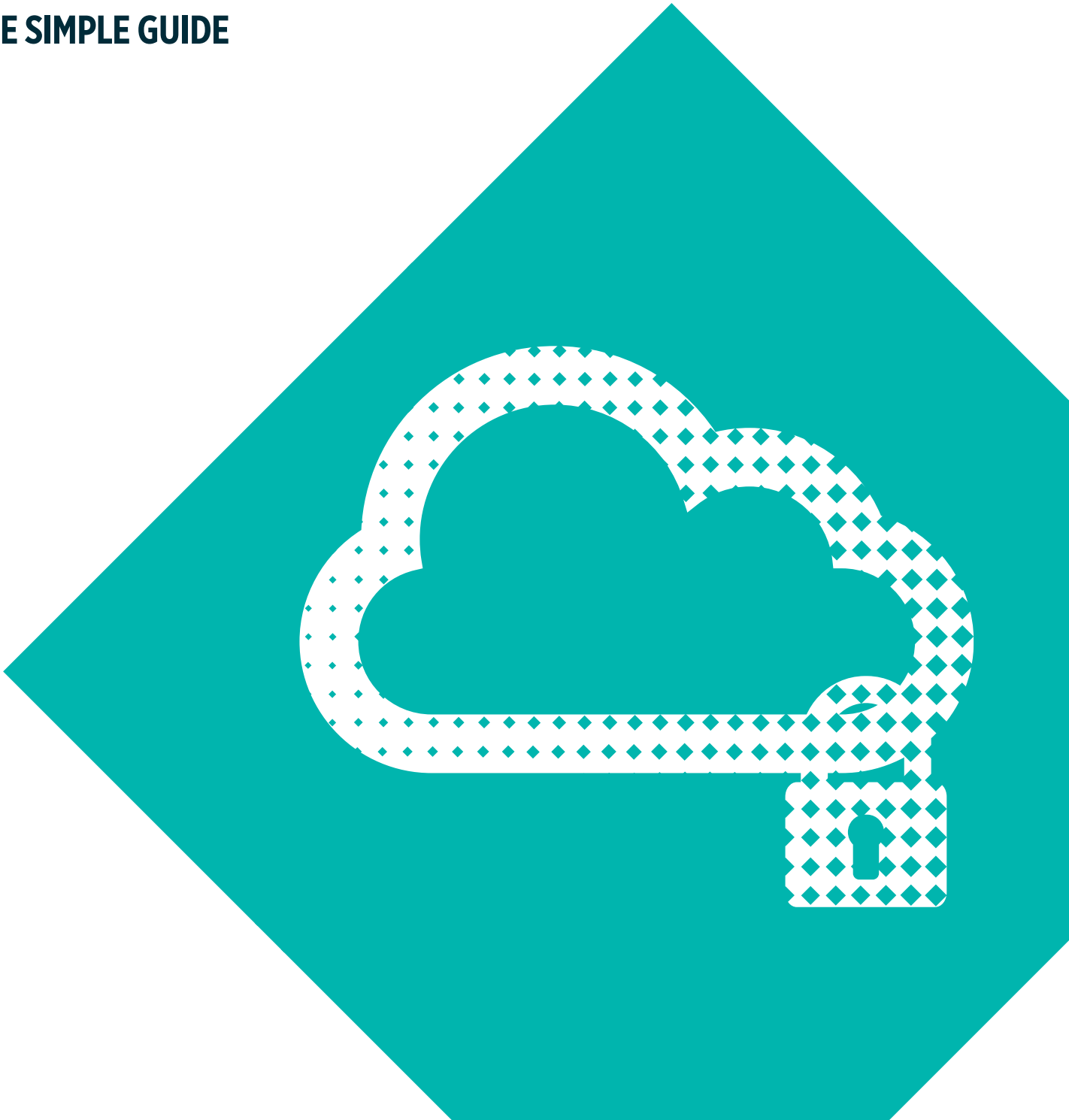
PENSIONS AND
LIFETIME SAVINGS
ASSOCIATION

September 2017

GENERAL DATA PROTECTION REGULATION (GDPR)

MADE SIMPLE GUIDE



ACKNOWLEDGEMENTS

We would like to thank Herbert Smith Freehills LLP for its help producing and sponsoring this guide.

HERBERT SMITH FREEHILLS

This guide is for information only.
It is not investment or legal advice.

Published by the Pensions and Lifetime Savings Association 2017

CONTENTS

FOREWORD

DATA PROTECTION IS SET TO BECOME BIG NEWS FOR PENSION SCHEMES. ON 25 MAY 2018 THE EU'S GENERAL DATA PROTECTION REGULATION (OR GDPR FOR SHORT) TAKES EFFECT IN THE UK, AUTOMATICALLY AND WITHOUT ANY ACTION BEING NEEDED ON THE PART OF UK GOVERNMENT.

It will, at a stroke, completely change the landscape within which substantial processors of data – of which pension schemes are a prime example – operate. The GDPR heralds a complete sea change to the way in which anyone processing data needs to think about conducting their activities, and a significant ratcheting-up of the underlying legal regime that governs what they do.

The GDPR will be supplemented by a substantial piece of new domestic legislation, the Data Protection Act 2018, which was introduced into Parliament as the Data Protection Bill on 13 September 2017. While it sets out some important features of the new regime, and contains additional detail that the GDPR doesn't, the Bill – which will become an Act once finalised – explicitly recognises that until our withdrawal from the EU, it will be the GDPR itself which lays down the requirements of the new regime. Accordingly, it is on this latter piece of supra-national legislation that we focus in this guide.

One of the main headlines accompanying much of the discussion about the GDPR is the vastly heightened sanctions that can be levied by regulators for a breach – up to €20m, or 4% of global annual (group) turnover if greater. This, combined with the absence of any 'phasing in' of its requirements, means that there are many steps that schemes can and should be taking now to ensure that their policies, procedures and documentation are fully GDPR-compliant by the time that 25 May 2018 comes around.

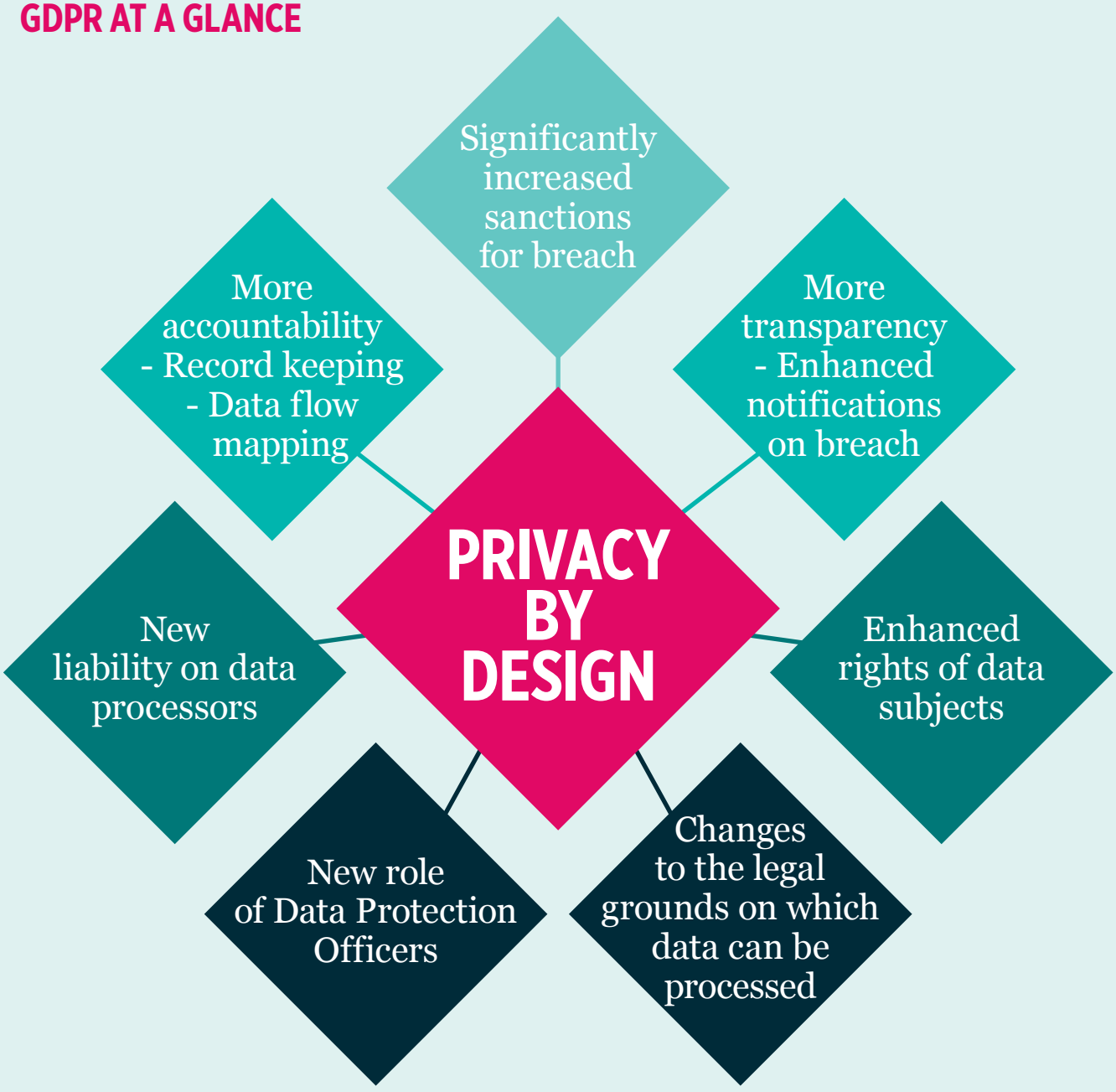
Putting in place the building blocks to ensure compliance with the GDPR undoubtedly requires input from professional advisers. Here at Herbert Smith Freehills we have a team of experts, drawn from our technology/media, pensions and employment divisions, who are assisting both longstanding and new clients with the not-insignificant task of getting 'GDPR-ready' by May next year. To the extent that we are able to help in any way, do please get in touch.

I would just like to conclude by thanking the team of people within Herbert Smith Freehills whose hard work has made the production of this guide possible. They are too numerous to name individually, but from within the pensions team the project has been spearheaded by Kris Weber, Charlotte Cartwright and Beth Casinelli, and they each deserve a special mention.

ALISON BROWN
Global Head of Employment, Pensions and Incentives
Herbert Smith Freehills LLP
18 September 2017

THE GDPR HERALDS A COMPLETE SEA CHANGE TO THE WAY ANYONE PROCESSING DATA NEEDS TO THINK

GDPR AT A GLANCE



1 INTRODUCTION

DATA, DATA, EVERYWHERE...

DATA ABOUNDS IN OUR TECHNOLOGY-DRIVEN LIVES, AND IMPACTS UPON ALMOST EVERY FACET OF THEM. WE NOW LIVE IN A WORLD IN WHICH DATA, AND ITS PROCESSING, HAS BECOME KEY TO THE PROPER FUNCTIONING OF OUR EVERYDAY LIFESTYLES.

Data is, of course, the bedrock of a pension scheme. It is a trustee's most fundamental duty to ensure that the right *benefits* are paid to the right *people* at the right *time*. But without data, this would be impossible. The length of a member's service for the purposes of calculating their 'formula pension' in a DB scheme; the returns achieved on a particular DC investment; the age at which a member is entitled, or permitted, to access their benefits. All simple, easily-understood concepts, and all 'data' – something upon which a pension scheme will be completely dependent for its very efficacy.

A natural corollary of the importance of data is that adequate systems should be in place to safeguard it. Those who own such data, or to whom it relates, expect nothing less. And it probably goes without saying that the use of such data – when, say, calculating a member's benefits – clearly involves that data being 'processed'.

But the concept of processing goes much wider than that. Receiving data, destroying data, even merely storing data, all constitute 'processing' for the purposes of the law. So too does passing it to a third party – e.g. for administration purposes, to undertake benefit calculations or a CETV, to obtain insurance, or to secure members' benefits via a buy-in or buy-out.

In short, where there is activity by a pension scheme, there is the processing of data. Even inactivity is likely to count. Just as data itself cannot be avoided, neither can the fact it is being processed all of the time by pension schemes – and nor can the need for its protection.

LET'S GET BACK TO BASICS

For those unfamiliar with this subject, its terminology can be confusing at best. In order to understand the issues that pension schemes face (and to get the most out of this guide) it is therefore first necessary to explain a little about some of these concepts, as a foundation for what follows.

Data and **personal data:** Not as obvious as they might sound!

- **"Data"** under the current (1998) Data Protection Act is any information relating to a living individual which is held electronically. Anything held manually will also constitute "data" if contained within a "relevant filing system" – a system structured by reference to individuals, and from which specific information relating to a particular individual can be readily ascertained. Data can therefore relate not just to a scheme member but also to nominated beneficiaries – it will include, for example, information about them contained on a member's 'expression of wishes' form.
- **"Personal data"** is then any data from which the living individual to whom it relates can be identified.
- The GDPR's requirements, and those of the new Data Protection Bill, all relate to what constitutes "personal data" under the current Act. For ease of reference, however, throughout this guide we simply refer to 'data'.

Data subject: The identifiable living individual who is the subject of the (personal) data.

Sensitive personal data: Any personal data that is 'sensitive' and defined as such in the GDPR. Pension schemes will find, for the purposes of the GDPR, that data revealing someone's racial or ethnic origin, their physical or mental health, and their sexual orientation, will constitute the most pertinent forms of "sensitive personal data".

Processing: Basically any activity involved with the collation, storage, dissemination, amendment or destruction of data. The concept of 'data processing' also requires that it is held safely and securely – a concept that is often referred to by its own term of art, 'cyber security'.

Data controller: The person who determines how, and for what purposes, data is to be processed. Under the law as it currently stands, all obligations regarding the proper processing of data fall upon the data controller – even if he or she doesn't actually do the physical processing. (Under the GDPR, however, this will change!) In the pensions context, it is generally the trustees who will be the data controller.

Data processor: The person who actually processes the data. This can be the data controller, or a third party doing so on the data controller's behalf. Under the GDPR, data

DATA IS, OF COURSE, THE BEDROCK OF A PENSION SCHEME

processors will for the first time become liable for breaches and open to fines to the same extent as data controllers – a salutary thought.

ICO: The Information Commissioner's Office, being the regulatory body tasked in the UK with enforcing implementation of (and compliance with) the GDPR. The fine detail of the ICO will be set out in the new Data Protection Act (rather than the GDPR itself) and the first draft of the Bill, which will become that Act, illustrates the extent of its likely powers to require the provision of information; issue 'enforcement notices' to compel breaches to be remedied; enter premises and inspect documents; and impose fines of a much greater magnitude than are currently permitted under the Data Protection Act 1998.

WP29: The pan-European regulatory working party, established under Article 29 of the original 1995 Data Protection Directive and made up of a representative from each Member State's regulatory body (as well as from the European Data Protection Supervisor and from the European Commission), that is tasked with promoting the consistent application of data protection legislation across the EU. Once the GDPR is in force, WP29 will be replaced by the European Data Protection Board.

"IF IT AIN'T BROKE...?"

Data protection in the UK – whether by pension trustees or others – is currently regulated by the provisions of the Data Protection Act 1998. This in turn implements the requirements of the 1995 EU Data Protection Directive. The 1998 Act sets down eight over-arching principles, requiring that data processing be fair, carried out for lawful purposes, secure, and that it respects individual rights; and stipulating that the personal data itself must be adequate and relevant, accurate, not kept for longer than is necessary, and not transferred outside the EEA without adequate safeguards in place.

But therein lies a problem. The world is a very different place to what it was 20 years ago. Technological advancement has rendered the systems and processes of the late 1990s – as well as the machinery used to implement them – obsolete. Yet the processing of data is still regulated via a framework of rules developed 'way back then'. The law needs to play catch-up, and quickly.

Enter the GDPR, stage left. Reportedly the most heavily-lobbied piece of European legislation ever, the General Data Protection Regulation applies with effect from **25 May 2018** and will bring about a sea change in the way that data processing is regulated (and the way in which that underlying data is processed) across the entirety of the EU. Which, given the likely timings of Brexit (and, irrespective of timing, our need to remain a competitive international financial player), includes the UK.

Consistency across the EU is one of the main aims of the GDPR. Because it takes the form of a Regulation it will have direct effect in all Member States – unlike Directives, which generally need a domestic Act to implement them, an EU Regulation does not. The GDPR will therefore apply automatically in the UK, as from 25 May 2018, even without the introduction of the proposed new Data Protection Act.

There will be very little scope to deviate from the requirements that the GDPR lays down, particularly given the UK's stated desire to ensure – via an 'adequacy plus' model – that our data protection regime remains aligned with that of the EU, notwithstanding our 'third country' status,

THE GDPR BRINGS WITH IT THE CONCEPT OF DATA PROTECTION BY DESIGN

post-Brexit. However, there will continue to be discretion for each regulatory authority (the ICO, in the case of the UK) in how they apply the requirements – in particular in the amount and frequency of sanctions that they impose. At the time of writing the ICO had recently taken steps to reassure people that it will use its powers to issue significant fines "proportionately and judiciously".

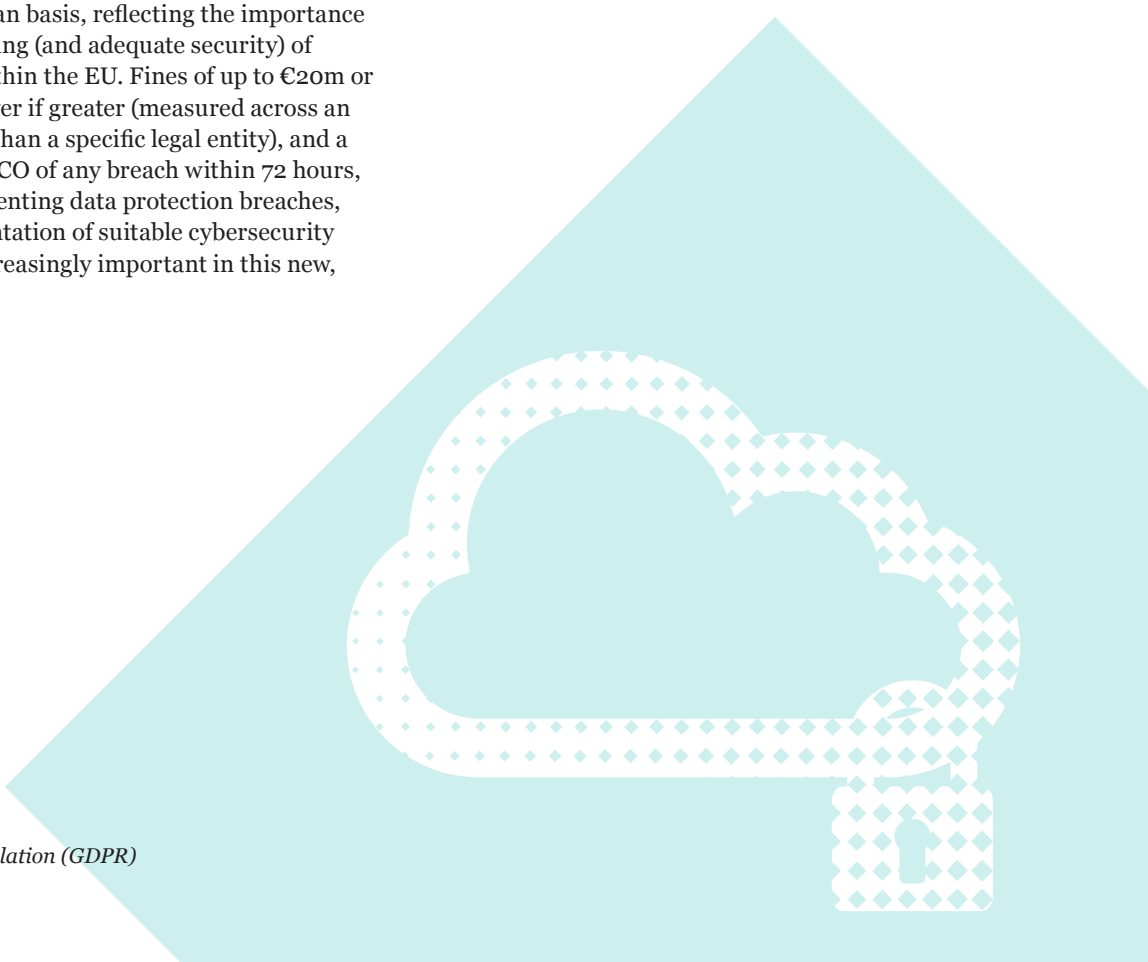
Further differences between the regimes of EU Member States can also be expected. Germany, for example, already intends that unauthorised disclosure of personal data will become a criminal offence under new federal laws due to take effect on the same day as the GDPR itself – this goes beyond the requirements of the GDPR. On the other hand, the GDPR itself contains scope (and in certain instances a requirement) to "derogate" from its terms via bespoke national legislation. One function of the new Data Protection Act will be to set out such derogations from the 'raw' GDPR.

The sanctions themselves will also be considerably more stringent on a pan-European basis, reflecting the importance with which proper processing (and adequate security) of personal data is viewed within the EU. Fines of up to €20m or 4% of global annual turnover if greater (measured across an entire undertaking rather than a specific legal entity), and a requirement to notify the ICO of any breach within 72 hours, speak for themselves. Preventing data protection breaches, including via the implementation of suitable cybersecurity measures, will become increasingly important in this new, post-GDPR world.

LET ME DEMONSTRATE

The GDPR brings with it the concept of data protection "by design" – another theme that goes to its very core. This goes hand in hand with its focus on "accountability". No longer can those who process data simply take a reactive approach to compliance, as has long been the trend under the 1998 Act. GDPR requires the design and implementation of systems on a proactive basis, to ensure that any processing activities can only be carried out in accordance with its requirements and are backed up by good record-keeping. And that those who process data are able to demonstrate – at any time after 25 May 2018 – that such systems and records are both in place and being followed.

This, in turn, means a lot of work for any entity involved in the processing of personal data to become 'GDPR-ready' by 25 May 2018. There will be no transitional or soft lead-in period. And pension schemes (and their trustees) are no exception – as we shall now see...



2 WHAT TRUSTEES NEED TO DO

1 MAP YOUR DATA FLOWS AND IDENTIFY ASSOCIATED RISKS

WHAT THE GDPR REQUIRES

Data protection "by design" and "by default" – in other words, proactive steps being taken to design and implement systems and processes which ensure that, as a default and from the outset, appropriate standards are maintained when processing personal data.

KEY CONSIDERATIONS

What data is being collected?
Why?
How is it being obtained?
When is it being processed?
Who is it being shared with?
Is the processing **proportionate** and **necessary?**
Is the data **secure?**
Which of these steps give rise to particular risks or concerns?

WHAT YOU NEED TO DO

Trustees need to fully understand what data-processing activities are being carried out and maintain records of them, and of how they comply with the GDPR. Initially this will require a thorough investigative process of data mapping, to identify data flows and the processes being applied to such data. Only by doing this will trustees be able to see what activities need to comply with the GDPR; understand which ones aren't complying; design systems which, by default, protect the data that is being processed; and, ultimately, demonstrate compliance with the GDPR.

As part of this exercise, you should document absolutely everything that you do. Consider every eventuality. Carry out further assessment of any risks identified, and adopt procedures to minimise them. If the assessment indicates a heightened risk to the "rights and freedoms" of individual data subjects, or if new methods of data processing are introduced, you will need to carry out a formal "Data Protection Impact Assessment". If, by contrast, it comes to light that non-essential data is being collected or processed – stop doing so!

This will be a substantial exercise. Many schemes may not be fully compliant with even the existing (i.e. 1998) Data Protection Act. Look at your current policies and procedures. Areas for improvement, prior to the GDPR applying as from 25 May 2018, will certainly come to light. Make these changes. Assess the knock-on impact on other policies and procedures. Make further changes if necessary. Once the exercise is complete, document everything. Your ultimate goal is to have in place systems which not only simply comply with the GDPR, but which demonstrably do so.

2 DETERMINE ON WHAT GROUNDS YOU WILL BE PROCESSING DATA

WHAT THE GDPR REQUIRES

Data processing will only be lawful if conducted on a recognised 'ground', of which the following are most relevant to pension trustees:

- Conducted with the consent of the data subject
- Necessary for the performance of a contract to which the data subject is a party
- Necessary for compliance with a legal obligation to which the data controller is subject
- Necessary for the purposes of the legitimate interests pursued by the controller

The GDPR also requires that the basis on which data is to be processed is made clear to the data subject (i.e. scheme member) "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".

KEY CONSIDERATIONS

The fundamental consideration here is the **basis on which processing will be carried out** (see box). In particular, "consent" (whether express or implied) will no longer be the panacea it once was; and particular thought will need to be given as to the treatment afforded to "sensitive personal data" whenever it is processed.

WHAT YOU NEED TO DO

Trustees will need to consider the output from their data mapping exercise (see section 1, above) and assess the basis (or bases) on which those processing activities are to be carried out under the GDPR – and both justify that basis (i.e. document the rationale for the basis, having taken advice if necessary) and record their thinking. It may not be a straightforward exercise, and input from professional advisers is likely to be appropriate. Member communications and other standard-form scheme documents will then need updating (see section 4, below).

In addition, members will need to be explicitly informed – prior to 25 May 2018 – of the basis on which their data will henceforth be processed. If the decision is that 'consent' continues to be the processing ground, fresh consents must be obtained from members to the extent that existing ones are not GDPR-compliant. In any event the communication to members should also be framed to comply with the other requirements laid down by the GDPR for privacy or 'fair processing' notices (see also section 4, below).

THE CONSENT CONUNDRUM – GROUNDS FOR THE LAWFUL PROCESSING OF DATA UNDER THE GDPR

Background

Under the current (1998 Act) regime little consideration was ever really given to the grounds upon which data was processed by pension schemes. While often sought, consent was generally obtained in circumstances where, in reality, refusal would have been unlikely. And when not sought, 'implied consent' would most likely have been put forward by trustees as the processing ground, if anyone ever asked – the argument being that the giving-over of data, and subsequent failure to object to its processing, constituted the implicit consent of the member concerned.

Position under the GDPR – consent

The GDPR will herald significant changes in this respect. Consent must be given by a "clear affirmative act" which establishes a "freely-given, specific, informed and unambiguous" indication of agreement. Silence, pre-ticked boxes and inactivity can each no longer constitute "consent".

CONSENT WILL NO LONGER BE THE PANACEA IT ONCE WAS

The GDPR goes on to make it clear that consent cannot be regarded as freely given if the data subject has no genuine or free choice, or is unable to refuse or withdraw consent without detriment. It also asserts that consent cannot have been freely given if there was a clear imbalance in the relationship between data controller and data subject. Consent is also regarded as not having been freely given if there are a number of different data-processing activities and the data subject was not afforded the opportunity to give (or withhold) that consent separately in respect of each one.

Guidance published by the ICO (but still in draft at the time of writing) reinforces this. Its clear message is that seeking consent, if processing would still be undertaken on a different ground were consent either not given or later withdrawn, is "misleading and inherently unfair". It even suggests that data will not be processed lawfully if the 'consent' that has been obtained is illusory (even if another lawful ground for processing that data does actually exist), and that 'fudging' things in this way leaves data controllers at risk of substantial fines (see section 5, below).

Additional complications also exist in cases of consent as a ground for processing data by pension trustees, in that it gives members both the right to withdraw consent (the existence of which must be notified to them) and the so-called right to erasure (or "right to be forgotten"), by which a data subject can insist that his data is permanently expunged from the records of the data controller. Insistence upon either of these by a member would make administration of the scheme or any particular benefit under it extremely difficult, if not impossible.

The inevitable conclusion, given these issues and the requirement under the GDPR to explicitly notify members of the basis upon which data is being processed, is that trustees should:

- avoid using consent as the ground for processing data wherever possible; and
- pin their colours to the mast, as to what ground they are actually using, as early as practicable.

Position under the GDPR – other lawful processing grounds

This in turn necessitates the use of another lawful ground for processing member data. "Necessary for compliance with a legal obligation" would appear pertinent for the day-to-day operation of a pension scheme. So too would "legitimate interests", although different views exist as to its suitability. And "consent" may continue to have its place in limited circumstances, for example when undertaking specific projects such as liability management exercises. But ultimately the position remains as unclear as it is unsatisfactory, and definitive guidance from the ICO is essential.

Sensitive personal data

Further complications may also arise in the case of "sensitive personal data". For pension scheme purposes this will essentially comprise data revealing a member's racial or ethnic origin, physical or mental health, or his/her sexual orientation. The grounds under the GDPR itself on which it can legitimately be processed, where the data subject (scheme member) has not given explicit consent, are extremely limited. Equally, it is difficult to see how any explicit consent could in fact be genuine, in relation to a matter where the data subject effectively had no choice but to give it.

However, the Data Protection Bill (in the form in which it was introduced into Parliament during September 2017) does contain provisions which seem to provide a specific derogation, to permit the processing of "sensitive personal data" by pension schemes without member consent provided certain additional safeguards are met.

Derogations are matters in respect of which Member States may (or in certain cases must) set down their own flexibilities or restrictions regarding a particular matter, and "sensitive personal data" is one such area. The 'additional safeguard' here is that the scheme's trustees have in place a documented, enforceable policy regarding (i) compliance with the over-arching data processing principles of the GDPR, and (ii) retention and erasure of data. The flexibility engendered by this derogation is something that seemingly has the potential to save schemes from a real headache.

3 APPOINT A DATA PROTECTION OFFICER (OR JUSTIFY NOT APPOINTING ONE)

WHAT THE GDPR REQUIRES

A new 'key player' under the GDPR is the Data Protection Officer (DPO). This will be a mandatory appointment for both data controllers and processors in certain situations. The GDPR contains prescriptive requirements around who has to appoint a DPO, what they do, and what must be done to facilitate their work.

Any DPO will have a central role for an organisation's GDPR compliance, and "directly report to the highest management level of the controller". DPOs are expected to be fully involved, in a timely manner, in all data protection issues, and informed and consulted on all data privacy developments as early as possible. DPOs will not, however, have personal liability for an organisation's compliance (or failure to comply).

The GDPR and its accompanying guidance envisage that, in practice, the role of a DPO is likely to have three main areas as its focus:

- Raising GDPR awareness (including training relevant individuals, and advising on the organisation's data protection policies)
- Record-keeping (e.g. creating inventories and keeping a register of processing operations)
- Monitoring GDPR compliance, acting as the ICO's main point of contact, and assisting with addressing, or taking steps in relation to, any actual or potential breaches that may occur

The DPO's role is primarily advisory. They must be left free to perform this role in an independent manner. They will enjoy protected employment status as a result – i.e. they cannot be dismissed or penalised for performing their DPO tasks. The data controller itself, however, remains ultimately responsible for GDPR compliance.

KEY CONSIDERATIONS

Do you **have to** appoint a DPO?

If you do not have to, do you **want to**?

If you do appoint a DPO, **who** should it be?

WHAT YOU NEED TO DO

The first step for pension trustees is to decide whether to appoint a DPO.

Many pension schemes' circumstances are unlikely to trigger the requirement for mandatory appointment of a DPO (see box).

Even if you do not have to appoint a DPO, you could do so voluntarily. However, a voluntary appointment results in the same stringent GDPR requirements as a mandatory appointment. If trustees do not want to be treated as having appointed a DPO, they should be careful with any data protection role assigned to a particular individual. Status and job specification should in particular be precisely determined. Be very careful even with job titles – merely calling someone a Data Protection Officer will be sufficient to bring them within the scope of the GDPR's requirements.

Regardless of whether a DPO is ultimately appointed, data controllers such as pension trustees will be expected to consider – and document their analysis of – whether or not a DPO is in fact required.

Next, if you wish (or are required) to appoint a DPO, decide who it should be.

If pension scheme trustees do decide to appoint a DPO, this could be an internal or external appointment – and it may be possible to appoint a DPO jointly with the scheme's employer(s).

The GDPR (and WP29 guidance) contain extensive provisions about who can act as DPO. For example, any such person must:

- have "expert knowledge of data protection law and practices";
- be sufficiently senior within the organisation;

- have adequate knowledge of the organisation (and the business sector in which it operates) as well as its processing operations and IT and data security systems; and
- have, and be able to demonstrate, integrity and high professional ethics.

Finally, you should put in place systems and processes to facilitate your DPO's work: continuous training, adequate financial resources, premises and facilities, and time to fulfil their duties, are all recommended by WP29. And in order to protect their independence, DPOs enjoy a high degree of employment protection – as already noted.

Breach of the GDPR's provisions on DPOs (whether the requirement to appoint a DPO in the first place or the role, suitability and/or status of any appointee) could result in a fine of up to €10 million or 2% of annual worldwide (group) turnover, whichever is greater (see section 5, below).

TO APPOINT OR NOT TO APPOINT – DPOs AND THE GDPR

Trustees, third-party administrators and in-house teams undertaking benefit administration will need to give careful thought as to whether they are required to appoint a DPO. This will not always be straightforward to determine and trustees should consider seeking input from professional advisers if any doubt exists.

The appointment of a DPO is required to be made where the core activities of the data controller or processor consist of operations which:

- involve processing of sensitive personal data; and/or
- require regular and systematic monitoring of data subjects;

on, in either such case, a large scale.

The highlighted terms are key to determining whether your processing activities require the appointment of a DPO. WP29 has issued guidance to help people navigate the GDPR's requirements. (For more about the status of both WP29 and ICO guidance on the GDPR, see Appendix.) For example:

- A "core activity" means something which is an "inextricable part" of an organisation:
  - a hospital processing patients' health records is a core activity; but
  - an organisation processing the HR data of its employees, in order to pay them, isn't.
- Data is "sensitive personal data" if:
  - it relates to a living individual and is held on a computer or "relevant filing system"; and
  - relates to such a person's racial or ethnic origin, their physical or mental health, or their sexual orientation.
- The concept of "regular and systematic monitoring" focuses on tracking and profiling, which is not something that is typically relevant to pension schemes. Examples include:
  - location tracking and behavioural advertising; or
  - profiling and scoring for credit rating purposes or setting insurance premiums.
- Factors for determining whether an activity is "large scale" include the number of individuals whose data is being processed, the volume of data and the geographic scope:
  - a bank or insurance company processing customer data is large scale; but
  - processing of patient data by an individual physician isn't.

  (There is a very large grey area between these examples! To help with this, WP29 has indicated that it intends to publish more detailed threshold guidance.)

Overall it appears unlikely that the majority of pension schemes will be required to appoint a DPO. Third-party administrators will almost certainly, by contrast, have to make such an appointment. The position of in-house benefit administration teams will be harder to determine and much will depend on the specifics of the organisation in question.

INDIVIDUALS ARE GOING TO HAVE MUCH STRONGER RIGHTS UNDER THE GDPR

4 REASSESS HOW YOU ENGAGE WITH YOUR MEMBERSHIP

WHAT THE GDPR REQUIRES

The main situations in which pension trustees will need to engage with members (and others) about their personal data are:

- when collecting or obtaining the data;
- if, at a later date, the data is to be used for a different purpose to that for which it was obtained;
- if the individual exercises one of their rights in relation to their data; and
- (in some circumstances) where there is a breach of the GDPR.

Notices given when collecting data are typically called "privacy (or 'fair processing') notices". As part of the GDPR's drive to greater fairness and transparency, there are comprehensive requirements both for privacy notices when data is collected, and for updates to those notices when the grounds on which the data is being processed change.

We discuss member engagement consequent upon the exercise of individual rights, or resulting from a breach of the GDPR, elsewhere in this guide (see section 5, below).

KEY CONSIDERATIONS

- **What have you already told people** about how you process their data?
- Do you need to prepare and issue **new notices** to members?
- What do you say to **dependants** about any of their personal data that you process?

WHAT YOU NEED TO DO

We have previously considered how there is likely to be a shift by pension schemes, away from 'consent', as the legal ground on which they process personal data (see section 2, above). But even if the ground remains the same, any existing privacy notice that fails to meet the GDPR's enhanced requirements will need to be refreshed. In either scenario, trustees will need – in advance of 25 May 2018 – to issue new or updated privacy notices. Even if you think that all of the enhanced GDPR requirements are met, you may want to use this opportunity to re-engage with data subjects in any event.

These new or updated notices must, at the very least, include the following pieces of 'core information':

- The trustees' name(s) and contact details
- The contact details of the Data Protection Officer (if there is one)
- The purpose of the processing and the legal basis upon which it will be carried out
- Whether provision of the data is a statutory or contractual requirement, and the consequences of non-provision
- Detail of (if applicable) the data controller's legitimate interests for processing the data, or the data subject's right to withdraw consent to processing
- Full details of any third parties with whom the personal data is to be shared (generic descriptions will not suffice!)
- If the data controller intends to transfer the personal data to a third country outside the EU, details of such arrangements (including the appropriate safeguards in place)
- The period for which the personal data will be stored or, if this is not possible, the criteria used to determine this period
- Individuals' rights in relation to the processing (including the right to lodge a complaint with the ICO and seeking recompense directly from the data processor or controller, see section 5, below)

These notices must be in an easily accessible form, using clear and plain language, and must be provided free of charge.

You should also consider when and how personal data is collected from individuals (see section 1, above) and review, and update or add as necessary, privacy or 'fair processing' wording in standard documents that are used to obtain personal data – such as scheme membership applications, expression of wishes forms, and transfer request forms.

Where personal data is collected and processed in relation to third parties – e.g. members' dependants or nominated beneficiaries – thought will also need to be given to when and how (if at all) 'fair processing' information is provided to those individuals by the trustee board. The processing of data relating to children is also subject to more stringent requirements in any event, while the very nature of information often contained in paperwork such as expression of wishes forms brings back into focus the much narrower grounds on which sensitive personal data can lawfully be processed by trustees (see section 2, above).

5 UPDATE POLICIES AND PROCEDURES

WHAT THE GDPR REQUIRES

Individuals are going to have much stronger rights under the GDPR. Some they will not have enjoyed before. By contrast some of these rights are not new, but they will be better than those which individuals currently enjoy. Similarly, these will bear varying degrees of relevance to pension schemes and their trustees. For completeness, however, this new 'suite' of rights will include:

- The right to rectification (i.e. to have incorrect personal data updated, or incomplete data completed)
- The right to be forgotten (i.e. to have personal data deleted)
- Certain rights to restrict, or object to, processing of personal data
- The right to data portability (i.e. to receive personal data in a structured, commonly-used and machine-readable format, and to have it transferred to a different data controller)
- The right to withdraw consent
- The right of subject access

Most of those are fairly self-explanatory, but the right of subject access merits further explanation as it has the potential to cause a real headache for schemes if the right policies are not in place ahead of time.

A 'data subject access request' or DSAR is the means by which an individual can request information about the personal data held in respect of them. The data controller then generally has one month to provide the data – with only limited situations permitting a further two-month extension. How the data is supplied could take one of a variety of forms although the GDPR certainly envisages it being provided, or made available, via secure electronic means.

Manifestly unfounded or excessive requests can be refused or a charge levied, although there is currently no guidance on how to determine when charging is appropriate or what is considered "manifestly unfounded or excessive". Current caselaw suggests that this is a high hurdle. Any response to a subject access request must include a variety of accompanying information, the most relevant to trustees being:

- The purpose of the processing
- The categories of personal data concerned
- Third parties to whom it has been or will be disclosed
- The data retention period or the criteria used to determine it
- The right to rectification, erasure, and to restrict or object to processing
- The right to lodge a complaint with the ICO
- Information as to the data's source (where it was not collected from the data subject)

KEY CONSIDERATIONS

What data protection policies and procedures do you **already have** in place? Do they need **updating**?

What **new policies and procedures** do you need (particularly in relation to individual rights and GDPR breaches)?

WHAT YOU NEED TO DO

Some trustee boards may already have comprehensive data protection policies and procedures in place. However, we suspect that many do not! This is the time to dust off those that you do have and consider whether they need revising in light of the GDPR, and what new policies and procedures you may need to put in place.

This is particularly relevant for responding to individual requests. For example, do you have template member letters for responding to an individual's subject access request, and processes for collating the information to respond to such requests; do you have policies for dealing with requests to amend or even delete data and sufficient IT functionality to do so? This will be even more important under the GDPR with the tightened timeframes for responses to member requests.

We would also expect all trustees to be able to demonstrate their procedures for identifying, remedying and notifying breaches to the regulatory authority within the required 72-hour period (see box). Given that this breach may happen at the level of third-party processors, trustees will need to work with those third parties to put in place a framework to enable the trustees to get the information that they need to make the notifications within the tight timeframes.

An important part of preventing GDPR breaches is ensuring that adequate cybersecurity measures are in place (in terms of, for example, IT security, back-up systems, disaster recovery plans and policies and procedures for testing those items at regular intervals). This goes hand in hand with putting in place policies and procedures to meet the GDPR requirements as unauthorised access to personal data, via say a security breach, is an obvious way that the GDPR could be breached.

MAKING THE HEADLINES – SANCTIONS FOR BREACHING THE GDPR

One of the reasons why the GDPR is (and should be) attracting so much attention is the significant increase in sanctions for breach.

Complete compliance with the GDPR will be required from 25 May 2018 – there will be no 'phasing-in' of its requirements. The sanctions below will apply to any breaches after that date.

Money, money, money

The existing maximum £500,000 fine in the UK will be replaced with a two-tier system (applicable to both data controllers and data processors):

1. Minor breaches of some of the more administrative provisions of the GDPR: a maximum fine of €10 million or 2% of annual worldwide (group) turnover, whichever is greater
2. More fundamental breaches: a maximum fine of €20 million or 4% of annual worldwide (group) turnover, whichever is greater

(At the time of writing there exists some uncertainty as to how these amounts are to be calculated where a pension scheme's corporate trustee is part of the employer group.)

Examples of 'fundamental' breaches, capable of attracting fines up to this higher level, include:

- failing to process data on a lawful ground;
- if consent is the lawful ground, failing to obtain or maintain it in a proper manner;
- processing breaches relating to sensitive personal data;
- failure to give proper 'fair processing' notices or to comply with data subject access requests;
- breaches of data subjects' individual rights (such as rectification, erasure, data portability, and the right to restrict or to object to the processing of personal data); and
- international transfers in breach of the GDPR.

If individuals are unhappy with the way in which their data is being processed, they are able to:

- complain to the ICO; and
- instigate court proceedings in order to seek compensation or another remedy from the data controller or data processor responsible, or indeed both.

"I have a confession to make..."

The general rule is that breaches should be notified by data controllers to the ICO without undue delay and, where feasible, no later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

To facilitate this, data processors such as scheme administrators are required to notify data controllers of any breach of the GDPR without undue delay after becoming aware of it.

If the breach is likely to result in a "high risk to the rights and freedoms of natural persons" (the meaning of which is however not entirely clear in a pensions context), the data controller must also notify data subjects of the breach without undue delay unless one of the situations below applies. This is a big change in the law and a big additional deterrent against behaviour or practices likely to result in serious breaches occurring.

- The data controller has implemented suitable protection measures which were applied to the personal data affected by the breach (in particular an action such as encryption which would result in the data being unintelligible to anyone not authorised to access it);
- The data controller has taken subsequent measures which ensure that the high risk to the data subjects' rights and freedoms is no longer likely to materialise; or
- It would involve disproportionate effort (in which case there must instead be a public communication or similar steps to inform data subjects).

There is a 'tick box'-style list of items for inclusion in breach notifications. The notices to the ICO must at least:

- Describe the nature of the breach and, where possible, the categories and approximate number of data subjects and personal data records concerned;
- Include the name and contact details of the Data Protection Officer (if there is one) or a contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach; and
- Describe the measures taken or proposed to be taken to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

The notices to data subjects (if required) must include the nature of the breach and contain at least the information in the second, third and fourth bullets above.

Data controllers also have to keep an internal register of breaches (with details about the breach, its effect, and remedial action).

6 REVIEW AND RENEGOTIATE THIRD-PARTY AGREEMENTS

WHAT THE GDPR REQUIRES

Under the new regime data processors will, for the first time, become subject to statutory obligations with regard to matters such as the security of data and the manner in which they assess, document and conduct their data-processing activities. In a number of important respects this will bring their status, and potential exposure, into line with data controllers such as pension trustees. From a statutory perspective no longer will it simply be the data controller's neck which is on the line for any breach!

Equally, data controllers will become subject to a related obligation – to ensure that any third parties to whom processing duties are delegated provide sufficient guarantees that such processing will be conducted in accordance with the GDPR's requirements. The GDPR goes on to provide that various specific matters must be addressed in the contract by which the activities are delegated to that third party. This brings into focus the 'supply chain contracts' by which trustees delegate and further subcontract data-processing activities to third parties.

Onward subcontracting is not permissible under the GDPR without the express consent of the original data controller – in other words, pension trustees must explicitly permit this (either generally or in relation to specific subcontractors). The GDPR also stipulates that, if onward subcontracting is to be allowed, the contractual provisions between the data processor and the further subcontractor must then precisely mirror those originally imposed by the data controller on the data processor. The GDPR envisages these 'supply chain contracts' utilising standard contractual clauses, laid down by the ICO, to govern relationships between data controllers, processors and subcontractors.

KEY CONSIDERATIONS

- What data-processing activities are **delegated**?
- Is any **subcontracting** carried out? (It is conceivable that, at present, trustees may not be explicitly aware whether it is.) If not, is the ability to do so likely to be needed?
- What **contractual provisions** govern service provision by delegates or sub-contractors, and are they GDPR compliant?

WHAT YOU NEED TO DO

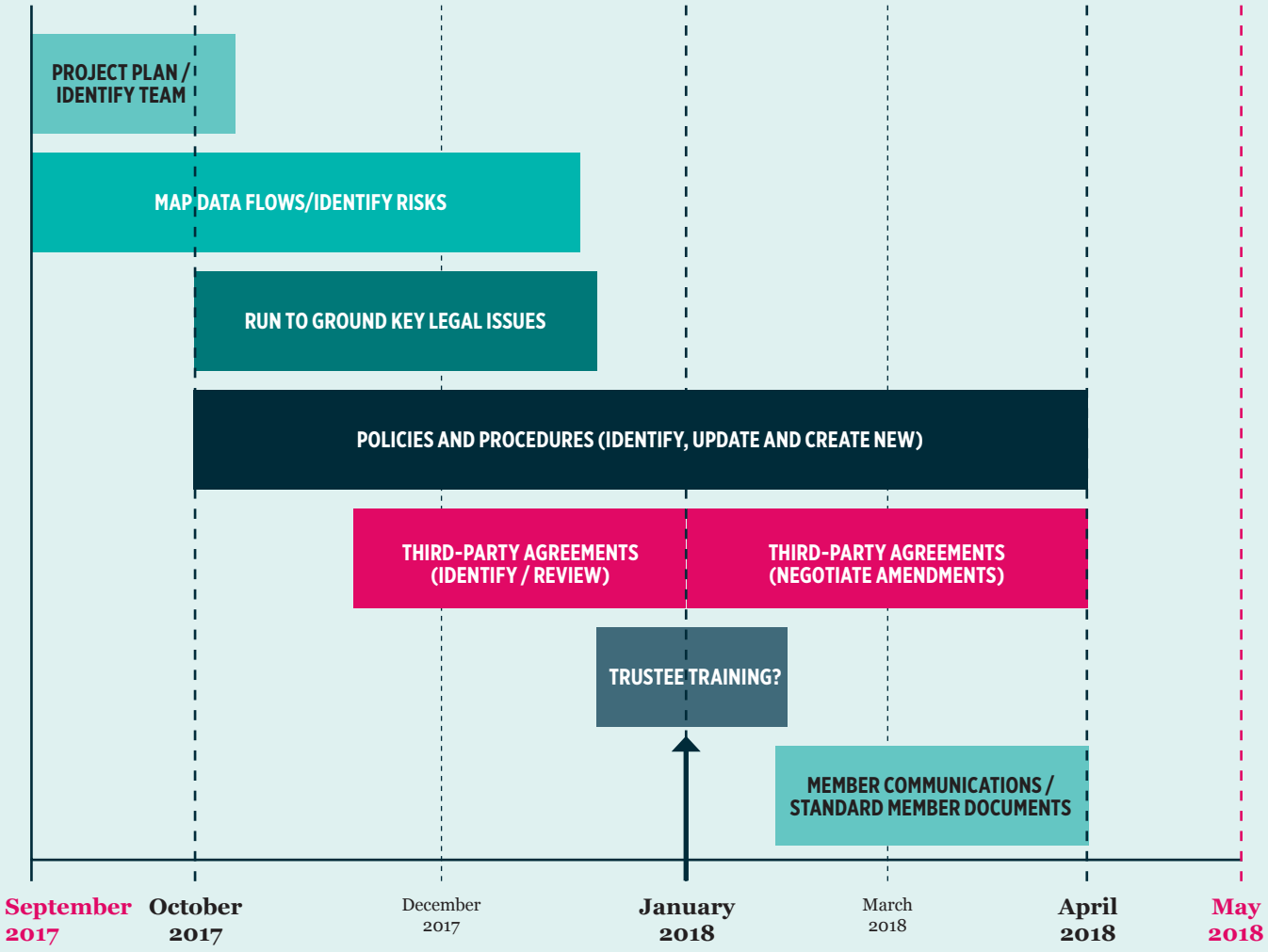
All third-party contracts should be reviewed and, if necessary (which is likely), renegotiated. Particular attention should be paid to provisions relating to:

- the supervision by the data controller (i.e. trustees) of the data processor's actions; and
- the inclusion in such contracts of the mandatory provisions listed in the GDPR.

In addition that review must ensure that the data processor's own obligations, to comply with the GDPR, are also spelled out in the contract with the data controller (trustees).

Renegotiation of any contracts will need to commence in good time before 25 May 2018, given that this will most likely involve detailed discussions with other parties over key terms. There may also be a number of such parties in the supply chain, all of whom are renegotiating with a line of others at the same time – all of which will take time.

ILLUSTRATIVE TIMELINE FOR GDPR READINESS



Date (based on quarterly trustee meetings)

3 AND TO CONCLUDE

It is difficult to cover all salient aspects of the GDPR even in a guide such as this, let alone to draw out meaningful conclusions by way of summary. In scratching the surface we hope nonetheless to have demonstrated that it is a subject which pension trustees and their fellow professionals need to be taking seriously, and that there is a lot to do in order to ensure that a pension scheme is "GDPR ready" by 25 May 2018. The key messages are to be thorough, keep an eye on developments (there is a lot still to come) and, given the number of workstreams and necessary involvement of third parties, to make a start as soon as practicable – to the extent, of course, that you have not done so already. Recognise too that whilst it is a difficult subject everyone is on the same learning curve, and remember always that your professional advisers are willing and able to help with any issues that you may encounter along the way.

THE KEY MESSAGES ARE TO BE THOROUGH, KEEP AN EYE ON DEVELOPMENTS AND MAKE A START AS SOON AS PRACTICABLE

4 APPENDIX

GUIDANCE FROM WP29 AND THE ICO

The key to a full understanding of the impact of the GDPR is the guidance relating to it, which demonstrates how the various regulatory bodies will police its requirements and the expectations they hold. Although compliance with the guidance will not (technically) be mandatory, were the ICO to become involved it would most likely have regard to any non-compliance when assessing whether there has been a breach and/or the appropriate sanctions to impose.

At the time of writing, while a certain amount of guidance has been issued, there is much yet to be finalised and a lot of substantive material awaited for the first time – which is far from ideal, particularly for those who have to implement the GDPR. The table below indicates the status of the various pieces of WP29 and ICO guidance as at September 2017, and sets out anticipated timescales for further development in these respects. Once the GDPR is in force WP29 will be replaced by the European Data Protection Board, which will also assume responsibility for the guidance it adopted.

SUBJECT	BODY	STATUS
Certification	WP29	Guidelines anticipated later in 2017. No draft yet issued.
Consent	ICO	Consultation on draft guidance closed March 2017. Will not be finalised until WP29 consent guidelines have been adopted.
	WP29	Aims to adopt guidelines by December 2017. No draft yet issued.
Data breach notifications	WP29	Aims to adopt guidelines by December 2017. No draft yet issued.
Data portability	WP29	Guidelines adopted April 2017 and now in force.
Data Protection Impact Assessments	WP29	Consultation on draft guidelines closed May 2017. Revised draft scheduled for adoption at October 2017 plenary session.
Data Protection Officers	WP29	Guidelines adopted April 2017 and now in force. More detailed 'threshold guidance' anticipated but timings unknown.
Data transfers	WP29	Aims to adopt guidelines by December 2017. No draft yet issued.
Derogations	DCMS	"Call for views" closed May 2017. ICO published its response to the consultation that same day. Various proposed derogations now contained in Data Protection Bill 2017.
Fines	WP29	Guidelines anticipated later in 2017. No draft yet issued.
General	ICO	Overarching "Guide to Data Protection" last updated July 2017.
	ICO	"12 Steps to Take Now" guidance updated May 2017.
	ICO	Online self-assessment toolkit for SMEs revised May 2017.
International transfers	WP29	Guidelines anticipated later in 2017. No draft yet issued.
Lead supervisory authorities	WP29	Guidelines adopted April 2017 and now in force.
Legitimate interests	WP29	Existing guidelines adopted April 2014 and remain in force.
	ICO	Guidance believed to be planned for late 2017.
Profiling	WP29	Aims to adopt guidelines by December 2017. No draft yet issued.
Subject access requests	ICO	Guidance updated June 2017.
Third-party agreements	ICO	Consultation launched September 2017; due to close October 2017.
Transparency	WP29	Aims to adopt guidelines by December 2017. No draft yet issued.

DISCLAIMER

ISBN: 978-1-907612-50-3

Pensions and Lifetime Savings Association
Cheapside House,
138 Cheapside,
London EC2V 6AE

T: 020 7601 1700
E: plsa@plsa.co.uk

www.plsa.co.uk

September 2017