directly disclose a natural person's identity but which may still identify a person in combination with additional information. Provided this additional information is kept separately and subject to appropriate security measures, the data will be pseudonymous data. Under GDPR, pseudonymous data is still regarded as personal information, and is therefore subject to the data protection guarantees, however the regime applicable to pseudonymous data is less stringent.

PRIVACY NOTICES

Data controllers are currently required to give information to data subjects about the purposes for which their data will be processed. This information is often included in a "privacy notice", given to members at the time of joining their scheme, or making enquiries about joining.

GDPR will increase the amount of information which must be given to data subjects beyond the current requirements, for example:

- the information must include the legal basis for the processing;
- where the processing relies on the individual having given consent, the individual must be told that they may withdraw consent at any time;
- the individual's rights to access his or her data, to have his or her data rectified or erased and to "data portability" (please see below); and
- where the data includes special categories of personal data, the notice must also set out the conditions for processing the special categories which are being relied on.

Where the data is collected from a third party, rather than from the data subject, additional information must be given, including:

- the source of the data and, if applicable, whether it came from publically accessible sources.

Impact on pension schemes?

- Trustees should aim for their updated privacy notices to be wide enough to cover all the different sorts of processing which they might potentially wish to do with their members' personal data.
- Should the trustees wish to process data at a later date for a purpose outside the scope of their privacy notices, then taking steps to pseudonymise the data (please see box above) might enable the processing to be done without updating the privacy notices. However, advice would be needed on the adequacy of the pseudonymisation in the particular circumstances.

Action for trustees

Trustees should either:

- review privacy notices previously given to members (and, where applicable, beneficiaries); and
- where necessary, update and reissue privacy notices to affected members and beneficiaries.

Or, trustees may decide to:

- issue a new GDPR-compliant privacy notice to all relevant members and beneficiaries, without first conducting a review of earlier privacy notices.

The second approach may be preferable where privacy notices may have been changed over the years and where checking what information different tranches of members received could prove more time consuming and costly than issuing a new notice to all members and beneficiaries.

- It would be sensible to issue privacy notices alongside another member communication, such as with the annual funding statement or a member newsletter, where possible.
- The GDPR-compliant privacy notices should also be given to any new members (or beneficiaries) or on obtaining further information from existing members/beneficiaries if the purpose for which the data will be processed is not covered by the previous privacy notice.

RECORD KEEPING AND ACCOUNTABILITY

A welcome change with GDPR is that pension trustees will no longer have to register with the ICO as data controllers. However, controllers will be subject to stringent record keeping requirements in relation to their processing activities and must make their records available to the ICO on request.

In addition, controllers must be able to demonstrate that they are taking their obligations under GDPR seriously. This will be much easier to do for trustees who have properly documented procedures.

As data controllers, trustees must ensure that their records include the following information:

- the name and contact details of the controller (and, where applicable, any joint controller or data protection officer);
- the purposes of the data processing;
- the categories of data subject and of personal data;
- the categories of recipient to whom the personal data has been, or will be, disclosed (including recipients in third countries);
- any transfers of personal data to a third country and, in some cases, the safeguards which apply;
- where possible, the anticipated timescales for deleting the different categories of data; and
- where possible, a description of technical and organisational measures taken to ensure a level of security appropriate to the risk.

Third parties who process data on behalf of the trustees must keep similar records.

There is an exemption from the record keeping requirements for organisations with fewer than 250 employees where the processing meets certain conditions. Unfortunately, the conditions are restrictive (for example, the processing cannot include special categories of personal data) and so the exemption is unlikely to apply to pension scheme trustees.

Impact on pension schemes?

- Trustees and scheme administrators will be subject to the record keeping requirements and should be able to demonstrate that they comply with them.

Action for trustees

- Identify what categories of personal data you currently process and the categories of individuals this data relates to. It is likely you will need to liaise with your administrators when doing this.

- Assess whether your current processes adequately record the information which will be required under GDPR. If not, ensure that any gaps in relation to existing data are filled before next May. Update your procedures and arrange for relevant staff to receive appropriate training in good time.

DEALING WITH THIRD PARTIES

Data processors

The GDPR introduces some fundamental changes to the legal relations between trustees (as data controllers) and many of their service providers (as data processors).

- Data processors will have direct obligations to comply with the requirements of GDPR and will be directly liable to compensate individuals for loss caused by their breach of GDPR's requirements. At present, a processor is liable to its data controllers only under the terms of the contract between them.
- Trustees' contracts with data processors must include various matters set out in the GDPR, including:
  - the subject matter and duration of the processing; its nature and purpose; the type of personal data and categories of data subject;
  - (unless otherwise required by law) the processor must only process personal data on the documented instructions from the controller, including in relation to transfers of data outside the European Union;
  - that the processor will assist the controller in giving effect to individual's rights (including rights to access their own data; the right to be forgotten; and the right to rectification – please see below);
  - an obligation to assist the trustees in complying with the requirements regarding security, breach notification, and undertaking data protection impact assessments (please see below);
  - a requirement that the processor must not sub-contract the processing to a second processor without the trustee's written authorisation; where the trustee gives general authorisation, the processor must notify the trustee if it proposes to add or replace a sub-contractor and must give the trustee opportunity to object to the changes;
  - any sub-contractor must be subject to the same obligations which are imposed on the processor;
  - an obligation to delete or return all personal data to the trustees at the end of the contract; and
  - an obligation to provide information to the trustees to demonstrate compliance and to allow the trustees inspection and audit rights.

Impact on pension schemes?

- From next May, scheme administrators and others who process personal data on behalf of the trustees will be directly liable to members if the member suffers loss from the processor's breach of the GDPR requirements. Processors may seek to limit their exposure through cross-indemnities from the trustees, where a breach occurs because of an act or omission of the trustees.
- Contracts with existing suppliers are likely not to be compliant with the new requirements. This will apply not just to contracts with scheme administrators but also to arrangements with any other provider which processes personal data on the trustees' behalf: including potentially: internet service providers, annuity providers or advisers; independent financial advisers; other advisers on corporate transactions.
- Scheme actuaries may be considered data controllers and so subject to the same requirements as trustees.

Action for trustees

- Ensure that any contracts which you are currently negotiating with third parties are GDPR compliant, to save having to renegotiate them next year.
- Identify which of your current suppliers are processing personal data on your behalf and ask them what they are doing to prepare for GDPR. It is likely that your contracts with suppliers will need to be amended – it may be simpler to do this by a side letter rather than by renegotiating the whole contract. Suppliers may expect to use their own standard side letter. Trustees should seek legal review of side letters or other amendments to existing contracts before agreeing to them.
- It would be sensible for trustees to start with their most significant contract – this is often likely to be their contract with the scheme administrator.
- Liaise with the scheme actuary to understand how they are planning to comply with GDPR.

Transfers outside the European Union

Both the current DPA98 and the GDPR restrict transfers of personal data to destinations outside the European Economic Area (EEA) and provide different options to legitimise such transfers. Under GDPR, the ways of legitimising an international data transfer will be changed and extended. The GDPR will also restrict further transfers of personal data by the recipient of the original transfer.

Impact on pension schemes?

The most likely relevance of this area to pension schemes is if their administrator outsources some or all of its processing functions to a third party (or to its own subsidiary or branch) outside the EEA. In practice, if trustees already comply with the requirements of the DPA98 in relation to transfers outside the EU then they are very likely to meet the requirements of GDPR.

Action for trustees

- Identify whether any personal data processed by the trustees is currently transferred outside the EEA, or is likely to be transferred in future.
- Ensure contracts with scheme administrators and other processors provide that international data transfers (if allowed) must comply with the new requirements of GDPR and will be subject to the trustees' consent.

DEALING WITH DATA BREACHES

The GDPR increases the obligations on data controllers where there is a "personal data breach".

- The controller must notify the ICO of the breach, if possible within 72 hours of becoming aware of it, unless the breach is unlikely to cause risk to individuals' rights and freedoms. Reasons for the delay must be given if the breach is not notified within 72 hours.
- Specified information must be included with the notification to the ICO, including the categories and approximate number of individuals concerned; the likely consequences of the breach; and measures taken (or proposed) to address the breach and to mitigate any possible adverse effects.
- The controller must also notify the individual of the breach, where the breach would be likely to cause a high risk to the individual's rights and freedoms. This requirement does not apply if the controller has subsequently taken steps to ensure that the high risk to the individual is no longer likely. In addition, where giving individual notification would involve disproportionate effort, the information may be given by a public communication or similar means.

In contrast, a data processor simply has to notify the data controller without undue delay after becoming aware of a personal data breach.

Sanctions for non-compliance

Penalties for non-compliance with GDPR may be severe. Breaches of certain provisions, including those relating to basic principles for processing; individuals' rights; or transfers of personal data to a third country, may result in fines of up to:

- 20m Euros; or, if higher,
- 4% of annual worldwide turnover.

In relation to some other breaches, the ICO may impose sanctions of up to 10m Euros or, if higher, up to 2% of an undertaking's total worldwide turnover.

It is not clear what "worldwide turnover" would be taken to mean in relation to a pension scheme. A fine calculated as a percentage of a scheme's assets would be a significant penalty. It is also not clear how a fine would be calculated and paid in relation to a defined contribution (DC) scheme, especially one where the employer was not liable to reimburse all scheme expenses.

In practice, if the ICO decides to sanction pension trustees for non-compliance, it would set the level of the penalty and, if the trustees considered it excessive, they could challenge the amount in the courts.

What is a "personal data breach"?

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Impact on pension schemes?

- Even the best run organisation can suffer security breaches from time to time. Trustees must face up to the real possibility of having to report a breach to the ICO at an unknown future time.
- Trustees will also be responsible for notifying breaches caused by the scheme administrator, or other third party who processes data on the trustees' behalf.

Action for trustees

- Assess the types of data you hold and ensure you can identify which data is personal data and so would fall within the notification duty if there were a breach.
- Consider whether your cyber-security measures are up to scratch and keep them under review. Include a review of the precautions taken by individual trustees (or individual directors of a corporate trustee) (to help you, we have prepared a separate note, "Data security for pension trustees").
- Adopt a data breach policy, including identifying individuals or teams who will take the lead in responding to a breach. This is an area where support from the sponsoring employer (including tying in with the employer's data breach procedures) may be particularly helpful.
- Conduct data breach exercises using sample scenarios to test your breach procedures and to familiarise key individuals with their roles in the event of a breach.
- Ensure that contracts with scheme administrators and other processors require the processor to report a breach to the trustees as soon as they are aware of it, and to assist the trustees with gathering information necessary to comply with the breach notification requirements.

OTHER AREAS TO CONSIDER

CONSENT: NOW MORE DIFFICULT

A common misperception is that personal data may only be processed with the individual's consent. However, there are other lawful grounds for processing, which may be more useful to pension schemes. These include that the processing is necessary:

- for the performance of a contract with the individual;
- to comply with a legal obligation;
- to protect the vital interests of an individual;
- in the public interest; and
- for the purposes of legitimate interests pursued by the controller (or a third party).

Why not use consent?

The GDPR will bring in further requirements for obtaining and relying on "consent", including that:

- the controller or processor must be able to demonstrate that the individual has given consent;
- a request for consent must be given in plain language and must be clearly distinguishable from other material; and
- the individual must be able to withdraw consent at any time, as easily as he or she could give consent.

These requirements, in particular that the individual must be able to withdraw consent at any time, will be impractical for many pension schemes to comply with. Trustees need to process individuals' data in order to administer their scheme correctly, and so can rely on the "legitimate interests" ground to justify their processing.

Is consent ever needed?

Additional requirements apply in relation to special categories of personal data, including:

- data revealing racial or ethnic origin;
- health data; and
- information concerning an individual's sex life or sexual orientation.

Trustees commonly process special category data when considering eligibility for ill health benefits or when deciding to whom to pay discretionary death benefits.

Processing of special category data is allowed only in specified circumstances, including:

- where the individual has given explicit consent; or
- where the processing is necessary for carrying out the trustees' obligations in relation to employment or "social protection" and is authorised under UK law.

The Data Protection Bill, currently before Parliament, will authorise processing of special category data in various circumstances, expected to be wide enough to include the provision of ill health benefits or death benefits from pension schemes.

Impact on pension schemes?

- Many trustees already do not rely on consent to legitimise their processing of personal data. Where trustees do currently use the consent justification, this will no longer be practical for most of their scheme's data processing.
- Before the Data Protection Bill is enacted, trustees will need to rely on consent for processing special category data.
- After the Bill comes into force (and assuming that the authorisation provisions are unchanged), trustees who process special category data may rely on the "authorised obligation" exemption described above.
- However, when deciding the appropriate legal basis for processing special category data, trustees should review their own approach and their attitude to risk, in consultation with their legal advisers.

Action for trustees

- Remove requests for consent from forms (such as new joiner forms) where the trustees may rely on the legitimate interests grounds for processing personal data.
- Review ill health early retirement application forms to ensure that the consent provisions are robust enough to meet the stricter requirements of GDPR. Ill health cases being handled now may still require processing after 25 May 2018, especially if decisions are subsequently appealed, so it is worth updating application forms well in advance of next May.
- When the Data Protection Bill is enacted, consider whether consent remains the most appropriate legal basis for the trustees' processing of special category data.

SUBJECT ACCESS REQUESTS

The DPA already gives individuals the right to access their personal data held by a data controller, by making a "subject access request". The GDPR gives individuals a similar right, although there are changes to some of the detailed requirements, including the following.

- The information must be provided within one month, rather than the current 40 days allowed under the DPA98. There is potential to extend this period by a further two months, but only in limited circumstances.
- The individual must be told the period for which his or her data will be stored or, if this is not possible, the criteria for deciding the storage period.
- The information must be provided free of charge (although requests which are manifestly unfounded or excessive may be refused or a charge levied).
- Individuals must be told about their rights to have their data corrected, deleted or to restrict the processing of their data.

Impact on pension schemes?

- Trustees will need to comply with the additional requirements concerning data subject access requests. In our experience, members can use the route of making

a subject access request when a complaint they have made against the trustee has failed.

Action for trustees

- Review and update procedures for dealing with data subject access request.

RIGHT TO BE FORGOTTEN

An individual may require a data controller to delete his or her personal data in various circumstances, including where:

- the data is no longer necessary for the purposes for which it was held; or
- the individual withdraws his or her consent and there is no other legal ground to make the processing lawful.

The controller does not need to delete the data if an exception applies, including that the processing is needed to comply with a legal obligation.

Impact on pension schemes?

- The right to erasure helps to demonstrate why pension schemes should rely on grounds for processing other than consent as much as possible. Clearly, trustees could not run their scheme and pay benefits to beneficiaries when due if members could demand that the trustees delete their data.
- In practice, requests for erasure of personal data may be rare in a pension context, as most individuals will want trustees to continue to hold data necessary for their benefits to be paid. It is more likely that individuals will request their data be removed where it includes confidential medical information, or information about family relationships used when deciding how to pay a discretionary death benefit.

Action for trustees

- Review the various sorts of processing carried out by the trustees and identify legal grounds other than consent, as far as possible.
- Be prepared to erase (or to require the scheme administrator or other third party to erase) a member's personal data in response to a request, where an exception does not apply.

RIGHT TO RECTIFICATION

The GDPR gives individuals the right to have incorrect personal data corrected without undue delay.

Impact on pension schemes?

- Likely to have little or no additional impact on schemes. Trustees and administrators will want to ensure their data is as correct and complete as possible, so should welcome any rectifications provided by members or beneficiaries.

Action for trustees

- Nothing specific: trustees and administrators should already correct errors in data which they become aware of.
- Trustees should nevertheless be aware of the requirement and should seek advice if a rectification request is ever received.

DATA PORTABILITY

In addition to the right of subject access (please see above), in some circumstances individuals will have a new "data portability" right: that is, a right to access their data in machine-readable format and, where technically feasible, to have the data transmitted directly from one data controller to another.

The right will only apply to data which has been provided to the controller by the individual and where the processing of the data is automated and is either:

- based on the individual's consent; or
- necessary for the performance of a contract to which the individual is a party.

Guidance from the Article 29 Working Group (WP29)[1] explains that the data covered by the portability requirement includes data provided by the individual and data assembled by observing the individual's actions but not any profiling or analysis carried out on the basis of that data or observations. It also makes clear that the transferring data controller is not responsible for processing handled by the individual or by another company which processes data following a data portability request.

Impact on pension schemes?

It is not immediately clear how the data portability right will impact on pension schemes. Because of the restrictions on when it applies, it may be of limited relevance.

Action for trustees

- Be aware of the data portability requirement and be prepared to respond to portability requests from May 2018 should any arise.

DATA PROTECTION IMPACT ASSESSMENTS

Data controllers will have to carry out a data protection impact assessment (DPIA), also known as a "privacy impact assessment" before carrying out processing which involves high risk for members (or beneficiaries). In particular, a DPIA will be required where:

- there will be a systematic and extensive evaluation of individuals, on which decisions will be based which will have a significant effect on the individuals;
- large scale processing of special categories of personal data; or
- systematic monitoring of publically accessible information.

The WP29 has produced guidelines on determining whether a processing activity is "high risk". In addition, the ICO must issue a list of the kind of processing which is subject to the DPIA requirement and may publish a list of activities which are outside the requirement.

---

[1] Article 29 Working Party 29 (WP29): an independent advisory group made up of representatives from data protection authorities from each EU member state.

The requirement applies to new processing but the WP29 strongly recommends carrying out a DPIA in relation to existing processing falling within the remit of the requirement within three years of May 2018. In addition, a significant change to a processing operation after May 2018, for example because new technology has come into use or because personal data is being used for a different purpose, would count as new processing and could require a DPIA.

The GDPR and the WP29 guidelines set out what must be covered in a DPIA, including a description of the proposed processing operations and the purposes of the processing; and an assessment of the risks to individuals and the measures proposed to address these risks.

Impact on pension schemes?

Activities which may be caught by the requirement to have a DPIA could include sharing member information with a new administrator or undergoing a medical underwriting process as part of a buy-in or buy-out negotiation. Processing of an individual's sensitive data in relation to an application for ill health early retirement would be unlikely to be caught by the requirement, as it would not be conducted on a large scale.

It would be helpful for the ICO's list of activities which are caught by the DPIA requirement to include a section on pensions. Hogan Lovells is actively engaged with the pension industry in liaising with the ICO on the impact on pension schemes.

Action for trustees

- No immediate action needed, but be aware of the requirement and the sorts of processing which may fall within it.
- Await publication of the ICO's list of "high risk" processing activities.

DATA PROTECTION OFFICERS

When is a data protection officer required?

The GDPR introduces a requirement for data controllers and data processors to appoint a data protection officer (DPO) in circumstances where:

- the processing is carried out by a public body (the WP29 guidelines consider that this could also include private bodies operating in sectors such as public transport or energy supply);
- the controller or processor monitors individuals systematically and on a large scale as a core activity; or
- the controller or processor's core activities consist of large scale processing of special categories of personal data.

The DPO's role

- The DPO's tasks must include: informing and advising the controller / processor about requirements of GDPR and any national provisions; monitoring compliance with these requirements; and cooperating with the ICO.
- However, responsibility for compliance with GDPR rests with the controller or processor, not with the DPO.
- A group of undertakings may designate a single DPO, provided that he or she is "easily accessible from each establishment".

Voluntary appointment

A controller or processor may choose to appoint a DPO where it is not required to do so (or where it is not clear whether it must appoint a DPO). It seems that a voluntarily appointed DPO will have the same status under the GDPR as any other DPO. Organisations should therefore take care with job titles and descriptions, to make sure that they do not inadvertently appoint a DPO where this is not intended.

Impact on pension schemes?

- This is an area in which additional guidance from the ICO would be really useful. Pension schemes process large amounts of data which could be sensitive (for example, details of spouses or partners, which can indicate sexual orientation). It is not clear though whether this would count as a "core activity". Scheme administrators, as data processors, may be more likely to fall within the DPO requirements than trustees, especially if the administrators process data for several schemes.
- It would also be helpful to have the ICO's views on whether trustees could share a DPO with the sponsoring employer.

Action for trustees

- Consider (with advice if necessary) whether the DPO requirements apply. Given current uncertainty, you may decide to wait for any further guidance before doing this.
- Document any analysis undertaken to determine that the DPO obligation does not apply (unless it is obvious that you fall outside the requirements).
- If you decide that you must (or wish to) appoint a DPO, recruit a suitable person.

SUMMARY OF ACTION POINTS

Red: start taking action now

General

- Discuss GDPR and cyber-security issues with the sponsoring employer. In many cases, linking with what the employer is doing, and making use of the employer's IT support, will result in lower overall costs.
- Arrange training for trustees and their pension team on GDPR and cyber security.

Privacy notices

Either:

- review privacy notices previously given to members (and, where applicable, beneficiaries); and
- where necessary, update and reissue privacy notices to affected members and beneficiaries.

Or (which will be more practical for many trustees):

- issue a new GDPR-compliant privacy notice to all relevant members and beneficiaries, without first conducting a review of earlier privacy notices.

Record keeping, procedures and accountability

- Identify what categories of personal data you currently process and the categories of individuals this data relates to. It is likely you will need to liaise with your administrators when doing this.
- Identify legal grounds for the processing you do (or which is carried out on your behalf). Where possible, identify a ground other than consent.
- Remove requests for consent from forms (such as new joiner forms) where the trustees may rely on the legitimate interests grounds for processing personal data.
- Assess whether your current processes adequately record the information which will be required under GDPR. If not, ensure that any gaps in relation to existing data are filled before next May. Update your procedures and arrange for relevant staff to receive appropriate training in good time.

Dealing with third parties

- Identify which of your current suppliers are processing personal data on your behalf and ask them what they are doing to prepare for GDPR. It is likely that your contracts with suppliers will need to be amended – it may be simpler to do this by a side letter rather than by renegotiating the whole contract. Suppliers may expect to use their own standard side letter. Trustees should seek legal review of side letters or other amendments to existing contracts before agreeing to them.
- Ensure that contracts with scheme administrators and other processors provide that international data transfers (if allowed) must comply with the new requirements of GDPR and will be subject to the trustees' consent.
- Ensure that contracts with scheme administrators and other processors require the processor to report a breach to the trustees as soon as they are aware of it, and to assist the trustees with gathering information necessary to comply with the breach notification requirements.
- It would be sensible for trustees to start by reviewing their most significant contract – this is often likely to be their contract with the scheme administrator.
- Ensure that any contracts which you are currently negotiating with third parties are GDPR compliant, to save having to renegotiate them next year.
- You and your data processors may want to revisit the indemnity provisions and liability caps in your contracts.

Preparing for data breaches

- Assess the types of data you hold and ensure you can identify which data is personal data and so would fall within the notification duty if there were a breach.
- Consider whether your cyber-security measures are up to scratch and keep them under review. Include a review of the precautions taken by individual trustees (or individual directors of a corporate trustee). More detailed recommendations are included in our note "Data security for pension trustees".
- Adopt a data breach policy, including identifying individuals or teams who will take the lead in responding to a breach. This is an area where support from the sponsoring employer (including tying in with the employer's data breach procedures) may be particularly helpful.
- Conduct data breach exercises using sample scenarios to test your breach procedures and to familiarise key individuals with their roles in the event of a breach.
- Ensure your contracts with third party processors include adequate provisions for dealing with breaches (please see Dealing with third parties above).

Amber: consider over the next six to 12 months

Consent

- Review ill health early retirement application forms to ensure that the consent provisions are robust enough to meet the stricter requirements of GDPR. Ill health cases being handled now may still require processing after 25 May 2018, especially if decisions are subsequently appealed, so it is worth updating application forms well in advance of next May.
- When the Data Protection Bill is enacted, consider whether consent remains the most appropriate legal basis for the trustees' processing of special category data.

Subject access requests

- Review and update procedures for dealing with data subject access requests.

Data protection officers (DPO)

- Consider (with advice if necessary) whether the DPO requirements apply. Given current uncertainty, you may decide to wait for any further guidance before doing this.
- Document any analysis undertaken to determine that the DPO obligation does not apply (unless it is obvious that you fall outside the requirements).

- If you decide that you must (or wish to) appoint a DPO, recruit a suitable person.

Green: points to bear in mind and possibly take action on in future

Right to be forgotten

- Be prepared to erase (or to require the scheme administrator or other third party to erase) a member's personal data in response to a request, where an exception does not apply.

Right to rectification

- Be aware of the right to rectification and seek advice if a rectification request is ever received.

Data portability

- Be aware of the data portability requirement and be prepared to respond to portability requests from May 2018 should any arise.

Data protection impact assessments

- Be aware of the requirement to undertake a data protection impact assessment and the sorts of processing which may fall within it.
- Await publication of the ICO's list of "high risk" processing activities.

This note is written as a general guide only. It should not be relied upon as a substitute for specific legal advice.

KEY HOGAN LOVELLS PARTNERS		
Katie Banks	**+44 20 7296 2545**	**katie.banks@hoganlovells.com**
Duncan Buchanan	**+44 20 7296 2323**	**duncan.buchanan@hoganlovells.com**
Claire Southern	**+44 20 7296 5316**	**claire.southern@hoganlovells.com**
Edward Brown	**+44 20 7296 5995**	**edward.brown@hoganlovells.com**
Faye Jarvis	**+44 20 7296 5211**	**faye.jarvis@hoganlovells.com**

About Pensions360

Hogan Lovells' broad cross-practice capability covers the full spectrum of legal advice from lawyers who understand pension clients; advising on issues from scheme investments, corporate restructurings and transactions, to funding solutions and interaction with the Regulator or the courts. The ability to draw on specialists from other practices who are not only experts in their field but have an in-depth understanding of pension issues sets us apart from our competitors.

www.hoganlovells.com