GDPR checklist

General Data Protection Regulation (GDPR) came in effect in the UK on 25 May 2018. It replaced the UK Data Protection Act (DPA), which had been in place since 1998 and needed to be updated due to the advance of technology.

GDPR contains many similarities to the UK Data Protection Act 1998 (DPA) as well as introducing some new or different requirements. It looks to ensure that individuals have more control over how their personal information is used, shared and updated. It includes six data protection principles that set out the main responsibilities for organisations.

As with the DPA, GDPR will be enforced by the **Information Commissioner's Office** (ICO). The ICO website contains useful information and will continue to publish regular guidance and updates after the regulations come into force.

This checklist is designed to help you fulfil your responsibilities under GDPR. It's a general guide rather than an exhaustive list, which you can adapt to suit the needs of your organisation. If you tick a shaded box, you need to put measures in place so that you can change your response. Please note that it cannot cover all eventualities and you therefore may need to seek further advice from the ICO. You can access the ICO Guide to GDPR **here**.

Audit

Question	Notes	Yes	No	Actions to take
1. Have you documented the personal information that the organisation collects?	A data audit will identify what information you are collecting, where it is held, the reason you are holding it and the legal basis for holding that information. This helps to understand the information in your organisation and make sure it is secure.	☐	☐	
2. Do you review the personal information you hold on a regular basis to ensure it is accurate and up to date?	The personal information that you hold should be accurate and up to date. How do you ensure that is the case? Are you checking on customer contact that their address and phone number are accurate?	☐	☐	
3. Are staff personal files held securely?	Staff files should be secure and accessed only by those who need to see them or action them.	☐	☐	
4. Is access to electronic customer records restricted with the use of passwords etc?	Any database storing personal information should be password protected.	☐	☐	
5. Do you have written agreements with contractors who have access to personal information you are collecting (such as debt collectors, cleaners or agency staff) that meet the	It is a requirement of the General Data Protection Regulation that any sub-contractor is subject to a written agreement which should outline their responsibilities and how they will ensure the security of the personal information shared with them.	☐	☐	

Question	Notes	Yes	No	Actions to take
GDPR requirements **detailed here**?				
6. Do your current contracts provide adequate security for personal information?	If your IT is outsourced or any part of your organisation where personal information will be shared or accessible, the contract in place should have some key clauses to ensure the security of the personal information that is accessible.	☐	☐	
7. Are the business laptops and removable media (USB drives) encrypted?	Where a laptop contains personal information, it is good practice to have the laptop encrypted, so if it was lost or stolen, the information on the laptop would not be accessible.	☐	☐	
8. Are you confident that your customer records are secure whilst in your custody?	Client records should be held securely. Paper records should be locked away and electronic records should have limited access to them. When moving records from one location to another, they should not be left unattended (for example, in a vehicle).	☐	☐	
9. Is any cloud storage you use based in the European Economic Area (EEA)?	The EEA is a group of countries where there is adequate security in place to protect personal information. If your cloud storage is outside the EEA, then there needs to be specific contract conditions or other measures in place.	☐	☐	
10. Are all your software programmes hosted in the EEA?	As with cloud storage if your software is hosted outside the EEA, then you will need to ensure that there is appropriate security or contract terms in place. If hosted in the USA, is the company registered with the Privacy Shield?	☐	☐	

Compliance

Question	Notes	Yes	No	Actions to take
11. Is the Privacy Policy on your website GDPR compliant?	There are new guidelines about Privacy Policies and any website now must give some specific information, so make sure your Privacy Policy is up to date.	☐	☐	
12. Are there clear privacy notices or statements provided at the time personal information is provided to your organisation?	At the point you collect information, there should be a clear statement showing what that information will be used for, who it will be shared with and how long it will be held.	☐	☐	
13. Do you understand the legal basis which you are processing	There has to be a legal basis for the collection, storage and processing of personal information.			

Question	Notes	Yes	No	Actions to take
personal information under?	The six bases are contract, legitimate interests, consent, legal obligation, public task and vital interests. More details can be found **here**.	☐	☐	
14. Where you have a newsletter sign up on your website – do you have a Privacy Notice in place and a mechanism for consent?	If you are collecting personal information (such as name or email address) from someone for the purposes of a newsletter and you don't already have a relationship with them, you will need to seek consent. A Privacy Notice should be provided prior to collecting the information.	☐	☐	
15. Where you are basing your processing on legitimate interests, is there a legitimate interests assessment in place for the processing?	Where you are basing your processing on legitimate interests this should be covered by a legitimate interest assessment.	☐	☐	
16. Where you are basing your processing on legitimate interests, have you disclosed these legitimate interests in your Privacy Policy?	Where you are basing your processing on legitimate interests this should be covered in your Privacy Policy.	☐	☐	
17. Where you are processing information on the basis of consent, does the historic consent you have obtained meet the requirements set down by GDPR for **consent**?	If historic consent does not meet the GDPR requirements for consent, you will need to refresh the consent to the new standard.	☐	☐	
18. If you are sending marketing text messages to customers, have you obtained appropriate customer consent?	Specific consent for marketing by text is a requirement of the Privacy and Electronic Communication Regulations (PECR).	☐	☐	
19. If you are marketing to your customers by phone, have you obtained specific consent?	Specific consent for marketing by phone is a requirement of the Privacy and Electronic Communication Regulations (PECR).	☐	☐	
20. Do you have a data protection policy setting out your data protection practices?	Create a simple data protection policy which sets out how you handle personal information. This should be available to both staff and customers.	☐	☐	
21. When recruiting new staff, do you delete and destroy unsuccessful	Unsuccessful applicants' information should be destroyed as a matter of course (as detailed in your retention policy). Remember			

Question	Notes	Yes	No	Actions to take
applicants information at the appropriate time?	emails containing CVs and applicant information will need deleting as well.	☐	☐	
22. Do you have a retention policy outlining how long information will be retained and how it will be destroyed? Is this relayed to customers?	A retention policy should be established outlining the periods you will retain various records. The period will vary depending on the record. There are some good practice periods such as seven years for accounting records.	☐	☐	
23. When deleting electronic files are you using an electronic file shredder that removes all trace of the original file?	You should be using an electronic file shredder. If you don't the data may be recoverable.	☐	☐	
24. Are you shredding paper files when they need to be destroyed?	Paper files should be shredded. Ensure any shredding business you employ to do this is reputable and will certify destruction.	☐	☐	
25. If you are using CCTV at your business premises, are the recordings appropriately secured?	You should have a CCTV code of practice which identifies the reason for using CCTV, how images can be viewed and by whom and the retention period.	☐	☐	
26. If you are recording telephone calls, is this clearly stated?	If you are recording telephone calls, this should be obvious to someone telephoning your organisation. You should also have a clear policy about recording calls and who can listen to them.	☐	☐	
27. When old electronic equipment has reached the end of its useful life, is it properly cleaned prior to disposal?	All old electronic equipment should be properly cleaned to remove any trace of electronic files before it is repurposed.	☐	☐	
28. Are paper files containing personal information held securely?	As with electronic files, paper files should be securely held too.	☐	☐	
29. Are emails with sensitive personal information (such as health and wellbeing data) encrypted or password protected?	Email messages can be intercepted. You therefore need to take special precautions when emailing sensitive personal information.	☐	☐	
30. Are staff using their own mobile phones, tablets or computers to access customer data?	How do you ensure that the information on those phones is secure? Are phones locked when not in use? Is two factor authentication in place where they have access to the client database? If the phone was lost or stolen, how	☐	☐	

Question	Notes	Yes	No	Actions to take
	much inappropriate access could be gained to your systems?			
31. Is there a secure method for exchanging files with customers in place?	Any email attachments can be intercepted and read, so what controls do you have to secure files in transit (such as file transfer protocol (FTP) and shared file facilities).	☐	☐	
32. Is it possible to download your customer or staff database onto a spreadsheet and save it to a USB memory stick or email it outside the organisation?	This could be a key area for data leakage and leaves your customer and staff files vulnerable. Computers can be locked down so as not to accept USB memory sticks and email attachment sizes can be limited.	☐	☐	
33. If a client moved to another organisation and requested, under data portability requirements, to transfer their data, would you be readily able to transfer their records?	Under GDPR, a customer has the right to be able to move their information from one provider to another. You need to consider how this would work in your organisation.	☐	☐	
34. AAT licensed members only - Do you have written letters of engagement in place with your clients that meet the GDPR requirements **detailed here**?	As a Data Processor for your clients, you should have a written agreement in place.	☐	☐	

Training

Question	Notes	Yes	No	Actions to take
35. Do you know what constitutes personal information under GDPR?	This covers anything that can be used to identify an individual, and includes information such as name, address, email address, telephone number, date of birth and IP address.	☐	☐	
36. Do you know what constitutes sensitive or special category personal information under GDPR?	This is information such as race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.	☐	☐	
37. Have all staff received training for confidentiality or data protection over the last year?	It is good practice for all staff to receive confidentiality training at least annually.	☐	☐	
38. Has the training undertaken been documented?	Any training for data protection should be documented so you can prove to the Information Commissioner's Office that it is taking place.	☐	☐	
39. Do all staff sign a confidentiality clause as part of their employment?	There should be a confidentiality clause in your employment contract.	☐	☐	
40. Do those taking telephone calls take steps to protect the privacy of the person they are talking to?	How do staff in public areas protect the identity of callers? Can they be overheard by clients?	☐	☐	
41. Do you verify the identity of a caller before providing any information?	Before you provide any personal information (and as good business practice) you should be clear who you are providing that information to.	☐	☐	
42. Would you be able to identify if a data breach had occurred in your organisation?	You should have in place various steps to ensure that any potential breach is identified promptly. This could include regular review of information.	☐	☐	
43. Do you know what you need to do in the event of a data breach?	There are obligations for reporting and handling a data breach so you should have a process in place to ensure you can meet your legislative requirements.	☐	☐	
44. Would your staff recognise a request to see the information held about an individual?	Staff should be aware what a subject access request looks like so they can pass it to the appropriate person for response. This should be covered as part of your annual data protection training.	☐	☐	

Question	Notes	Yes	No	Actions to take
45. Would you know how to handle a **subject access request**?	Subject access requests can vary in complexity and there should be a process in place to respond appropriately to a request. This can be usefully included in your Data Protection Policy.	☐	☐	
46. An individual can exercise the right to be forgotten. Do you understand what this would entail in your organisation and which records you would need to delete?	Right to be forgotten is where an individual can request that you remove all their personal data. There are exceptions to this if the data is required as part of a legal requirement so you need to be sure what can and cannot be deleted.	☐	☐	

Definitions

Privacy Policy – A Privacy Policy is a statement, usually on a website, which discloses some or all of the ways a business gathers, uses, discloses, and manages a customer or client's data.

Privacy Notice –This is information required at the point of collecting personal information telling the individual how their information will be used. It must meet GDPR requirements.

Data Controller – A Data Controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

Data Processor – A Data Processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.