GDPR Checklist

Review your data protection measures with our simple GDPR checklist

REMEMBER

We are always here to help if you need us. We are just a phone call or an email away.

The GDPR (General Data Protection Regulation) came into effect across the EU on the 25th May 2018. Once the UK left the EU on 31st January 2020, the EU GDPR was brought into UK law. The Data Protection Act 2018 amended certain details to make it applicable to the UK and together they're both referred to as the UK GDPR.

Aside from the fact that all organisations need to be GDPR compliant, the benefits of compliance should be clear by themselves. Building and maintaining trust with your customers, peers, clients, and the general public; preventing reputational damage and costly data breaches; avoiding fines and penalties; and, helping to foster, support, and raise everyone's awareness of the importance of data privacy.

It's likely that back in 2018, during the great GDPR scramble, measures were hurriedly put in place and staff were given hastily assembled training required to become GDPR compliant. However, now with some breathing room and time to reflect, it's useful to review the risks to data your organisation faces and assess whether the measures you have in place are up to the task of preventing them.

Cyber security plays a role in the protection of personal data from loss, theft, or any kind of unauthorised access. Therefore you may wish to also download our cyber security checklist to review your practices when it comes to keeping your systems and data safe from threats.

Print off the grid part of this document (Page 2-3) and work through it to find out if your organisation completes these tasks. If concerns are raised on any of the fields, you should do all that is reasonably practicable to sort out the issue as soon as possible.

Disclaimer *- this checklist is not a definitive list and GDPR responsibilities/duties vary depending on the type and size of businesses. This checklist is to be used as rough guidance only. iHASCO assumes no responsibility for errors or omissions in the contents of this document.*

GDPR Checklist

Review your data protection measures with our simple GDPR checklist

Task	Status	Completion Date
Do you have a Data Protection Officer or an appointed GDPR expert? (If needed)		
Have you carried out a data audit and mapped where data comes into your organisation, where it goes, and who has access to it?		
Do you have day-to-day procedures in place to protect personal data? (Are they reviewed regularly and updated, if needed? Do you regularly check whether the data you hold is still necessary?)		
If you rely on consent to process data, are there procedures in place for regularly reviewing your methods of obtaining consent and whether consent is still valid?		
Are there procedures in place for data subjects to request access to their data? To restrict your use of it? To alter or correct it? To delete it? (In other words, to exercise their Individual Data Rights)		
Are there procedures in place for reviewing your privacy notice? Have you made any changes to how you collect or process data which need to be reflected?		
Is there any data you can delete or destroy that is no longer needed?		

Task	Status	Completion Date
If you use processors or sub-processors, do you have a written Data Processing Agreement in place with them?		
Have employees read and understood your GDPR policies?		
Have employees completed GDPR training or had recent refresher training?		

Comments:

For Employers/Responsible Person

1. Do you have a Data Protection Officer or an appointed GDPR expert? (if needed)

If you're a public authority, systematically monitor people, or regularly process special category data then you must appoint a DPO. But even if it's not a requirement for you, it's still a good idea. A DPO will help you comply with the GDPR; they'll provide advice; and they'll act as your spokesperson to the ICO - and the general public.

If you're not required to appoint a DPO, it's still worth appointing somebody to act as a GDPR expert or a group of people to act as a Data Protection Team. They must be broadly familiar with Data Protection legislation in order to help the organisation achieve compliance.

2. Have you carried out a data audit and mapped where data comes into your organisation, where it goes, and who has access to it?

You need to know where data is at any point of its life-cycle within your organisation, from the moment you obtain it to the moment it is deleted. To achieve this, you need to carry out a data audit to help you map out the journey that data takes. You should include a list of all the types of personal data you hold, where it came from, whether you share that information with other organisations, what you need it for and how long you'll keep it for.

The need to take stock of all the data you hold is ongoing. You should have regular data audits to keep on top of what you hold and trim away anything unnecessary.

3. Do you have day-to-day procedures in place to protect personal data? (Are they reviewed regularly and updated, if needed? Do you regularly check whether the data you hold is still necessary?)

Any organisation which processes personal data in any capacity must ensure that there are appropriate safeguards in place to keep data secure. For example, hardcopies of data should be shredded or redacted; employees should be encouraged to store personal data away from sight, lock their computers when they leave, and not to write their passwords on sticky notes; digital data should be password protected; communications encrypted; and unnecessary data deleted or anonymised.

4. If you rely on consent to process data, are there procedures in place for regularly reviewing your methods of obtaining consent and whether consent is still valid?

When somebody gives their consent for you to use their data, they are agreeing to a specific use/s. Sometimes, over time, due to various small changes here and there, the exact purpose/reason/methods of data collection/processing can gradually drift. If left unchecked, you may find that people who gave their consent for their data to be used in one way are now having their data used in a completely different way.

Make sure you regularly review your consent process - this includes how you obtain consent, where you obtain it, what information you provide people with when you collect data, and how long you intend to use their data.

5. Are there procedures in place for data subjects to request access to their data? To restrict your use of it? To alter or correct it? To delete it? (In other words, to exercise their Individual Data Rights)

The GDPR gives everyone certain rights over their personal data. Procedures should be in place to accommodate people who wish to exercise their rights. However, depending on the lawful basis you rely on for processing data in the first place, certain rights do and don't apply. Your process for accommodating people's rights should include a process for establishing whether they, in fact, can exercise that right and a way of explaining this to them.

6. Are there procedures in place for reviewing your privacy notice? Have you made any changes to how you collect or process data which need to be reflected?

The GDPR requires businesses to be transparent with how they collect, use, share, secure and process personal data. Your privacy policy must be easily accessible as well as clear and easy to understand. Changes to how you process data must be clearly reflected in the privacy policy. You should regularly review your policies to make sure everything is accurate and up-to-date.

7. Is there any data you can delete or destroy that is no longer needed?

When data is no longer needed it must be destroyed safely and securely - whether physical or digital. In fact, this is one of the central principles of the GDPR. If it's not needed, get rid of it. You should regularly review the data you

hold to make sure you absolutely need it still and you should always communicate how long you hold data for in your Privacy Policy.

8. If you use processors or sub-processors, do you have a written Data Processing Agreement in place with them?

Under the GDPR you must have a Data Processing Agreement (DPA) in place with any third parties that help you process data. A DPA is a legally binding contract between two organisations and outlines each other's roles and responsibilities.

9. Have employees read and understood your GDPR policies?

A business is responsible for communicating it's GDPR policies to every employee. The best way to do this is to ensure staff have read and are familiar with the contents of your privacy policy and any GDPR procedures you have in place. If anything changes, staff should be made aware. New starters should be given full GDPR training and this should be followed up with regular refresher training.

10. Have employees completed GDPR training or had recent refresher training?

Quality training in GDPR compliance will help your staff feel more confident about protecting personal data, as well as consolidate their understanding of their responsibilities. Keeping personal data secure requires every employee to arm themselves with the right knowledge and training is the way to do this. But like any training, it needs to be regularly reinforced.

How iHASCO can help you...

Here at iHASCO we have a range of online GDPR courses to suit your needs. Having already helped over 483,000 people work towards GDPR compliance you can be confident that our online GDPR courses make training simple.

GDPR EU Essentials: This course is aimed at all workers so they understand their responsibilities towards working with personal data, to ensure your organisation remains GDPR compliant.

GDPR EU for Management: It is essential that you have an in-depth understanding of the GDPR to ensure that your business is complying with the legislation. Personal data breaches can be incredibly damaging to your business, so if you make decisions about collecting and storing data this course is for you.

GDPR EU Refresher training: This slimmed down version of the GDPR Essentials training course is perfect to provide a refresher to staff that have previously undergone GDPR training.

GDPR UK Essentials Training: For those organisations handling UK data, this course will help users gain a full understanding of the Regulation, its importance, and how it applies to their role. By the end of the course, users will feel confident in carrying out their role safely and effectively and feel empowered to make a genuine difference in their workplace.

GDPR UK Advanced (Management) Training: Based on handling UK data, this course is for anyone responsible for creating, maintaining, managing, or overseeing data protection and/or data handling within their organisation. It is comprehensive, covering every possible aspect of the GDPR, providing users with an in-depth understanding of the Regulation and its implications, including interactive scenario-based questions so that users can apply their newly acquired knowledge to real-life examples.

GDPR UK in Education Training: This course is for all those working in the education sector, to understand their legal responsibilities when it comes to handling a wide range of personal data in an educational setting, and why it's so important to do so.