Implementing the General Data Protection Regulation

A practical guide for members of AFM

Version: March 2018:
(highlighted text= recent updates and comments from ICO)
# Definitions of key terms in the GDPR and data protection

*(specific GDPR terms in italics)*

<table>
<thead>
<tr>
<th>Terms used in the Guide</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, or other forms of identifier such as IP address</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 make 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 outside the European Union regardless of whether they have 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 ........................................................................................................ 3
SECTION 2: INTERPRETATION FOR AFM MEMBERS ............................................................ 6
SECTION 3: PLANNING FOR GDPR: GAP ANALYSIS AND IMPLEMENTATION PLAN ..........12
SECTION 4: ASSESS: USE ICO SELF-ASSESSMENT TO VERIFY YOUR PLAN DELIVERS .......13
SECTION 5: COMMUNICATIONS WITHIN THE BUSINESS ......................................................14
SECTION 6: DATA PROTECTION PRIVACY IMPACT ASSESSMENT (PIAS) .........................15
SECTION 7: PRIVACY NOTICES AND CONSENT FOR CUSTOMERS ...................................16
SECTION 8: AUDIT CHECKLIST, INCLUDING DATA INVENTORY .........................................19
SECTION 9: SOURCES OF SUPPORT- WORKING GROUP AND ONLINE FORUM .................20
SECTION 10: KEEPING UP TO DATE .....................................................................................22

ANNEX: draft implementation plan

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. The UK Data Protection Act 2018 is currently being finalised and will replace the DPA1998 and fill in any national gaps from the GDPR.

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. The ICO is the UK data protection regulator, established by government and supplied with strengthened powers in order to uphold the GDPR. 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. Solely automated decision making is now effectively prohibited except in certain situations.
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, and consider whether and how to make GDPR compliance a Board level responsibility (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. For more, see: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
<table>
<thead>
<tr>
<th><strong>OVERVIEW: Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Awareness</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>2 Information you hold</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>3 Communicating privacy information</strong>  &lt;br&gt;You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.</td>
</tr>
<tr>
<td><strong>4 Individuals’ rights</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>5 Subject access requests</strong>  &lt;br&gt;You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.</td>
</tr>
<tr>
<td><strong>6 Lawful basis for processing personal data</strong>  &lt;br&gt;You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.</td>
</tr>
<tr>
<td><strong>7 Consent</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>8 Children</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>9 Data breaches</strong>  &lt;br&gt;You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.</td>
</tr>
<tr>
<td><strong>10 Data Protection by Design and Data Protection Impact Assessments</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>11 Data Protection Officers</strong>  &lt;br&gt;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.</td>
</tr>
<tr>
<td><strong>12 International</strong>  &lt;br&gt;If your organisation operates in more than one EU member state (ie 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.</td>
</tr>
</tbody>
</table>
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>Typically AFM members:</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>• use opt-out boxes</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</td>
<td>• specify methods of communication (eg by email, text, phone, recorded call, post)</td>
</tr>
<tr>
<td></td>
<td>• ask for consent to pass details to third parties for marketing and clearly describe those third parties</td>
</tr>
<tr>
<td></td>
<td>• record when and how we got consent, and exactly what it covers</td>
</tr>
<tr>
<td></td>
<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>
</tr>
</tbody>
</table>
methods (e.g., a binary choice given equal prominence).

- **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 (e.g., online forms should include a prominent opt-out box, and staff taking down details in person should specifically offer an opt-out).

Marketing rules come from Privacy and Electronic Communications Regulations 2003 (PECR) rather than GDPR. PECR is also being revised and will eventually be replaced by the new E-Privacy Regulation, though this will take effect after GDPR implementation. There will therefore be a period where PECR will continue to have effect, but with the GDPR definition of consent.

Marketing and consent are dealt with in more detail in the revised section 7 below.

**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 significant fines.

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/.

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.

The latest version of the Data Protection Bill 2018 includes conditions and exemptions for process special category data for insurance purposes.

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.

We asked ICO for their interpretation of this for AFM members: their response was:

“It isn’t possible to provide a clearer definition of “large scale” processing at this stage, particularly a numeric value such as a number of data subjects affected or the turnover of a data controller, as this would inevitably result in some data controllers being caught by the requirement when they don’t really need a DPO, and others not being caught despite the fact they are carrying out very intrusive processing that affects a lot of people. As the Article 29 Working Party guidance itself acknowledges, this is a concept that will develop over time, based on real world examples*. We are considering the issue and may release more detailed guidance in the future as our lines develop.

This is why the best thing for members to do now is to make a decision based on the guidance that is available, and to document their logic for that decision. Even if a data controller decides not to appoint an “official” GDPR defined DPO, we would still strongly recommend that there is a clear understanding within the organisation of who is responsible for compliance with data protection and privacy law.”

As a DPO needs to be a subject matter expert, the requirements may be onerous. 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.

If you decide not to appoint a DPO you should carefully document the reasons why, and ensure it is clear who within the organisation has responsibility for control of data protection.
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 outside the EU

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 your 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, Personal Data Handlers</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 Processors</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, Procurement</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:

GDPR messages for the boardroom

In the video below, Information Commissioner Elizabeth Denham talks about “the biggest change to data protection law for a generation”. The video is aimed at boardrooms and calls on businesses to see the commercial benefits of sound data protection, and act now to ensure they’re compliant by 25 May 2018.
Section 6: Data Protection Privacy Impact Assessment (PIAs)

PIAs 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 PIA when:

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

ICO recommends that PIAs are carried out in any circumstances where there may be an impact on data subjects’ privacy. It is a good habit to get into.
Section 7: Privacy notices and consent for customers

You will need to review existing privacy notices/ statements where they are used 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.

Currently the Privacy and Electronic Communications Regulations 2003 (PERC) sets out when consent is needed, whereas GDPR defines what form that consent must take. Note that the draft E-Privacy Regulation will replace PERC in due course.

Privacy Notices

Your business will not be able to rely on existing Privacy Notices after GDPR implementation. From 25 May 2018 the extent of consents changes and a new form of Privacy Notice is required.

The ICO website considers a range of good and bad examples of privacy notices: click on the example below to see more:
The GDPR focuses on making privacy notices more understandable and accessible. The Regulation says that the information you provide to people about how you process their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The explicit emphasis on adapting privacy notices for children goes beyond current DPA requirements.

For a full breakdown of what should be included, and for ICO’s Code of Practice on privacy notices, see: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/.

**Obtaining consent**

Basing your processing of customer data on GDPR-compliant consent means giving individuals genuine choice and ongoing control over how you use their data, and ensuring your organisation is transparent and accountable.

Getting this right should be seen as essential to good customer service: it will put people at the centre of the relationship, and can help build customer confidence and trust. When relying on consent, your method of obtaining it should:

- be displayed clearly and prominently;
- ask individuals to positively opt-in, in line with good practice; and
- give them sufficient information to make a choice. If your consent mechanism consists solely of an “I agree” box with no supporting information then users are unlikely to be fully informed and the consent cannot be considered valid.

In addition if you are processing information for a range of purposes you should:

- explain the different ways you will use their information; and
- provide a clear and simple way for them to indicate they agree to different types of processing. In other words, people should not be forced to agree to several types of processing simply because your privacy notice only includes an option to agree or disagree to all. People may wish to consent to their information being used for one purpose but not another.

ICO has published a guide to Direct marketing, drawn from the requirements of PERC: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

The following generic example of a consent statement takes account of ICO’s guidance on how to obtain consent.
When drafting a consent statement, bear in mind that:

- consent needs to be as easy to withdraw as it was to give: so if consent was given electronically, it would not be enough to provide a postal address on its own.
- SMS and telephone calls to mobiles should be separated out as the rules are different - rules for calling mobiles are the same as for any other phones (consent is not needed, but you need to screen against TPS and internal suppression list). However SMS rules are the same as email rules (covering prior consent or soft opt-in).
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.
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/](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>Organization</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><a href="mailto:andrew.horsley@cirencester-friendly.co.uk">andrew.horsley@cirencester-friendly.co.uk</a></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. Their main GDPR page is https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

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 has established a new online training portal with Skillcast; this has an extensive library of training that members can use, including a free GDPR training template here
- ICO’s support for smaller businesses has now been rolled out; for more information, see: https://ico.org.uk/for-organisations/business/
- One aspect of the GDPR that we have not covered extensively elsewhere in the Guide is profiling where, as stated above, the use of solely automated processing is largely prohibited under GDPR. 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.daceachcroft.com/en/gb/articles/2016/june/gdpr-deep-dive-profiling-in-the-insurance-industry/
- ICO has published draft guidance on Children and the GDPR, and seeks comments by 28 February. This will affect many AFM members; see: https://iconewsblog.org.uk/2017/12/21/ico-seeks-comment-on-draft-children-and-gdpr-guidance/
- ICO has updated its guide to the GDPR, and has a page which may be useful to bookmark on What’s New: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/
- ICO has produced an updated Guide to its fees structure, and the basis for the fees payable by firms from 25 May onwards (and the conditions for the exemptions it provides): https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf
### Planning for GDPR: gap analysis and implementation plan, v. March 2018

This grid provides an overview of 13 key requirements in the GDPR, and 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.

<table>
<thead>
<tr>
<th>New GDPR Requirement</th>
<th>Any Significant Changes?</th>
<th>What Work is Required?</th>
</tr>
</thead>
</table>
| **1 Data Protection Principles** | No                       | 1. Review current Data Protection policies, codes of conduct and training to ensure these are consistent with the revised principles.  
2. Undertake an information audit to understand what data is held, where it is held, in what format it is held, where it is obtained from, basis for holding it (consent/legal basis).  
3. Identify means to “demonstrate compliance” i.e. How we are meeting the requirements, following codes of conduct as they are issued, paper trails of decisions relating to data processing and, where appropriate, privacy impact assessments. |
| The Data Protection Act principles are revised down to six, which are broadly similar to the current principles: |                          |                                                                       |
| • fairness, lawfulness and transparency;  
• purpose limitation;  
• data minimisation;  
• data quality;  
• security;  
• integrity and confidentiality. |                          |                                                                       |
| A new accountability principle makes Data Controllers responsible for demonstrating compliance with the Data Protection principles. |                          |                                                                       |
New GDPR requirement | Any significant changes? | What work is required? | Team/ Dept/ System | Owner
--- | --- | --- | --- | ---
2. Lawfulness of processing/ further processing | Yes | 1. Ensure we are clear about the grounds for lawful processing; check these will still be applicable under the GDPR. 2. Review information sharing agreements for any that rely on legitimate interests and amend, to show either proper legislative basis or consent. 3. Where relying on consent, ensure quality of consent meets new requirements i.e. clear, unambiguous, and properly recorded. 4. Consider whether new rules on children’s data are likely to affect us (more under point 4) 5. Is consent appropriate? If the processing is something the organisation “has” to do, consent is unlikely to be appropriate 6. Ensure that internal governance processes will enable us to demonstrate how decisions to use data for further processing purposes have been reached, and that all relevant factors have been considered. | | |

The grounds for processing personal data under the GDPR are broadly the same as now.

However, there are new limitations on the use of consent and the processing of children’s data (see sections 3 and 4 below).

There are specific restrictions on the ability to rely on “legitimate interests” as a basis for processing and some clarification as to when this may be used.

There is a non-exhaustive list of factors to be taken into account when determining whether the processing of data for a new purpose is incompatible with the purposes for which the data was initially collected.

Consent is more restrictive.

It is now much more important to select the appropriate lawful basis for processing before you begin, as you cannot change it once you have decided, and what you choose will have knock on effects, such as which rights apply to the processing (for example, data portability only applies to processing based on consent or contract).
<table>
<thead>
<tr>
<th>New GDPR requirement</th>
<th>Any significant changes?</th>
<th>What work is required?</th>
<th>Team/ Dept/ System</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3 Consent</strong></td>
<td>Yes: Article 4(8) of GDPR defines “the data subject’s consent” as “any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, which signifies agreement to personal data relating to them being processed”.</td>
<td>Complete review of the consent process. Need to be sure where we are relying on consent as the basis for lawful processing, that:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consent is subject to additional conditions under the new GDPR:</td>
<td></td>
<td>• consent is active, and does not rely on silence, inactivity or pre-ticked boxes;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• There is an effective prohibition on consents and the offering of services which are contingent on consent to processing.</td>
<td></td>
<td>• consent to processing is distinguishable, clear, and is not “bundled” with other written agreements or declarations;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• However, this remains a live issue, particular for special category data on the basis of consent, and there are amends for insurers proposed in the latest version of the Data Protection Bill</td>
<td></td>
<td>• supply of services cannot be made contingent on consent to processing which is not necessary for the service being supplied;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Consent must also now be separable from other written agreements, clearly presented and as easily revoked as given.</td>
<td></td>
<td>• data subjects are informed that they have the right to withdraw consent at any time, but that this will not affect the lawfulness of processing based on consent before its withdrawal;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• there are simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• separate consents are obtained for distinct processing operations; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• the organisation does not rely on consent where there is a clear imbalance between the data subject and the controller (especially if the controller is a public authority).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Need to look at how consent is captured and stored. How can users withdraw consent and for this to be actioned within systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New GDPR requirement</td>
<td>Any significant changes?</td>
<td>What work is required?</td>
<td>Team/ Dept/ System</td>
<td>Owner</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------</td>
<td>------------------------</td>
<td>-------------------</td>
<td>-------</td>
</tr>
<tr>
<td>4 Children</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Children</td>
<td>The current Act does not contain any specific restrictions on processing children’s data, and rules on children’s ability to consent have been drawn from national laws.</td>
<td>1. This is likely only to affect us if we are offering what the new act describes as “information society services directly to children”. This might include social media type services, or any online service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Children</td>
<td>The major provision in relation to children is Article 8, which requires parental consent to be obtained for information society services offered directly to a child under the age of 16 – although this ceiling can be set as low as 13 by a Member State, and only applies where the processing would be based on the child’s consent.</td>
<td>2. We will need to assess which national rules will apply in terms of age and ensure that appropriate parental consent mechanisms are implemented, including verification processes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Children</td>
<td>The controller is also required, under Article 8(1a) GDPR, to make “reasonable efforts” to verify that consent has been given or authorised by the holder of parental responsibility in light of available technology. This only affects certain online data – offline data will continue to remain subject to usual Member State rules on capacity to consent.</td>
<td>3. Keep a watching brief of national legislation for offline data processing relating to children’s data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Children</td>
<td>Article 8(1) is also not to be considered as affecting the general contract law of Member States regarding the validity, formation or effect of a contract with a child.</td>
<td>4. Where products and services are offered directly to a child, ensure notices are drafted clearly with a child’s understanding in mind.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Children</td>
<td>Organisations will still need to consider UK laws.</td>
<td>5. Even where specific children’s provisions do not apply, data controllers still need to consider the age of the data subject into account, for example when deciding what would be within their reasonable expectations and in appropriately wording their privacy notice.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New GDPR requirement</td>
<td>Any significant changes?</td>
<td>What work is required?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>-----------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Sensitive data and lawful processing</td>
<td>Genetic data (new); and biometric data where processed to uniquely identify a person (new). Interestingly, data relating to criminal convictions and offences are not categorised as “sensitive” for the purposes of GDPR. The rules under the GDPR in relation to data concerning criminal convictions and offences provides that such data may be processed only under the control of official authority or where the processing is authorised by Union law or Member State law that provides adequate safeguards.</td>
<td>1. Ensure we have clarity about the grounds relied on when processing sensitive/ special categories of data, and check these grounds will still be applicable. 2. Where relying on consent, ensure the quality of consent meets new requirements in relation to the collection of consent (see section 3 above) 3. Consider whether rules on children are likely to affect us, (see section 4 above). 4. If we process substantial amounts of genetic, biometric or health data, ensure we keep up-to-date on national developments as Member States have a broad rights to impose further conditions – including restrictions – on the grounds set out in the GDPR.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Conditions for processing criminal record/offence data are in the DP Bill. Any of the additional conditions within the Bill for processing special category data also apply to criminal records, along with some extra conditions specifically for criminal records.**
<table>
<thead>
<tr>
<th>New GDPR requirement</th>
<th>Any significant changes?</th>
<th>What work is required?</th>
<th>Team/ Dept/ System</th>
<th>Owner</th>
</tr>
</thead>
</table>
| **6 Privacy Notices** | Article 13 and 14 now lay out exactly what must be in privacy notice, so in practice privacy notices may be bigger. | 1. Audit existing privacy notices, review and update them. Look at the ICO guidance on this.  
2. For data which is collected indirectly, ensure that a notice is given at the appropriate time i.e. websites  
3. Work with relevant partners who may collect data on our behalf to assign responsibility for notice review, update and approval. | | |
<table>
<thead>
<tr>
<th>New GDPR requirement</th>
<th>Any significant changes?</th>
<th>What work is required?</th>
<th>Team/Dept/System</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Subject access, rectification and portability</td>
<td>We need to provide confirmation whether his/her personal data are being processed:</td>
<td>1. Review the organisation’s processes, procedures and training – are they sufficient to understand the SAR rights as this will impact on time and compliance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• to access the data (i.e. to have a copy); and</td>
<td>2. Develop template response letters, to ensure that all elements of supporting information are provided i.e. covering the detailed supporting information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• to be provided with supplemental information about the processing.</td>
<td>3. Can we provide data in a portable format (CSV etc). It may be necessary to develop formatting capabilities to meet access requests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>As with all data subject rights, the controller must comply “without undue delay” and “at the latest within one month”, although there are some possibilities to extend this.</td>
<td>4. Consider if the data relates to more than one data subject and how to address the difficulties this raises</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The controller must also use reasonable means to verify the identity of the person making the request – but must not keep or collect data just so as to be able to meet subject access requests.</td>
<td>5. Consider developing data subject access portals, to allow direct exercise of subject access rights.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>These points are particularly pertinent to online services.</td>
<td>6. Ensure that the function is adequately resourced and able to meet the one month response timescale.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Any charge for data access to be removed.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data controllers must, on request:

- confirm if they process an individual’s personal data;
- provide a copy of the data (in commonly used electronic form in many cases); and
- provide supporting (and detailed) explanatory materials.

Data subjects can demand that their personal data be ported to them or a new provider in machine readable format if the data in question was:

1) provided by the data subject to the controller;
2) is processed automatically*;
3) is processed based on consent or fulfilment of a contract.

The request must be met within one month (with extensions for some cases) and any intention not to comply must be explained to the individual.

Access rights are intended to allow individuals to check lawfulness of processing and the right to a copy should not adversely affect the rights of others.

* This includes data that the data subject “generates” through their activity, such as a transaction history in a bank account, listening history in a music service or data recorded by a telematics box on a car about the way an individual is driving.
**New GDPR requirement** | **Any significant changes?** | **What work is required?** | **Team/ Dept/ System** | **Owner**
--- | --- | --- | --- | ---
**8 Right to object** | | | | |
There are rights for individuals to object to specific types of processing:
- Direct marketing;
- Processing based on legitimate interests or performance of a task in the public interest/exercise of official authority; and
- Processing for research or statistical purposes.

Only the right to object to direct marketing is absolute (i.e. no need to demonstrate grounds for objecting, no exemptions which allow processing to continue).

There are obligations to notify individuals of these rights at an early stage – clearly and separately from other information.

Online services must offer an automated method of objecting.

This right has changed from section 10 of the new Data Protection Act. It is now restricted to the legitimate interests or performance of a public task lawful basis (which is not the case under the DPA '98). Also, this right can now be enforced directly by the ICO; under the DPA '98 an individual would need to go to court to enforce a section 10 request.

In practice, the default position is now that the organisation will have to comply with the request unless it can demonstrate that it is justified in not doing so. This is a change from the current situation under the DPA98, where the individual would need to demonstrate that they were suffering unwarranted damage or distress to enforce a request to stop processing.

1. Audit privacy notices and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of ‘first communication’.
2. For online services, ensure there is an automated way for this to be effected.
3. Review marketing suppression lists and processes (including those operated on behalf of the organisation by partners and service providers) to ensure they are capable of operating in compliance with the GDPR.
<table>
<thead>
<tr>
<th>New GDPR requirement</th>
<th>Any significant changes?</th>
<th>What work is required?</th>
<th>Team/ Dept/ System</th>
<th>Owner</th>
</tr>
</thead>
</table>
| **9 Right to erasure and restrict processing**                | Yes                      | 1. Ensure that members of staff and suppliers who may receive data erasure requests recognise them and know how to deal with them.  
2. Determine if systems are able to meet the requirements to mark data as restricted whilst complaints are resolved, or indeed to delete data required. |                    |       |

More extensive rights are introduced: a right to be forgotten (now called erasure) and for processing to be restricted. Individuals can require data to be 'erased' when there is a problem with the underlying legality of the processing or where they withdraw consent.

The individual can require the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved, or if the processing is unlawful but the individual objects to erasure.

Controllers who have made data public which is then subject to a right to erasure request, are required to notify others who are processing that data with details of the request. This is a new wide-ranging and challenging obligation.
New GDPR requirement | Any significant changes? | What work is required? | Team/ Dept/ System | Owner |
|------------------------|------------------------|-----------------------|------------------|-------|
| **10 Governance obligations** | Yes | 1. The organisation needs to assign responsibility and budget for data protection compliance.  
2. Organisation may need to appoint a DPO and make arrangements for reporting structures, i.e. the need for the DPO to be autonomous, how this sits with other workloads etc.  
3. Supervisory authorities will expect a line direct to the board/ senior management and the job specification for those designated with DPO responsibilities will need to be created.  
4. The DPO will need to ensure that a full compliance programme is designed incorporating features such as: Privacy Impact Assessments, regular DP audits, policy reviews and updates, and training and awareness raising programmes.  
5. Audit existing supplier arrangements and update template RFQ’s and procurement contracts to reflect the GDPR’s data processor obligations.  
6. Monitor the publication of supervisory authorities / EC and industry published supplier terms and codes of practice to see if they are suitable for use by the organisation.  
7. **Need to keep written records of processing activity.** | | | | |
<table>
<thead>
<tr>
<th>New GDPR requirement</th>
<th>Any significant changes?</th>
<th>What work is required?</th>
<th>Team/ Dept/ System</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 Privacy by design</td>
<td>Some</td>
<td>Adopting appropriate staff policies is specifically mentioned, as is the use of pseudonymisation (to ensure compliance with data minimisation obligations).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*It is now an expectation under the GDPR that organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into their data processing activities.*

*Privacy Impact Assessments are an important part of taking a privacy by design approach.*
### New GDPR requirement

**12 Breach notification**

In case of an incident defined as:

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

In some circumstances you need to notify data subjects (where breach poses a "high risk" to data subjects). AFM members must consider their procedures for doing this.

- GDPR provides only 72 hours to notify of a breach.
- There are larger fines for breaches, though there may be an exemption if:
  - The breach is unlikely to result in a risk for the rights and freedoms of individuals;
  - Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or
  - This would trigger disproportionate efforts (instead a public information campaign or "similar measures" to notify data subjects should be relied on so that affected individuals can be effectively informed)

A breach is still reportable even if the appropriate technical and organisational measures are in place.

There is no "disproportionate effort" exception for notifying the ICO.

---

<table>
<thead>
<tr>
<th>New GDPR requirement</th>
<th>Any significant changes?</th>
<th>What work is required?</th>
<th>Team/ Dept/ System</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>12 Breach notification</strong></td>
<td>GDPR provides only 72 hours to notify of a breach.</td>
<td>Develop and update internal breach/ incident notification procedures, including incident identification processes and incident response plans.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>There are larger fines for breaches, though there may be an exemption if:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The breach is unlikely to result in a risk for the rights and freedoms of individuals;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- This would trigger disproportionate efforts (instead a public information campaign or “similar measures” to notify data subjects should be relied on so that affected individuals can be effectively informed)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A breach is still reportable even if the appropriate technical and organisational measures are in place.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is no &quot;disproportionate effort&quot; exception for notifying the ICO.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Fines not just for data breaches but for any contravention of the GDPR. Data breaches actually fall into the lower category of fines (10million Euros or 2% annual global turnover, whichever is higher)
<table>
<thead>
<tr>
<th>New GDPR requirement</th>
<th>Any significant changes?</th>
<th>What work is required?</th>
<th>Team/ Dept/ System</th>
<th>Owner</th>
</tr>
</thead>
</table>
| **13 Transfer of personal data outside the EU** | No | 1. Review questions included in standard procurement templates and contract clauses to ensure that information about a supplier’s proposed transfer of personal data for which you are responsible is understood and conducted in a compliant way.  
2. Contractual clauses may need redrafting.  
3. Review where appropriate Binding Corporate Rules and Standard Contractual Clauses; for more see:  
| | | | | |
| Transfers of personal data to recipients in “third countries” (i.e. outside of the European Union) continue to be regulated and restricted in certain circumstances. | | | | |
| Breach of the GDPR’s data transfer provisions is identified in the band of non-compliance issues for which the maximum level of fines can be imposed (up to 4% of annual turnover). | | | | |