ASSOCIATION FOR ROAD TRAFFIC SAFETY AND MANAGEMENT

GUIDANCE DOCUMENT

EXEC/01
APRIL 18

GDPR – What's it all about?

Introduction

At first glance GDPR doesn't seem to apply to Membership Associations substantially as we can assume the aim is to "protect natural persons from unlawful processing personal data which is not already in the public domain".

However, it does affect us and all our members in some way or other. I will try to outline in simple terms what it all means and what we should all be doing.

GDPR becomes enforceable from May 2018 replacing the Data Protection Act 1988. However it should be acted upon now. The UK Government is already re-drafting UK policy to bring this into line with the GDPR for after Brexit.

Basics

Who is protected?

A natural person is a human individual and applies to everyone in any capacity (referred to in GDPR as data subjects).

What is personal data?

Personal data includes such things as names, addresses, emails, bank account details, credit card details, driver number, passport, mobile and/or landline phone numbers, genetic and/or biometric data, and anything else that can identify a living subject. In addition, there are further special categories of data which will always require explicit consent (see later). It does not cover personal data which is already in the public domain – be careful what you put on social media!

Who might be asking for and processing this information?

Human Resource Departments, payroll and accounting departments, publications and editorials, marketing and sales departments, membership administrators, IT departments, external bodies who provide services on behalf of your business, government bodies who require information from you as an employer, companies asking for references, debt recovery agencies.

Who does GDPR apply to?

- Anyone who carries out activities involving goods or services;
- Anyone who monitors behaviour of data subjects;
- Anyone within the EU, EEA and Member States;
- Where data is shared outside the EU or EEA then that location must have signed up to the GDPR. The European Commission produces a journal of places that are accepted;
- Where a controller of data is outside of the EU then they must have a representative within the EU

What rights do people have regarding their data?

- The right to be informed
- Right of access
- Right to rectification (to correct errors) *
- The right to erasure **
- The right to restrict processing
- The right to data portability (authorising data to be sent elsewhere)
- The right to object
- Rights in relation to automated decision making and profiling

* Rectification is not removal. You must not remove a prior record, you must add to it.
** Erasure is not removal – make a note on the data that the subject has requested removal.
Article 17 provides full information on non removal of information for the purposes of potential dispute

So what should you do?

What must you do at the outset?

- Make sure you are registered with the Information Commissioners Office (ICO)
- Ensure your policies are up-to-date
- Check your security systems for data
- Ensure your website has a privacy statement and details of how to opt out of cookies
- Create a GDPR folder to include all the relevant information
- Appoint a Data Protection Officer (not mandatory for everyone but recommended)

What next?

You need to appoint a "controller" – this will be the person who is responsible for holding all the data. In the case of ARTSM this is the General Secretary (me). You will also need to appoint a "processor" and this will be the person who uses the data for identified purposes. Both (unless the same person is both) are liable jointly and severally for data breaches. It therefore pays to make sure they both know what they are doing!

The controller is the person who determines what the processor can do with the data and this should be recorded in the same way as you would record evidence in your QMS files, so make your file and get it ready for all the information you receive.

What should you collect?

Under Article 5 you must ensure that the data you collect:

- Is collected fairly and lawfully
- Is for specified, explicit and legitimate purposes
- Is adequate, relevant and limited for what is necessary
- Accurate and kept up to date
- Kept no longer than is necessary
- Processed in a manner than ensures appropriate security

What are you required to show?

You must be able to demonstrate accountability.

- Have you risk assessed to ascertain what you actually do collect
- Have you created a folder of how you control and process data
- Can you show that you delete personal data no longer required
- Can you show that your suppliers provide you with any data corrections necessary (eg payroll)
- Can you show that you keep data secure
- Do you have a policy for processing for your suppliers that they must follow
- Do you have a log of data processing
- Do you have a statement of privacy and is this accessible

What is lawful?

You must be able to demonstrate you have good grounds for processing data (Article 6)

- Are you using it for the purposes of contractual obligations (eg do you need to see a copy of an employee's driving licence so they can use your cars)
- Are you using it for legitimate interests (eg do they have to register as a member to access information)
- Are you using it due to a legal obligation of the controller (eg providing information to the tax office)
- Is it necessary to protect the vital interests of the data subject (eg. Under DDA)
- Is it in the public interest
- Is it in the exercise of authority vested in the controller (eg to comply with the voting register)

What is consent?

You must be able to demonstrate how consent has been given and it can be withdrawn at any time. You may not now use tick boxes that are ticked, they must be unticked so that the user must physically act upon it.

Consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she by a statement or action …..

What are special categories?
These categories are similar to the protected characteristics under the Equality Act but go further to include: race, ethnic origin, political opinion, philosophical beliefs, religion, trade union membership, genetic data, biometric data, health, sexual preference and others (please refer to the Articles for a complete list)

What happens if it goes wrong?

All breaches need to be reported to the ICO and to the data subject(s) concerned.

You will be required to identify breach and demonstrate what appropriate measures you have taken to rectify breach.

Every data subject has the right to launch a complaint with the ICO who may issue compliance notices, judicial remedies and fines.

You are required to act within 72 hours.

Claims can be in relation to material or non material damage

Article 83 provides details regarding fines which have can reach €20 Million or 4% of worldwide annual turnover. Many companies have already fallen foul of GDPR and prosecuted for breaches caused by failure to comply with risk management and taking steps to avoid breaches.

Some examples:

- sending out information to people who had opted out – company fined
- leaving IT unattended and unsafe – company had server stolen – fined
- not ensuring data was sufficient protected – fined
- computers stolen when taken home for night – fined
- hacked into payroll system – fined

In summary?

PROTECT **PREVENT** **PREPARE**

Demonstrate Compliance

- Establish and maintain a data inventory
- Audit internal controls and processes
- Review privacy risks – www and personal computers
- Introduce documents such as data subject access request forms
- Examine supplier relationships
- Check your insurance details

The ICO has a wealth of information on its website (below) and there are a lot of other good resources on the internet

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Kealie Franklin
General Secretary
April 2018
www.artsm.org.uk

For further information, please contact general.secretary@artsm.org.uk