The General Data Protection Regulation

Accountability Checklist

Under the General Data Protection Regulation, your business can be held directly liable for the security of personal data. Failure to comply with the General Data Protection Regulation could lead to the Information Commissioner's Office imposing a fine of up to 4% of your annual turnover therefore it is imperative that you could evidence how your business has implemented the regulations if required.

The following checklist may guide you through initial steps to take to implement the General Data Protection Regulation in your business:

Data Protection Principles

☐ Understand the General Data Protection Regulation principles and review any policies, codes of conduct and training that you already have in place to ensure that they are consistent with the principles. This may include creating a policy where one does not already exist within your business.

☐ Identify how you will "demonstrate compliance" i.e. How are you meeting the requirements? This may include adherence to codes of conduct, paper trails of decisions relating to data processing and ensuring the existence of up to date process documents, company policies etc.

Lawfulness of Processing, Further Processing and Consent

☐ Identify your business' reasons for processing information and document them

☐ Where you capture consent ensure that this meets the requirements of the General Data Protection Regulation

☐ Ensure that you document your ability to demonstrate how decisions to use data for further processing purposes have been reached and what factors have been considered in making these decisions

☐ Review any agreements you have where information is shared with a third party to ensure they meet the requirements of the General Data Protection Regulation

☐ Ensure that consent gathered prior to the implementation of the General Data Protection Regulation that does not meet requirements is recaptured or removed from your marketing lists and databases

Sensitive Data and Lawful Processing

☐ Ensure that you have clarity about why you process sensitive and/or special categories of data, and check these grounds will still be applicable for your business - this includes capturing and recording of a customer's religion

The General Data Protection Regulation
Accountability Checklist

PrivacyPolicy

☐ Review existing privacy policies and update them if required – the Information Commissioner's Office website and the Privacy Policy awareness document provided can provide further guidance

☐ Ensure privacy notices and policies detail customer rights in a manner that is clear and unambiguous to the customer

☐ Where data is collected indirectly (website, coupon etc.) ensure that notice is given at the appropriate time

☐ Work with partners/third parties who collect data on your behalf to assign responsibility for notice review, update and approval

Customer Rights

☐ Confirm that your systems are able to meet requirements of data subject rights including right to be forgotten, right to object and right to rectification

☐ Review your current business' processes, procedures and training to ensure that they are sufficient and in line with the new General Data Protection Regulation requirements

☐ Develop template response letters, ensuring that all elements of the supporting information is captured

☐ Consider and document within your business' processes and procedures how you will address difficulties raised should data relate to more than one data subject, e.g. if a funeral is arranged with two arrangers noted, a subject access request would only apply to one individual therefore the details of the second arranger should be redacted prior to being shared

☐ Ensure that your business can respond to customers regarding their rights within one calendar month

☐ Ensure that staff who may receive data subject requests (also known as Subject Access Requests or SARs) recognise them and know how to deal with them

The General Data Protection Regulation
Accountability Checklist

Breach Notification

☐ Develop and update internal breach notification including identification processes and incident response plans. Processes should include notification to funeral plan providers where affected customers hold a funeral plan.

☐ Develop Information Commissioner's Office notification process

Key Responsibilities

☐ Complete the Information Commissioner's Office registration self assessment to confirm if you are required to register your business as a Data Controller

☐ Consider if your business needs to appoint a Data Protection Officer - businesses must appoint a Data Protection Officer if they process sensitive data on a large scale

☐ Where no Data Protection Officer is required, it is best practice to assign responsibility for data protection compliance to a member of your team

☐ Review your current compliance strategy to ensure there are sufficient assessments, audits, training and reviews of policy to ensure ongoing adherence with the General Data Protection Regulation

☐ Monitor the Information Commissioner's Office for updates on codes of practices, guidance and supplier terms for contracts

Privacy by Design- considering how changes in your business impact customer data

☐ Ensure that where you are making changes to your processes, systems, premises etc. that you document how these changes impact your customer data, e.g. if you opt to change your data storage procedures from hard copy to electronic storage, you must document any potential impact it may have on the customer and store the document with your decisions log

☐ Ensure you document what actions you are taking to minimise risk of unauthorised or unlawful processing and against accidental loss, destruction or damage before any changes are made

The General Data Protection Regulation
Accountability Checklist

Data Security

☐ Ensure that physical customer documentation is held in a secure area e.g. locked room, locked filing cabinet, locked drawer

☐ Consider how you dispose of and evidence destruction of physical customer data

☐ Ensure that electronic customer data is secured with a password and devices are stored securely when not in use

☐ Consider who has access to the customer documentation and why they are required to access the data e.g. can prospective customers see previous customer funeral arrangements on the desk?

☐ Ensure that passwords/code for doors, devices or electronic files are updated periodically or when team members leave the business

---

If you require further information on implementing the General Data Protection Regulation in your business, we recommend the Information Commissioner's Office (ICO) website or helpline for small businesses (0303 123 1113- Option 4)