GENERAL DATA PROTECTION REGULATION (GDPR)

Being GDPR compliant is not just about 'fixing a website' – it is part of your entire organization irrespective of whether you are a sole trader, a partnership, LLP, a limited company or a larger plc. There are only a few situations where businesses don't process information at all.

In most cases, if you are trading and selling a product or service or if you have a larger team where different levels of key personnel (HR, IT, marketing, security teams) interact with customers' data you should be aware of the General Data Protection Regulation. It isn't a one-person show. You need both technical and legal implementations.

Understanding the regulations is a big step and here are the key terms that are often addressed in relation to data and GDPR.

- ***Data subject*** – a natural person whose personal data is processed by a controller or processor.
- ***Data controller*** – the entity that determines the purposes, conditions, and means of the processing of personal data.
- ***Personal data*** – any information related to a natural person or Data Subject that can be used to directly or indirectly identify the person.
- ***Data processor*** – the entity that processes data on behalf of the Data Controller.

For anyone wanting to take the pain out the process we can recommend a service provider who will generate all your GDPR documents quickly and easily with their GDPR wizard – let us know and we can send you the link.

Added Simple Series advice on data collection

1. You need to make people aware of what data you are collating and why.
2. If you are keeping payment details these must be secured or deleted once a transaction has happened.
3. It's important to keep data up to date so regular checks on data is a must.
4. Make sure your CRM is data protected.
5. You can not transport data out of the UK.
6. You need to have an unsubscribe button on all your marketing materials so people can leave at any time.

7. You can not cross sell or market for another business unless you have had prior permission to do so.

8. You need to be registered at the Information Commissioner's Office – check their website - https://ico.org.uk/ (there is a small fee for this).

9. Set up your policies, procedures and processes around your data.

10. Delete customer data when no longer needed.

11. Monitor and audit frequently.

12. If you are not compliant you can be fined.

Here are the 7 principles that you need to abide by

The UK GDPR sets out seven key principles:

These principles should lie at the heart of your approach to processing personal data.

Lawfulness, fairness and transparency

(a) processed lawfully, fairly and in a transparent manner in relation to individuals.

Purpose limitation

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data minimisation

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage limitation

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

Integrity and confidentiality (security)

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

Article 5(2) of the regulations adds that: The controller shall be responsible for and be able to demonstrate compliance.

For more detail on each principle, please read the relevant page of this link.

Click here