The law is changing regards the data you hold – act now to avoid a large potential fine from enforcement agencies for non-compliance with the GDPR. *It might take you months to become compliant.*

Effective 25th May 2018 – *BUT ACT NOW*

General Data Protection Regulation (GDPR)

- Guide -

(This guide is available only to AIPP members)

Date of publication: October 2017

Context and Framework

This document provides guidance to prepare for the new General Data Protection Regulation (GDPR) coming into effect in the UK on 25 May 2018.

The GDPR is an EU, Europe-wide initiative relevant not only to countries in the EU but non-EU countries doing business with the EU. BREXIT will **not** affect the need for UK companies to comply with GDPR.

This guidance uses the UK Data Protection Act 1998 (DPA) as a base and sets out the changes required to be GDPR compliant.

The UK Information Commissioner's Office (ICO) has provided a *'12 steps to take now'* guide for businesses to use in preparation for GDPR. Here is the link: **ICO link**

The GDPR is only part of the overall data protection framework now being planned – driven by the many large-scale data theft scandals around the world with increasingly serious consequences.

In response, the Government has confirmed it will introduce a new Data Protection Bill into Parliament. This should become law in 2018 replacing the current 1998 Act.

If your business operates outside the UK you should check local data protection regulations and details surrounding the GDPR implementation date in your country.

This document is now in 2 sections:

Section 1 – GDPR guidance

Section 2 – Data Protection Act 1998

SECTION 1 - GDPR GUIDANCE

General Data Protection Regulation (GDPR)

The GDPR will apply in the UK and throughout the EU from 25 May 2018
The UK government has confirmed UK's decision to leave the EU will not affect this

The goal of the new regulation is to put individuals in control of their personal data.
All language used must be clear, easily understood and pitched at the user group.
Failure to enable this control could lead to fines of up to 4% of your turnover or €20m, whichever is greater.

The GDPR has two mains aims:

A. To protect the rights, privacy and freedoms of EU citizens
B. Reduce barriers to business by facilitating free movement of data in the EU

1. Who does the GDPR apply to?

The GDPR applies to any organisation that handles the personal data of EU citizens.

This means that, unlike the law it replaces, the GDPR also applies to businesses that provide outsourced services, e.g. cloud providers and external payroll.

It also means it applies to businesses based outside the EU offering goods or service to people in the EU, e.g. via their website.

Existing compliance with UK Data Protection Act 1998 (DPA) means a lot of the work to be done should already have been completed but, to meet GDPR requirements, enhancements to processes, procedures and documentation will still be needed.

2. Documents and processes

As part of the GDPR requirements, documents and processes must be enhanced to guarantee the protection of personal data:

Consent

- Consent must be given by a positive action on the part of the individual - a pre-ticked opt-in box on a form does not comply with the regulation.
- Consent text must be clear and specific, unrelated to other text (such as terms and conditions) and must name any third parties who have access to the data.
- Records of consent must be kept and information on how to withdraw consent must be easily accessible and understandable.

Subject Access Requests (SAR)

- A SAR is a request by an individual to discover what personal data is held on them by the organisation. The request must be in writing.
- Such requests anticipated to become more frequent, perhaps create a template form so individuals can give all information necessary to identify them easily allowing you to comply with the request.
- SAR request must be dealt with in one month of receipt (the present rule is forty days), and although currently an organisation can charge a fee, after GDPR, the first copy of personal data must be supplied free of charge.

Privacy notice

- The DPA required the privacy notice to display the name of the data controller, why the data is processed and other relevant information relating processing.
- The GDPR goes further and states information should be written concisely and be easily understood, written with the user in mind, and provided free of charge.
- The notice should be tested by volunteers from the target group, rolled-out when any amendments are completed and reviewed regularly, with feedback given.

Privacy Impact Assessments (PIA)

- The use of a PIA could be the difference between the safeguarding of personal data and a data breach and potential fine.
- While not mandatory, PIA are recommended to measure the impact on personal data of any projects or plans implemented by the organisation.
- The project or plan could be new, or it could be enhancing an existing system.
- An example where a PIA could be used is with a new computer system, or an upgrade of an existing computer system, where personal data is impacted.

3. Implementation

The Information Commissioner's Office (ICO) identifies '12 steps to take now.
Link to ICO document: **ICO link**

The twelve steps can be broken into three distinct areas:

A. Information
B. Management
C. Procedures.

By identifying the three areas, the tasks and actions can be distributed so that no single person is overwhelmed by the volume of work to be done. The suggested method of handling the implementation of GDPR is to create a steering committee.

Steering Committee

The steering committee would oversee the whole project, identify and allocate tasks, monitor and document progress, helping to ensure requirements met by the deadline

If there are not enough people in your company to form a committee, here are some options to consider:

- You could work with fellow AIPP members locally and combine your efforts. Teaming up in this way ensures the workload is reduced with more ideas and solutions generated, benefit both organisations and customers alike.
- Another option would be to divide the tasks, information, management and procedures as below, and allocate time to work on the tasks identified.

3.1 Information

- Organisations will have to audit all personal information that they hold. The audit should cover what information is collected, how it is processed, where it is stored, who it is shared with, how long it is retained and when it is destroyed.
- There is a fundamental question that needs be addressed: is the information needed at all? That question is very relevant to sensitive personal data such as racial or ethnic origin, political opinions, religious beliefs or sexual orientation, but may not be relevant to the service given to the customer or client.
- All information on GDPR must be easily accessible, internally and externally, on a webpage, with links to important information and documents as necessary.

3.2 Management

- Management will need to understand the resourcing implications of firstly, meeting the GDPR requirement, and secondly, maintaining and monitoring compliance.
- Appointing a senior level manager to oversee and take ownership of the GDPR will indicate your company is committed to the regulation and sees data protection as paramount. Use this as a marketing tool.
- A programme of staff training will need to be implemented - not only on initial implementation of the enhanced procedures but regularly on an ongoing basis.
- Third party audits and contracts will need to be actioned by management to ensure the protection of any personal data accessed by third parties. Again, having a named manager at senior level authority over the whole process will give it the importance and formality needed. *This commitment is very relevant in the event of a data breach, given that there is a legal requirement to report the breach within 72 hours of it becoming known.*

3.3 Procedures

- All procedures need to be documented and reviewed for compliance with the current DPA (or local equivalent), and either enhanced or created for meeting the individual's rights to data access, data amendments and data deletions.
- For example, because the timescale for complying with SARs has been reduced to one month, existing procedures must be amended or new ones written to encompass this change.

Section 2 – Data Protection Act 1998

Data Protection Act 1998 (DPA)

The UK Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (DPA) in the UK and for promoting good practice in information handling. You should check your local equivalent of the UK DPA.

The DPA consists of eight principles with which all organisations processing personal data must comply.

1. Policies and procedures

Essential to have written data protection policies and procedures to ensure compliance and promote good information handling. Organisations should:

- Ensure policies consider the additional security risks associated with home / remote working where applicable, as well as staff working within the office environment;
- Ensure policies are approved by a director or senior manager, have a clearly identified owner and version number;
- Store policies on the organisation's intranet or a shared network drive and communicate to all staff; and
- Review policies on a periodic basis and update when necessary.

2. Data protection training

Training is a key tool for ensuring staff awareness of data protection obligations, confidentiality and the security of personal data. Good practice in training include:

- Data protection training as part of the induction process for all staff;
- Annual data protection refresher training for staff who have access to personal data; and
- Maintaining a record of training completed and reminding staff when their training is due.

3. Third party contractors

Organisations must have a contract in place with any 3rd party who processes or has access to personal data on their behalf. Organisations should:

- Be satisfied third parties provide sufficient guarantees about security measures implemented to protect any personal data it is processing for you;
- Take reasonable steps to check that those security measures are being put into practice;
- Have a written contract setting out what the third party is allowed to do with the personal data including security measures outlined above; and

- Where applicable, ensure certificates of destruction are received from reputable 3rd parties detailing safe destruction of confidential waste and IT equipment.

4. Technical security controls including encryption and endpoint control

Organisations should:

- Ensure appropriate anti-virus, anti-malware, and firewalls are installed on their systems and portable devices all of which should be automatically updated on a regular basis;
- Use approved encryption software to ensure the information remains protected in the event of a device being lost or stolen;
- Lock down ports and drives to limit the risk of unauthorised removal of personal data and the introduction of malware and viruses to the network;
- Provide staff with encrypted memory sticks where there is a business need and allow a designated open USB port to be used only in such circumstances where authorisation from a manager or designated member of staff has been obtained; and
- Keep a log of all portable media devices and the names of the individual owners.

5. System access and password requirements

In order to reduce the risk that personal data may be accessed inappropriately, organisations processing personal data electronically on systems should:

- Have controls in place to restrict access to systems;
- Review access on a regular basis and update when staff change roles within the organisation; and
- Ensure system access procedures include prompt removal of access for all leavers and in cases where staff are suspended or away from the office for a prolonged period of time such as long term sickness or maternity leave.

Robust passwords prevent unauthorised access to information, system intrusion and provide a record of who has accessed or amended data and when this may have happened. Organisations should implement password controls including:

- Outline password rules in a written policy and ensure all staff are aware of their responsibilities;
- Issue all staff with unique usernames and passwords for the network and systems containing personal data;
- Do not keep a list of employee passwords;
- Do not allow users to share passwords with their colleagues;
- Enforce changing temporary passwords when users log on for the first time;
- Create rules regarding the complexity of passwords such as at least eight characters long including a combination of upper and lower case numbers, letters and symbol characters; and
- Prompt regular password changes at least every 90 days and restrict the number of failed logon attempts before a user's account is locked and needs re-setting.

6. Storage of manual records and locked screens

The open layout of many Company offices now means there is a high risk that anyone who enters the premises could view or even remove personal data left on desks or visible on unlocked screens. Therefore, organisations should:

- Ensure security controls in relation to the storage of manual records such as securing personal data in lockable filing cabinets when not in use and at the end of the day are implemented, enforced included in the data protection or equivalent policy;
- Introduce mandatory clear desk and locked screen procedures using 'Ctrl-alt-delete', formalise in policy and take steps to ensure they adhered to by staff.

7. Fair processing, including CCTV

Organisations who process individual's personal data should:

- Create a detailed. fair processing notice outlining how they may use or share a customer or client's information, including the circumstances in which this may occur;
- Share the notice with clients and customers in writing, before obtaining personal data;
- Make the notice available in a reasonably prominent place on their website;
- Obtain consent prior to sharing personal data with any third parties unless a valid exemption applies;
- Ensure customers and staff made aware if CCTV recording is used on premises by use of appropriately-sized notices containing contact details and explained to staff in a policy;
- Ensure retention period for CCTV data is documented in a written schedule; and
- Ensure CCTV recording is reflected in the company's notification details to the ICO or local data enforcement agency. In the UK, this can be done by calling the Registration helpline: 0303 123 1113 or by emailing: Registration@ico.org.uk.

8. Retention of personal data

Organisations should review the personal data they hold and identify how long it needs to be retained for based on why it was obtained.

Agreed timeframes for each category of data should be documented in a retention schedule to help safeguard against holding personal data indefinitely - a breach of the Act.

When creating a retention schedule, organisations should consider the following:

- Identify all categories/ types of personal data held by the organisation;
- any additional legal and statutory requirements;
- standard industry practice;
- whether the whole record needs to be retained to meet a business requirement or just a specific section of it;
- identifying secure appropriate disposal methods for both electronic and manual data;
- who will be responsible for periodic weeding and destruction of records and how compliance of this is to be monitored.