Getting Ready for the General Data Protection Regulation (GDPR) Changes

Audit Check List

Getting Started

Your guide to becoming compliant with the General Data Protection Regulations (GDPR)

GDPR comes into force **25 May 2018.**

While the new GDPR law will undoubtedly introduce a number of changes to data protection practices, such as understanding the reasons "**why**" you collect data and "**seeking permission"**, it should not itself radically alter how you approach data protection compliance.

Many of the core principles will remain the same so for organisations that currently follow sound data protection practices, getting ready for the GDPR will not be an insurmountable task!

Brexit will not affect commencement – GDPR is here to stay

It is important that decision makers and key people in your organisation are aware of the changes in the General Date Protection Regulation (GDPR) law.

Under the Data Protection Act, individuals and organisations that process personal information need to register with the Information Commissioner's Office (ICO)		
Suggested Actions A good starting point is to check if your company needs to be registered with the Information Commissioner's Office (ICO)	**Completed**	**Additional Comment/Action**
1. Are you registered with the ICO?	Yes/No	
2. Complete a quick 5-minute self-assessment online with the ICO https://ico.org.uk/for-organisations/register/self-assessment/	Yes/No	
3. Do you have a plan for a more general awareness campaign across your company to educate staff and how the GDPR changes can impact them?	Yes/No	

Getting Ready for the General Data Protection Regulation (GDPR) Changes

Audit Check List

What constitutes personal data?

To help you decide what data you hold, you should **map out** how the information you collect flows through your organisation and how you process it, recognising that you might be doing several types of processing.

You should work out:

- What information you hold that constitutes **personal** data.
- What you do with the **personal** data you process.
- What you need to carry out your processes – a **Privacy Notice** can help answer this question
- Are you collecting the information you need? Could you be collecting too much data on one indivdual?

What constitutes personal data?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from:

- A name
- A photo
- Storing information
- An email address
- Bank details
- Medical Information
- Computer ID address

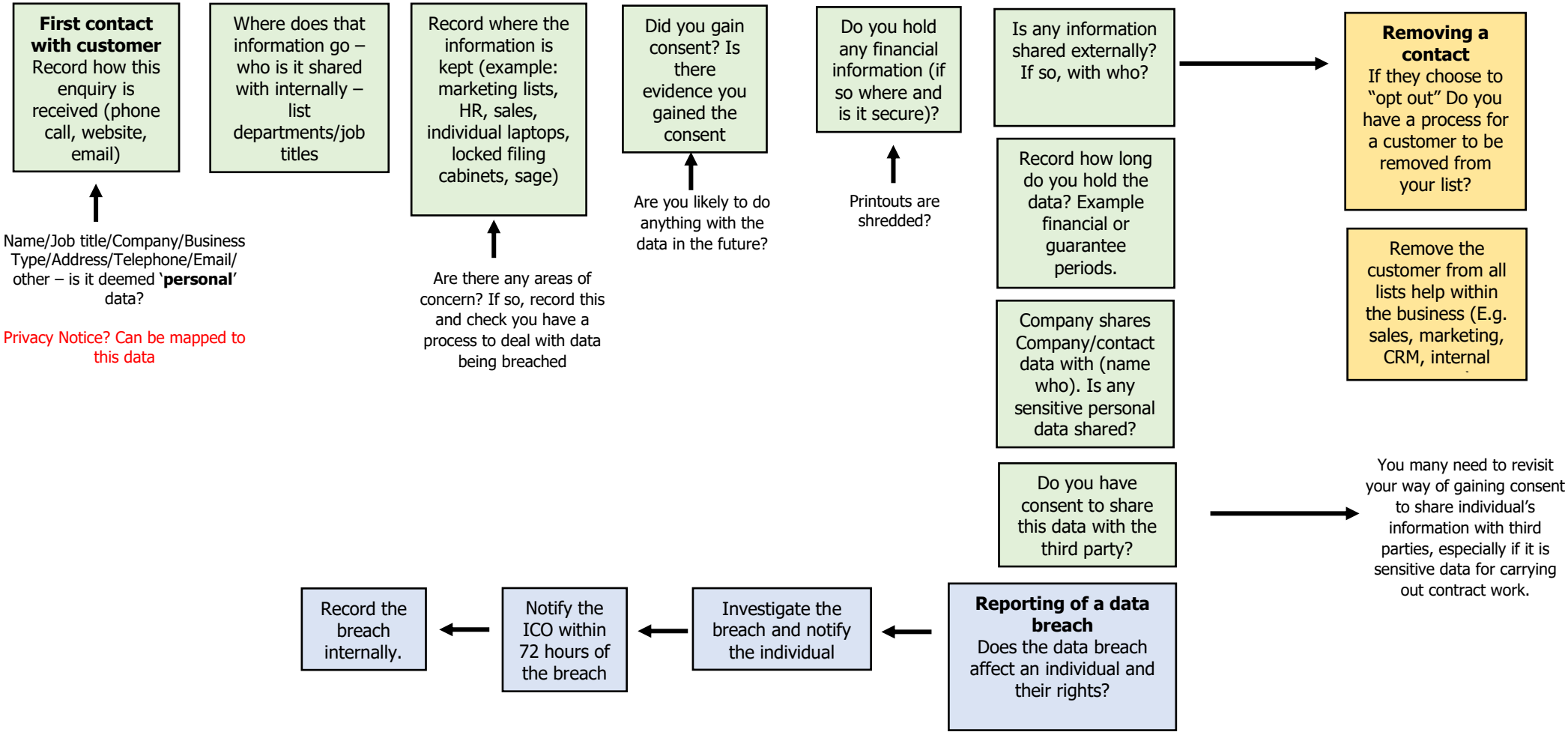
Your business should document what personal data you hold, where it came from and who you share it with and carry out an internal information audit.		
Suggested Actions A good starting point for an internal audit is to document any information you hold in relation to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person.	**Completed**	**Additional Comment/Action**
1. Have you carried out an internal audit on the personal data you hold in the organisation?	Yes/No	
2. You should map out how your information flows through your organisation and how you process it, recognising that you might be doing several types of processing (see page 3 as an example)	Yes/No	
3. Do you know where the information came from?	Yes/No	
4. Do you know how long you hold the information for?	Yes/No	
5. Did you seek permission to hold the individual's data?	Yes/No	

Getting Ready for the General Data Protection Regulation (GDPR) Changes

Audit Check List

Example of a template to help map your data collection process, this is an example only and should be used as a guide, please adapt to your own internal processes and activities. The same mapping tool can be used for mapping other business activities such as your HR process for data capture for new (and existing employees).

START HERE



Getting Ready for the General Data Protection Regulation (GDPR) Changes

Audit Check List

Gaining consent and understanding individual's rights and understanding your Privacy Notice

The GDPR will be introducing stricter rules on the way consent for holding an individual's personal data is gained. You should review how you seek, record and manage consent and whether you need to make any changes to your current way of gaining permission.

There is a fundamental difference between telling a person how you're going to use their personal information and getting their consent. Check if you have a Privacy Policy (Privacy Notice) or a Fair Processing Information Sheet – this should be provided when you are collecting a person's data.

The starting point should be understanding the reason behind gaining consent from an individual.

- What data has been collected?
- Why data has been collected?
- Who it will be shared with?
- Was permission granted, when and where from?
- For non-sensitive data, "unambiguous" consent will suffice.

Privacy Notice, opt-in examples

The ICO have tested some samples of wording and opt-in options with the public. This is their recommendation of good practice when seeking consent for direct marketing.

Post ☐ **Email** ☐ **Telephone** ☐

Text message ☐ **Automated call** ☐

Your business should review the way you seek, record and manage consent for the processing and use of data.		
Suggested Actions To be able to move onto writing Privacy Notice there are the basics you need to understand first with regards to the collection of date.	**Completed**	**Additional Comment/Action**
1. Do you know what data you are collecting?	Yes/No	
2. Do you know why you are collecting the data?	Yes/No	
3. Do you know who is using the data?	Yes/No	
4. Did you activity ask them to opt-in? If you want individuals to consent to direct marketing, you should have a separate unticked opt-in box for this, prominently displayed. **Consent may not be needed to undertake direct marketing by post or phone call (unless the individual is registered with the Telephone Preference Service)**	Yes/No	

Getting Ready for the General Data Protection Regulation (GDPR) Changes

Audit Check List

Writing the Data Consent Form

Good practice would be to list the different purposes with separate unticked opt-in boxes for each or Yes/No buttons of equal size and prominence. Opt-in boxes can be prominently placed in your privacy notice. Alternatively, with online products and services you may wish to use 'just-in-time' notices so that relevant information appears at an appropriate time; see the section on just-in-time notices for more detail.

The ICO have written a set of words to get you started on your Data Consent Form.

Here at (organisation name) we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

However, from time to time we would like to contact you with details of other (specify products)/(offers)/(services)/(competitions)/(contracts)/(sub-contracting opportunities) we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

Post ☐ Email ☐ Telephone ☐

Text message ☐ Automated call ☐

We would also like to pass your details onto other (name of company/companies who you will pass information to)/(well defined category of companies), so that they can contact you by post/email or phone with details of (specify products)/(offers)/(services)/(competitions)/(contracts)/(sub-contracting opportunities) that they provide. If you consent to us passing on your details for that purpose please tick to confirm:

I agree ☐ Date _____

Getting Ready for the General Data Protection Regulation (GDPR) Changes

Audit Check List

Privacy Notice

Do you have a Privacy Policy (Privacy Notice) or a Fair Processing Information Sheet – this should always be provided when you are collecting a person's data.

The starting point of a Privacy Notice should be to tell people:

- Who you are
- What you are going to do with their information
- Who it will be shared with
- Think about how you use their information

Your business should review your Privacy Notice, if you do not have a Privacy Notice you should look to write one. A Privacy Notice can also tell people more than the basics and should do so where you think that not telling people will make your processing of that information unfair.		
Suggested Actions To write a Privacy Notice, these are the basics upon which all privacy notices should be built:	**Completed**	**Additional Comment/Action**
1. Check to see if you have a Privacy Notice	Yes/No	
2. Be clear about who you are (your company).	Yes/No	
3. Be clear on what you plan to do with the personal information such as used for marketing, securing contracts etc.	Yes/No	
4. Be clear on how long you store the information for.	Yes/No	
5. Be clear if you are holding personal data, you are clear on where you store it and if you need to keep all their details.	Yes/No	
6. Be clear on the individual's rights and access to their data.	Yes/No	
7. Have they given consent?	Yes/No	
8. You can download the ICO Privacy Notice checklist here https://ico.org.uk/media/for-organisations/documents/1625126/privacy-notice-checklist.pdf/		

Getting Ready for the General Data Protection Regulation (GDPR) Changes

Audit Check List

How do you deal with a breach in data?

Under the GDPR breaches must generally be notified to the Information Commissioner's Office (ICO) normally within **72** hours. A personal data breach is "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 in connection with the provision of a public electronic communications service".

- Check you have a procedure to detect a personal breach
- You should report and investigate a personal data breach
- The data controller must also notify the **individual affected**, if there is likely to be a high risk to their rights and freedoms

Data Breaches

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

Your business should ensue you have a Data Breach Policy and you know when and why to report a breach in data.

Suggested Actions In preparing for a data breach you would benefit from understanding the following	**Completed**	**Additional Comment/Action**
1. Are you prepared for a data a breach?	Yes/No	
2. Do you have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if you do not have all the details yet?	Yes/No	
3. Do you know what information you need to give to the individual if it effects their rights and freedom?	Yes/No	
4. Do you document all breaches even if they do not need reporting?	Yes/No	

Note: Whilst every effort has been made to ensure the accuracy of advice given, the BWF cannot accept liability for loss or damage arising from the use of the information supplied in this publication.