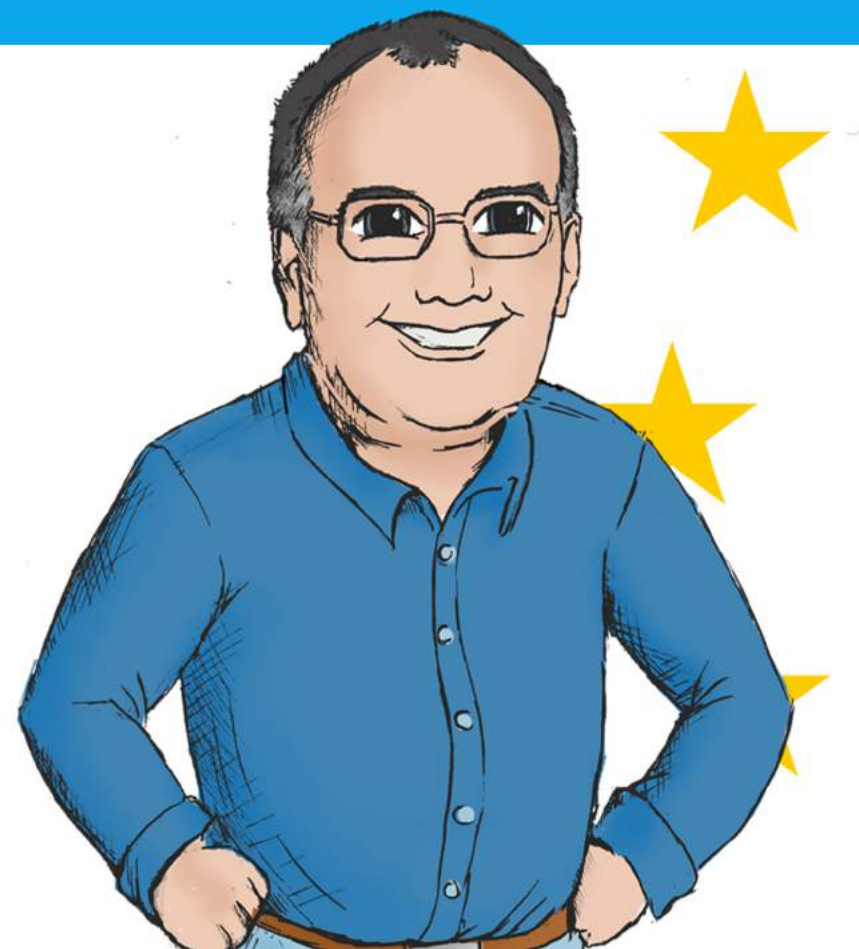


# THE BOOKKEEPERS GUIDE TO GDPR



Noel Guilford

# Contents

---

Introduction .....	3
What does this mean for Bookkeepers? .....	4
What is in the Regulation and why does it apply to Bookkeepers? .....	5
What do Bookkeepers need to do now? .....	6
Further information .....	12
My Bookkeeping Business .....	13
GDPR CHECKLIST .....	15
DATA INVENTORY CHECKLIST .....	18
Definitions.....	19
Data protection principles .....	22
Data subjects rights .....	26
Record Keeping.....	27





# The Bookkeepers guide to GDPR

---

## Introduction

The General Data Protection Regulation (GDPR) was adopted by the EEA States (of whom there are a few more than in the EU) in April 2016. A two year transitional period, which expires on 25th May 2018, was given for businesses to comply with the new Regulation, which is why this date is being widely quoted as the date the Regulation come into force.

Unlike an EU Directive, the Regulation does not require national governments to pass any enabling legislation and it is, therefore, directly binding and enforceable, although there will nevertheless be a Data Protection Act 2018 in the UK, which will encompass the Regulation and will remain in force if the UK leaves the EU.

The GDPR will be regulated and enforced by the Information Commissioners Office ([www.ico.org.uk](http://www.ico.org.uk)) and replaces the current legislation in the UK, called the Data Protection Act (DPA). Most bookkeepers will already be registered for data protection purposes with the ICO, but if you are not now is the time to do so.

GDPR impacts the way you collect identity information, how long you store it, what processes you need to introduce to control its use, what you may do with the data, and what security arrangements you need to implement to protect that data against risks such as loss or unauthorised disclosure.

Despite the publicity surrounding GDPR, and its significance for businesses, awareness has not yet translated into a high level of readiness even though much attention has been placed on the fines for noncompliance. But there are 'carrots' to balance the 'stick' of regulatory obligation. Chief amongst these is the opportunity for businesses to earn the respect of their clients by adhering to the new Regulation - improving client trust is what GDPR has been designed to support. When data is put under increased scrutiny, then, by definition, it is taken more seriously. Its role in how a business functions will become clearer, and businesses will need to examine the value of their data and the benefits of keeping that data fit for purpose and well protected.

The GDPR also introduces terms that have a precise meaning in the Regulation such as **personal data**, which I've highlighted for you each time they are used. A full list of these with definitions is in Appendix 1.

The changes introduced by GDPR are necessary to give individuals, called **data subjects**, more control over how information about them, referred to as their **personal data**, is used. This is because the DPA was drawn up before the internet, cloud based technology, smartphones, search engines and social media even existed.

## What does this mean for Bookkeepers?

Well first of all, as Corporal Jones would say “Don’t panic”. As bookkeepers we are already conscious of the need to keep client data confidential. This gives us a big advantage over most other businesses, although the Regulation does require more than this as we must also keep the data secure, retain it for only as long as necessary and only when we have authority to do so.

Most of the Regulation, however, is common sense and bookkeepers, who are complying with the existing legislation, will be meeting most of the Regulation already.

That said, moving towards a data strategy that allows businesses to flourish in the new regulatory environment is likely to throw up some challenges. One challenge is that the Regulation introduces a new principle of accountability. This requires bookkeepers to show how they comply with the data protection principles for example by:

- Having policies and procedures in place;
- Providing comprehensive, clear and transparent privacy policies;
- Integrating data protection into your processing activities.

Unfortunately some of the information about GDPR online is either wrong or misleading and some unscrupulous people are actually lying to scam businesses, as in a post I saw recently which said it’s a legal requirement to have your IT systems audited! So be aware.

The changes that will be most noticeable to bookkeepers are the need to:

- Document what personal data they hold, where it came from and why they hold it;
- Document more of their processes;
- Obtain up to date **consent** to contact clients and prospects;
- Review current privacy notices and update these for GDPR;
- Encrypt information, accounts etc., sent to clients;
- Check their computer systems are up to date;
- Ensure that third parties (Sage, Xero etc.) to whom information is transferred are able to comply with GDPR and document this appraisal;
- Put procedures in place to report data breaches.

I will cover each of these in this paper, but none of them is onerous with a little planning.

There are two more points to make:

1. The ICO wants to help businesses to comply with GDPR. They provide a great deal of information on their website (although some of it is a bit technical) and they are not out to fine Bookkeepers who are doing their best to comply.
2. Data protection is ongoing. It isn’t something you implement and forget about so you need to keep up to date with changes in the law.

## What is in the Regulation and why does it apply to Bookkeepers?

The ICO guidance on the lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

- 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.)*

Bookkeepers need to comply with GDPR when they are:

1. Processing personal data for their own business. They need to explain to their clients how they are doing this. **Personal data** is any information that makes a person identifiable such as their name, email address, telephone number, address or any other contact details.
2. Processing personal data for their clients' businesses. This is where the bookkeeper is acting as a data processor (as opposed to a data controller) of a third party's data.

Processing can be automated (e.g. by computer) or by other means such as paper records. Storage of personal data can be in a computer system, filing cabinet, files, notebooks or scraps of paper.

All processing of **personal data** must be in accordance with the six data protection principles; again these are largely common sense and are set out in Appendix 2. The rights of data subjects are set out in Appendix 3.



## **What do Bookkeepers need to do now?**

### **Make an inventory of the data you hold.**

Just as your clients may take an inventory of the stock they hold you should undertake a data inventory, which is a list of all the data you hold, whose data it is, where it is stored and what you do with it (**processing** in GDPR jargon). I suggest you have different lists for the personal data you store about different groups of people, for example clients, prospects, suppliers, contractors and employees (if any) for your own business, and the personal data you process for your clients' businesses.

A checklist for undertaking a data inventory is attached.

### **Identify how you process data.**


#### **1. Client data**

The data you hold on, say, your clients is held for a specific purpose - usually to write up their books, prepare accounts and tax returns and possibly pay their bills. All of these tasks are called '**processing**' and they are either carried out by you, software or someone else.

You should now make a list of each of these processes and identify and document who carries out each process. If it's you that all you need to do but if it's either software or another person (or business) there are extra steps:

- a) Software - if the software you use in on your desktop and your IT systems are secure (see later) then you need take no further action. If, as is likely, you use cloud based software then you need to determine where the server that holds the data is located. All being well it will be in another EEA country (regulated under GDPR) for software such as Reckon which is in Eire, or the US, for software such as Xero, QuickBooks, Dropbox etc.. For information stored on US based servers you can access the Privacy Shield framework at the US Department of Commerce on which all such software will be registered and a statement made as to whether it is GDPR compliant. As you can imagine given the importance of Europe to these businesses most are already able to comply. The ICO has produced '[Guidance on the use of Cloud Computing](#)' which outlines best practice in relation to the use of cloud based services.

Privacy Shield is an agreement between the EEA and US allowing for the transfer of personal data from the EU to US. The GDPR has specific requirements regarding the transfer of data out of the EEA. One of these requirements is that the transfer must only happen to countries deemed as having adequate data protection laws. The EEA does not list the US as one of the countries that meets this requirement. Privacy Shield is designed to create a programme whereby participating companies are deemed as having adequate protection, and therefore facilitate the transfer of



information. In short, Privacy Shield allows US companies, or EEA companies working with US companies, to meet this requirement of the GDPR.

- b) A third party – the transfer of data to a third party may be the area where Bookkeepers are most at risk because if a third party to whom you have transferred data suffers a breach you may be liable as the data controller. Third parties may be a contractor, person or another business; under GDPR they are known as **data processors**.

An example from my business is payroll processing. I don't do this myself but outsource to a specialist payroll provider. Under GDPR, I must make sure that they are GDPR compliant and have them sign a **Data Processing Contract** to ensure that they are only processing the data I give them in a manner that I have instructed and that they have adequate procedures to safeguard that data. If your business outsources processing to third parties you can either ask them for their contract (payroll providers should have one) or create one yourself. My Bookkeeping Business members will be able to download one from their members' area.

## 2. Data you process relating to your clients' businesses

In processing data for your clients you will often be required to process personal data relating to their customers, suppliers etc. To be GDPR compliant you must only process this data for the purposes your client specifies and put in place a **Data Processing Contract** to ensure that you are only processing the data they give you in a manner that they have instructed and that you have adequate procedures to safeguard that data.

### Update your engagement letters

All bookkeepers will have to update their engagements letters to reference GDPR rather than the DPA and include reference to:

- ☐ Your privacy notice and where this can be found;
- ☐ Your data retention policy (how long you retain personal data);
- ☐ Your approach to sending updates and news to clients and whether clients are required to consent to this.

At the time of writing GDPR guidance for engagements letters is still awaited from most accounting and bookkeeping bodies who are themselves awaiting further guidance from the ICO. When these become available, GDPR compliant engagement letter templates will be available on the My Bookkeeping Business website.



## **Update your privacy notices**

Under the transparency principle (see Appendix 2) the GDPR includes rules on giving privacy information to **data subjects**. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

All bookkeepers will need to update their privacy notices to comply with GDPR; it is likely that these new privacy notices will be longer and more detailed than existing privacy notices. Although there is no single template privacy notice that will cover every eventuality (because every bookkeeper's practice will be different) a generic GDPR compliant privacy notice will be available to My Bookkeeping Business members which they can edit to reflect the way they use **personal data**.

Reference to where your privacy notice can be found must be included in engagement letters, opt-in forms and all documents from which clients and prospects can subscribe to your updates and newsletters. This will usually be on your website (if you have one) or in a separate printed document which you can include and refer to when sending information to clients and prospects

## **Obtain ongoing consent to use clients' data**


If some of your clients and prospects have been on your list for some time it is advisable to have them re-consent for you to store and use their data. This applies particularly to prospects and other contacts on your e-mailing list.

Consent means that a data subject has explicitly and freely given their consent by a 'statement or clear affirmative action' to the processing of personal data relating to him or her. You must be able to provide evidence that they have done this and they must be able to withdraw their consent at any time.

To achieve this there must have been some active communication between you and your clients to demonstrate active consent, as consent cannot be inferred from non-response to a communication.

This area is likely to be 'grey' for Bookkeepers who, for example, meet a prospect at a networking meeting and are given their card with a request to join the Bookkeeper's mailing list. There is clear consent, in fact simply giving the card is probably consent, but can it be evidenced? In this situation I recommend that a follow up email be sent requesting the data subject to confirm their request. It is likely that if you use an email marketing system such as MailChimp, Active Campaign or AWeber that you can use their double opt-in process to do this.





The ICO makes it clear that you are **not** required to automatically refresh all existing consents in preparation for GDPR, but it's important to check your processes and records to be sure that your existing consents meet the new standard.

If they do not, and to obtain ongoing consent, I recommend sending an email to all your **data subjects** asking them to confirm that they are happy for you to continue to process their data. This request must be specific about the type of data you hold and what you use it for and will, therefore, need to be tailored for each client, prospect, supplier and employee.

My Bookkeeping Business members will be able to download a suitable email template from their members' area.

### **Document to whom you transfer data**

The most common forms of data transfer are emails, memory sticks or notes written on paper and posted or handed to the recipient. These forms of data transfer are no longer suitable as emails can easily be sent to the wrong recipient, memory sticks easily misplaced and pieces of paper go missing.


So, what can the Bookkeeper do to secure individual data transferred to a third party? The ICO has written a document on these matters, and it is specifically aimed at the small organisation. The document is called '**A practical guide to IT security**' which outlines ten practical ways to keep your IT systems secure and covers the following areas:

- ☐ Threats and risks to the data held by the business
- ☐ Different types of IT security available
- ☐ Moving, securing and backing up of data
- ☐ Staff training and awareness
- ☐ Identifying that an attack has taken place
- ☐ Minimising data and data breaches
- ☐ Checking third party compliance

By following these suggestions, the personal data held by Bookkeepers and security over data transfers will be enhanced.

It is likely that in most cases of data transfer bookkeepers will use encryption, which is a means of ensuring that data can only be accessed by authorised users. Typically, a (strong) password is required to 'unlock' the data.

Encryption comes in many different forms and offers protection under different circumstances.

- 
- Full disk encryption means that all the data on the computer is encrypted.
  - File encryption means that individual files can be encrypted.
  - Some software offers password protection to stop people making changes to the data but this may not stop someone reading the data.

Make sure you know exactly what protection you are applying to your data. Some mobile devices support a remote disable or wipe facility. This allows you to send a signal to a lost or stolen device to locate it and, if necessary, securely delete all data. Your devices will normally need to be pre-registered to use a service like this. If you permit employees or other users to connect their own devices to your network you will be increasing the range of security risks and these should also be addressed.

An alternative form of encryption is to use an online secure portal, such as Virtual Cabinet; these work by providing a secure data store in the cloud to which firms can transfer information for their clients to login and retrieve.

### **Create a system for identifying and reporting a personal data breach**

Planning for the worst-case scenario makes good business sense so you must check that you have procedures in place to detect report and investigate a **personal data breach**. Make sure that you are effectively monitoring your security environment, and reporting on risks and possible improvements. The most effective way to do this is to carry out a regular checklist assessment of your systems, covering a range of topics such as:

- IT industry trends/issues relating to data security;
- review of access control logs;
- enforcement of security and password access rules;
- maintaining regular software updates – security/anti-virus and day to day operational applications;
- review security software messages;
- erase and dispose of data on old computers (you may be responsible if personal data gathered by you is extracted from your old IT equipment).

Data breaches must be reported to the ICO within 72 hours, but do not stress unduly over data breaches; they will happen – hopefully not too frequently – and as long as they are identified and reported promptly the ICO are more concerned with ensuring that the cause of the breach is identified and prevented from recurring than fining the business. Clearly, repeated breaches will not be looked on as sympathetically.

## **Manage your mailing list**

A question I have been asked quite often recently is whether you can still market to existing clients?

Best practice when email marketing and building a database is never to add anyone on to your database automatically unless you have their consent or permission first, and you must always give the client the option to unsubscribe.

However, regardless of whether you have or haven't followed these rules in building your database, there are certain steps you must take now to be compliant – and protect your mailing list.

The first is to establish the lawful basis for processing **personal data** on which you are going to rely. These are set out in Article 6 of the GDPR (see page 2), but there is no need to focus exclusively on using consent.

There is an argument about 'legitimate interest' and how this may get around being able to keep contacting your existing clients but this is another 'grey' area which argues that if a contact is a past client or current one or has some genuine link to your business, they can still be marketed to. I recommend not relying solely on the 'legitimate interest' argument and getting all past and present clients to whom you want to send your marketing information to re-consent, but even if they don't you may still have a legitimate business interest in mailing them on which you can rely


Some simple steps like incorporating a prominent unsubscribe link on all your marketing emails and not emailing people from no reply emails will also go a long way to avoiding annoying recipients of your emails.

I mention these as examples of what not to do. In my view it's important to avoid attracting unwanted attention, and potential fines.

If you can demonstrate that all the marketing material you have used to gain sign ups to date was double opt-in, then you don't need to do any more work on this. If not, which is likely for most Bookkeepers, you'll need to ask your list to re-sign-up to continue to keep receiving emails from you.

As I said earlier, it is likely that if you use an email marketing system such as MailChimp, Active Campaign or AWeber that you can use their double opt-in process to do this. Using this it only takes a minute for your subscribers to re-sign up and give their consent. It's all automated and all trackable, so you are covered in the event of an investigation. This signing up process isn't a one-off exercise, however; it should be repeated at regular intervals.

If you have a loyal and engaged audience, most will sign up and then you are good to go. But note that using a pre-ticked opt-in/tick box will not be acceptable under the new Regulation.



However after you have set up a sign-up form on your email marketing software, and you have emailed this out to your current list don't despair if not everyone signs-up – some won't and this is fine. It is better to have 100 subscribers signed up who all read, click and engage with your content than 500 who never open an email.

But how can you engage clients in addition to using the traditional database and email marketing route? Given GDPR and its limitations on us going forward, what else can you do to engage and grow?

Firstly, try and be positive about this. See this as an excuse to get in touch with them by phone or a meeting to engage them and catch up. You could consider:

- telephoning to boost sign ups or chase non-responders. By making these calls you never know where this may lead!
- finding and following the contacts on your various social media profiles to keep connected. Then you could message them as well as posting general content to them and everyone else to engage them and draw them in.

### Further information

The implementation of the Regulation in the UK is still developing and it is likely that further guidance from the ICO will be forthcoming. There are, however, numerous tools and templates on the ICO website to assist organisations in become GDPR compliant. One of the most useful is their self-assessment tool which can be found at <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>.

*This content is not intended to constitute legal advice. Users of this document should consult their own legal advisers for legal advice specific to their own circumstances before taking or refraining from taking any action in relation to the matters outlined.*





# My Bookkeeping Business

My Bookkeeping Business is a complete 'business in a box' for anyone wanting to set up and run their own bookkeeping business. In it we show you how to set up your bookkeeping business from scratch and gain the clients you want to work with, without having to become a salesperson....and how the clients you want will actually come to you.

It has been developed by Business Success Coach and Chartered Accountant Noel Guilford and his partner Sarah Rugg who for 12 years has run her own successful Virtual Assistant business.

The programme comprises seven modules:

## Module

1.       Setting up your business
  - Have you got the right mindset?
  - Name your business (including your 'done for you' logo and branding)
  - Business structure, HMRC, ICO and VAT
  - Accounting, banking, billing and invoicing
2.       Systems and IT
  - Registering your domain name and email account
  - Equipment and technology
  - Do I need a website?
  - GDPR requirements
  - Secure data transfer
3.       Dealing with compliance
  - Engagements letters
  - Money Laundering (MLR)
  - GDPR
4.       Achieving confidence
  - The 10 module Boost your Confidence programme
5.       Marketing
  - Finding your niche
  - Your ideal client
  - Your unique selling proposition (USP)
  - Become an expert
  - Creating a lead magnet
  - Pricing your services
  - Creating your LinkedIn profile

- 
6. Services and software
    - Cloud accounting
    - Business workflow
    - Monthly reporting
    - MTD and VAT
    - Payroll services
    - Management accounts
  7. Getting and keeping clients
    - Selling your services...the easy way
    - Networking
    - LinkedIn
    - Onboarding
    - How to wow your clients
    - Getting referrals.

A unique feature of the programme is that our members get access to our exclusive private Facebook group and unlimited access to Noel and Sarah during the first three months of their membership<sup>1</sup>. Thereafter membership can be purchased for a small monthly fee.

We also provide a full money back guarantee so **you have absolutely nothing to lose**. As long as you follow every step of our programme we are so certain that you will be successful (and get several times your money back in client fees) that we offer a no quibble money back guarantee.

With My Bookkeeping Business the only limitation to growing your business is you... How big you want it to be and how hard you are prepared to work.

Visit [mybookkeepingbusiness.co.uk](https://mybookkeepingbusiness.co.uk) to find out more and join our early bird list for an exclusive 10% discount when we launch.

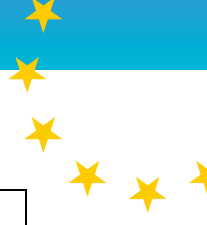
---

<sup>1</sup> A reasonable use policy applies

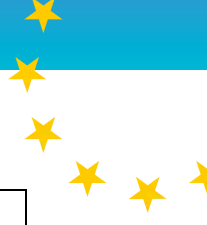


## GDPR CHECKLIST

CONSIDERATION	COMMENTS
Consider the quality and integrity of the personal data we hold. Is it accurate and up to date?	
In terms of retention, do we need to keep it at all? What is the value of this data to the business and what have we told clients about how long we will retain their data for? Create a Data Retention Policy.	
What are main data risks in the business?	
<p>What are the legal grounds on which we currently collect and use personal data. How are consent, legitimate interests and other grounds used as basis for processing personal data?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> the data subject has given consent to the processing of his or her personal data for one or more specific purposes;</li> <li><input type="checkbox"/> processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</li> <li><input type="checkbox"/> processing is necessary for compliance with a legal obligation to which the controller is subject;</li> <li><input type="checkbox"/> processing is necessary in order to protect the vital interests of the data subject or of another natural person;</li> <li><input type="checkbox"/> 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;</li> <li><input type="checkbox"/> processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.</li> </ul>	
Map the personal data we hold and how this	



data flows through the business (system by system). Identify personal data flows which happen between us and clients and how this data is transferred.	
Identify personal data capture points (e.g. online forms, registrations). Are we validating at point of entry? What are clients told about how their data will be used?	
Review and update Privacy Policies and Notices: add these to the footer of our website so that it appears on every page of the website.	
Send our Privacy Notice to our subscribers to confirm how we collect and process their personal data, for what purposes we use their data, the legal grounds of processing such data, how we keep their data secure and their rights in relation to such data.	
Create a Data Processing Contract for each client and incorporate into standard engagement letters. Consider whether existing engagement letters need refreshing.	
Ensure that we have GDPR compliant opt in box wording at the point of collection on our website where we collect email addresses (ie underneath the sign up box) together with a link to our Privacy Notice.	
Obtain GDPR compliant consent for e-mail marketing communications. If we do not have compliant consent, email our list for fresh consent.	
Put in place a system for managing opt outs/ withdrawing of consent and keeping records of opt outs.	
Put in place a system for data subject requests. Note: we can no longer charge for data subject requests and we must respond within 30 days.	



Review all our relationships with third party data processors, Sage, Xero, Dropbox etc., who now have responsibilities and consider whether they meet the GDPR standard.	
Put in place a system for data breach notification. A data breach occurs when there is a loss, unauthorised disclosure of or access to personal data AND there is a risk to the rights and freedoms of individuals. If there is a data breach, we must notify the ICO within 72 hours of the breach.	
Consider whether our insurance cover is adequate to cover any increased liability due to GDPR such as increased liability as a data processor.	
<p>Employees (only applicable if you employ staff)</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> determine the lawful grounds for processing employee data and obtain signed copies of an Employee Privacy Notice.</li> <li><input type="checkbox"/> arrange for data protection training for all employees on how to properly process data, record consents, how long to store data, when to report data breaches and how to respond to data subject requests.</li> <li><input type="checkbox"/> put in place systems for employee subject access requests which are most likely to be submitted from employees in the context of a dispute. Make sure that we have appropriate templates for the employee to make the request and for our reply.</li> </ul>	

## DATA INVENTORY CHECKLIST

We recommend that you complete a separate data inventory for each type of data subject, eg clients, suppliers, contractors, employees, etc.

TYPE OF DATA	LOCATION
Name	
Former name(if any)	
Address	
Email address(es)	
Telephone number(s)	
Gender	
Age	
Unique tax reference (UTR)	
National insurance number	
Date of Birth	
Next of kin	
Nationality	
Passport number and expiry date	
Bank	
Solicitor	
Government Gateway ID and password	
Directorships	
Copy of will	

This list is for illustrative purposes and is not exhaustive. Alternative or additional information will be required for each data subject type.