GDPR Auditing®

GDPR Self-Assessment Workbook and Portal

Why worry about GDPR?

"I don't think we need to worry about GDPR…" "I am not sure that GDPR applies to our business…." "These new regulations are over the top for SMEs, there's no way they are going to apply to someone like us and anyway the costs of complying are ridiculous…" ….are some of the statements we have heard from organisations who are actively considering GDPR, rather than ignoring it completely.

GDPR would not apply if an organisation deals with absolutely NO personal data and has no employees and does nothing to record personal data from clients, or visitors, or suppliers, for example. In reality of course, most organisations have some of the following:

- Employees - they have personal data
- Customers - who have personal data
- Suppliers - who might have personal data, particularly sole traders
- marketing contacts - who have personal data
- support contacts - for whom there may be personal data
- and more…

Personal Data might be in one system, or they might be in

- HR systems
- Customer Relationship Management databases
  Contracts databases or Accounts databases
- Email marketing systems
- IT support tools or helpdesk software
- Email, desktop applications, spreadsheets, local or network storage

But that is only the data view and, in reality, only some of the things you need to be worrying about when it comes to personal data. What about the other areas of GDPR?

- Who is going to be the nominated ICO contact?
- Who will write the data processing statement for one or all departments?
- Who will be responsible for incident management or breach reporting?
- Who will respond to data subject access requests?

Many businesses have had very little to do under the Data Protection Act. GDPR changes all that with enhanced rights for data subjects, obligations on organisations to show they are compliant and a dramatically increased regime of fines and penalties.

To help small businesses address GDPR in a low cost way, we have built the GDPR Auditing Self-assessment workbook and portal.

One of our earliest clients gave us the following feedback: *"I have been using GDPR Auditing's Workbook and Portal for several months, as we prepare for the introduction of the GDPR on 25 May. These resources contain a set of logical steps, which navigate a course towards data protection compliance. The sheer volume of detail in the materials is impressive and reassuring for the user. The resources are useful, both as a practical workbook and as a source of reference information about the GDPR, something I've found invaluable to augment my knowledge and understanding of the new legislation."*

What is included?

The core of the Workbook outlines a recommended 12-step quick start plan to get you well on the way to GDPR compliance. These are a tailored series of tasks that will enable your practice to comply with the GDPR.

The Workbook starts with a list of the 12 steps. Work your way through each of the tabs in turn. We have designed it in such a way that you should only have to enter a piece of information once and it will automatically be populated in the relevant places elsewhere in the workbook. As you work through the workbook you will almost certainly identify areas needing further detailed attention. In some cases, these can be addressed from internal resources, but in some cases, you may need to seek external advice or services.

It is also important to note that the Workbook is not just an aid to achieving compliance it is also a record that you have complied with legislation. It should be retained as a living document and produced as evidence if required by the ICO or other regulatory authority.

The workbook contains a further 7 tabs all relating to GDPR tasks, and the portal contains details guides, examples, templates, and downloads, all to help you on your way.

GDPRAuditing — Licensed to A N Other Company

Quickstart 12 Steps

Quick Link	Tab Name	Description	Guide Title
1	Data Security Owner	Assign responsibility for GDPR Compliance, ensuring Data Protection and completing this pack.	Data Security Owner
2	Record of Processing (RoP)	Complete the items in the Record of Processing Column with your own details	Record of Processing
3	Data Retention Schedule (DRS)	Check the Retention Schedule, make sure it reflects your practice and add, remove amend as necessary	Data Retention Schedule
4	Privacy Notice Online	Some of the data for this is inserted from the RoP, check and ensure the notices reflects your practice	Privacy Notice Online
5	Privacy Notice Employee	Compare your employment contracts against the checklist and complete new privacy notices for employees to review and sign	Employee Contracts
6	Privacy Notice Client	Compare your client engagement letters against the checklist and complete new privacy notices for clients to accompany agreements	Client Agreements
7	Marketing Consent	Consent, what you need, where you need it, checklist for getting consent right	Consent
8	Sec Awareness - ISP Review Log	Add all your employees to the schedule, have them read the Information Security Policy and read the awareness training	12 Steps or Data Security Owner
9	3rd Party Contracts	Ensure all 3rd party contract contain appropriate GDPR clauses	3rd Party Contracts
10	Data Subject Request Tracker	Know how to recognise, track, and respond to requests from data subjects	Data Subject Requests
11a	Incident Log	Know how to handle incidents, categorise as data incidents and report breaches when required	Incidents and Breach Reporting
11b	Breach Notification Template	Report Breaches using the Breach Template, 72 hours and 4 week intervals.	Incidents and Breach Reporting
12	(TOSM) Checklist	Work through the checklist and ensure you are following or have a plan to address each item	TOSM

Step 1 – Data Security Owner. Provides advice on the selection of a person in your organisation to manage the various tasks. This could be the Data Protection Officer if you decide to appoint one, but otherwise could be anyone in your organization.

1	Data Security Owner	Assign responsibility for GDPR Compliance, ensuring Data Protection and completing this pack.

Step 2 – Record of Processing. You will need to enter information about your organisation on this page and edit standard text that describes details of the way you process personal data; about whom the information is processed and so on. The completed text on this page will be drawn into various other sections of the Workbook.

2	Record of Processing (RoP)	Complete the items in the Record of Processing Column with your own details

Step 3 – Data Retention Schedule. Records details of the data you retain in your organisation. To save time we have pre-populated this page with many of the data types that most firms will process together with other required information, including: who owns the data, what is the retention period, legal reasons for retention, classification, storage, disposal actions, where did the data come from, where does the data go to, 3rd party and international aspects. You should edit the pre-filled content to reflect your practice preferences.

3	Data Retention Schedule (DRS)	Check the Retention Schedule, make sure it reflects your practice and add, remove amend as necessary

3. Data Retention Schedule

Back To 12 Steps

Record Reference	Record Type	Owner/Area	Retention Period	Legal Reference	GDPR	Cl
(cross reference from Data Asset Inventory)	(Description)	(responsible for creation and maintenance)	(or criteria for determining if not stated)	(where there is a legal or compliance reason for retention)	(Does this record contain GDPR relevant data)	Oth this
Example 1.1	Employee File	HR	3 years past leaving	Employment reference	Yes	Re
Example 1.2					Yes	Pu
1	Prospect contact details	Marketing	No retention period once prospect withdraws permission to use their personal data.	None	Yes	Inte
2	Employee records	HR	Maximum 6 years after employment has ceased	Data protection Act, Taxes Management Acts	Yes	Co
3	Health and safety records	HR	3 years for general records, permanently if refers to hazardous substances.	Commercial best practice	Yes	Inte

Step 4 – Privacy Notice Online. This is a template that creates a Privacy Notice that you would use on your website.

4	Privacy Notice Online	Some of the data for this is inserted from the RoP, check and ensure the notices reflects your practice

Step 5 – Privacy Notice Employee. This is a template that creates a new privacy notices for employees to review and sign. Compare your employment contracts against the checklist.

5	Privacy Notice Employee	Compare your employment contracts against the checklist and complete new privacy notices for employees to review and sign

Step 6 – Privacy Notice Clients. This is a template that creates a privacy notice to accompany your customer contracts. Compare your customer terms and conditions against the checklist and amend as necessary.

6	Privacy Notice Client	Compare your client engagement letters against the checklist and complete new privacy notices for clients to accompany agreements

Step 7 – Marketing Consent. The management of marketing mailing lists will require more rigorous consent processes under the GDPR. This step describes the principle of consent, what you need, where you need it and checklists for getting consent right.

7	Marketing Consent	Consent, what you need, where you need it, checklist for getting consent right

7. Marketing Consent

What to check when seeking consent

		Check
1	Is consent the most appropriate (lawful) basis for processing?	No
2	The request for consent is easily recognisable and separate from any other agreement	No
3	Terms and conditions are visible separate from any other consents	No
4	Data subjects have to make a conscious and informed decisions to opt-in	No
5	All options and agreements are unticked by default	No

Step 8 - Security Awareness. This template is logging when your staff have read your Information Security Policy and completed data protection awareness training.

8	Sec Awareness - ISP Review Log	Add all your employees to the schedule, have them read the Information Security Policy and read the awareness training

Step 9 – Third Party Contracts. This template is a checklist that ensures you record that you have reviewed and received appropriate assurances that contracts with third parties that have access to personal data controlled by your organization are managed in accordance with GDPR.

9	3rd Party Contracts	Ensure all 3rd party contract contain appropriate GDPR clauses

9. 3rd Party Contracts

Overall Status of 3rd Party Contracts

		Check
1	I have reviewed all on my 3rd part contracts where the processing of personal data is actual or possible	Yes
2	I have changed my 3rd party contracts so that they are now suitable for GDPR	No
3	I have agreed the new GDPR contracts with my relevant 3rd parties.	No
4	I am seeking new suppliers for 3rd parties who will not sign up to the GDPR contracts	No
5	I am confident that my 3rd party contracts are fit for purpose and are unambiguous as to who is responsible under GDPR	No
6	Where I am a processor I am confident that my contract with the controller is fair and reasonable under GDPR	n/a

Step 10 – Data Subject Access Requests. This template records requests you have received from individuals regarding any personal data you may hold.

10	Data Subject Request Tracker	Know how to recognise, track, and respond to requests from data subjects

Step 11A – Incident Log. This template records incidents and breaches.

11a	Incident Log	Know how to handle incidents, categorise as data incidents and report breaches when required

11a. Incident Log

Based on the ITIL Framework

Incident Number	Category	Urgency	Impact	Priority	Priority Description	Resolution Hours	
Unique ID Number	Incident Type	How urgent is this	What is the impact	Calculated from Urgency and Impact			D in
	Select from drop down list	Select from drop down list	Select from drop down list	Calculated	Calculated	Calculated	Dat
1	Availability	Med	Low	4	Low	48	1
3		Low	Low	5	Planning	Planned	
4		Low	Low	5	Planning	Planned	

Step 11B – Breach Notifications. This template records breach notifications.

11b	Breach Notification Template	Report Breaches using the Breach Template, 72 hours and 4 week intervals.

Step 12 – Technical and Organisational Security Measures Checklist. This template is the Technical and Organisational Security Measures checklist required by GDPR. This is a comprehensive checklist that will demonstrate that you have performed all the necessary actions to achieve compliance.

12	(TOSM) Checklist	Work through the checklist and ensure you are following or have a plan to address each item

Apart from these 12 steps, the Workbook has additional check lists and logs that you may want to use. And, finally, when you subscribe to a Workbook, you will be licensed to use our online knowledge base. This is a series of guides that gives you more information about each of the 12 steps.

If you would like to subscribe to the *GDPR Self-Assessment Workbook and Portal* or simply want more information, then click on this link: www.gdprauditing.com/gdpr-sa.