

# GDPR IMPLEMENTATION PROJECT PLAN

**PLAN NOTE:** This plan has been designed to provide steps for implementing the GDPR and assessing your readiness and gaps. It is a lengthy document and whilst the GDPR is not a **'one-size-fits-all'** Regulation, it is impossible for us to create a specific plan that suits all businesses. The **'Condition or Purpose'** column provides guidance on whether the actions are **'mandatory'**, **'condition-based'** or **'guidance'**, which aids in excluding those areas not relevant to you.

The suggested actions in this plan will **not** give you a complete approach for implementation; because there will be specific requirements and functions that are unique to your business. However, through the actions that have been provided, you will be able to review each business area and GDPR requirement and systematically assess your organisation against the standards and expectations.

**For small and micro-organisations**, the only specific exemption relative to your size is the Article 30 Processing Activities Requirement; however, the GDPR states several times that all measures and requirements should be *'proportionate to your size, nature and nature'*. It is likely for many small businesses, policy sections on *'Appointing a DPO', 'International Transfer'* and *'Third-Party Processor'* can be reduced or even removed. However, there will also be SME's or sole traders who must comply with these areas, as inclusion of all requirements is essential in a GDPR Toolkit. Our documents take a universal approach, meaning all requirements for all businesses are included and you then customise or reduce if not applicable. This method is essential for compliance and to ensure that smaller firms are not being given an *'easier'* package that opens them up to penalties and enforcement down the line.

**BUSINESS REVIEW:** At the end of the plan, you will see 2 additional sections titled *'Small & Micro Business'* and *'Medium & Large Organisation'*. Obviously, the size of a business is only one part of the equation (nature and scope being just as important); however, these sections provide some business specific guidance that may be useful for business functions and the GDPR.

**GDPR CHECKLIST:** We recommend starting by working through our GDPR Checklist and answer all questions (where applicable). This is to give you a written list of the areas where you have gaps, are non-compliant or just need to make some improvements.

Our checklist is extensive and may seem geared to larger organisations (i.e. overall for small firms); however, businesses big and small must comply with the GDPR and except for Article 30 - Processing Activities records, there are no limited or diluted exceptions or conditions based on size. It is all about the type and volume of the personal data you process, which is not dependent on how many employees you have!

## GDPR IMPLEMENTATION PROJECT PLAN

REQUIREMENT	CONDITION OR PURPOSE	ACTIONS	NOTES
Review Existing Data Protection Policies, Processes & Documents	Most of the organisations processing personal data will have been aligned under the existing Data Protection Act 1998. This means many will have some form of program already in place	<ol style="list-style-type: none"> <li>Identify any documents, policies, processes, systems and job roles that relate to data protection (i.e. risk forms, employee handbooks, bank details templates, assessment reports, approvals etc)</li> <li>If you are continuing to use any existing data protection relevant documents, ensure that any reference to Data Protection Act 1998 is replaced with the GDPR (or you can use Data Protection Laws reference to the GDPR &amp; Data Protection Act)</li> <li>If the document, policy, application or online form collects personal data, ensure it is accompanied by a compliant Privacy Notice (see Privacy Notice section) and if applicable, consent request</li> </ol>	<p>It is important to remember that many parts of the GDPR are the same as those in the current DPA. With as much emphasis on the GDPR, many firms are starting from scratch with processes that may just need tweaking.</p> <p>As you have purchased our GDPR documents, you are likely to be replacing any policies &amp; templates; however, you will likely have forms, documents &amp; templates specific to your business type that can be revised instead of replaced.</p>
<b>Accountability Principle</b> (Article 5(2))	The controller shall be responsible for, and be able to demonstrate compliance with, the data protection principles	<ol style="list-style-type: none"> <li>To demonstrate compliance with the GDPR, you need to be documenting all procedures, processing activities, training, measures and controls that evidence compliance with the principles and requirements</li> <li>Ensure that you have and can maintain a clear, structured set of records for all GDPR requirements</li> <li>For organisations with managerial levels, providing Management Information on a regular basis is an essential part of demonstrating compliance</li> </ol>	Accountability is a new addition to the data protection principles and focuses on demonstration and documentation

REQUIREMENT	CONDITION OR PURPOSE	ACTIONS	NOTES
<b>GDPR Awareness &amp; Staff Training</b>	<p><b>Guidance:</b></p> <p>The GDPR will affect all staff and all business functions, so ensuring that everyone is aware of the changes is essential</p>	<ol style="list-style-type: none"> <li>1. Organise a meeting with Management to discuss the timeframe, requirements &amp; impact of implementing GDPR</li> <li>2. Decision makers &amp; key people must understand the changes and what is expected</li> <li>3. Dependant on your size &amp; scope, allocate the resources &amp; budget required</li> <li>4. Identify which employees handle personal data or are directly involved in, affected by data protection</li> <li>5. Provide those identified above with GDPR staff training sessions as soon as possible</li> <li>6. Roll out training to all other staff (<i>in stages or in full dependant on your size</i>)</li> <li>7. Create an intranet or location where GDPR support and resources can be accessed</li> <li>8. Create/revise training records for all staff and document all training sessions, support &amp; resources</li> </ol>	<p>This part of the implementation project can run alongside the other requirements; however, it is important not to lead awareness and training to the last minute. Large organisations can end up with gaps if not planned correctly and smaller ones with duplications, which can cost time &amp; money.</p> <p>Know Your Compliance have a self-delivery <b>GDPR Staff Training Package</b> that can be used for initial and ongoing sessions for a one-off cost. You can also find training online or used an external provider</p> <p>For small organisations, working through this plan, reading the policy documents and templates &amp; referring to ICO's extensive guidance can serve as training</p>
<p><b>Appoint a Data Protection Officer (DPO) or Lead</b></p> <p>(Article 37)</p>	<p><b>A DPO is mandatory when:</b></p> <ol style="list-style-type: none"> <li>a) Processing is carried out by a public authority or body</li> <li>b) Core activities consist of processing operations which require regular &amp; systematic monitoring of data subjects on a large scale; <b>or</b></li> <li>c) consist of processing on a large scale of special category or criminal convictions personal data</li> </ol>	<ol style="list-style-type: none"> <li>1. Designate a Data Protection Officer or Lead</li> <li>2. Ensure adequate training and support is made available to the appointed person</li> <li>3. Document reporting lines to and from the DPO to employees, senior management &amp; third-parties</li> <li>4. Complete the <b>DPO Responsibilities</b> template with the DPO/Leads details</li> <li>5. Register the details of your DPO with the ICO</li> </ol>	<p>See Article 9 for definitions of special category data &amp; Article 10 for criminal convictions</p> <p>Even if you are not obligated to appoint a DPO, having a designated lead is useful for carrying out DPO duties &amp; maintaining compliance with the GDPR requirements</p> <p><b>Note:</b> if it is not clear from the conditions whether you need to appoint a DPO, you should record your assessment determination process</p>

REQUIREMENT	CONDITION OR PURPOSE	ACTIONS	NOTES
<b>Carry out an Information Audit</b>	<p><b>Guidance:</b></p> <p>Essential for documenting data flows &amp; recommended by the ICO to assist with GDPR preparation &amp; ongoing compliance</p>	<ol style="list-style-type: none"> <li>1. Decide if you are completing one audit for the whole company or one per business area</li> <li>2. Use the <b>Information Audit</b> template map the personal data flowing through your organisation</li> <li>3. Review all personal data sources and document in the audit which legal basis you using to process under Article 6(1) &amp; 9(1)</li> <li>4. Aim to have a separate line for each processing purpose (i.e. you collect name, address, email &amp; DOB from customer; the name &amp; address are for delivery; the email is opt-in marketing &amp; the DOB for a credit check. These categories have different processing purposes and so should be on a separate line, despite being collected at same time &amp; from same source)</li> </ol>	<p>If completing multiple audits, you must bring the data together and review for gaps and duplications at the end</p> <p><b>Optional:</b> You can add a column to the audit template for <b>'Rights'</b> with details of which rights apply to each category (i.e. <i>Employee have the right to request access, but not to erasure; those under legal obligation processing can request rectification of data, but not object to processing</i>).</p> <p>This would then give you an at-a-glance view of which data subject rights are applicable for the personal data categories you have detailed on the audit and can be reference when you receive a request.</p>
<p><b>Record Processing Activities</b></p> <p>(Article 30)</p>	<p><b>Not applicable to organisations with less than 250 employees, unless processing: -</b></p> <ul style="list-style-type: none"> <li>• is likely to result in a risk to data subjects</li> <li>• is not occasional; or</li> <li>• includes special category or criminal conviction data (Article 9(1) or 10)</li> </ul>	<ol style="list-style-type: none"> <li>1. Using the headings in the register template, you can gather the required information per business area using a questionnaire</li> <li>2. Review existing retention periods, processor agreements, information security measures &amp; recipients of data to obtain the necessary data</li> <li>3. Complete the <b>Processing Activities Register</b></li> <li>4. The register should be reviewed regularly to ensure it is still accurate and up-to-date. Choose a frequency based on your size and add review date to a calendar or audit register</li> </ol>	<p>You can use some of the information already documented in your Information Audit</p> <p>Controllers and processors have slightly different documentation obligations</p> <p>If you are a controller and process special category or criminal conviction offence data, also complete the blue section of the register to comply with Schedule 1 of the Data Protection Bill</p>

REQUIREMENT	CONDITION OR PURPOSE	ACTIONS	NOTES
<b>Review Existing Privacy Notice(s)</b> <i>(Articles 12, 13, 14)</i>	<b>Mandatory requirement:</b> All controllers are required to have a Privacy Notice in place providing the GDPR information disclosures	<ol style="list-style-type: none"> <li>Using the Information Audit data, you will be able to identify where personal data is initially obtained</li> <li>Assess how many notices you need &amp; what format they should be in*</li> <li><b>Review/create a new Privacy Notice noting: -</b> <ol style="list-style-type: none"> <li>Name &amp; contact details of the controller &amp; if applicable, their representative &amp; DPO</li> <li>Purposes &amp; legal basis of the processing (&amp; if applicable, the legitimate interests)</li> <li>Recipients of personal data &amp; details of transfers to third country and safeguards</li> <li>Retention period or criteria to determine period</li> <li>Details of data subject's rights</li> <li>If processing based on consent, right to withdraw consent at any time</li> <li>Right to lodge complaint with supervisory authority</li> <li>Whether the provision of personal data is a statutory or contractual requirement (<i>&amp; consequences of failure to provide data</i>)</li> <li>Existence of automated decision-making</li> </ol> </li> <li>Use the <b>Privacy Notice template</b> for revise/create your notice(s) &amp; customise to suit your business</li> <li>Ensure your notice is legible, clear &amp; is not bundled with any other information or T&amp;C's</li> <li>If relying on consent for processing data, the notice needs to be accompanied by a consent form</li> </ol>	<p>*It is best practice to have a notice for each processing activity (<i>i.e. a paper format customised to employees, an electronic notice for online forms etc</i>)</p> <p>If data is not obtained directly from individual, you must also specify the categories and source of personal data</p>

		If you offer promotions, offers, newsletters, marketing etc as an option when obtaining personal data, you <b>must</b> have a clear opt-in section towards the end of the notice with unticked, opt-in boxes ( <i>see template</i> )	
REQUIREMENT	CONDITION OR PURPOSE	ACTIONS	NOTES

**PAGES 6-21 REMOVED IN SAMPLE  
DOCUMENT**