GDPR COMPLIANCY 10 STEP CHECKLIST
"In Laymens Terms"

GDPR (General Data Protection Regulation) comes into force early next year – do you know how the new rules will affect your business? Below are tips about the data protection issues you need to consider. And it is NOW you need to start implementing the new rules...Once understood and done you hopefully will not have to worry about it much more.

1. Do any data subjects you are collecting data from, including your employees, reside in the EEA/EU? Do your customers reside in the UK?

Then GDPR applies to you, even if you are based in a country outside the EU.

If YES:

It doesn't matter where your organisation is located so long as you collect and store information about customers. This can be in paper form or digital. So this means in physical folder/computer folders/CRM systems/mobile devices or even scrap pieces of paper!

2. Is your organisation aware of what personal data means under the GDPR?

The GDPR's definition of personal data is 'any information relating to an identified or identifiable natural person'. So basically...any type of information you hold about an individual.

If YES:

Then you need to make sure that information is dealt with according to the new rules.

3. Have you assessed the impact of the new definition of consent under the GDPR and how this affects your surveys?

GDPR's revised approach means you must have clear documentation that people are happy for you to email them. And remember, you will need to obtain new consent from any current contacts in your database as well.

If YES:

Consent for taking personal data will require the following elements under the GDPR:
. Be explained in plain language
. Be separate from other matters of the form
. Be made by a clear affirmative action (as opposed to silence, inactivity or pre-ticked boxes) . Be for all purposes of the data processing

. Must not be to the detriment of the data subject or a pre-condition for providing the service.

. Consent cannot be bundled for different processing activities – the data subject must be able to consent or refuse for each individual processing activity

. Consent must be withdrawable and the data subject must be told of right to withdraw consent at any time prior to giving his consent.

. If processing sensitive personal data consent must be explicit, meaning that there must be the express word "consent", as opposed to just personal data where it can be implied through a course of conduct.

So you would send an email (sounds strange this one but this is it) to a customer to say basically "are we ok contacting you by email in the future?"...then when they reply 'yes' then keep that email safe as proof you can email them!!!

4. Do you have a process for breach notification?

There will be a duty for all organisations to report certain types of data breaches and, in some cases, inform the individuals affected by the breach as well.

If YES:

So lets say you lost your mobile phone and it has customers numbers on it, then you would need to inform those customers within 72 hours. Other examples are break ins to office/car/van or a computer hack.

Anything like this needs to be sent to the ICO. The data subject must also be notified without undue delay after the main person resposible for your data protection becomes aware of the data breach, if the breach is likely to result in a high risk to the rights and freedoms of individuals.

For any staff who are dealing with customer data, they must notify the 'named' person who is responsible without undue delay after becoming aware of the data breach

5. Have you given the data subject the right to access his or her information?

Your customers must have the right to access any personal data that you store about them and this must be provided free of charge.

If YES:

Your customer (or anyone else you hold person information about) has the right to obtain from the named responsible person confirmation of whether personal data concerning them is being used, where it is being used and for what purposes.
This must be provided free of charge and you can only charge a reasonable fee if request is repetitive, excessive or unfounded.

6. Where a Customer /or any other person) has asked for his or her information, is the information given in a commonly useable and machine readable format?

When asked, you must use "reasonable means" to supply the information. For example, if the request is made electronically, you should provide the information in a commonly used electronic format.

If YES:

Basically...send them an email or text!

7. Does your organisation have the process of erasing the subject's data at his/her request?

Make sure you have a process in place for when an individual asks you to delete their personal data. Would you know where to find the data, who has to give permission to delete it and what internal processes are in place to make sure that it happens?

If YES:

So...if you are the person responsible for looking after the data you hold the person asking for removal of their personal information has the right to request you remove it....and...if you have passed their personal information to someone else you would be obliged to make that third party delete it.

The person asking for the removal of their information has this right if the information you hold on them is no longer valid. For example it could be an ex customer. You can object on the grounds of public interest or for the grounds of legal defence (For example if they were looking to sue you then that would be grounds to object to their request).

8. Does your organisation hold and process data only if it is absolutely necessary for the completion of its duties?

GDPR will introduce the concept of 'privacy by design' and by default to encourage organisations to consider data protection throughout the entire life cycle of any process. Organisations will need to implement internal policies and procedures to be compliant.

If YES:

The GDPR requires privacy by design. This means put together a plan of action to ensure they have the necessary tools. For example a paper shredder might come in handy! "Privacy by Design" includes processing data only when it is absolutely necessary for the completion of duties, and limiting access of personal data to those doing the processing.

9. Have you trained your staff on the GDPR and how to properly handle data?

The majority of data breaches occur because of human error. To make sure staff are aware of their obligations, organisations are encouraged to implement GDPR staff awareness training and provide evidence that they understand the risks.

If YES:

It is very important to train staff on the importance of the GDPR and how it can affect their business function. At the very least, all staff need to be made aware of the importance of looking after personal information and should have a point of contact to help them with queries regarding GDPR compliance.

10. Have you considered if you need to appoint a Data Protection Officer (DPO)?

For many businesses, it will be mandatory to appoint a DPO, for instance if your core activity involves the regular monitoring of individuals on a large scale. You should consider now whether or not you need to appoint a DPO and to make sure they have the required expertise and knowledge.

If YES:

It will be compulsory to have a Data Protection Officer if: (a) your business involves regular and systematic monitoring of people on a large scale; (b) you deal with special categories of data relating to criminal convictions and offences; or, (c) you are a public authority.

It is simply naming the person responsible for looking after the data you collect on people in your data protection policy. So it gives anyone worried about the data you collect on them a contact point of reference.

The named person obviously has to be aware of GDPR and is responsible for implementing it.