

The background of the slide features a hand pointing at a digital financial chart on a tablet screen. The chart displays various data points and lines in shades of green, blue, and red. The overall aesthetic is modern and professional, with abstract geometric shapes in white and lime green framing the central image.

Hogan
Lovells

GDPR for pension schemes

A practical guide

Your new practical guide to GDPR and pension schemes

Change is coming . . .

Data protection law is undergoing radical change that is impacting employers and trustees of pension schemes and all service providers to them. With effect from 25 May 2018 the European General Data Protection Regulation (“GDPR”) will apply directly in the UK. Getting on top of the obligations is daunting but we have prepared a practical guide to enable those responsible for pension schemes to hit the ground running. We focus very much on the practical steps that need to be taken. A key feature of GDPR is the requirement to demonstrate your compliance. We are suggesting trustees adopt a Data Protection Policy to this end.





Key terms

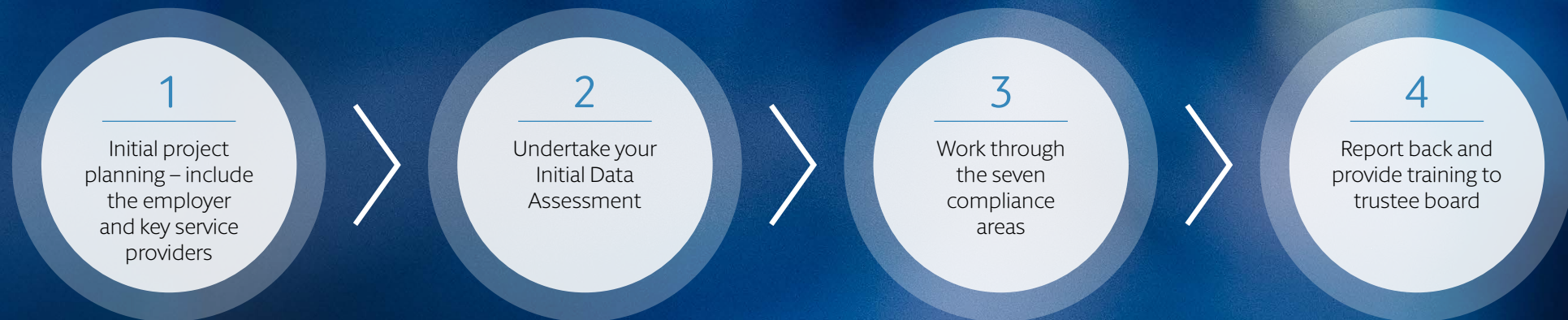
- **Controller:** a person who decides how and why data is processed.
- **Data Protection Policy:** a policy adopted by the trustees setting out how they will comply with all relevant elements of the GDPR.
- **Data Subject:** an identifiable living human being.
- **Filing System:** any structured set of personal data which are accessible according to specific criteria.
- **GDPR:** the General Data Protection Regulation.
- **ICO:** the Information Commissioner's Office, responsible for enforcement of GDPR within the UK.
- **Personal data:** any information relating to a Data Subject.
- **Privacy Notices:** information which must be given to Data Subjects about the processing of their personal data.
- **Processing data:** includes collecting, storing, recording, organising, altering, using, disclosing, and erasing personal data.
- **Processor:** a person who processes data on behalf of a controller.
- **Special data:** personal data concerning the Data Subject's race, ethnicity, political opinions, religion, trade union membership, sex life, sexual orientation or his / her genetic or biometric data.

Planning your project

Complying with GDPR is potentially a very substantial undertaking, although pension schemes which have already adopted good practices in this area may have less to do.

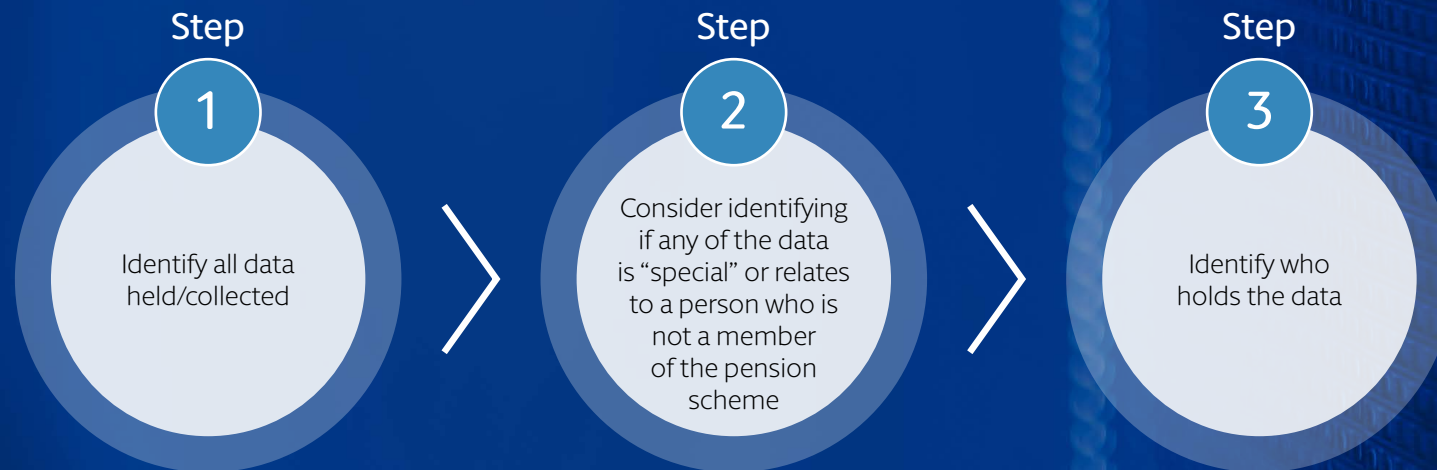
We suggest that pension schemes work with their sponsoring employers from the outset to plan the project. Employers frequently try to wrap up the pension scheme in their general approach to data protection. Whilst a shared and consistent approach is sensible, our experience shows that simply treating the trustee and pension scheme in the same way as other areas of the employer's business generally does not work. Trustees should remember that they are data controllers themselves, and therefore liable separately from the employer for compliance with GDPR. It is helpful if the employer is willing to share resources – particularly specialist IT resource – to assist pension schemes with data protection. Including your key service providers (especially your administrator) early on in the process is also recommended.

The following approach may be helpful:



Your initial data assessment

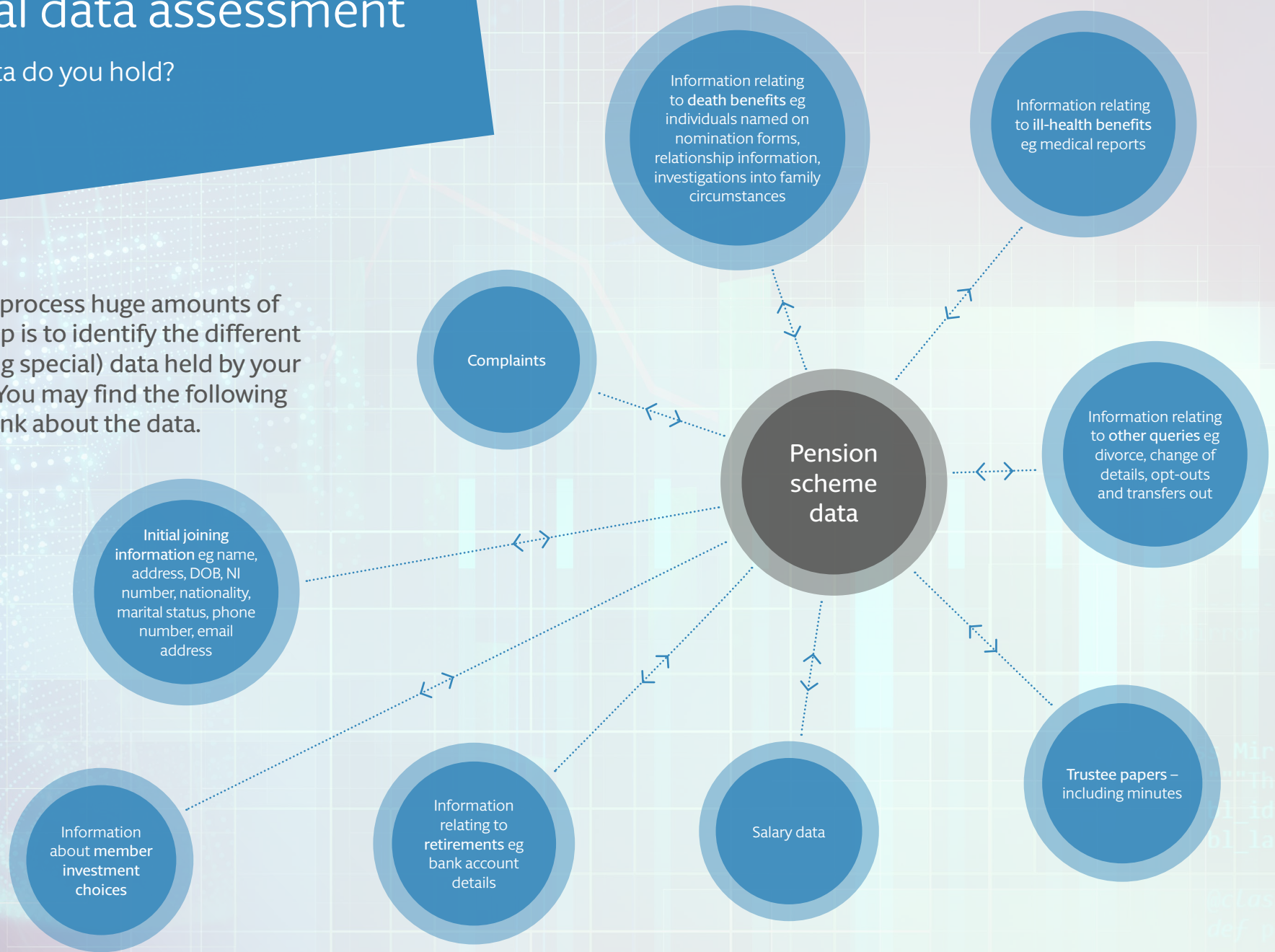
Before getting to grips with GDPR compliance, you should undertake a detailed assessment of your data. This will be essential in enabling you to comply with your obligations and also allows you to build up a record of your compliance – a key feature of GDPR. Think about all the data that is collected and held, plus who holds it – a key part of this task is to look at which service providers and other third parties are holding your data. It is important to remember all of your data – don't forget your paper records!



Your initial data assessment

Step 1 – what data do you hold?

Pension schemes process huge amounts of data. Your first step is to identify the different personal (including special) data held by your pension scheme. You may find the following a useful way to think about the data.



Your initial data assessment

Step 2 – what special and non-member data do you hold?

Once you have identified the different types of data, the next step is to consider whether any of it is “special data” or relates to a person who is not a member of the pension scheme in their own right. This information may be helpful later on to make sure that you comply with your GDPR duties.

Special data includes data concerning: racial and ethnic origin, sex life, sexual orientation, religious or philosophical beliefs, health, political opinions or trade union membership.

Non-members that pension schemes may hold data about include: spouses, partners and children, potential recipients of death benefits, people who have provided information to the pension scheme in connection with member benefits, etc.

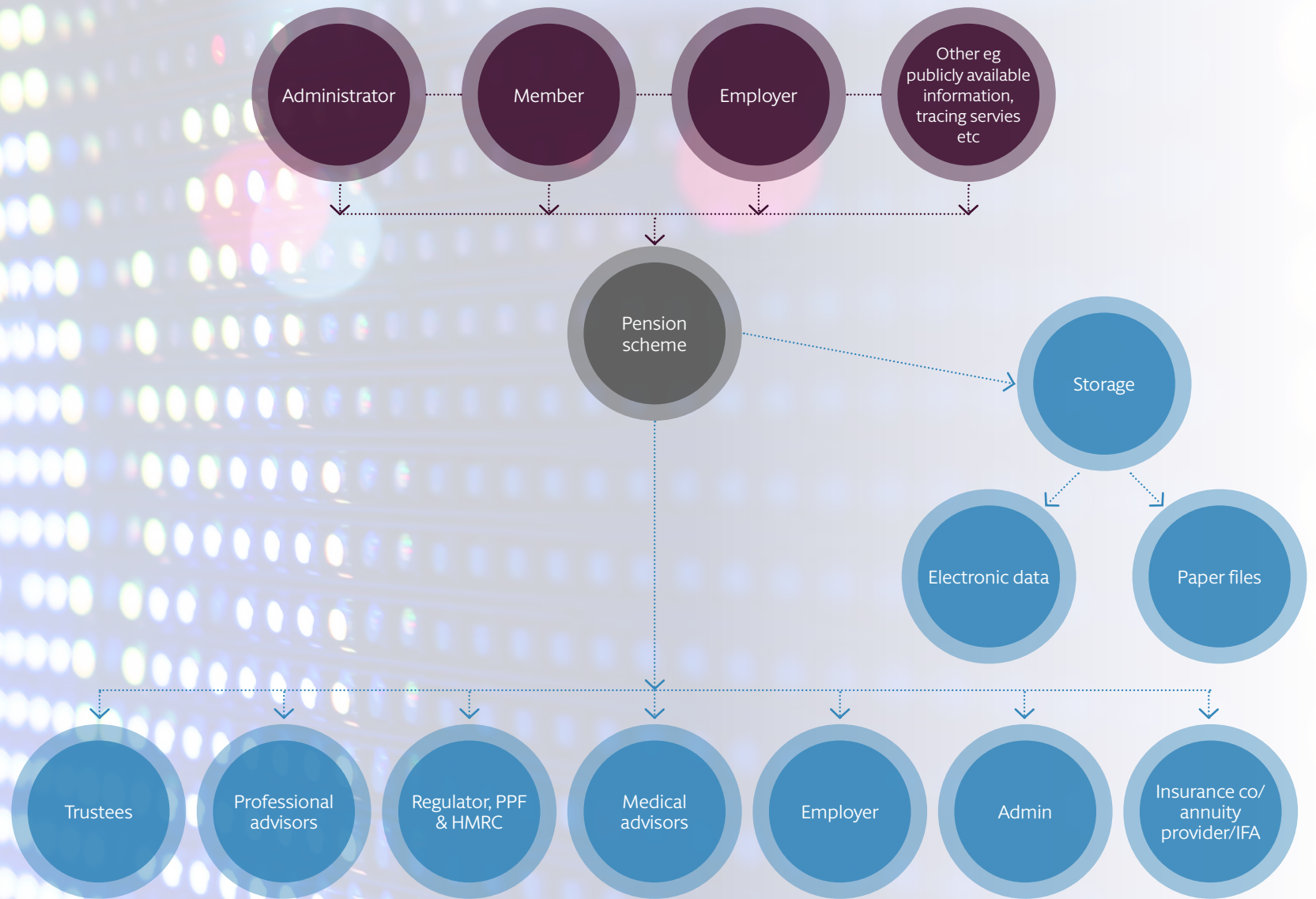
	Information on joining	Ill health pensions	Death benefits	Retirement	etc
Is any of it special data?					
Is any of it non-member data? Eg spouse, child, ex partner					

Your initial data assessment

Step 3 – who holds the data?

The next step is to identify who actually holds the information. We suggest that you use the diagram on the next page to help you identify who holds the data and then populate a table similar to the one opposite. It would also be sensible to consider which of these parties you have contractual agreements with and which govern the data.

	Contract in place?	Information on joining	Ill health pensions	Death benefits	Retirement	etc
Employer						
Administrator						
Actuary						
Investment advisor/manager						
Covenant advisor						
Auditor						
Communications advisor						
Insurer						
TPR						
HMRC						
PPF						
Medical advisor						
Other?						



The seven GDPR compliance areas

Once you have undertaken your Initial Data Assessment, you can work through the seven key compliance areas below to ensure that you meet the requirements of GDPR.

Compliance area

1

Record of Processing: complete a Record of Processing Form for your own data and distribute Record of Processing Form Questionnaires to each service provider and relevant third party. Retain both your own Record of Processing Form and service providers' Record of Processing Form Questionnaires.

Compliance area

2

Data Protection Principles: work through the requirements of each of the new data protection principles. We recommend that as part of this you adopt a Data Protection Policy and amend member forms where relevant.

Compliance area

3

Data Subject Rights: understand and ensure you can respond to the requirements around Data Subjects' rights – you should consider preparing standard letters to deal with requests.

Compliance area

4

Privacy Notices:
prepare and issue new Privacy Notices to members and, potentially, other individuals that you hold data about.

Compliance area

5

Third Party Contracts:
ensure your third party contracts comply with GDPR, including the requirements governing transfers outside the EU.

Compliance area

6

Data Security:
ensure that that you meet your obligations to keep data secure and are ready to manage any security breaches – this will include assessing the security of your data systems (possibly with specialist IT support) and consider preparing notices to the ICO and members for use if there is a breach.

Compliance area

7

Other requirements:
for completeness, there are other areas of the GDPR (specifically concerning Data Impact Assessments and Data Protection Officers) that you should consider but where we do not anticipate changes will be needed.

Compliance area 1

Preparing a Record of Processing Form

What is the obligation?	Actions	Demonstrating you comply
<p>GDPR requires data controllers and their processors to keep a record of certain specified information, in particular details about:</p> <ul style="list-style-type: none">– the controller and processor;– the processing undertaken, including: the purpose of processing; categories of data subjects; whether the data is “special data”; how long the data is retained;– overseas data transfers;– the security in place for the different types of data. <p>We would also suggest that thought is given to some additional queries, such as whether data is accurate, which may help you form a view on other compliance areas.</p>	<ul style="list-style-type: none">– Use your Initial Data Assessment to prepare a list of third parties who hold your data.– Send each third party a Record of Processing Form Questionnaire to complete and review the results.– Complete your own Record of Processing Form.	<ul style="list-style-type: none">– Record of Processing Form– Record of Processing Form Questionnaire– Your Data Protection Policy should reference the Record of Processing Form and Record of Processing Form Questionnaire

Compliance area 2

Making sure you comply with the data protection principles

The new data protection principles

Data protection law has long had over-riding principles that apply when processing personal data. GDPR specifies six high level principles that pension schemes will need to comply with.

Data must be processed lawfully, fairly and transparently

Data must be accurate

Data must be collected for specific, explicit and legitimate purposes

High level principles

Data must only be kept for as long as necessary

Data must be adequate, relevant and limited to what is necessary

Data must be kept secure

NODE 03

NODE 02

NODE 04

BLOCK 01

BLOCK 01




NODE 01




NODE 05

```
#selection at the end - add back the deselected
mirror_ob.select
modifier_ob.select
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob))
#mirror_ob.select = 0
#one = bpy.context.selected_objects[0]
#bpy.data.objects[one.name].select = 1
except:
    print("please select exactly two objects")

----- OPERATOR CLASSES -----
class Tool
    def poll(cls, context):
        # This adds an X mirror to the selected objects
        # idname = "object.mirror_mirror_x"
        # label = "Mirror X"
    @classmethod
    def poll(cls, context):
        return context.active_object is not None
    def mirror_mod = modifier_ob.modifiers.new("Mirror", "Mirror")
# set mirror object to mirror_ob
mirror_mod.mirror_object = mirror_ob
```

Compliance area 2

Principle	What is the obligation?	Actions	Demonstrating you comply
 <p>Data must be processed lawfully, fairly and transparently</p>	<p>GDPR requires pension schemes to process data lawfully, fairly and transparently.</p>	<ul style="list-style-type: none">– Agree the basis on which you are lawfully processing. For pension schemes we expect this to be primarily on the basis of “legitimate interest” and “legal obligation”.– Prepare a Privacy Notice that explains the basis for your lawful processing. We will cover more on Privacy Notices later on.– Ensure that express consent is given for the processing of special data. Ill-health forms in particular should contain appropriate consent provisions.	<ul style="list-style-type: none">– Your Data Protection Policy should include this.– Record of Processing Form and Record of Processing Form Questionnaire.– Privacy Notices.
 <p>Data must be collected for specific, explicit and legitimate purposes</p>	<p>GDPR requires pension schemes to collect data only for specific, explicit and legitimate purposes.</p>	<ul style="list-style-type: none">– You will have considered the purposes in your Record of Processing Form and your service providers should have done this in their answers to the Record of Processing Form Questionnaire. This should be retained to show your compliance.– Your Privacy Notice (which we will consider later on) should also explain the purposes of processing the data.	<ul style="list-style-type: none">– Your Data Policy should include this.– Record of Processing Form and Record of Processing Form Questionnaire.– Privacy Notices.
 <p>Data must be adequate, relevant and limited to what is necessary</p>	<p>GDPR requires pension schemes to process data only where it is adequate, relevant and necessary.</p>	<ul style="list-style-type: none">– You will have considered this in your Record of Processing Form and your service providers should have done this in their answers to the Record of Processing Form Questionnaire. This should be retained to show your compliance.– You should make sure that your Privacy Notice (which we will consider later on) explains why the processing is necessary.	<ul style="list-style-type: none">– Your Data Policy should include this.– Record of Processing Form and Record of Processing Form Questionnaire.– Privacy Notices.

Principle	What is the obligation?	Actions	Demonstrating you comply
	<p>GDPR requires pension schemes to process data only where it is accurate.</p>	<ul style="list-style-type: none"> – Review your existing safeguards which ensure that your data is accurate. You may have already considered this in your Record of Processing Form and Record of Processing Form Questionnaire. – Consider whether a sampling or audit of data accuracy should be undertaken. Review any existing assessments that you undertake (including to meet the tPR requirements around common data, etc) before making this decision. 	<ul style="list-style-type: none"> – Your Data Protection Policy should record this. – Potentially, your Record of Processing Form and Record of Processing Form Questionnaire. – Potentially – the outcome of any audit undertaken. – Your common data score and any other assessments you undertake.
	<p>GDPR requires pension schemes to keep data only as long as necessary.</p>	<ul style="list-style-type: none"> – You will have considered this in your Record of Processing Form and your service providers should have done this in their answers to the Record of Processing Form Questionnaire. These should be retained to show your compliance. – Consider how long data should be retained and include this in your Data Protection Policy. Careful thought should be given to the “right to be forgotten” and our own view is that pension schemes in most cases can revisit requests to be “forgotten”. 	<ul style="list-style-type: none"> – Your Data Protection Policy should cover this. – Record of Processing Form and Record of Processing Form
	<p>One of the key data protection principles is that data must be kept securely. GDPR has a number of provisions governing data security and we have therefore dealt with this under a separate compliance area.</p>		

Compliance area 3

Responding to Data Subjects' rights

What is the obligation?	Actions	Demonstrating you comply
<p>GDPR gives Data Subjects new rights to request pension schemes provide them with certain information and, in particular circumstances, to take certain actions in respect of the data held about them. The key relevant rights are:</p> <ul style="list-style-type: none">– to request certain information about the data held and to see a copy of it;– to have inaccurate information corrected;– to have data erased (the “right to be forgotten”);– to restrict the processing of data;– to object to data processing; and– to have data transferred to another controller.	<p>➤</p> <ul style="list-style-type: none">– Agree a process for dealing with these matters – specifically, who will deal with the requests; how recipients of the requests will know where to send them; what systems will need to be searched, etc.– Appoint a senior person to make a judgement call on certain matters – for example, where there is a request that would breach confidentiality to another person or where information is contentious.– Ensure that the Data Protection Policy deals specifically with the right to be forgotten.– Consider preparing standard responses so that requests can be dealt with quickly.	<p>➤</p> <ul style="list-style-type: none">– Your Data Protection Policy should record the process for dealing with these requests and the right to be forgotten.– Potentially standard letter to members.

Compliance area 4

Privacy Notices

What is the obligation?	Actions	Demonstrating you comply
<p>Pension schemes must provide certain information – referred to as a Privacy Notice – automatically to any Data Subject that they hold data about. This document must clearly set out the information required.</p>	<ul style="list-style-type: none">– Draft new Privacy Notices.– For simplicity we suggest that all pension scheme members are alerted to the new Privacy Notice. We believe that in most cases it is reasonable for members to be referred to an online document.– Agree a process for providing the Privacy Notice to new members or survivors – it could be included in the welcome pack and in initial correspondence.– Amend all forms where data is collected to reference the new Privacy Notice.– Identify any non-members of the pension scheme who you hold (or may in the future hold) information about. Your Initial Data Assessment will assist you in this. A decision should be taken about sending Privacy Notices to them – especially in sensitive cases – for example where people are nominated for death benefits.	<ul style="list-style-type: none">– Your Data Protection Policy should record the process.– Data Privacy Notices.– Amended forms.

Compliance area 5

Ensuring your third party contracts comply with GDPR, including provisions governing transfers outside the EU

What is the obligation?	Actions	Demonstrating you comply
<p>GDPR requires contracts between pension scheme trustees and those processing data on their behalf to include certain terms – including about sub-contracting and assistance with giving effect to individuals’ rights.</p> <p>Additionally, where data is to be exported outside the European Economic Area (EEA), specific terms must be included in the contract with the recipient of the data.</p> <p>It would also be prudent to ensure that contractors are obliged to comply with GDPR generally.</p>	<p>– Identify all the processors of your data and the contracts that govern those relationships. Also identify all transfers of data outside the EEA. Your Initial Data Assessment, Record of Processing Form and Record of Processing Form Questionnaire should assist with this.</p> <p>– Processors/recipients should be asked to agree amendments – if you have numbers of contracts a standard letter can be prepared.</p> <p>– All future contracts should include the standard clauses – those responsible for your contracts should be made aware.</p>	<p>– Your Data Protection Policy should include this.</p> <p>– Your Initial Data Assessment.</p> <p>– Record of Processing Form and Record of Processing Form Questionnaire.</p>

Compliance area 6

Meeting your obligations to keep data secure and respond to any breaches

What is the obligation?	Actions	Demonstrating you comply
<p>GDPR imposes a requirement to keep data secure – this is one of the high level principles and there is also a specific regulation that sets out particular security requirements. There are also requirements for dealing with breaches and informing members of the pension scheme and ICO of breaches in certain circumstances.</p>	<ul style="list-style-type: none">– Consider discussing your Initial Data Assessment with an IT specialist with an understanding of security with a view to getting advice on the robustness of your systems.– Consider the paper records that are held by the pension scheme and, in particular, whether they are secure.– Consider reviewing how information is passed to advisors, in particular the security of any personal data sent by email. This should be included in the Data Protection Policy.– Establish a protocol for data held by trustees – for example meeting papers, etc – this should be included in the Data Protection Policy.	<ul style="list-style-type: none">– Your Data Protection Policy should record the security measures including any protocols agreed with advisors and trustees and the process for dealing with breaches.– The Record of Processing Form and Record of Processing Form Questionnaire should cover security.– Potentially the IT specialist’s written confirmation.

Compliance area 7

Other requirements – requirements around data protection impact assessments – data protection officers

What is the obligation?	Actions	Demonstrating you comply
<p>There are a number of less relevant obligations that need to be considered under GDPR. Specifically:</p> <ul style="list-style-type: none">– There is a requirement where data processing is high risk for an impact assessment to be undertaken. This is particularly the case where special data is being processed or new technology is being used. In practice, we think this is unlikely to apply to pension scheme data but the process of considering the requirement must be gone through.– The ICO is expected to publish a list of “high risk” activities, which may help schemes decide whether or not the requirement applies.– There is a requirement to consider whether a data protection officer should be appointed. In most cases, we do not believe that this is required but consideration should be given to it.	<p>➤</p> <ul style="list-style-type: none">– Consider whether your processing is high risk and record the result of this.<ul style="list-style-type: none">– you may wish to wait until the ICO’s list of high risk activities is published.– If you do consider your processing to be high risk, seek assistance as you should consider a discussion with the ICO.– Consider whether to appoint a data protection officer and record your decision and reasoning.	<p>➤</p> <ul style="list-style-type: none">– Your Data Protection Policy should record the process about high risk processing and data protection officers.– The record of your assessment of the risk should be retained.



“

The ‘first-class team is one of the best all-rounders in the field’ and acts for some of the biggest clients.

Tier 1, Pensions, Legal 500 UK 2017

”

Checklist

Have you...

1

Retained the records of your Initial Data Assessment

2

Completed your own Record of Processing Form

3

Sent and reviewed Record of Processing Form Questionnaires to your service providers

4

Prepared a Data Protection Policy

5

Prepared and made available new Privacy Notices

6

Considered preparing standard letters to members dealing with Data Subject requests and other members' rights

7

Considered preparing standard letters dealing with breaches of security

8

Amended your member forms to incorporate references to the new Privacy Notices and ensure that consent is given where necessary

9

Agreed amendments to your third party contracts

10

Considered obtaining a report on your security from an IT specialist?

Reporting back

We recommend that you engage with your trustee board to bring them up to date with matters. We suggest a session that talks them through:

- the key features of GDPR;
- the process that you have gone through to ensure compliance;
- the key new documents that have been produced, with specific emphasis on the Privacy Notice and the Data Protection Policy; and
- any steps that individual trustees need to take to make sure that they personally comply with the new requirements.

“

They are all very thorough, knowledgeable and very personable.

Band 1, Pensions, Chambers UK 2017

”

The Hogan Lovells Team

We have extensive experience in advising trustees and employers on complying with data protection requirements. We are able to:

- Work with you to plan your project;
- Help you carry out your Initial Data Assessment and work with you and your service providers on the workstreams;
- Prepare all your key documents – including your Data Protection Policy, Privacy Notices, Record of Processing Form, Record of Processing Form Questionnaire, standard letters to members and amendments to member forms; and
- Run training for your trustee bodies and personnel.

“

Hogan Lovells have an ability to express themselves simply and to provide a clear explanation of the law in specific circumstances and also provide succinct options with guidance as to which option is the most practicable.”

Band 1, Pensions, Chambers UK 2016

”

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami

Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2016. All rights reserved. 12000_CM2_1017