‘Signpost the way’ - GDPR Readiness

On 25 May 2018, any organisations processing personal data will have to comply with the new General Data Protection Regulation (GDPR). Under the new regime, fines for serious breaches can be up to €20m or 4% of annual global turnover.

In the UK, the use of personal data is currently governed by a law (The Data Protection Act 1998 or DPA), which is almost 20 years old and which was not written for the technologically advanced world in which we currently operate. This is set to change with the implementation of the GDPR, a new European regulation, which was enacted on 25 May 2016 and will be in force from 25 May 2018.

If you process (hold, use, store, transmit, delete) personal data about your customers, clients, employees or suppliers, you will be legally obliged to comply with the GDPR.

What information does the GDPR apply to?

Personal data

The GDPR applies only to ‘personal data’ - which means any information relating to an identifiable living person who can be directly or indirectly, identified from that information.

This definition, reflecting changes in technology and the ways in which organisations collect information about people, provides for a wide range of personal identifiers to constitute personal data, including:

- Name
- Address
- Email address
- Telephone number
- Registration number
- Unique identification number
- Location data
- Online identifier

The GDPR applies to personal data held both electronically, such as on computers or on CCTV etc. and to manual (paper) records held in filing systems.

Personal data that has been deleted or completely anonymized, falls outside of the scope of the GDPR.

Regulator Guidance

The ICO has produced a package of tools and resources to help you get ready. These resources include:

- A guide to the GDPR;
- A getting ready for the GDPR self help checklist;
- A GDPR FAQs document;
- A new advice service helpline for small organisations; and
- A ‘12 steps to take now’ graphic.

The ICO data protection self-assessment toolkit can help you assess your compliance with the Data Protection Act and find out what you need to do to. There are seven checklists covering a number of areas of compliance including Getting ready for the General Data Protection Regulation (GDPR), Information Security, and CCTV.

‘Signpost the way’ - GDPR Readiness

Data protection guidance for small businesses

Getting it right: a brief guide to data protection for small businesses (pdf)

Getting it right: small business checklist (pdf)

Personal information online: small business checklist (pdf)

A practical guide to IT security: ideal for the small business (pdf)

A practical guide to IT security: ideal for the small business (Welsh language) (pdf)

Training checklist for small and medium-sized organisations (pdf)

Outsourcing - a guide for small and medium-sized businesses (pdf)

Collecting information about your customers: small business checklist (pdf)

Our High Level Guidance - Top 10

1. Do understand, in detail, the personal data you hold, why you hold it, who you share it with, how it is kept secure and how long you retain it.
2. Do only collect and process data for the legitimate reasons set out under the GDPR.
3. Do make sure you only collect the minimum amount of data you require for the purpose it is needed.
4. Do make sure you keep the data accurate and up to date.
5. Do make sure you know what security is being applied to protect the data, make sure that this is adequate, and ensure any qualifying breaches are reported to the regulator.
6. Do make sure that you do not retain data indefinitely, and that you follow a retention strategy, or that the data is anonymised.
7. Do make sure you are able to respond to requests to have access to, or delete, the data from the individuals.
8. Do make sure you do not send data outside of the EEA without the required additional protections being applied.
9. Do make sure that you have written contracts in place with any third parties who you may share personal data.
10. Do make sure your privacy notices, which advise customers or employees how you use their data, contain the information required under the GDPR and are readily available.

Marketing

If you undertake any direct marketing via telephone, email or other electronic means then you need to comply with the Privacy and Electronics Communications Regulations as well.

For further information for small businesses, see the ICO direct marketing checklist or guidance notes.

Direct marketing guidance

Direct marketing checklist

All documents are hosted on the Information Commissioner’s Office website.

TOGETHER WE CAN BEAT CARAVAN THEFT

www.cassoa.co.uk

CSTW08012018

CaSSOA
THE CARAVAN STORAGE SITE OWNERS’ ASSOCIATION