# GDPR Compliance for Small Businesses

This playbook outlines the steps required for small businesses to achieve compliance with the General Data Protection Regulation (GDPR). It aims to guide businesses through the process of protecting customer data in accordance with the regulation.

## Step 1: **Awareness**

Raise awareness among key people in your organization about the requirements of GDPR. Ensure that decision-makers and key people in your organization are aware that the law has changed, and understand the impact this is likely to have.

## Step 2: **Information Audit**

Document what personal data you hold, where it came from, who you share it with, and what you do with it. This may require an information audit.

## Step 3: **Privacy Notices**

Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

## Step 4: **Individuals' Rights**

Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically in a commonly used format.

## Step 5: **Access Requests**

Update your procedures and plan how you will handle requests within the new timescales and provide any additional information required under GDPR.

## Step 6: **Legal Basis**

Identify the legal basis for your processing activity in the GDPR, document it, and update your privacy notice to explain it.

## Step 7: **Consent**

Review how you seek, record, and manage consent and whether you need to make any changes. Refresh existing consents if they don’t meet the GDPR standard.

## Step 8: **Children**

If your business processes children’s personal data, verify if you need to put systems in place to verify individuals’ ages and to gather parental or guardian consent for the data processing activity.

## Step 9: **Data Breaches**

Make sure you have the right procedures in place to detect, report, and investigate a personal data breach.

## Step 10: **Data Protection Impact Assessment**

Familiarize yourself with the guidance from the relevant regulatory authority and work out how to implement an impact assessment in your organization.

### Step 11: **Data Protection Officers**

Designate a Data Protection Officer or someone to take responsibility for data protection compliance and assess where this role will sit within your organization’s structure and governance arrangements.

### Step 12: **International Operations**

If your business operates in multiple EU member states, determine your lead data protection supervisory authority and document this.

# General Notes

## Documentation

Keep detailed records of all data processing activities, including the purpose of all activities, which will help you comply with the accountability principle of GDPR.

## Continuous Review

Regularly review your data protection processes and policies to ensure continual compliance with the GDPR regulations.

## Training

Provide your staff with GDPR training to make them aware of the importance of GDPR and to ensure they understand the compliance requirements.