UK Data Protection Regulation

Maintenance & Review Guidelines

A practical guide for members of AFM

Version: 2

Date: October 2020

Definitions of key terms in the GDPR and Data Protection Act 2018

Term	Meaning
Consent	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
Data Controller	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
Data Processor	A natural or legal person, public authority, agency or other body who Processes Personal Data on behalf of the Data Controller
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction
Data Subject	The identified or identifiable natural living person to which the Personal Data refers. Examples include customers and web users, individuals on email or marketing databases, employees, contractors or suppliers
Legitimate Interests	A lawful basis for organisations to Process Personal Data without obtaining Consent from the Data Subject. However, the interests of the Data Controller must be balanced with the interests and fundamental rights and freedoms of the Data Subject
Personal Data	Any information (including opinions and intentions) which relates to an identified or identifiable natural living person, or other forms of identifier such as IP address
Personal Data Handlers	Staff of the Data Controller who have been given responsibility for handling Personal Data as part of their operational activities
Privacy Notice	A statement or document that discloses the ways an organisation gathers, uses, discloses and manages a customer's Personal Data
Process, Processing, Processed	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
Specialist Category Data	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 living person, data concerning health or data concerning a natural living person's sex life or sexual orientation
Third Country	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
Third Party	Any outside organisation with which your organisation has either previously, or currently conducts business, includes business partners, vendors, suppliers and service providers.

Contents

Note

The Guide to Implementing the GDPR was first produced in 2018 by a working group of the Association of Financial Mutuals. It was written for members of AFM, using best judgement, at the time of writing, to identify the implications of the General Data Protection Regulation (GDPR).

The GDPR framework has continued to evolve after implementation and this updated version of the original Guide reflects more recent developments and guidance offered by the Information Commissioner's Office and experiences from the mutual sector.

Where necessary, this updated Guide is tailored to also meet the requirements of the Data Protection Act 2018 in the UK, and therefore may not reflect the legislation in other jurisdictions.

If you identify and inaccuracies or changes, or would otherwise like to comment, please email martin@financialmutuals.org.

This Guide is not intended to be an authoritative or full interpretation of the Data Protection Act 2018 or the GDPR.

Section 1: Introduction

Background and Purpose of the GDPR

The General Data Protection Regulation 2016/679 ("GDPR") has applied since 25 May 2018. Being a Regulation, not a Directive, and applying before the United Kingdom left the European Union, it had direct effect in the UK without the need for any other (UK) legislation, including during the transition period after Brexit (until 31 December 2020 at the time of writing). After this date, it is probable that it will remain part of UK law under the European Union (Withdrawal) Act, with some technical changes that are likely to make it work in a UK context (and is likely to be known as "UK GDPR").

The GDPR gives some scope for EU Member States to amend some parts of the Regulations (known as 'derogations'). Therefore, the Data Protection Act 2018 ("DPA 2018"), also effective from 25 May 2018, sits alongside the GDPR and sets out the data protection framework and law in the UK. The differences between the two are mostly subtle and, for the purpose of this guide, we refer to 'data protection' or the 'regulations'.

The Information Commissioner's Office ("ICO") is the UK agency responsible for overseeing data protection in the UK. For more information, see the remainder of this guide, and keep a regular eye on their website, which includes a range of toolkits to promote implementation and good practice: 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?

The regulations apply to 'personal data', meaning information that relates to an identified or identifiable living individual. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors. Single pieces of data that could be used in combination with other pieces of data to identify a specific individual are often referred to as Personally Identifiable Information ("PII").

If it is possible to identify a living individual directly from the information you are processing, then that information will be personal data.

An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals. For example, a name is a common means of identifying someone. However, whether any potential identifier identifies an individual depends on the context. In most cases, many people will share the same name and, usually, a combination of identifiers (PII) may be needed to identify an individual.

The key principles:

The GDPR sets out seven key principles:

- Lawful, fair and transparent processing – understanding the 'lawful basis' and honesty about the purposes for holding data
- Purpose limitation – requires clarity on what data is needed, and why
- Data minimisation – collecting only the data that is needed, and deleting anything that isn't

- Accuracy – including correcting and recording any mistakes and identifying matters of opinion
- Storage limitation – clarity on retention periods and erasure when data is no longer required
- Integrity and confidentiality – appropriate security measures
- Accountability – keeping records to demonstrate compliance and the role of the Data Protection Officer.

These principles must be central to a firm's approach to processing personal data. This guide is intended to help understand how to comply with these principles.

What is the aim of the GDPR?

The broad aim of the regulations is 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.

What are the rights of individuals?

In summary, individuals ("data subjects") have the right to the following:

- The right to be informed – i.e. about the personal data held and the processing carried out.
- The right of access – i.e. to obtain the personal data held on them.
- The right of rectification – i.e. to correct inaccurate or incomplete personal data.
- The right of erasure – not an absolute 'right to be forgotten', but essentially complete deletion of personal data, subject to the 'lawful basis for processing' (see below).
- The right to restrict processing – i.e. to block the processing of their personal data.
- The right to data portability – i.e. the right to obtain, move, copy or transfer their personal data from one IT environment to another in a safe and secure way.
- The right to object – i.e. the right to object to the processing of personal data, subject to the 'lawful basis for processing'.
- The rights in relation to automated decision-making and profiling – i.e. safeguards for individuals where firms make decisions without human intervention, if this personal data 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.

Top Tips!

- ✓ Firms should consider making available procedural guides for customer-facing staff with instructions on how to respond to requests under each of these rights.
- ✓ The procedural guides should include what is acceptable for customer identification verification before responding under any of these rights – otherwise data may fall into the wrong hands!
- ✓ Firms that process data for minors should specifically include any different processing methods in the relevant policies and procedures.

What does the 'lawful basis for processing' mean?

Under GDPR, processing shall be lawful only if and to the extent that at least one of the following applies (known as the *lawful basis for processing*):

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (we cover consent in more detail on page 8).
- 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.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- 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 data controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the data 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.

No single basis is better or more important - the most appropriate one to use will depend on the purpose the data is to be used for and the individual concerned.

Top Tips!

✓ It is worth bearing in mind that whilst each lawful basis is valid, consent can most easily be withdrawn, so other bases may be a better option – we cover consent in more detail on page 9.

What is 'Processing'?

Most uses of data will be considered 'processing', including collecting, recording, storing, using, analysing, combining, disclosing or deleting personal data.

What is the difference between a 'data controller' and a 'data processor'?

At a very high level, the data controller controls the procedures and purpose of the data use, and a data processor will process any data that the data controller gives them and should do so under their instructions.

The data controller will:

- Collect the personal data and must have legal authority to do so
- Decide what personal data to collect
- Be able to change or modify the personal data
- Decide where and how to use the personal data and towards what purpose

- Decide whether to keep the personal data in-house or to share it with third parties
- Decide how long the personal data is to be kept, and when and how to dispose of it.

The data processor will:

- Receive personal data from the data controller, or be told what data to collect
- Follow instructions from the data controller regarding the processing
- Store personal data gathered by the data controller
- Not be able to make any of the decisions above that rest only with the data controller.

The regulations apply to both data controllers and data processors, but place different obligations on each of them (with greater obligations on the data controller), so it is important to identify which of the two apply. In some cases, the boundaries can be blurred, making it confusing to figure out if a party is the data controller or the data processor. Further, there are also instances where a party can be both the data processor and the data controller, and other circumstances where there may be joint controllers! The parties should formalise responsibilities under a contract to reduce the risk of compliance breaches.

Key Steps in complying with the GDPR

1 Awareness
You should make sure that decision makers and key people in your organisation are aware of the impact of the regulations and ICO guidance on business operations.

2 Information you hold
You should document what personal data you hold, where it came from, who you share it with and keep it up to date. You should consider regular information audits.

3 Communicating and reviewing privacy information
You should review your current data protection policies and privacy notices regularly to ensure compliance with ICO guidance.

4 Individuals' rights
You should ensure newly developed procedures or processes cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Data Subject Access Requests
You should have a clear plan for how you will handle requests within the maximum one-month timescale, recognising these can be very time consuming.

6 Lawful basis for processing personal data
You should periodically review if the lawful basis for your processing activity is correct, document it and, if necessary, update your privacy notice.

7 Consent
You should periodically review how you seek, record and manage consent and whether you need to make any changes.

8 Children
You should periodically review systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches
You should send reminders on procedures in place to detect, report and investigate a personal data breach. Does the volume of breach reports meet expected numbers? If not, why not? (see page 14)

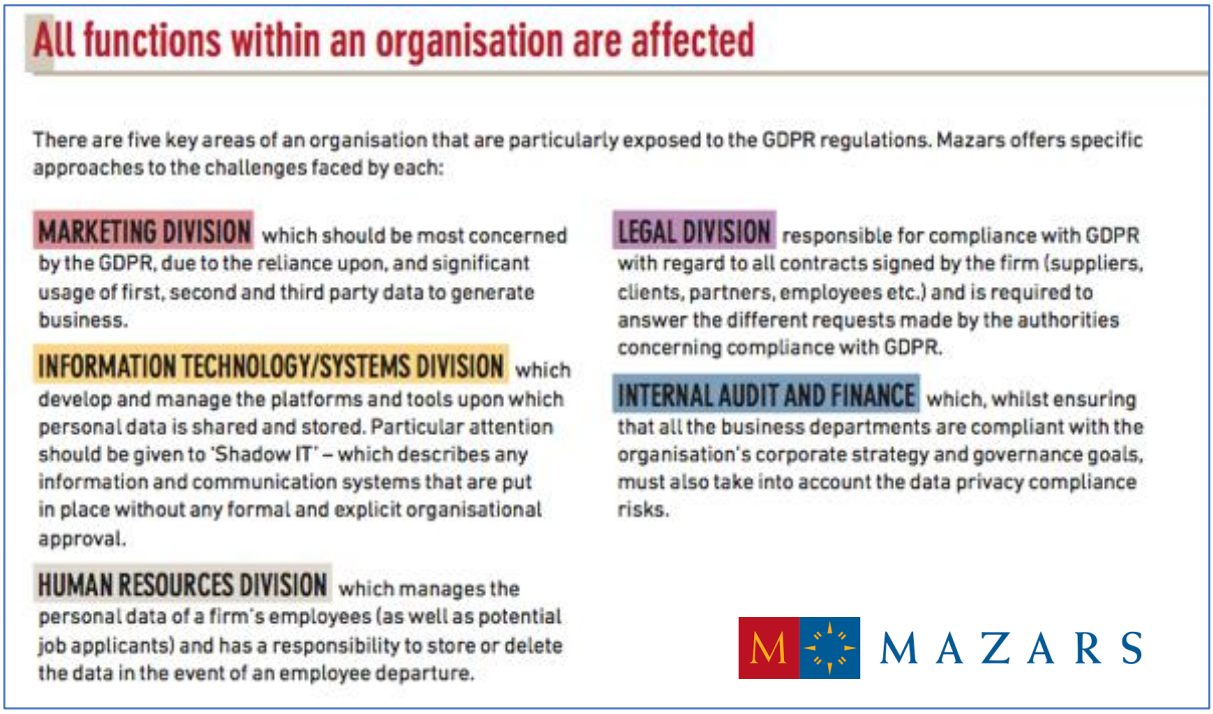
10 Data Protection by Design and Data Protection Impact Assessments
Are you carrying out Data Privacy Impact Assessments? Are people clear when to implement them in your organisation? (see page 14)

11 Data Protection Officer
If your organisation's structure and governance arrangements have changed, have you considered whether you are required to formally designate a Data Protection Officer, or it would be desirable to do so?

12 International
If your organisation intends to start operating in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. The EU's Article 29 Working Party guidelines will help you do this.

Section 2: Interpretation for AFM members

The regulations have important consequences for AFM members. As the chart below demonstrates, the impact will be widely felt across the organisation.



Further detail on lawful basis and when to obtain consent

You must have at least one of six valid lawful bases to process personal data (see page 5). It is important to determine the lawful basis before you begin processing, and you should document it when implementing new systems (usually in a data protection impact assessment). It is not always easy to swap to a different lawful basis at a later date without good reason (particularly when relying on consent).

As a reminder, some key points are:

- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category (e.g. medical) data or criminal record data, you need to identify both a lawful basis for general processing and an additional condition for processing these types of data.

The lawful basis for processing will determine which rights customers will be able to use, such as the right to erasure.

When should we use 'consent'?

There can be a tendency to think of consent as the best lawful basis, but this is not the case (and can make life more difficult than necessary for customers). This is because mechanisms to obtain consent must meet requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn. The key points are as follows:

- *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.
- *Active opt-in*: pre-ticked opt-in boxes are invalid – you should use unticked opt-in boxes or similar active opt-in 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 regulations.
- *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).

However, when processing special category data (see page 11), consent is often the most appropriate lawful basis to use, but there are exceptions. The ICO's consent checklist sets out the steps you should take to seek valid consent under the regulations:

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. This also means that, where possible, we provide a consistent service to individuals, regardless of their consent preferences.

What are the other lawful bases, and when should they be used?

When processing does not require consent, at least one of the following lawful bases must be identified:

- **Contract:** This applies when the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. Clearly many financial services firms and mutual societies will often find this is the most appropriate lawful basis for their processing due to the contractual agreements between firms and their customers or employees. However, if the processing includes special category data, consent will also be required in relation to that data (unless another separate condition can be relied upon). Special care must also be taken when using this lawful basis for contracts with children under 18.
- **Legal obligation:** This can be used when the processing is necessary for you to comply with the law (not including contractual obligations). This has some application for mutual societies, for example to disclose employee information to HMRC in compliance with employment law.
- **Vital interests:** This applies when the processing is necessary to protect someone's life. This is unlikely to be used by mutual societies.
- **Public task:** This can be used if the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. This also is unlikely to be used by mutual societies
- **Legitimate interests:** This can be helpful if the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. It is usually used where you use data in ways that people would reasonably expect and that have a minimal impact on their privacy. It is useful for mutual societies in their marketing activities or sometimes if processing children's data.

  The ICO recommends considering the following questions before deciding upon the legitimate interest basis:

- **Purpose test:** Are you pursuing a legitimate interest?
- **Necessity test**: Is the processing necessary for that purpose?
- **Balancing test:** Do the individual's interests override the legitimate interest?

Top Tips!

✓ When using legitimate interest as a lawful basis, fully document the analysis and reasons for deciding on its use, and why other lawful bases were not appropriate.

Special Category Data

The following data is classified as special category data and stricter regulations are in place reflecting the higher risk when processing this data:

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions
- Personal data revealing religious or philosophical beliefs
- Personal data revealing trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation.

Mutual societies processing health data should be aware that a very broad range of information is in the special category, including medical opinions and sometimes appointment details and invoices.

It is commonly thought this includes personal data about criminal allegations, proceedings or convictions. This is not the case, but separate rules apply instead that require lawful authority.

The DPA 2018 provides a list of 'conditions for processing' that have to apply for using special category data. This means that one of the lawful bases must apply and one of the conditions, usually 'explicit consent'. However, in some circumstances, such as fraud investigations, it will be impossible to obtain consent without tipping off a customer and, in such cases, mutual societies may be able to rely on the 'substantial public interest' condition that permits processing of special category data for insurance purposes (subject to a company policy that outlines the measures taken).

A risk assessment (see section 4) is necessary prior to processing special category data.

Appointing a Data Protection Officer

Under the regulations, 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.

When determining if processing is on a large scale, the ICO guidelines say you should take the following factors into consideration:

- The numbers of data subjects concerned
- The volume of personal data being processed
- The range of different data items being processed
- The geographical extent of the activity
- The duration or permanence of the processing activity.

Mutual societies should make a decision regarding the appointment of a DPO based on the guidance that is available, and documented their logic for that decision. Even if a data controller decides not to appoint an "official" DPO, we would strongly recommend that there is a clear understanding within the organisation of who is responsible for monitoring and reporting on 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.

Marketing

Marketing rules are drawn from the Privacy and Electronic Communications Regulations 2003 (PECR) and sit alongside the GDPR and DPA 2018. The PECR is currently being revised and will eventually be replaced by the new E-Privacy Regulation, although the extent of application in the UK will depend on how they are transposed after the Brexit transition period.

The PECR sets different consent requirements depending on the method of marketing (telephone, electronic mail) and whether the recipient is a business or individual. In many cases, mutual societies marketing to intermediaries should remember that some 'one-man bands' will probably use personal telephone and email addresses and the stricter rules for marketing to individuals will apply.

If consent for marketing is required, a suitable template consent form can be found in Appendix 1.

Top Tips!

- ✓ Review cookies procedure – what cookies are placed? Which are necessary? How long do they last and are they out of date? Is consent given explicitly before placement (except for those recording such consent)?
- ✓ Are all third-party cookies described in the cookies policy?

Section 3: Review compliance - ICO self-assessment

Compliance against the regulations should be periodically verified against the ICO's self-assessment tool. A risk-based approach should be taken when setting the review period that best suits a firm.

There are currently eight self-assessment tools on the ICO website which you can link from here:

Small business owner & sole trader self-assessment: Recommended for first time users. Assess your high-level compliance with the DPA 2018. Includes registration, fair processing, subject access, data quality, accuracy and retention.
Start now

Information security checklist: 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 checklist: Assess yourself in the areas of consent and bought-in lists, and telephone, electronic and postal marketing.
Start now

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

Data sharing and subject access checklist: Data sharing policy and agreements, compliance monitoring, maintaining sharing records, registration and subject access process.
Start now

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

Data processor's checklist: Helps you to assess the compliance of processors, the rights of individuals and data breaches.
https://ico.org.uk/for-organisations/data-protection-self-assessment/processors-checklist/

Data controller's checklist: Helps you to assess the compliance of controllers, the rights of individuals and data breaches
https://ico.org.uk/for-organisations/data-protection-self-assessment/controllers-checklist/

Section 4: Ongoing Communications within the business

Regardless of whether a firm appoints a DPO, the business areas will need to play their part in complying with the regulations. In this section, we explore some areas that require a team approach to staying compliant.

Data Security Breaches

All organisations must report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach. Additionally, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

This requires mutual societies to have robust breach detection, investigation and internal reporting procedures in place. Decisions on whether or not the ICO and affected individuals have been informed must be recorded.

Processes to comply with the breach reporting requirements should be reviewed regularly and refresher training provided to relevant areas. ICO has published a useful guide: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

You should be able to respond positively to the following – '*if a breach is reported at 5pm on a Friday, could we send notification in the required timescale*?'

Top Tips!

- ✓ Record all breach reports – regardless of whether any action was taken, or reporting was required
- ✓ Consider also recording 'near-misses' to learn from what could have happened and improve processes or highlight training needs

Data Protection Privacy Impact Assessment (DPIAs)

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 DPIA will enable organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might occur otherwise.

The ICO has published a guide to help organisations undertaking a DPIA: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

When do I need to conduct a DPIA?

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. This is especially relevant when processing health or other special category data

The ICO recommends that DPIAs are carried out in any circumstances where there may be an impact on individuals' privacy. It is a good habit to get into.

Privacy statement for customers (Privacy notice)

You will need to periodically review existing privacy notices to ensure that they comply with current good practices.

The regulations say 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 ICO website provides a template privacy notices for organisations to tailor for their own needs (see appendix 2).

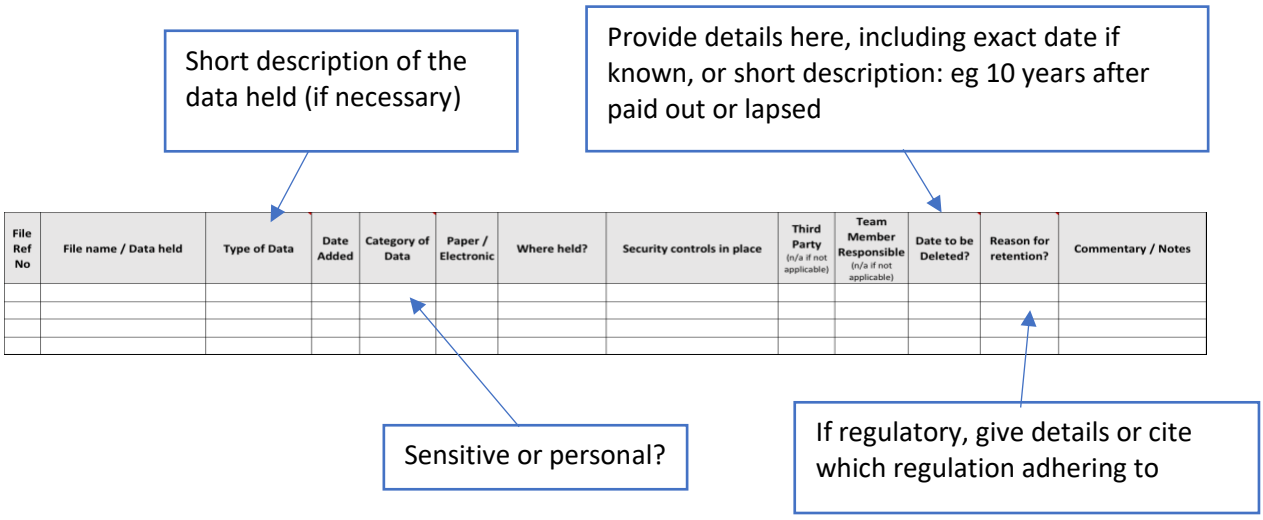
Top Tips!

✓ Each of the eight rights should be explained in a privacy notice
✓ Many firms include a privacy notice for employees and directors in their staff handbook

Updating the data inventory

Organisations should maintain a data inventory and review it on a regular basis. Article 30 of the GDPR requires both controllers and processors to maintain a record of processing activities under its responsibility, and lists the information required to be held.

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



Larger businesses, as an alternative (or complimentary) approach to a data inventory, may wish to set up an Information Asset Register.

The National Archives define an information asset as: "*A body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles*."

Further information on Information Asset Registers is available at: https://www.nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf

Top Tips!

- One of the data protection principles is 'storage limitation' – organisations should not keep data for longer than needed and justify how long that period is. The data inventory (or Information Asset Register) is often a good place to record such decisions.

Training

Many areas of the business will be involved in data protection and firms should also be able to show that they have implemented and adhered to relevant policies. This could include raising awareness by training, monitoring and audits.

Refresher training is essential – particularly for customer-facing staff that may need to respond to a customer exercising their rights or to report data breaches (and near-misses).

Top Tips!

- Consider the training needs of all members of staff, regardless of seniority. Include Non-Executive Directors in the assessment.
- Users of the AFM online training portal, supplied by Skillcast, can undertake the GDPR training modules.

IT – Remote Working

At the time of writing, many firms have a large number of employees working from home in response to the coronavirus pandemic. This could create challenges for data protection.

Mutual societies should note that data protection legislation has not changed during this period, although the ICO may be taking a more flexible and pragmatic approach in enforcing the regulations.

IT challenges may be more apparent, and organisations should consider:

- Logging all faults and errors centrally
- Documenting all firewall rules
- Documenting a standard build configuration (hardware, software, servers, systems)
- Monitoring capacity management, for future planning.

It may also be a good idea to consider providing guidance to remind staff that printed documentation or hard copies should be used, stored and disposed of in line with this guidance and GDPR regulations.

Cookies

Whilst covered mainly by the PECR, there are new cookies' requirements related to GDPR. Cookies will be valid only where consent is freely given, specific and informed (the GDPR definition of consent). It must involve some form of unambiguous positive action – for example, ticking a box or clicking a link – and the person must fully understand that they are giving you consent. You cannot show consent if you only provide information about cookies as part of a privacy policy that is hard to find, difficult to understand, or rarely read. Similarly, you cannot set non-essential cookies on your website's homepage before the user has consented to them. Please see the ICO page (below) for more information.
https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

Section 5: Keeping up to date

The best source of information is of course the ICO website. Their main GDPR page is: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

It provides regular news articles, blogs and tweets (@ICOnews), and provides 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/.

Brexit – what can we expect?

Good question! It's too early to say exactly what will change after the transition period. The UK government has indicated it will transpose and merge the GDPR into UK legislation ("UK GDPR"), but little information is currently available. At present, personal data can continue to be processed in the EU, but following the transition period, there will be limitations on the transfer of data to the UK without an adequacy decision.

Keep reading updates from the AFM as more information and guidance will be sent to members in due course.

Appendix 1 – Consent Form

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

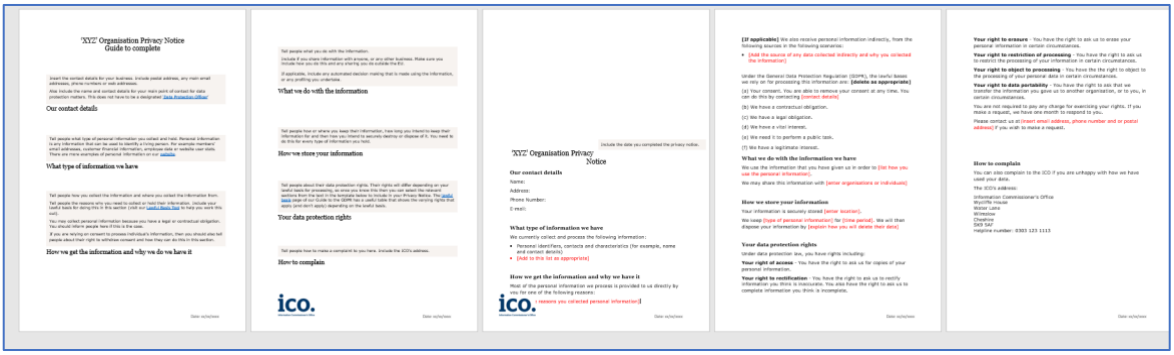
If you're happy to receive marketing information from NAME OF FIRM, please let us know how you prefer to be contacted. You can tick as many of the boxes below as you wish. If you do not wish to be added to our marketing list, simply leave the tick boxes empty.
Please detach and return the slip below 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....☐
Telephone (home)....☐
Email....☐
Telephone (Mobile – including SMS/ MMS)...☐

Appendix 2 – ICO Draft Privacy Notice


'XYZ' Organisation Privacy Notice
Guide to complete
Our contact details
What type of information we have
How we get the information and why we do we have it
What we do with the information
How we store your information
Your data protection rights
How to complain
ico.
'XYZ' Organisation Privacy Notice
Our contact details
What type of information we have
How we get the information and why we have it
ico.
What we do with the information we have
How we store your information
Your data protection rights
Your right to erasure
Your right to restriction of processing
Your right to object to processing
Your right to data portability
How to complain