GDPR COMPLIANCY 10 STEP CHECKLIST

GDPR (General Data Protection Regulation) comes into force on May 25th 2018 – do you know how the new rules will affect your organisation? Start preparing for GDPR compliance now by finding out how well prepared you are or if there are still some data protection issues you need to consider.

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

If you are collecting data from citizens or employees that reside in EEA then GDPR applies to you, even if you are based in a country outside the EU.

If YES:

Make sure you are aware of your obligations, the GDPR has increased its scope of application. It doesn't matter where your organisation is located so long as it is processing or data belonging to a data subject residing in the EEA/EU

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'. There is, however, a wide interpretation – it could mean a nickname, an ID number, an IP address or other indirect identification.

If YES:

Make sure your organisation is aware that personal data under the GDPR means much more than it used to under the old regime. Personal data now means any information relating to an identified or identifiable natural person. This now includes unique identifiers, including: IP addresses and cookies (where they are used to uniquely identify the device, or in combination with other data, to identify the individual associated with the device, regardless of the use of pseudonymisation of cookies)

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 the audience is 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.

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:

Breach Notification is now compulsory for data controllers, where the breach is likely to result in a risk for the rights and freedoms of the individuals. This must be done within 72 hours of becoming aware of the breach and needs to be sent to the ICO. The data subject must also be notified without undue delay after the controller 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 data processors, they must notify the data controller 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?

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

If YES:

The data subject has the right to obtain from the data controller confirmation of whether personal data concerning them is being processed, where it is being processed and for what purposes.
This must be provided for free of charge and you can only charge a reasonable fee if request is repetitive, excessive or unfounded.

6. Where a data subject 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:

If the data subject has requested to receive the personal data concerning him, it must be provided in a commonly useable and machine readable format.

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:

The data subject can compel the data controller to erase all personal data about him and stop processing of it by third parties. Data subject has this right if: he withdraws consent, or if the data is no longer relevant to original purpose of processing. When considering such request, the controller can object based on grounds of public interest – if there is a public interest in the availability of the data, or for grounds of legal defence.

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 that organisations must implement appropriate technical and organisational measures, this 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, staff need to be aware of the new developments at a high level 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 core activities consist of regular and systematic monitoring of data subjects 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.