GDPR FOR SMES

You must be GDPR (General Data Protection Regulation) compliant if you or your business store, acquire or use personal information in any capacity. This is regardless of the size of the company.

Below we have put together a short guide for SMEs (Small & Mid-Size Enterprises) to be considered when thinking about how GDPR rules and regulations affect your business.

THE KEY PARTIES

Two terms describe the person, company or organisation that is processing and collecting the data: Data Controller and Data Processor.

DATA CONTROLLER

The person or business that decides how and why personal data is collected. The data controller must be fully compliant with GDPR's policies on transparency, data storage, data confidentiality and accuracy of data collected and stored.

The data controller must notify the Information Commissioner's Office (ICO) if a data breach happens or if data is stolen or lost by the business.

DATA PROCESSOR

The person/business responsible for personal data, collected by the Data Controller, being processed. A Data Processor is anyone with access to personal information and uses it. A processor must ensure that data is processed in accordance with GDPR requirements and record processing activities.

DATA AUDIT

An audit enables a company to understand the data the company maintains on clients, employees, suppliers and other stakeholders. If you do not maintain and track details currently then ensure you carry out a data audit.

Under GDPR your company should only ever hold data for as long as necessary and for an appropriate period of time, essentially as short as possible.

REGISTER WITH THE ICO

You are likely going to have to register with the ICO. Every organisation or sole trader who processes personal data is required to pay a data protection fee to the ICO. If your are unsure whether you need to pay the registration fee then please click the link at the bottom of this guide and complete the questionnaire.

DATA CONSENT

Your company must get consent which is clear and explicit in allowing your company to gather and store their data. This consent must come before the data is acquired.

You must clearly explain what information is being collected and how it will be used. If you do not obtain permission then you can not acquire or store their information under any circumstances.

In practical terms: Implement a Privacy Policy and implement a Cookie Policy.

Ensure that your company's T&Cs are GDPR compliant, therefore before using your services, clients explicitly will consent to their data being captured as outlined in your T&Cs.

Your company must always be in a position to provide evidence of consent being provided.

RECORDS RETENTION POLICY

A policy should be made informing all employees of how they are expected to handle, collect and destroy data appropriately. Policies should contain details such as how long the data will be stored for and what processes need to be carried out to ensure that data data is not stored for longer than necessary.

INFORMATION SECURITY

Security policies should contain principles, processes and frameworks being implemented to protect against unauthorised access, alteration, disclosure, or destruction of the company's data.

TRAINING STAFF

ICO statistics showed during a 3 month period that 97% of data breaches were caused by employees. Training employees on how to appropriately handle and look after data is essential. Employees should also be trained on how to handle a breach.

SUBJECT ACCESS REQUEST PLAN

Any UK or EU citizen can request access to all their data you hold about them, they can also amend any inaccuracies and tell you to delete it entirely. This right is known as the Subject Access Request (SAR).

Dealing with SAR can be time consuming so having a plan in place for when someone requests their data can help save a lot of time and can teach employees how to deal with a request.

THIRD PARTY RISK MANAGEMENT

A company should always check that their suppliers are compliant with GDPR. You can send a GDPR compliance assessment to review how they handle data, security and storage procedures, and what type of data they handle.

Contracts a company has with suppliers should include that they are GDPR compliant.

USEFUL LINKS:

- Registration Fee Questionnaire: https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/
- Guide To General Data Protection Regulation (GDPR): https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
- List of mandatory documents required by the GDPR: https://www.itgovernance.co.uk/blog/the-documents-you-need-to-comply-with-the-gdpr