Helpful information derived from the ICO guidelines for the General Data Protection Regulation – some things you may need to know and consider before 25th May 2018.

What is GDPR?

The General Data Protection Regulation applies to data processing carried out by organisations operating within the EU and those who have day-to-day responsibility for data protection. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR stipulates how 'personal data' **and/or** 'sensitive personal data' should be processed within organisations.

What is personal data?

Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This includes name, identification number, location data or an online identifier.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

What is sensitive personal data?

This is the processing of personal data which is more sensitive and needs more protection. There are "special categories of personal data" which include 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 (see Article 9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).

How to find out what personal data you use and hold?

Doing an information audit or data-mapping exercise can help you find out what personal data your organisation holds and where it is.

You can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of your organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts and agreements.

When documenting your findings, the records you keep must be in writing. The information must be documented in a granular and meaningful way.

If you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records.

6 Data Protection Principles to fulfil when processing data

Under the GDPR, the data protection principles set out the main responsibilities for organisations when processing personal data.

The full description of these principles can be found in Article 5 of the GDPR but are summarised in short below:

a) processed lawfully and fairly;

b) collected for specified, explicit and legitimate purposes

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

f) processed in a manner that ensures appropriate security of the personal data

The role of data ‘controllers’ and ‘processors’

The GDPR applies to data ‘controllers’ **and** ‘processors’ where; a controller determines the purposes and means of processing personal data; and a processor is responsible for processing personal data on behalf of a controller.

Data controllers

A controller determines the purposes and means of processing personal data. The controller will be responsible for, and be able to demonstrate compliance with the data protection principles.

This includes the new rights of individuals, handling subject access requests, consent, data breaches, and designating a data protection officer.

Whenever a controller uses a processor it needs to have a written contract in place so that both parties understand their responsibilities and liabilities.

If you are a controller, where a processor is involved – you need to ensure your contracts with processors comply with the GDPR.

Data processors

A processor is responsible for processing personal data on behalf of a controller.

Processors must only act on the documented instructions of a controller set out in the contract. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

Processors will have some direct responsibilities under the GDPR. They are required to maintain records of personal data and processing activities and may be subject to fines or other sanctions if they don't comply. They will therefore have legal liability if they are responsible for a breach.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

Contractual agreement between controllers and processors

Whenever a controller uses a processor it needs to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities.

The contract is also important as controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

The GDPR sets out what needs to be included in the contract such as the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subject; and the obligations and rights of the controller. It also defines a number of compulsory terms which the processor has to adhere to.

Processors as well as controllers will be liable to pay damages or be subject to fines or other penalties.

The need to document data processing activities

Controllers and processors both have documentation obligations.

You must maintain records (documentation) on your processing activities such as processing purposes, data sharing and retention as you may be required to make the records available to the ICO on request.

Records must be kept in writing but can be maintained electronically. These records must be kept up to date and reflect your current processing activities.

ICO have produced some basic templates to help you document your processing activities.

Who needs to document data processing activities?

- If you have 250 or more employees, you must document all your processing activities.
- If you have less than 250 employees, you only need to document processing activities that: are not occasional; or could result in a risk to the rights and freedoms of individuals; or involve the processing of special categories of data or criminal conviction and offence data.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.

6 Lawful bases for processing personal data

There are six available lawful bases for processing which are set out in Article 6 of the GDPR. You must have a valid lawful basis in order to process personal data and you should document it.

The lawful basic required to process personal data depends on the specific purposes and the context of the processing. You should consider which lawful basis best fits the circumstances. You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: 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.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: 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.

(f) Legitimate interests: 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

You need to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form

for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies.

You can choose a new lawful basis if you find that your old condition for processing is no longer appropriate under the GDPR, or decide that a different basis is more appropriate. This is however a one-off opportunity to bring your processing in line with the GDPR. Once the GDPR is in effect, you will not be able to swap between lawful bases at will if you find that your original basis was invalid. Take care to get it right first time.

Using 'Consent' as a lawful basis

Consent means offering individuals real choice and control. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent

The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.

If you decide consent is the lawful basis for processing personal data ensure that you record when and how you got consent from the individual and exactly what they were told at the time. Always keep evidence of consent and separate it from Terms and Conditions.

Check your consent practices and your existing consents. Name any third party controllers who will rely on the consent.

Refresh your consents if they don't meet the GDPR standard and keep consent under review.

Using 'Legitimate interests' as a lawful basis

Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.

Review your existing processing to identify your lawful basis and document where you rely on legitimate interests, update your privacy notice, and communicate it to individuals.

It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

There are three elements to the legitimate interests basis. You need to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – and if you don't need consent under PECR. See the Guide to PECR https://ico.org.uk/for-organisations/guide-to-pecr/ for more information on when you need to get consent for electronic marketing.

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them.

You must include details of your legitimate interests in your privacy notice.

Be aware of the 8 Individual rights

The GDPR also provides the following rights for individuals when you are processing their personal data.

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Informing individuals about their data processing

The GDPR sets out the information that you should supply and when individuals should be informed.

You must inform people upfront about your intended purposes for processing the personal data and your lawful basis for processing it, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data.

The GDPR requires the information to be provided in concise, easy to understand and clear language and this needs to be communicated to individuals by 25th May 2018.

Dealing with subject access requests

You should update your procedures and plan how you should deal with access requests as you will have a month to comply.

In most cases you will not be able to charge but you can charge or even refuse a request if the requests are manifestly unfounded or excessive. If you refuse a request you must tell the individual why and inform them that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this with undue delay and within one month.

Update your privacy notices

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice.

Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

You will need to explain your lawful basis (bases) for processing personal data in your privacy notice.

Ensure your means of processing data are secure

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

Ensure you keep your IT systems safe and secure. If you process or hold personal data on your IT system you need to assess the risks and threats to your business and implement security controls and measures to protect your data. These could include encrypting data, backups, secure network configuration, malware protection, anti-virus security and carrying out patch management and software updates.

What is a personal data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

You should make sure that your staff understands what constitutes a data breach, and that this is more than a loss of personal data. You should ensure that you have

an internal breach reporting procedure is in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

Do you need to appoint a Data Protection Officer?

The GDPR makes it a requirement that organisations 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.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

The DPO is the first point of contact for supervisory authorities and for individuals whose data is processes. The role includes advising the organisation and its employees about their obligations to comply with GDPR and data protection laws, monitoring compliance, training staff and conducting audits.

The DPO can be an existing employee and needs to report to the highest management level of your organisation – ie board level. The GDPR does not specify the precise credentials a data protection officer is expected to have but it does require that they should have professional experience and knowledge of data protection law which should be proportionate to the type of processing your organisation carries out.

Provisions for Automated individual decision-making and Profiling

Automated individual decision-making is a decision made by automated means without any human involvement.

The GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual).

Profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

You will need to have a lawful basis to carry out profiling and/or automated decision-making and document this in your data protection policy.

The GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

Promoting accountability and governance

The GDPR includes provisions that promote accountability and governance and you are expected to put into place measures that meet the principles of data protection.

You should implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.

Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Use good practice tools – Privacy by design and Privacy Impact Assessments

Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

The GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

Use a 'Privacy by design' approach for data protection compliance

Privacy by design is an approach to projects that promotes privacy and data protection compliance. The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

Identify privacy risks by conducting a Privacy Impact Assessment

Privacy Impact Assessments (PIAs) are an integral part of taking a privacy by design approach.

Privacy impact assessments (PIAs) are a tool that you can use to identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

You can integrate the core principles of the PIA process with your existing project and risk management policies. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy throughout your organisation.

If you want to find out more about PIA's, ICO have published a Code of practice for Conducting PIAs https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Special protection for children's personal data

The GDPR is bringing in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully.

Restriction on transferring data internationally

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards.

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

For the Information Commissioner's Office full Guide to the General Data Protection Regulation (GDPR) go to https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/