A guide to GDPR

WRIGHT HASSALL

CONTENTS

Getting
Data
Protection
Right

GDPR GENERAL COMPLIANCE

DATA PROTECTION FLOWCHART

1 RAISE AWARENESS

- Make sure the key people within your organisation are aware of the GDPR and of what effect the GDPR will have on your organisation.
- Arrange meetings between the people that will need to drive through the changes within your oganisation.
- Consider whether you need to allocate resources towards implementing the GDPR.

2 CONSIDER WHAT DATA YOU HOLD

- Conduct a review of what personal data you currently hold. This may require a full data protection audit.
- Consider and record for what purposes you process personal data, where it comes from and who you share it with.

3 IDENTIFY AREAS OF RISK

- Identify areas of non-compliance, either under the existing data protection regime or under the GDPR.
- Identify which areas of non-compliance are high risk and need to be actioned straight away.
- Put together a plan of action to remedy those areas of non-compliance.

4 CONSIDER KEY DP ISSUES

- Assess whether you're prepared for a situation where an individual wants to exercise their rights under the data protection regime. e.g. subject access requests, erasure of data, removal from mailing lists.
- Determine to what extent you use personal data to market your (or other parties') goods and/or services.
- Establish where personal data is stored (geographically, physically and elctronically) and whether it is shared with or hosted or processed by any third parties.

5 REVIEW EXISTING PROCEDURES

- Review the processes for how you seek, obtain and record personal data and obtain consent.
- Review existing privacy notices and privacy policies. Are they easy to understand? Do they include all the information that controllers must now give to data subjects? How are these communicated to data subjects?
- Review your procedures for detecting, reporting, investigating and remedying a data breach.
- Evalute your general compliance with the current data protection regime.

6 IMPLEMENT CHANGE

- Draft new internal and external policies and procedures and review contracts in your supply chain.
- Identify all contracts which include the processing of personal data and vary these to include the new mandatory contract clauses.
- Consider whether you need to invest in new technology to help you comply with the GDPR.
- Provide training to all members of staff on what changes your organisation is/will be making in order to comply with the GDPR.

7 MONITOR COMPLIANCE

- Appoint a Data Protection Officer **(if required)** who will take responsibility for monitoring compliance going forward.
- Schedule regular reviews and training across the business to ensure you remain compliant.
- Continue to refine your policies and procedures with any future changes in the law.

1. INTRODUCTION

In May 2016, after four years of work, the European Union ("EU") published legislation which was the starting gun for the biggest shake-up of data protection in over 15 years: the General Data Protection Regulation (the "GDPR"). In a bid to harmonise data protection laws across the EU, the GDPR will come into force in every EU Member State on 25 May 2018 without the need for any additional domestic legislation.

> ***"I think it's clear that a lot people feel they've lost control of their own data. People feel that keeping control of their most important information used to be simple, but that over the years, their sense of power over their personal data has slipped its moorings."*** [1]
>
> **- Elizabeth Denham, Information Commissioner, (January 2017)**

The changes in data protection legislation recognise the increased sharing of personal data and the concerns of individuals whose personal data is being commodified and exploited by businesses. In a digital age, personal data is a valuable commodity to organisations but it is one which must be protected on the individuals' behalf.

The GDPR is designed to bring a sea change to current attitudes to data protection. It is bringing more power to the people; it is imposing controls on businesses and ensuring that people have the freedom to take control over the personal data that is held about them.

> ***"The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks. It's about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation."*** [2]
>
> **- Elizabeth Denham, Information Commissioner, (January 2017)**

Since May 2016, organisations have been working towards compliance with the GDPR, to ensure that the principles of the GDPR are embedded in their culture and day-to-day practices. With the clock ticking and the threat of fines for non-compliance from 25 May 2018, it is important that all organisations sit up and take notice of the changes coming into force.

When the UK does officially leave the EU, the GDPR will no longer be directly applicable into UK law, but the provisions of the GDPR will be embedded in UK law in the provisions of the new Data Protection Bill (which will replace the Data Protection Act 1998). Brexit cannot therefore be used as an excuse for non-compliance.

> ***"To meet the challenges, […] we need to move from a mindset of compliance to a mindset of commitment: commitment to managing data sensitively and ethically"***
>
> **- Elizabeth Denham, Information Commissioner, (January 2017)**

In brief, the changes consist of:

- Wider geographical application;
- Enhanced obligations for data controllers and data processors, which will impact on outsourcing and supply contracts;
- Enhanced rights for data subjects;
- Affirmative and recordable consent for the collection and processing of individuals' data;
- Stronger focus on the lawful pathways a controller or processor can rely on to collect and process data;
- Onerous reporting obligations to report data breaches;
- Privacy by design and privacy impact assessments;
- Published and applied governance controls, policies and procedures;
- Requirement to determine if a controller or processor have to put in place a mandatory Data Protection Officer; and
- Greater enforcement power.

We take a look at each of these in turn, followed by setting out our recommendations for approaches that can be taken in relation to each.

[1] Information Commissioner's Office. Information Commissioner talks GDPR and accountability in latest speech (January 2017) Available from: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/information-commissioner-talks-gdpr-and-accountability-in-latest-speech/
[2] Ibid.

2. FAST FACTS ABOUT THE GDPR

There will be new rules around profiling and the use of **children's data**

The GDPR imposes an **obligation on controllers** and processors to have a **WRITTEN CONTRACT** between them, which contains certain mandatory details.

The new **Data Protection Bill** (incorporating the GDPR) will replace the Data Protection Act 1998 and is the **biggest shake-up** of data protection law in over **15 YEARS**

Organisations will no longer be able to charge for subject access requests

Supervisory authorities **must** be notified of a breach if an individual is at risk of **suffering harm**

For some organisations, it will become mandatory to appoint a **DATA PROTECTION OFFICER**

TRANSPARENCY IS KEY

information about the processing of personal data must be concise, intelligible and easily accessible

Organisations can be fined up to **4%** of their annual worldwide turnover or €20m (whichever is higher) for breaches of the GDPR

INDIVIDUALS' RIGHTS will be **SIGNIFICANTLY STRENGTHENED** (they will have new rights to data portability and the 'right to be forgotten', i.e. to have information about them erased)

3. WHO IS AFFECTED?

- On 25 May 2018, the GDPR will automatically be transposed into the law of every EU member state. The GDPR will also expand the territory in which its obligations must be complied with and obligations will now also apply to data processors.
- The GDPR will apply to all organisations "established" in the EU.

What is "establishment"?
An "established" organisation may be one which exercises "any real and effective activity – even a minimal one", through "stable arrangements" in the EU.

- It can also apply to organisations without an "establishment" in the EU, depending on the location of the data subjects. In the case of non-EU established organisations, the GDPR will apply whenever the use of personal data by that organisation relates to:
  - The offering of goods or services to individuals in the EU, irrespective of whether a payment is required.
  - The monitoring of those individuals' behaviour in the EU.

4. KEY TERMINOLOGY

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 any other body which processes personal data on behalf of the data controller.
DPIA / PIA	Data protection impact assessments, also known as 'privacy impact assessments' or PIAs.
DPO	Data Protection Officer (you may also see reference to MDPOs, which are Mandatory Data Protection Officers).
Joint controllers	two or more controllers which jointly determine the purposes and means of processing. Joint controllers must determine their respective responsibilities for compliance with obligations under the GDPR by means of an arrangement between them and make a summary of such arrangement available to the data subject.
Personal data	any information relating to an identified or identifiable natural person ("data subject") an identifiable person is one who can be identified (directly or indirectly) in particular by reference to an identifier, e.g. name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Personal data breach	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.
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Profiling	any form of automated processing consisting of the use of personal data to evaluate certain personal aspects of a data subject, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour, location or movements.
Pseudonymisation	the processing of personal data in such a way that the personal data can no longer be attributed to an individual without the use of additional information, e.g. a key that is stored separately.
SAR	Subject Access Request
Special categories of data ('Sensitive 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 data subject, data concerning health or data concerning a data subject's sex life or sexual orientation.
Supervisory authority	an independent public authority which is established by a Member State to be responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of data subjects in relation to processing and to facilitate the free flow of personal data within the EU.

5. PRINCIPLES

Article 5 of the GDPR sets out the data protection principles that underpin the processing of personal data under the new regime:

Lawfulness, fairness and transparency

Personal data shall be **processed** lawfully, fairly and in a transparent manner in relation to individuals.

Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data minimisation

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are **processed**.

Accuracy

Personal data shall be accurate and, where necessary, kept up to date.

Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of which the personal data are **processed**.

Integrity and confidentiality

Personal data shall be processed in a manner than ensures appropriate security of the personal data, including protection against unauthorised or unlawful **processing** and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The **controller** shall be responsible for, and be able to demonstrate compliance with, the GDPR.

Organisations must keep these principles at the forefront of their mind when thinking about how the GDPR applies to their organisation and how they can demonstrate that they are acting in accordance with the principles.

6. PROCESSING: LAWFUL BASES & CONSENT

6.1 LAWFUL BASES

- You must identify a lawful basis for processing personal data before you can process it.
- Lawful bases on which you are processing personal data should be documented.
- Individuals' rights will vary depending on the lawful basis on which organisations hold their data (e.g. consent), which makes it important for businesses to understand how they hold data. For example, if you rely on someone's consent to process their data, they will generally have stronger rights to have their data deleted.

These are 6 lawful bases for processing personal data under the GDPR:

1. the individual has given **consent** to the processing of his or her personal data for one or more specific purpose
2. processing is **necessary for the performance of a contract** to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract
3. processing is necessary for **compliance with a legal obligation** to which the controller is subject
4. processing is necessary in order to **protect the vital interests** of the data subject or another individual
5. 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
6. 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 individual which require protection of personal data, in particular if the individual is a child.*

**Note: this may not apply in part if the data controller is a public authority in the performance of their task.*

The lawful basis for your processing can also affect which rights are available to individuals:

	Right to erasure	Right to portability	Right to object
Consent	✓	✓	× (but right to withdraw consent)
Contract	✓	✓	×
Legal obligation	×	×	×
Vital interests	✓	×	×
Public task	×	×	✓
Legitimate interests	✓	×	✓

6. PROCESSING: LAWFUL BASES & CONSENT

Special categories of data

Different lawful bases apply to the processing of special categories of data, i.e. sensitive data relating to a data subject's data racial or ethnic origin, political opinions, religious or philosophical beliefs, etc.

Lawful bases for processing of special categories of data include where:

1. the individual has given consent to the processing of his or her personal data for one or more specific purpose
2. processing relates to personal data which are manifestly made public by the data subject
3. processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim in the course of its legitimate activities with appropriate safeguards and on condition that the processing relates solely to current (or former) members

And where processing is necessary:

4. for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law
5. to protect the vital interests of the data subject or of another individual
6. for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
7. for reasons of substantial public interest, on the basis of EU or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
8. for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or pursuant to contract with a health professional
9. for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or Member State law
10. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6.2 CONSENT

The GDPR sets a high standard for consent. It is defined under the GDPR as 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.***

Consent (where used as justification for fair and lawful processing) therefore needs to be actively given; it can no longer be inferred from inactivity

Pre-ticked 'opt-in' boxes are banned under the GDPR.

Individuals can withdraw their consent at any time and must be clearly informed of their right to withdraw consent.

6. PROCESSING: LAWFUL BASES & CONSENT

Organisations will need to demonstrate they have obtained 'affirmative' consent. This means a clear record that the individual:

- Was informed of the name of the data controller
- Unquestionably understood how their data would be held, processed, shared, retained and secured
- The purposes for which their data would be processed
- What their rights are
- How to activate their rights

Only when these conditions have been satisfied consent to the processing will be lawful and fair.

There is a specific provision under the GDPR relating to data processing for scientific research purposes. This acknowledges that it is not always possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection.

Children

Children are defined as 'vulnerable individuals' requiring special protections when their personal data is collected and processed. Each Member State can decide on the age at which an individual is able to provide their own consent (between the ages of 13 and 16) – the draft UK Data Protection Bill indicates that children can provide their own consent in the UK from the age of 13.

Where children are too young to provide their own consent, you must obtain consent from a parent or guardian.

Children have the same rights as other individuals over the processing of their data, i.e. the rights access, the right to rectification, erasure, restriction, data portability, to object and in relation to automated decision-making.

Privacy Notices should be written in plain, age-appropriate and clear language, in a way which they can understand. Diagrams, cartoons, graphics and videos could all be good ways of presenting information to children. Fresh consent must be obtained when the child becomes an adult.

KEY TASKS

- Ensure that any request for consent from a data subject is prominent, concise, separate from any other terms and easy to understand
- Include:
  - the name of your organisation and any third party controllers who will be relying on the consent,
  - why your organisation wants the data,
  - what will be done with it, and
  - be clear they have the right to withdraw consent at any time.
- Don't use pre-ticked boxes or any default settings or opt-out boxes which presume consent
- Wherever possible, give separate options allowing data subjects to consent separately to different types of processing and for different purposes
- Keep records to evidence consent being given – including records of who consented, when, how, and what they were told.
- Consider using preference-management tools, to make it quick and easy for people to withdraw their consent
- Keep consents under review. Include regular consent reviews into your organisation's operational processes and update them when required.

7. INDIVIDUALS' RIGHTS

7.1 RIGHT TO BE INFORMED

- You must provide data subjects with various pieces of information about the data processing activities you carry out.
- This information is usually given in a **Privacy Notice** or **Privacy Statement**.
- The information must be:
  - concise, **transparent**, intelligible and easily accessible;
  - written in **clear and plain** language; and
  - provided free of charge.
- There is certain information which must be included in a Privacy Notice or Privacy Statement under the GDPR. The information required will vary depending on where the personal data is obtained – see **8.6**.

7.2 THE RIGHT OF ACCESS

- You must provide data subjects with confirmation that their data is being processed
- This is known as a Subject Access Request (SAR).
- You must comply with any SAR at the latest **within one month** of receipt.
- If requests are complex or numerous, the compliance period can be extended by a further two months. In this case, you must inform the data subject within one month of the receipt of the request and explain why the extension is necessary.
- Where you process a **large quantity of information** you can ask the data subject to specify the information they want to access.
- Responses to SARs must be made electronically.
- You cannot charge a fee unless the request is "manifestly unfounded or excessive".
- You may refuse to comply with an SAR where the request is "manifestly unfounded or excessive".

7.3 THE RIGHT TO RECTIFICATION

- Data subjects can have their personal data rectified if it is **inaccurate** or **incomplete**.
- You must comply with any request to rectify at the latest within **one month** of receipt.
- If requests are complex or numerous, the compliance period can be extended by a further two months. In this case, you must inform the data subject within one month of the receipt of the request and explain why the extension is necessary.
- If you have disclosed the personal data to third parties then you must inform them about the rectification of the personal data (unless this proves impossible or involves disproportionarte effort).

7.4 RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN')

- Data subjects have the right for their data to be erased where:
  - the personal data is **no longer necessary** in relation to the purpose for which it was collected/processed;
  - the data subject **withdraws their consent or objects to the processing** and there are no overriding legitimate interest to continue processing;
  - the personal data was **unlawfully processed** or has to be erased in order to **comply with a legal obligation**; or
  - the personal data is processed in relation to the offer of **information society services to a child**.
- You can refuse to erase a data subject's personal data where it is processed:
  - to exercise a right of **freedom of expression** and information;
  - to comply with a **legal obligation** or for the performance of a task of public interest;
  - for the exercise or defence of **legal claims**; or
  - for purposes relating to public health, archiving in the **public interest**, scientific/historic research or statistics.
- You must comply with any request to erase personal data at the latest **within one month** of receipt.
- If requests are complex or numerous, the compliance period can be extended by a further two months. In this case, you must inform the data subject within one month of the receipt of the request and explain why the extension is necessary.
- If you have disclosed the personal data to **third parties** then you must inform them about the erasure of the personal data (unless this proves impossible or involves disproportionarte effort).

7.5 RIGHT TO RESTRICT PROCESSING

- Data subjects have the right to restrict the processing of personal data where:
  - they have **contested its accuracy**;
  - they have **objected to the processing** and you are considering whether you have a legitimate ground which overrides this;
  - **processing is unlawful**;
  - you no longer need the data but the data subject requires it to **establish, exercise or defend a legal claim**.
- You must comply with any request to restrict the processing of personal data at the latest **within one month** of receipt.
- If requests are complex or numerous, the compliance period can be extended by a further two months. In this case, you must inform the data subject within one month of the receipt of the request and explain why the extension is necessary.
- If you have disclosed the personal data to third parties then you must inform them about the restriction of processing of the personal data (unless this proves impossible or involves disproportionarte effort).

7.6 THE RIGHT TO DATA PORTABILITY

- The right to data portability allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.
- The right to data portability only applies:
  - to personal data a data subject has **provided to a controller**;
  - where the processing is based on consent or the **performance of a contract**; and
  - where processing is carried on by **automated means**.
- You must provide the personal data in a structured, commonly used and machine readable form (e.g. CSV files).
- If the individual requests it, you may be required to transmit the data **directly to another organisation** if this is technically feasible.
- You must comply with the data subject's request free of charge and at the latest **within one month** of the request.
- If requests are complex or numerous, the compliance period can be extended by a further two months. In this case, you must inform the data subject within one month of the receipt of the request and explain why the extension is necessary.

7.7 RIGHT TO OBJECT

- Data subjects have the right to object to direct marketing (including profiling). Where the data subject objects to direct marketing you must do so immediately. There are no exemptions or grounds to refuse.
- Data subjects also have the right to object to:
  - processing based on **legitimate interests, the performance of a task in the public interest or the exercise of official authority** (including profiling) except where:
    i. you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
    ii. the processing is for the establishment, exercise or defence of legal claims; and
  - processing for **scientific/historic research or statistics** – except where the processing of personal data is necessary for the performance of a public interest task.
- You must inform **data subjects of their right to object** to the processing of personal data about him or her as soon as possible – at the time of the first communication with the data subject, at the latest.
- The data subject's right to object to the processing of their personal data must also be included in Privacy Notices.
- You must comply with the data subject's request at the latest **within one month** of the request.
- If requests are complex or numerous, the compliance period can be extended by a further two months. In this case, you must inform the data subject within one month of the receipt of the request and explain why the extension is necessary.

7.8 RIGHTS RELATING TO AUTOMATED DECISION-MAKING & PROFILING

- Data subjects have the right not to be subject to a decision when:
  - it is based on **automated processing**; and
  - it **produces a legal effect or a similarly significant effect** on the individual.
- You must ensure data subjects are able to:
  - obtain **human intervention**;
  - **express their point of view**; and
  - obtain an **explanation of the decision** and challenge it.
- You must comply with the data subject's request within one month of the request.
- If requests are complex or numerous, the compliance period can be extended by a further two months. In this case, you must inform the data subject within one month of the receipt of the request and explain why the extension is necessary. "**Profiling**" is any form of automated processing intended to evaluate certain personal aspects of a data subject, in particular to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, behaviour, location or movements.
- **The above right does not apply** if the automated decision:
  - is necessary for **entering into or performance of a contract** between you and the individual;
  - is **authorised by law** (e.g. for the purposes of fraud or tax evasion prevention);
  - is based on **explicit consent**; or
  - **does not have a legal or similarly significant effect** on the data subject.
- When processing personal data for profiling purposes, you must ensure that **appropriate safeguards** are in place. For example:
  - being **fair and transparent** about the logic involved;
  - using **appropriate mathematical/statistical procedures**;
  - implementing appropriate **technical and organisational measures** to correct inaccuracies and minimise the risk of errors; and
  - keeping personal data **secure** in a proportionate way.
- As a general rule, it is best to avoid making automated decisions based on **sensitive personal data** unless you have the explicit consent of the data subject or have reasons of substantial public interest.

8. WORKING TOWARDS GDPR COMPLIANCE

We have set out some initial critical (and time sensitive) steps/considerations that should be taken to prepare your business for May 2018 and to maintain a level of compliance with the GDPR going forward. These are presented alongside Key Tasks to undertake at each stage.

8.1 CONDUCT AN AUDIT

An audit is the critical first step to identifying risks and understanding what your organisation needs to do to get compliant.

KEY TASKS

- Conduct an audit to gain an overview of all the personal data you collect or process, for example:
  - what types of data do you process?
  - is it shared with third parties?
  - from where did you source the data?
  - is it moved outside the EEA?
  - what lawful grounds have you recorded for this processing?
  - how did / do data subjects give consent for processing of their data? do they positively opt-in or has consent been presumed as a default position (e.g. using a pre-ticked box)?
- Determine whether you are acting as a data controller or a data processor (or both).

Although there is some overlap between the roles of a data controller and a data processor, particular requirements apply to each role. Identifying whether you are a data controller or a data processor is therefore vital to ensure you make the appropriate preparations.

Remember the definitions of data processor and data controller under the GDPR:

DATA PROCESSOR - a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller

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

Do you determine the purposes of processing of personal data?
Do you determine the means of processing personal data?
If so, you are likely to be acting as a data controller.

Do you process personal data on behalf of a data controller?
Do you act under a data controller's instructions?
If so, you are likely to be a data processor.

You may find you operate in both capacities depending on whether you determine the purposes for processing data (controller) and/or act on the instructions of a third party in respect of the processing of data (processor).

8. WORKING TOWARDS GDPR COMPLIANCE

8.2 RAISE AWARENESS

It is vitally important that everyone in your organisation who deals with personal data – i.e. your employees – understand their obligations under the GDPR.

First, your organisation should raise general awareness about the changes to data protection legislation under the GDPR. You could put up posters at key spots around the building or send out regular updates on progress, for example.

You can then move onto rolling out staff training to all departments across your organisation. You should consider specifically targeting training at particular roles. Giving examples of situations in which your marketing team or your accounts team may be dealing with personal data, for example, will be more engaging and relevant than giving staff an overwhelming amount of information that may not necessarily be relevant to them.

KEY TASKS

- Ensure that the key people in your organisation receive regular briefings and updates on the organisation's preparations for GDPR implementation
- Add GDPR compliance as a risk to your organisation's risk register
- Consider the resource implications of implementing the GDPR – have you got enough money and personnel to prepare for implementation of the GDPR?
- Plan a programme of staff training and awareness to all departments
- Familiarise yourself with guidance on the Information Commissioner's Office (ICO) website and sign up for their regular email updates

8.3 GET TO GRIPS WITH NEW ACCOUNTABILITY REQUIREMENTS

The GDPR requires organisations to demonstrate that they comply with the accountability principle and Article 5(2) explicitly states that this is the responsibility of each organisation. In practice, this is likely to involve producing more policies and procedures, or updating existing ones.

KEY TASKS

- Ensure that your organisation can demonstrate compliance with the GDPR by:
  - implementing appropriate technical and organisational measures and internal data protection policies that ensure and demonstrate compliance, e.g. reviews of internal HR policies, staff training and internal audits of processing activities;
  - keeping accurate records of all processing activities;
  - where appropriate, appoint a data protection officer;
  - implement measures that meet the principles of data protection by design and data protection by default.
  - using data protection impact assessments, where appropriate.

Data controllers must now keep a record of, and be accountable to provide on request, a wide range of information relating to the personal data it processes, including (but not limited to) categories of data subjects, of data types, lawful grounds for all processing activity, the data processing activity itself, location of databases, transfers of personal data, retention periods, and so on.

Records which must be maintained by organisations will depend on the number of employees that it has.

If your organisation has fewer than 250 employees

You are only required to maintain records of activities related to higher risk processing, such as:

- processing personal data that could result in a risk to the rights and freedoms of individual; or
- processing of special categories of data (as defined); or
- personal data relating to criminal convictions and offences.

If your organisation has more than 250 employees

You must maintain additional internal records of processing activities, including the following information:

- name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer);
- purposes of the processing;
- description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
- retention schedules; and
- a general description of technical and organisational security measures employed.

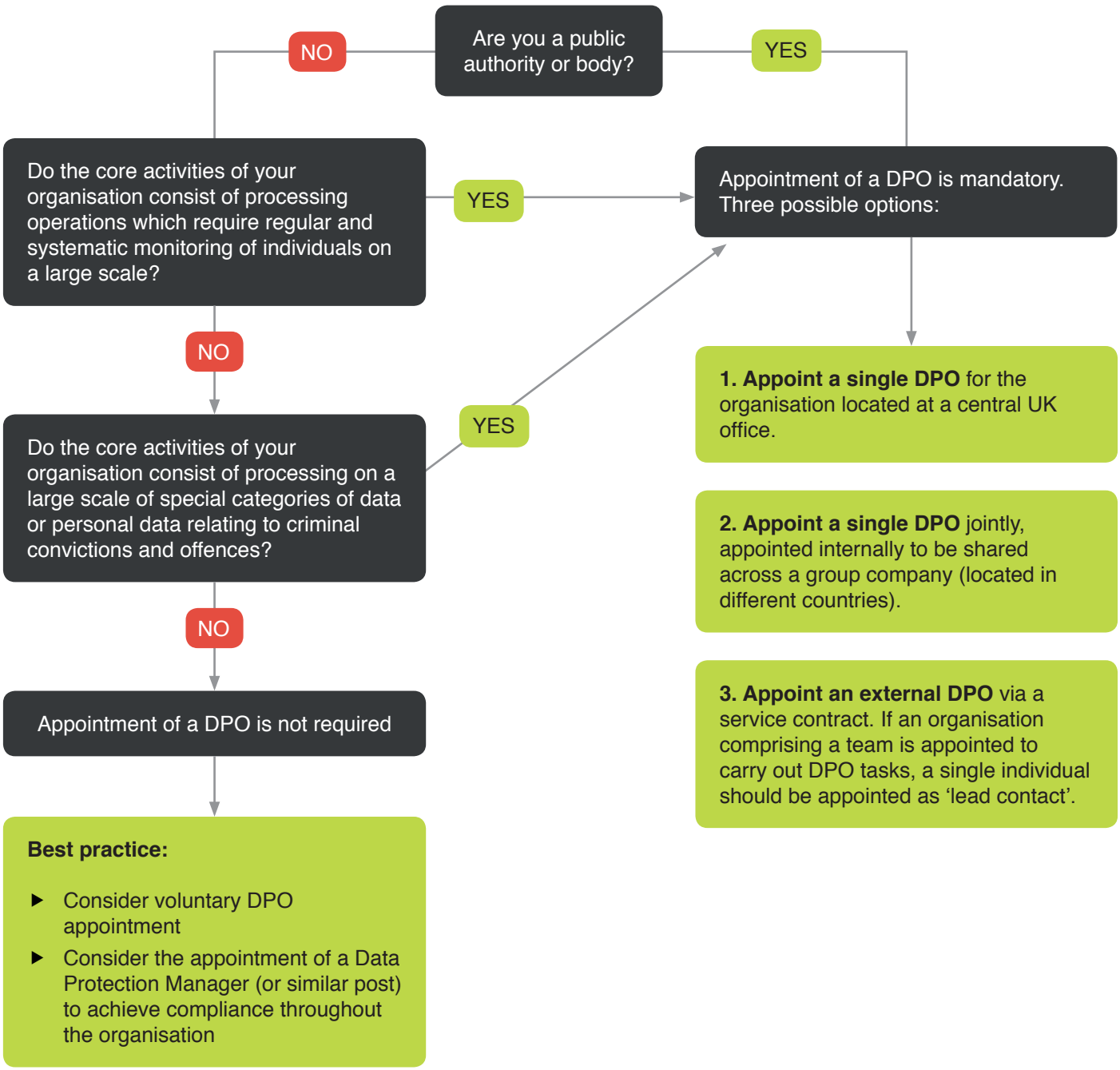
Organisations may be required to make these records available to the relevant supervisory authority on request.

8. WORKING TOWARDS GDPR COMPLIANCE

8.4 CONSIDER IF YOU ARE REQUIRED TO APPOINT A DATA PROTECTION OFFICER (DPO)

In certain circumstances it will become a statutory requirement to appoint a Data Protection Officer (DPO). In other cases, although appointing a DPO is not mandatory it may be best practice to appoint a DPO in any event, or to consider appointing a Data Protection Manager (or similar) to take responsibility for your organisation's compliance.

Our flowchart should help you determine which course of action to take:



8. WORKING TOWARDS GDPR COMPLIANCE

TERMS

Core activities are likely to be the key operations undertaken in order to achieve the organisation's objectives.

Large Scale: consider the number of individuals concerned, the volume of data and/or range of different data, and geographical extent of the processing.

Systematic could include occurring according to a system, pre-arranged, organised or methodical, taking place as part of a general plan for data collection or carried out as part of a strategy.

Special categories of data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Objectives of the DPO

- Ensuring and monitoring GDPR compliance
- Providing training and raising awareness
- Conducting audits
- Advising on Privacy Impact Assessments
- Co-operating with supervisory authorities

The role of the DPO
A DPO must have "... professional qualities and expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 [of the GDPR]"

Resources to be provided by an organisation

- Senior management support of the DPO's function
- Sufficient time provided to enable the DPO to fulfil his/her duties
- Relevant support to be provided to the DPO whether that be financial resources, appropriate infrastructure, staffing and support from any other services within the organisation where required
- Official communication of the DPO appointment to all staff
- Continuous training
- A secure and confidential channel via which employees can communicate with the DPO

DPO contact details must be published and communicated to the relevant supervisory authorities, (e.g. the ICO in the UK) and is recommended to be located within the EU.

The above is a brief overview of DPO requirements. If you think you may require a DPO in your organisation, we will be delighted to discuss this with you further.

KEY TASKS

- Consider if your organisation is caught by the statutory requirement to appoint a DPO.
- Assign budget and personnel resources to data protection compliance.
- If a DPO is mandatory:
  - scope out the DPO role.
  - decide where the DPO should sit within your organisation's structure and governance arrangements.
  - ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- If a DPO is not mandatory:
  - document your reasoning, analysis and conclusion for not appointing a DPO.
  - consider if it would be appropriate to appoint a Data Protection Manager (or similar) to take overall responsibility for your organisation's compliance.

8.5 REVIEW AND UPDATE CONTRACTS

Given that data processors as well as data controllers will now be liable under GDPR, it is in both parties' interests to ensure that data protection is adequately considered in commercial contracts, whether as a wholly outsourced function or where the processor is processing data as part of a wider service contract to the data controller.

Data protection considerations should, as a minimum at present, be in a written agreement between the parties. Whenever a controller engages a third party processor it must have a written contract in place.

Data controllers should only use processors 'providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of GDPR and ensures the protection of the rights of data subjects' (as set out in Article 28(1) of GDPR).

The contract must state details of the processing, and must set out the processor's obligations. This includes the standards the processor must meet when processing personal data and the permissions it needs from the controller in relation to the processing.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the documented (written) instructions of the data controller;
- ensure that people authorised to process the personal data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing of the personal data;
- engage sub-processors only with the prior consent of the controller and under a written contract;
- assist the controller by appropriate technical and organisational measures in responding to subject access requests and other data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- at the choice of the controller, deletes or returns all personal data to the controller at the end of the contract for provision of processing services;
- provide the controller with whatever information it needs to ensure that it is meeting its obligations under the GDPR and contributing to audits conducted by the controller (or other appointed auditor); and
- inform the controller immediately if it is asked to do something which, in its opinion, infringes the GDPR or other data protection law of the EU or a Member State.

8. WORKING TOWARDS GDPR COMPLIANCE

As well as the 'mandatory' obligations, the data controller and processor will need to decide the risk and liability allocation for any data breach. This is typically reflected in several clauses of a contract, namely (in a customer / supplier context):

- Controller (customer) obligations
- Processor (supplier) obligations
- Liability clauses
- Indemnity clauses

In a customer / supplier context, the customer will usually be the controller and the supplier will usually be the processor.

KEY TASKS

For existing contracts:

- audit your supply chain and key contracts with customers to identify those which may require renegotiation where the processing of personal data is present to ensure that they are compliant with the GDPR.
- check contracts to see if there are express provisions relating to who is responsible for implementing changes in law.
- where possible, update existing contracts to include the mandatory data processor clauses.
- when in discussions with your suppliers and customers, you should consider:
  - the date from which new contract provisions should apply, i.e. from now or from May 2018?
  - whether to use the opportunity as a wedge in the door for a wider renegotiation of the terms – this will ultimately depend on your bargaining position and if you are contractually able to do so.

For your contracts going forward:

- review your procurement and processor selection process (if you have one) – do you need to carry out increased due diligence or an impact assessment on the potential relationship?
- ensure your standard contracts are up to scratch. GDPR has been published so you should include GDPR ready provisions in arrangements that will likely continue beyond May 2018.
- include the data protection regime in any mandatory change of contract terms clauses.
- take legal advice on the liability provisions and consider the scope of indemnities – how is GDPR risk apportioned; how is the risk of the other party contributing to your loss managed?

8.6 REVIEW, UPDATE AND CREATE YOUR INTERNAL POLICIES AND PROCEDURES

Data protection by design and default

The ICO has consistently championed privacy by design as an implicit requirement of data protection. Under the GDPR, the importance of privacy by design has been elevated and organisations must implement technical and organisational measures to demonstrate that they have considered and integrated data protection into its processing activities.

Examples of such measures of integration and consideration could include:

- **data minimisation –** this is the GDPR principle by which personal data being processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Holding less data will lower the risk of breaching data protection legislation. Consider your existing processes and IT provision. What changes/developments are needed to act fast when an individual exercises its rights to rectify, erase, access or transfer their data?
- **pseudonymisation or encryption –** these are means by which personal data can be safeguarded.
- **allowing individuals to monitor processing –** ideally, individuals should be able to monitor processing of their own personal data and control what personal data is held by organisations in an automated way, e.g. through an organisation's website.
- **technology –** new technology developments must be entered into only after careful assessment of privacy risks. Security features should be created and improved on an ongoing basis.

Data Protection Impact Assessments (DPIAs)

Data protection impact assessments (also known as 'privacy impact assessments' or PIAs) provide a way of helping organisations identify the most effective way to comply with their data protection obligations and to meet individuals' expectations of privacy. DPIAs are an integral part of taking a privacy by design approach to data protection.

Where there is any danger that an organisation could be at risk of a breach of personal data or non-compliant with the GDPR it is important for organisations to manage and reduce that risk. Effective use of DPIAs allows organisations to identify and deal with problems at an early stage, which will reduce the associated costs and damage to reputation, which might otherwise occur.

The ICO places great value on the use of DPIAs as an integral part of taking a privacy by design approach. Use of DPIAs are currently optional but will become mandatory under the GDPR in certain circumstances.

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.

A DPIA can address more than one project.

8. WORKING TOWARDS GDPR COMPLIANCE

As a minimum, a DPIA should contain:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller.
- An assessment of the necessity and proportionality of the processing in relation to the purposes.
- An assessment of the risks to the rights and freedoms of individuals.
- The measures envisaged to address any risk(s), including:
  - safeguards
  - security measures
  - mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

Where necessary, the data controller must carry out a review to assess if processing is performed in accordance with the DPIA when there is any change of the risk represented by processing operations.

What is 'high risk' processing?

Processing that is likely to result in a high risk includes:

- systematic and extensive evaluation of personal aspects relating to individuals, including profiling and on which decisions are based that have legal (or similarly significant) effects on individuals.
- processing on a large scale of special categories of data (as defined) or of personal data relation to criminal convictions or offences.
- systematic monitoring of a publicly accessible area on a large scale, e.g. through the use of CCTV.

Privacy Notices

These will need to be updated and are essential in complying with the obligations in the first principle of the GDPR ('fair, lawful and transparent processing').

Under the GDPR, privacy notices must contain additional information to that which is required under the Data Protection Act 1998, including:

- the lawful basis for processing data;
- how long the data will be retained for;
- information about individuals' right to complain to supervisory authorities (e.g. the ICO).

Your approach to reviewing privacy notices will depend on whether you have (i) obtained data directly from the data subject, or (ii) obtained data indirectly, e.g. from a third party.

The highlighted areas show where the requirements differ depending on whether data comes from the individual themselves or from someone or somewhere else.

8. WORKING TOWARDS GDPR COMPLIANCE

Data obtained from the individual	Data not obtained from the individual
What needs to be included in a privacy notice? ▶ Identity and contact details of the data controller (and, where applicable, the controller's representative) and the Data Protection Officer (the 'DPO'). ▶ Purpose of the processing and the lawful basis for the processing. ▶ The legitimate interests of the data controller or third party, where applicable. ▶ Any recipient or categories of recipients of the personal data. ▶ Details of transfers to third country and safeguards. ▶ Retention period or criteria used to determine the retention period. ▶ The existence of each of data subject's rights. ▶ The right to withdraw consent at any time, where relevant. ▶ The right to lodge a complaint with a supervisory authority. ▶ Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data. ▶ The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	**What needs to be included in a privacy notice?** ▶ Identity and contact details of the data controller (and, where applicable, the controller's representative) and the DPO. ▶ Purpose of the processing and the lawful basis for the processing. ▶ The legitimate interests of the controller or third party, where applicable. ▶ Categories of personal data. ▶ Any recipient or categories of recipients of the personal data. ▶ Details of transfers to third country and safeguards. ▶ Retention period or criteria used to determine the retention period. ▶ The existence of each of data subject's rights. ▶ The right to withdraw consent at any time, where relevant. ▶ The right to lodge a complaint with a supervisory authority. ▶ The source the personal data originates from and whether it came from publicly accessible sources. ▶ The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.
When should this information be provided? At the time the data is obtained.	**When should this information be provided?** Within a reasonable period of having obtained the data (within one month). If the data is used to communicate with the data subject, at the latest, when the first communication takes place. If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

KEY TASKS

- Consider any measures that your organisation could take to incorporate data protection by design or default, including data minimisation, pseudonymisation or encryption, allowing individuals to monitor their own processing and incorporation of technology.
- Undertake DPIAs to identify any risks to the organisation and possible areas for improvements and/or increased efficiencies.
- Consider where personal data is obtained from and update your privacy notices to ensure they are compliant with the GDPR accordingly.

8.7 MAKE CONTINGENCY PLANS

On a practical level, how will you deal with requests from data subjects? What would you do in the event of a data protection breach? Who should you contact and within what timeframe? How will you contact data subjects if a breach has put them at risk? How would you deal with a Subject Access Request (SAR) from a data subject?

By May 2018, you should be able to answer these questions and feel confident that your organisation could deal efficiently with these scenarios, as and when they arise.

Dealing with a Personal Data Breach

A '**personal data breach**' means '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.'

Organisations must notify the relevant supervisory authority of any notifiable personal data breach.

A notifiable personal data breach is one which is likely to result in a risk to the rights and freedoms of individuals, i.e. one which may result in significant detrimental effect on individuals, such as one which leaves individuals open to identity theft, or which may result in discrimination, financial loss, damage to reputation, etc.

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it.

Where the resulting risk to the rights and freedoms of individuals of a breach is high, organisations must notify the individual(s) concerned directly. The threshold for notifying individuals (high risk to the rights and freedoms of individuals) is higher than for notifying the relevant supervisory authority (risk to the rights and freedoms of individuals).

In some cases, a breach will warrant notification to the public if it is sufficiently serious. In those circumstances, the relevant organisation must notify the public without delay.

Notification of a personal data breach (whether to the relevant supervisory authority, an individual or the public at large) shall, as a minimum:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach; and
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide all of the information required for the notification at the same time, a notification can be given in phases (although without undue delay).

For major breaches, the lead supervisory authority will look to see how the breach has been handled by an organisation; inspections can and do currently happen.

In the event of a data protection breach, acting quickly (and in any event within 72 hours) is important. If an organisation fails to notify the relevant supervisory authority of a breach when required to do so a substantial fine can be imposed, namely up to €10 million or 2% of global turnover.

8. WORKING TOWARDS GDPR COMPLIANCE

Dealing with Subject Access Requests (SARs)

You must comply with a data subject's Subject Access Request (SAR) electronically, free of charge and within one month of receipt. This can be extended by a further two months where the request is complex or if you receive a number of requests.

You must provide data subjects with:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information.

Where you process a large quantity of information you can ask the data subject to specify the information they want to access.

You cannot charge a fee or refuse to comply with a SAR unless the request is "manifestly unfounded or excessive", in which case you must provide evidence of how you reached that decision.

KEY TASKS

Personal Data Breaches

- Prepare a template letter to send to the ICO (or other relevant lead supervisory authority within the EU).
- Ensure that your staff understands what constitutes a personal data breach.
- Ensure that you have an internal breach reporting procedure in place. In the event of a personal data breach, this will help the organisation decide whether it needs to notify the relevant supervisory authority or the public.
- Ensure that the organisation has robust breach detection, investigation and internal reporting procedures in place.

Subject Access Requests (SARs)

- Ensure that your organisation has policies in place to determine how it will respond to SARs to ensure that your organisation is compliant with the relevant timeframes for a response under the GDPR.
- Determine how you will deal quickly and efficiently with requests from data subjects to exercise their new rights, e.g. the right to be forgotten, the right to portability, etc. Get policies, procedures and checklists in place.
- Put safeguards in place to ensure that no confidential or sensitive information about the organisation is inadvertently disclosed when responding to data subject requests.
- Prepare template letters to data subjects in response to any requests.
- Get legal advice on what information you can lawfully withhold.

8. WORKING TOWARDS GDPR COMPLIANCE

8.8 KEEP RAISING AWARENESS AND REVIEWING COMPLIANCE

Ensuring compliance with GDPR and other data protection legislation should not be a tick-box exercise carried out only once and then forgotten. The changes to the data protection regime are designed to change the way organisation's think about data and how they treat it.

KEY TASKS

- Diarise mini audits and/or reviews of your data processing on a regular basis to ensure that your organisation remains compliant.
- Review your data processing any time a significant change to the law is considered or implemented, or when the ICO issues any new or updated guidance on a particular area.
- Schedule training updates for existing employees.
- Make data protection part of your induction training for any new employees.

In essence, GDPR needs to become part of each business or organisation in every aspect of its operations. If this is driven from management level it will encourage the necessary culture change to ensure ongoing compliance from May 2018.

9. TIMELINE

January 2018

- Obtain buy-in from the Board and Senior Management
- Allocate resources to GDPR compliance
- Allocate resources to GDPR compliance
- Conduct a data audit:
  - what data do you hold?
  - on what lawful bases do you hold that data?
  - establish whether you are a data controller and/or a data processor
  - prepare a supplier contracts database, identify key contracts
- Consider the need for a mandatory Data Protection Officer
- Plan an organisation-wide compliance programme
- Consider your existing processes and IT provision - can they deal with the new rights of individuals (i.e. to demand rectification, erasure, access or transfer of their data)?

February 2018

- Update contracts with mandatory data processor clauses - leave enough time to renegotiate
- Review and update internal policies/procedures and Privacy Notices
- Plan your staff training
- Implement changes to IT provision and other processes

March 2018

- Create a Subject Access Request Response Plan and a SAR Response Plan
- Finalise staff training action plan
- Conclude supplier contract renegotiations

April 2018

- Obtain Board approval of finalised Breach Response Action Plan, Subject Access Response Plan, Privacy Notices and any other GDPR matters
- Implement staff training
- Keep raising awareness and continually monitor compliance

May 2018

- Conclude all outstanding GDPR items
- GDPR is a matter of good business hygiene – GDPR should be on all relevant operational agendas on an ongoing basis
- GDPR is embedded in your culture

25 May 2018

GDPR comes into force

WRIGHT HASSALL

www.wrighthassall.co.uk