Implementing the General Data Protection Regulation

A practical guide for members of AFM

October 2017
### Definitions of key terms in the GDPR

<table>
<thead>
<tr>
<th>GDPR term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent</td>
<td>Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her</td>
</tr>
<tr>
<td>Data controller</td>
<td>A natural or legal person, Public Authority, agency or other body which, alone or jointly with others. Determines the purposes and means of the Processing of Personal Data</td>
</tr>
<tr>
<td>Data processor</td>
<td>A natural or legal person, Public Authority, agency or other body who Process Personal Data on behalf of the Data Controller</td>
</tr>
<tr>
<td>Data protection</td>
<td>The process of safeguarding personal data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction</td>
</tr>
<tr>
<td>Data subject</td>
<td>The identified or identifiable natural person to which the data refers. Examples include customers and web users, individuals on email or marketing databases, employees, contractors or suppliers.</td>
</tr>
<tr>
<td>Legitimate interests</td>
<td>A lawful means for organisations to Process Personal Data without obtaining consent from the Data Subject. However, the interest of the Data Controller must be balanced with the interests and fundamental rights and freedoms of the Data Subject</td>
</tr>
<tr>
<td>Personal data</td>
<td>Any information (including opinions and intentions) which relates to an identified or identifiable natural person</td>
</tr>
<tr>
<td>Personal data handlers</td>
<td>Staff of the Data Controller who have been given responsibility for handling Personal Data as part of the operational activities</td>
</tr>
<tr>
<td>Privacy notice</td>
<td>A statement or document that discloses the ways an organisation gathers, uses, discloses and manages a customer’s Personal Data</td>
</tr>
<tr>
<td>Process, processing, processed</td>
<td>Any operation performed on Personal Data, whether or not by automated means, such as collecting, recording, organisation, storage, alteration, retrieval, use disclosure by dissemination or otherwise made available, alignment, restriction, erasure or destruction.</td>
</tr>
<tr>
<td>Specialist categories of data</td>
<td>Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.</td>
</tr>
<tr>
<td>Third country</td>
<td>Any country not recognised by the European Commission as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data</td>
</tr>
<tr>
<td>Third party</td>
<td>Any outside organisation with which your organisation has either previously, or currently conducts business, includes business partners, vendors, suppliers and service providers.</td>
</tr>
</tbody>
</table>
Contents

Section 1: Introduction ...................................................................................................................... 2
Section 2: Interpretation for AFM members ......................................................................................... 6
Section 3: Planning for GDPR: gap analysis and implementation plan .................................................. 11
Section 4: Assess: use ICO self-assessment to verify plan delivers .................................................... 12
Section 5: Communications within the business ...................................................................................... 13
Section 6: Data Protection Privacy Impact Assessment (DPIAs) ............................................................. 14
Section 7: Privacy statement for customers ............................................................................................ 15
Section 8: Audit checklist, including data inventory ............................................................................... 17
Section 9: Sources of support—working group and online forum ......................................................... 18
Section 10: Keeping up to date ............................................................................................................. 20

Note

This Guide to Implementing the GDPR has been produced by a working group of the Association of Financial Mutuals. It is written for members of AFM, using our best judgment, at the time of writing, of the implications of the General Data Protection Regime.

The Regime will continue to evolve ahead of, and after implementation, and AFM members should keep an active eye on developments, and particularly on the website of the Information Commissioners’ Office, www.ico.org.uk.

We will consider providing an updated version of the Guide as the Regime develops; if you identify and inaccuracies or changes, or would otherwise like to comment, please email martin@financialmutuals.org.
Section 1: Introduction

Background and Purpose of the GDPR

The General Data Protection Regulation 2016/679 ("GDPR") will apply from 25 May 2018. Being a Regulation, not a Directive, and applying before the UK leaves the EU, it will have immediate and direct effect in the UK without the need for any other (UK) legislation. In effect it will sweep away the UK Data Protection Act (DPA) 1998.

The Information Commissioner’s Office (ICO) will remain the UK agency responsible for overseeing the GDPR in the UK. For more information, see the remainder of this guide, and keep a regular eye on development of their website, which includes a range of toolkits to help implementation: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment-toolkit/.

There is also a section on the ICO website devoted to small businesses: https://ico.org.uk/for-organisations/business/.

What information does GDPR apply to?

Like the DPA, GDPR applies to ‘personal data’. However, GDPR’s definition is more detailed and makes it clear that information such as an outline identifier - eg an IP address – can be personal data.

For most organisations, keeping HR records, customer lists, or contract details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of DPA, it will also fall within the scope of GDPR.

The broad aims of GDPR are to give individuals greater control over their data by empowering them to find out the type of data firms hold on them, where it is stored, what it is used for and how it will be deleted. To do so the Information Commissioners Office (ICO), the data protection regulator, has either strengthened where existing regulations existed, or created new powers. As such, individuals now have the right to the following:

1. The right to be informed – the information held and the processing carried out.
2. The right of access – members being able to obtain the information we hold on them.
3. The right of rectification – if data is inaccurate/ incomplete, this is can be corrected.
4. The right of erasure – not an absolute ‘right to be forgotten’ but essentially complete deletion of information where certain specifications have been met.
5. The right to restrict processing – members right to block the Society processing their data.
6. The right to data portability – the right to obtain their personal data, to move, copy or transfer their personal data from one IT environment to another in a safe and secure way.
7. The right to object – where processing under legitimate interest (or reasons other than consent) the member will have the right to object.
8. Rights in relation to automated decision-making and profiling – provides safeguards to individuals where firms make decisions without human intervention, if this information might be damaging when used in relation to a particular product or service such as a loan application.
Under GDPR processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c. processing is necessary for compliance with a legal obligation to which the controller is subject;

d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

**Key Steps in Implementing the GDPR**

1. Ensure you have established a project team to support implementation, with:
   - regular meetings,
   - reporting progress to Leadership team and a committee,
   - with action points,
   - whose responsibility they are,
   - target dates and
   - a review system.

2. Create a gap analysis, to understand what changes you need to make (see section 3).

3. Check your gap analysis and action plan against the ICO’s self-assessment checklists (section 4).

4. Set out a communication plan, for the Board and more generally in the business, to explain the work required (section 5).

5. Incorporate new Privacy statements (section 6).

6. Add to Internal Audit plan, and Compliance Monitoring Plan (section 7).

7. Make sure you keep up to date on developments, and seek help where necessary (sections 8 and 9).

The ICO has set out a set of actions that firms should be taking now, as covered on the next page.
## OVERVIEW: Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now

**1 Awareness**  
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

**2 Information you hold**  
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

**3 Communicating privacy information**  
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

**4 Individuals’ rights**  
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

**5 Subject access requests**  
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

**6 Lawful basis for processing personal data**  
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

**7 Consent**  
You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don’t meet the GDPR standard.

**8 Children**  
You should start thinking now about whether you need to put systems in place to verify individuals’ ages and to obtain parental or guardian consent for any data processing activity.

**9 Data breaches**  
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

**10 Data Protection by Design and Data Protection Impact Assessments**  
You should familiarise yourself now with the ICO’s code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

**11 Data Protection Officers**  
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation’s structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

**12 International**  
If your organisation operates in more than one EU member state (i.e., you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.
Section 2: Interpretation for AFM members

GDPR has important consequences for AFM members. As the chart below demonstrates, the impact will be widely felt across the organisation.

Consent: a key change in the new regime

The UK Data Protection Act 1998, whilst modified, is 20 years old, and ill-equipped to deal with today’s environment. Compare the approach in the table below.

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Pre-GDPR rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>You will need to review your consent mechanisms to make sure they meet the GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn. The key new points are as follows:</td>
<td></td>
</tr>
<tr>
<td>Typically AFM members:</td>
<td></td>
</tr>
<tr>
<td>• Unbundled: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.</td>
<td></td>
</tr>
<tr>
<td>• Active opt-in: pre-ticked opt-in boxes are invalid – we need to use unticked opt-in boxes or similar active opt-in methods (eg a binary choice given equal prominence).</td>
<td></td>
</tr>
<tr>
<td>• use opt-out boxes</td>
<td></td>
</tr>
<tr>
<td>• specify methods of communication (eg by email, text, phone, recorded call, post)</td>
<td></td>
</tr>
<tr>
<td>• ask for consent to pass details to third parties for marketing and clearly describe those third parties</td>
<td></td>
</tr>
<tr>
<td>• record when and how we got consent, and exactly what it covers</td>
<td></td>
</tr>
<tr>
<td>Marketing by mail typically means screening names and addresses against the Mail Preference Service and the individual has providing at least a general statement that they are happy to receive marketing.</td>
<td></td>
</tr>
</tbody>
</table>
- **Granular**: you need to give granular options to consent separately to different types of processing wherever appropriate.
- **Named**: you must name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR.
- **Documented**: keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.
- **Easy to withdraw**: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you need to have simple and effective withdrawal mechanisms in place.
- **No imbalance in the relationship**: consent will not be freely given if there is imbalance in the relationship between the individual and the controller (this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis).

**Marketing by email or text** should only be with opt-in consent (unless contacting previous customers about our own similar products, and we offered them an opt-out when they gave their details).

**Existing customers**: the ‘soft opt-in’ means organisations can send marketing texts or emails if they have obtained the contact details in the course of a sale (or negotiations for a sale), they are only marketing their own similar products or services; and they gave the person a simple opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

Organisations must give the customer the chance to opt out – both when they first collect the details, and in every email or text. Organisations should not assume that all customers will be happy to get marketing texts or emails in future, and cannot rely on the soft opt-in rule unless they provided a clear opportunity to opt out first.

It must be simple to opt out. When first collecting a customer’s details, this should be part of the same process (eg online forms should include a prominent opt-out box, and staff taking down details in person should specifically offer an opt-out). In subsequent messages, we consider that the individual should be able to reply directly to the message, or click a clear ‘unsubscribe’ link. In the case of text messages, organisations could offer an opt-out by sending a stop message to a short code number: eg ‘text STOP to 12345’. The only cost should be the cost of sending the message.

---

**Can we continue to use existing DPA consents?**

You are not required to automatically ‘repaper’ or refresh all existing DPA consents in preparation for the GDPR. But it’s important to check your processes and records in detail to be sure existing consents meet the GDPR standard.
Recital 171 of the GDPR makes clear you can continue to rely on any existing consent that was given in line with the GDPR requirements, and there’s no need to seek fresh consent. However, you need to be confident that our consent requests already met the GDPR standard and that consents are properly documented. You will also need to put in place compliant mechanisms for individuals to withdraw their consent easily.

On the other hand, if existing DPA consents don’t meet the GDPR’s high standards or are poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing.

The ICO’s consent checklist sets out the steps you should take to seek valid consent under the GDPR. This checklist can also help to review existing consents and decide whether they meet the GDPR standard, and to seek fresh consent if necessary:

**GDPR**

**Asking for consent**
- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don’t use pre-ticked boxes, or any other type of consent by default.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we’re going to do with it.
- We give granular options to consent to independent processing operations.
- We have named our organisation and any third parties.
- We tell individuals they can withdraw their consent.
- We ensure that the individual can refuse to consent without detriment.
- We don’t make consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.

**Recording consent**
- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time.

**Managing consent**
- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We consider using privacy dashboards or other preference-management tools as a matter of good practice.
- We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We don’t penalise individuals who wish to withdraw consent.
Data Controllers & Data Processors

Under the DPA, only the controller is held liable for data protection compliance, not the processor.

In contrast, the GDPR places direct statutory obligations on data processors. These obligations mean that data processors may be subject to direct enforcement by supervisory authorities, serious fines for non-compliance and compensation claims by data subjects for any damage caused by breaching the GDPR.

These obligations include:

- **Data Processing Agreements** – processors may only process personal data on behalf of a controller where a written contract is in place, which imposes a number of mandatory terms on the data processor, as set out in the GDPR.
- **Sub-processors** – processors may not engage a sub-processor without the prior written authorisation of the controller.
- **Controller instructions** – processors may only process personal data in accordance with the instructions of the controller.
- **Accountability** – processors must maintain records of data processing activities and make these available to the supervisory authority on request.
- **Co-operation** – processors must co-operate with the supervisory authority.
- **Data security** – processors must take appropriate security measures and inform controllers of any data breaches suffered.
- **Data Protection Officers** – processors must, in specified circumstances, designate a data protection officer.
- **Cross-border transfers** – processors must comply with restrictions regarding cross-border transfers.
- **Sanctions** – non-compliant processors risk fines of up to 4% of global annual turnover.

The GDPR also makes data controllers and processors jointly and severally liable. This means that, where a controller or processor has paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controller or processor involved, that part of the compensation corresponding to their responsibility for the damage. The ICO have recently published a consultation on GDPR guidance on contracts and liabilities between controllers and processors: [https://ico.org.uk/about-the-ico/consultations/consultation-on-gdpr-guidance-on-contracts-and-liabilities-between-controllers-and-processors/](https://ico.org.uk/about-the-ico/consultations/consultation-on-gdpr-guidance-on-contracts-and-liabilities-between-controllers-and-processors/).

What action is required?

Any changes are likely to take time to implement and both data controllers and processors should act early in order to:

- **Identify, review and**, where necessary, **revise their data processing agreements** to ensure that they are GDPR-compliant. Any new agreements should be agreed in accordance with the requirements of the GDPR.
- **Consider mechanisms for resolving disputes** regarding respective liabilities to settle compensation claims, given the new provision allowing for joint liability for data protection breaches.
- **Ensure that you have clear documentation and recording procedures** in place to prove that you meet the required standards. Implement measures to prepare and maintain records of your organisation’s processing activities.
Sensitive/ Special Category data

“Special categories of personal data” now expressly include “genetic data” and “biometric data” where processed “to uniquely identify a person”.

The grounds for processing sensitive data under the GDPR broadly replicate those under the current Act, although there are wider grounds in the area of health and healthcare management. These are continuing to evolve: for example, for insurers who underwrite using health insurance, it remains uncertain whether it will remain possible to process certain health or fraud data without explicit consent.

Appointing a Data Protection Officer

Under the GDPR, you must appoint a data protection officer (DPO) if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Most AFM members are unlikely to fall into any of these three categories. Whilst this does not prevent you from appointing a DPO, we consider that the minimum requirements are quite onerous, as a DPO needs to be a subject matter expert. As an alternative, you can contract out the role of DPO if you feel one is necessary, or you can appoint a Data Protection Adviser from within the business, who may already carry out data protection responsibilities.
Section 3: Planning for GDPR: gap analysis and implementation plan

We have developed a grid to provide an overview of 13 key requirements in the GDPR, which offers an assessment of the type of work that might be needed to comply. AFM members should consider and adapt the tables to identify for themselves the work required.

The key requirements are:

1. Data protection Principles
2. Lawfulness of processing/ further processing
3. Consent
4. Children
5. Sensitive data and lawful processing
6. Privacy Notices
7. Subject access, rectification and portability]
8. Right to object
9. Right to erasure and restrict processing
10. Governance obligations
11. Privacy by design
12. Breach notification
13. Transfer of personal data

See the separate plan at the end of this document for an outline of the new requirements, and what work might be required to comply.
Section 4: Assess: use ICO self-assessment to verify plan delivers

Having completed your gap analysis above, and using this to develop an implementation plan, you should verify this against the ICO’s self-assessment tool. This will help ensure the plan is likely to be effective, and will help in justifying to the Board and other audiences, what work is needed. There are currently 8 self-assessment tools on the ICO website which you can link from here:

**Data protection assurance:** Recommended for first time users. Assess your high-level compliance with the Data Protection Act. Includes registration, fair processing, subject access, data quality, accuracy and retention.

[Start now]

**Getting ready for the GDPR:** Designed to help you get your house in order, ready for the new legislation. Includes getting to grips with the new rights of individuals, handling subject access requests, consent, data breaches, and designating a data protection officer, under the upcoming General Data Protection Regulation.

[Start now]

**Information security:** Assess your compliance with data protection in the specific areas of information security policy and risk, mobile working, removable media, access controls and malware protection.

[Start now]

**Direct marketing:** Assess yourself in the areas of consent and bought-in lists, and telephone, electronic and postal marketing.

[Start now]

**Records management:** Records management policy and risk, record creation, storage and disposal, access, tracking and off-site storage.

[Start now]

**Data sharing and subject access:** Sharing policy and agreements, compliance monitoring, maintaining sharing records, registration and subject access process.

[Start now]

**CCTV:** Helps you to assess the compliance of your CCTV including the installation, management, operation, and public awareness and signage.

[Start now]
Section 5: Communications within the business

Implementing GDPR is likely in most cases to involve a range of business areas, changes to processes, revised documents and website updates.

<table>
<thead>
<tr>
<th>GDPR requirement</th>
<th>Target audience</th>
<th>Related Training and Awareness Content</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a policy that addresses Data Protection for all staff</td>
<td>Management</td>
<td>Data Protection policy</td>
<td>Improving results for policy related knowledge assessments</td>
</tr>
<tr>
<td>Implement a formal awareness program to make all personnel aware of Personal Data breach handling procedures</td>
<td>Management, Personal Data Handlers</td>
<td>Personal Data breach notification procedures, Personal Data breach management policy, Personal Data breach response plan</td>
<td>Increase in reporting of Personal Data related issues, Decrease in Personal Data breach incidents and near-misses</td>
</tr>
<tr>
<td>Maintain and implement policies and procedures to manage Third parties with whom Personal Data is shared, or that could affect the security of Personal Data</td>
<td>Management</td>
<td>Third Party management and monitoring policy, Third party risk assessment procedures</td>
<td>Decrease the number and severity of audit findings associated with Third Party Processing</td>
</tr>
</tbody>
</table>

source: MetaCompliance

In addition, the ICO has also produced a video with GDPR messages for the boardroom; click on the on the slide to view it:
Section 6: Data Protection Privacy Impact Assessment (PIAs)

DPIAs are a tool which helps organisations identify the most effective way to comply with their data protection obligations and meet individuals’ expectations of privacy. An effective PIA will enable organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might occur otherwise.


When do I need to conduct a PIA?

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.
Section 7: Privacy statement for customers

You will need to review the privacy statement you currently use in communications with customers, both on paper and electronically. An article in a recent edition of AFM’s Mutually Yours considered the background for changing privacy notices and consents.

The following generic example of a consent statement takes account of ICO’s guidance.

The General Data Protection Regulations
Consent for Use of Personal Data

The information we hold about you is used to administrate your policy. We, NAME OF FIRM, will never share your data with any third party without your consent. We may, however, wish to contact you in the future with marketing material that we believe may be of interest to you. However, NAME OF FIRM will only do this if you are happy to receive such information. Once your marketing preferences have been updated they will remain in place until you let us know otherwise. You can update us at any time, opting in or out of marketing, or change the ways in which you’d prefer us to contact you. You can update your marketing preferences by contacting us:

- **Phone** XXXX XXX XXXX
- **Post** Generic Department, Generic Firm, Generic Town A1 1BC
- **Email** enquiries@genericfirm.co.uk

If you’re happy to receive marketing information from NAME OF FIRM, please let us know how you prefer to be contacted. You can tick as many of the boxes below as you wish. If you do not wish to be added to our marketing list, simply leave the tick boxes empty.

Please detach and return the slip below using the enclosed envelope.

Consent for Use of Personal Data Slip

**METHOD OF IDENTIFYING INDIVIDUAL HERE: XXXXXXX**

I am happy to be contacted and prefer to be contacted by the following route:

- **Post**...☐  Email...☐
- **Telephone (home)**...☐  **Telephone (Mobile – including SMS/MMS)**...☐
The ICO website considers a range of good and bad examples of privacy notices: click on the example below to see more:
Section 8: Audit checklist, including data inventory

We would expect an audit would cover the following areas:

- Data governance and accountability
- Privacy impact assessments
- Individuals’ rights: Consent, Data portability, Right to be forgotten / informed, right to access / rectification / erasure / restrict processing / object
- Automated decision making and profiling
- Breach notification
- Transfer of data
- National derogations

For an example of a data inventory, see the table below.

<table>
<thead>
<tr>
<th>File Ref No</th>
<th>File name / Data held</th>
<th>Type of Data</th>
<th>Date Added</th>
<th>Category of Data</th>
<th>Paper / Electron</th>
<th>Where held?</th>
<th>Security controls in place</th>
<th>Third Party? (if applicable)</th>
<th>Team Resonsible (to be filled in)</th>
<th>Date to be Deleted?</th>
<th>Reason for retention?</th>
<th>Commentary / Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Short description of the data held (if necessary)

Provide details here, including exact date if known, or short description: eg 10 years after paid out or lapsed

Sensitive or personal?

If regulatory, give details or cite which regulation adhering to
Section 9: Sources of support- working group and online forum

AFM established a working group to help provide guidance for members on the GDPR. The working group brought together a range of members of the AFM Regulation and Governance Committee, as well as other members of AFM, all of whom recognised that the changes required under the Regulation would be significant, and that there was significant benefit in working with other members to develop an effective approach.

All the members of the working group have agreed to act as a sounding board for members on particular issues. We have established an online forum, so that members can post issues in a safe environment, and seek answers to their queries.

You can join the online forum by clicking on this link:

https://discuss.oddfellows.co.uk/

This will take you to following page:

Click on register and complete registration. Once completed you will be taken to following page:

Once you have received an email confirming your account has been activated, log in and you will be taken to the following page:
The online forum is easy to use. There is a Q&A tab, which provides further information on what you can do.

*Note that when creating a new post or responding to one, the number of characters included in the note should be limited to 5,000 characters.*

**Members of the AFM GDPR working group are:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Darren McCormack</td>
<td>Benenden Healthcare</td>
<td><a href="mailto:Darren.mccormack@benenden.co.uk">Darren.mccormack@benenden.co.uk</a></td>
</tr>
<tr>
<td>Louise Eden</td>
<td>BHSF</td>
<td><a href="mailto:LouiseEden@bhsf.co.uk">LouiseEden@bhsf.co.uk</a></td>
</tr>
<tr>
<td>Georgina Rose</td>
<td>British Friendly</td>
<td><a href="mailto:g.rose@britishfriendly.com">g.rose@britishfriendly.com</a></td>
</tr>
<tr>
<td>Andrew Horsley</td>
<td>Cirencester Friendly Society</td>
<td>andrew.horsley@ciренcester-friendly.co.uk</td>
</tr>
<tr>
<td>Alan Goddard</td>
<td>Cornish Mutual</td>
<td><a href="mailto:Agoddard@cornishmutual.co.uk">Agoddard@cornishmutual.co.uk</a></td>
</tr>
<tr>
<td>Claire Longman</td>
<td>Cornish Mutual</td>
<td><a href="mailto:clongman@cornishmutual.co.uk">clongman@cornishmutual.co.uk</a></td>
</tr>
<tr>
<td>John Midlane</td>
<td>Metropolitan Police</td>
<td><a href="mailto:john.midlane@mpfs.org.uk">john.midlane@mpfs.org.uk</a></td>
</tr>
<tr>
<td>Gary Morley</td>
<td>Oddfellows Friendly Society</td>
<td><a href="mailto:gary.morley@oddfellows.co.uk">gary.morley@oddfellows.co.uk</a></td>
</tr>
<tr>
<td>Tim Bateman</td>
<td>Mazars</td>
<td><a href="mailto:tim.bateman@mazars.co.uk">tim.bateman@mazars.co.uk</a></td>
</tr>
<tr>
<td>Paul Andrews</td>
<td>Ai-London</td>
<td><a href="mailto:paul.andrews@ai-london.com">paul.andrews@ai-london.com</a></td>
</tr>
<tr>
<td>Martin Shaw</td>
<td>AFM</td>
<td><a href="mailto:martin@financialmutuals.org">martin@financialmutuals.org</a></td>
</tr>
</tbody>
</table>
Section 10: Keeping up to date

GDPR goes live in May 2018. At the time of writing (September 2017), we are still waiting for final guidance from the ICO on how it intends to apply the Regulation. However, they have indicated that the principles are well established and there is enough for firms to be getting preparations in place.

We recommend though that AFM members keep a close eye on developments.

One of the best sources of information is of course the ICO website. They provide regular news articles, blogs and tweets (@ICOnews), and provide helpful summaries of action they’ve taken against organisations. We recommend you sign up to the ICO newsletter: https://ico.org.uk/about-the-ico/news-and-events/e-newsletter/.

The press are now writing regularly articles on the GDPR, and in August the UK government published a Statement of Intent, setting out its plans for a new Data Protection Bill.

Other sources of information include:

- AFM is working with Skillcast on a suite of new online training materials; in the meantime you can view a free GDPR training template here
- ICO has confirmed that from 1 November it will be providing a dedicated phone service for smaller businesses; see: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/ico-announces-more-help-for-small-and-micro-businesses/
- One aspect of the GDPR that we have not covered extensively elsewhere in the Guide is profiling, which deals with the automated processing of personal data. This may not be a significant issue for most AFM members, but if you wish to understand the issue further, this article is helpful: https://www.dacbeachcroft.com/en/gb/articles/2016/june/gdpr-deep-dive-profiling-in-the-insurance-industry/