Starting your GDPR Journey
A Guide for Small Businesses

Many small businesses are fearful of the publicity surrounding the introduction of GDPR. Some businesses don't even think that the regulations apply to them. So, to set the record straight, if you keep someone's name and contact details in any form of database that you use for business within the EU then the GDPR regulations apply. The only time that GDPR does not apply is if the processing is carried out for purely personal or household activities or for Law Enforcement or National Security reasons.

The term "personal data" means any information that relates to an identifiable person who could be directly or indirectly identified through this data. This includes name, contact details, CCTV, photographs, car registrations as well as dates of birth etc. Even if the amount of data you hold is negligible you must still ensure that you comply with GDPR. It doesn't matter if the data is held in paper files, on your phone or in a computer database. There are 4 things you should do as soon as you can:

1. Identify how GDPR applies to your business.
2. Understand your role – who is the Controller or Processor of the data.
3. Complete a Data Audit for your business.
4. Write a Privacy Policy/Privacy Notice.

1 Identify how GDPR applies to your business

First you need to work out how big the task is. Here are 3 questions to ask:

- Do you collect, use, store or do anything else with the personal information of employees, customers or both?
- Do you think your business complied with the previous data protection laws?

If the answer is no to the first question then GDPR does not apply
If the answer to both questions above is yes you will need to take steps to make sure you comply with the new law.


The good news is that if you're following the current law you're already on your way to being compliant under GDPR. Many of the new rules and themes build on the previous law so should not be a complete change to what you are already doing.

If the answer is yes to the first question and no to the second question you will need to do quite a lot of work to make sure you comply with all your statutory obligations and include GDPR in this.

- Do you work with sensitive personal information or special category data?
  This includes things like health information, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, sexual orientation and genetic or biometric data.

If the answer to the third question is yes. Then you will need to do some work in addition to the work above to comply with the new law as the rules relating to this category of information are more stringent.


To help you with this the Information Commissioner's Office has produced a package of tools and resources to help you and it is available on their website (https://ico.org.uk/for-organisations/business).

Do you collect/use/store personal information	Did you comply with the previous Data Protection Laws	Do you work with Sensitive Personal Information
✓	✓	✗ or ✓
Then the GDPR Regulations Apply to Your Business		

2 Understand your Role in the Process – Are you a Controller or Processor of Data

Once you are aware of how far the regulations apply to your business the next thing to do is to work out whether you process personal data as a "controller" or "processor" (in some cases you may be both a controller and a processor).

A "data controller" is the person who (alone/jointly) determines the purpose for which data is processed and the way it is processed.

The "data processor" can be any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

"Processing" means obtaining, recording or holding data or carrying out any operation on the information or data. This can include:

- Organising, adapting or altering the information or data.
- The use, retrieval or consultation of the information or data.
- Any disclosure of the information.
- alignment, combination, blocking, erasure or destruction of the information or data.

The main roles for controllers and processors are as follow:

Data Controllers decide	Data Processors may decide
To collect data in the first place Which items of personal data to collect The purpose or purposes the data are to be used for Which individuals to collect data about The legal basis for collecting data Whether to disclose the data, and if so, who to Whether subject access and other individuals' rights apply Whether to make non-routine amendments to the data How long to retain the data	How to store the personal data Which IT systems or other methods to use to collect personal data The detail of the security surrounding the personal data The means used to transfer the personal data from one organisation to another The means used to retrieve personal data about certain individuals The method for ensuring a retention schedule is adhered to The means used to delete or dispose of the data.

The controller has overall responsible for the data and should make sure that they have a GDPR compliant contract with their processor. Particularly the controller should specify the legal obligations of the processor for example, to maintain records of personal data and processing activities and who has legal liability if there is a breach.

3 Complete a Data Audit (also referred to as an Information Audit)

Once you know which elements of personal information you process and what your role is you will need to undertake a data audit. This can be quite a daunting task. At the minimum, you will need a table or an excel spreadsheet that identifies every piece of personal data that you hold and provides the following information:

- Who are your data subjects?
- What the source of personal data is (is it collected or received)
- The approximate volume of data held and how often it is processed (per day/week/month)
- A description of each item of personal data to be processed
- Whether the organisation is a processor or controller
- What the purpose of processing is
- What the lawful basis of processing is
- What the retention period is
- The category of the data
- What format the data is held in (electronic/paper)
- How the data is transferred to others (if it is)

- The geographic location of the processing
- Is the data processed by automated means?
- Who has access to the data

Other Questions to ask as part of the audit:

- Are Third parties or data processors involved?
- Is there Cross-border processing?
- Are there any privacy risks?
- What are the risk to rights and freedoms of data subjects?
- Have you got an appropriate privacy notice?
- Have you applied Data limitation policies?
- How do you ensure accuracy?
- Have you ensured data minimisation?
- Have you implemented storage limitation?
- What Security have you in place?
- Where you get consent how you ask for and record consent?
- How you record and manage ongoing consent?

4 Write a Privacy Policy/Privacy Notice for your business

The term 'privacy notice' is used to describe the way you look after someone's privacy and it can be provided in a range of way; it is not necessary to restrict privacy information to a single notice or page on your website. Some of the ways you can provide privacy information are:

- By use of signage - for example an information poster in a public area.
- Electronically - in text messages; on websites; in emails; in mobile apps.
- In writing – through printed media; printed adverts; contact or medical forms forms such as financial applications or job application forms.
- Orally either face to face or on the telephone (make sure you document this).

It is considered good practice to use the same medium you use to collect personal data to deliver privacy information. So, if you are collecting information through a form your privacy notice would be on that form or pop up as the individual completes an on-line form. You can then combine this basic information with more detailed information on your website. This is referred to as a blended approach but you should remember to focus on the individual when you make decisions how to deliver privacy information.

A layered approach to delivering privacy information typically consists of providing people with a short notice containing key information, such as the identity of your organisation and the way you use the personal data (which you get from the Data mapping exercise described before). You can then expand each section or provide a link to more detailed information.

Privacy Notice basted on the Case Study in section 3.

The form that individual staff fill out could contain a privacy statement with a link to the company staff privacy policy. A statement such as:

"We are required to hold the personal data you have completed in this form for legal and practical purposes, without it we would be unable to employ you. Holding this data enables us to meet various administrative and legal obligations (e.g. for tax purposes) and gives us the ability to notify your emergency contact in case of an accident involving you. Further details of our Privacy Notice may be found on the website or on the staff intranet in the GDPR folder."

Your privacy notice should contain:

- Organisation name
- Who it relates to (staff/patients/emergency contacts)
- Details of the date on which it is to be reviewed next

- Introductory paragraphs showing why this policy is necessary/relevant for staff.
- Information on why you collect and use personal information. e.g. to enable staff to be paid
- Confirmation of the Lawful Basis on which you process this information. These may be:
    - Legitimate Interests
    - Necessary for a Contract
    - Legal Obligation
    - Vital Interests
    - Public Interest
- Details of any "Special Categories of Personal Information". These must be processed under one of the following categories as well as have a lawful basis as above:
    - Substantial Public Interest
    - Vital Interest
    - Legal Claims
    - Medical Purposes
- Details of any information obtained on a consent basis
- Details of how you will store this information
- Details of how you collect this information
- Details of who you share information with (and why it is shared)
- Details of how individuals can request Access to their Personal Data
- The individuals' rights in respect of the data. Individuals have the right to
    - object to processing of personal data that is likely to cause, or is causing, damage or distress
    - prevent processing for the purpose of direct marketing
    - object to decisions being taken by automated means
    - in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed
    - a right to seek redress, either through the ICO, or through the courts
- You should provide details of the person in your organisation to contact to discuss anything in your privacy notice {name, number, email}

To ensure that you can document that the data subject has read and understood your Privacy Notice you can prepare a "Declaration" for them to complete

I, _____, declare that I understand:

- *{organisation} collects and processes the following items of my personal data (insert items) because they are "necessary for a contract" to meet statutory and contractual requirements.*
- *{organisation} will not share my data to any other third parties without my consent, unless the law requires them to do so.*
- *The nature and personal categories of this data, where the personal data originates from and where my data is obtained from third parties (if it has).*
- *That my data is retained in line with {organisation} Records Management Policy.*
- *My rights to the processing of my personal data.*
- *That my nominated emergency contact(s) is to be made aware that {organisation} has their contact details for use in an emergency and that they will be asked to confirm that they are content for this information to continue to be held.*

Name and signature and date of staff member:

_____

For further information please contact Sam Alford via e-mail: sam.alford@pppmanagement.co.uk