GDPR Update & Open Legal Forum

Mandy E Peters

Legal Manager

Affiliates Conference 2018

- GDPR Update:
    - Individual Rights
    - Registration/fees
    - Volunteers
    - Data Processing Agreements
    - Compliance Folder
    - Insurance
    - Resources – where to get help
- Open forum to discuss other legal matters

Individual Rights

- Right to be informed
  - Privacy Notices:
    - Setting out:
      - Your purposes for processing.
      - The legal basis upon which the data will be processed.
      - How long the data will be retained.
      - Data subject rights.
      - If and the extent to which it will be transferred overseas/outside of the EEA appropriate safeguards in place to protect it.

Individual Rights

- Right to erasure (NEW)
  - Right to have personal data erased
    - Request can be made verbally/in writing:
      - When the use of the data is no longer necessary for the purpose it was obtained.
      - Consent is withdrawn and there is no other legal basis for processing.
      - When relying on legitimate interest, individual objects and there is no other overriding legitimate interest.
      - Data unlawfully processed.
      - To comply with legal obligations.

Individual Rights

- Right of Access
  - Subject Access Request
- Right to Rectification
  - Data that is inaccurate/incomplete
- Right to Restrict
  - Block/supress the processing of personal data in certain circumstances.
- Right to Data Portability (NEW)
  - Obtain and use personal data for own purposes across different services under certain circumstances.

Individual Rights

- Right to Object
  - Applies as of Right:
    - If processing is for direct marketing (including profiling).
  - Right not absolute where:
    - Processing based on legitimate interests.
    - Performance of a task in the public interest.
    - Exercise of official authority vested in you (including profiling).
  - Right more restricted where:
    - Processing for purposes of scientific/historical research and statistics.
- Rights relating to automated decision making including profiling

Registration and Fees

- Registration:
  - (also referred to as notification) was due to have been removed by the application of the GDPR into UK law. However a new fee scheme is being created in order to fund the ICO.
- Fees:
  - Clubs which are not-for-profit organisations are likely to be exempt from having to pay the fee.
  - ICO's data protection fee – a guide for controllers will assist in establishing whether you are exempt from having to pay the fee.
  - Clubs using CCTV will have to pay the fee.

Volunteers

- Types of volunteer: Club officers and regular helpers, or occasional contractor style relationship.
- Ensuring volunteers are aware of and compliant with GDPR undoubtedly presents a challenge.
- ICO has not produce any specific guidance.
- Club is responsible for the data it’s volunteers handle.

Volunteers

- Club is responsible for the data it's volunteers handle, and for it's volunteer's data. A club may store more information about its volunteers than its members e.g. qualifications, DBS checks etc.
- Basics: Tell people what you are doing with their data.
- Club should ensure appropriate procedures/policies in place:
  - Provide training to volunteers in relation to security/confidentiality/passwords/locks/access/data retention etc.
  - Produce policy dealing with the use of data by volunteers.
- Document procedures.

Volunteers

- All volunteers:
  - Consider what data they need in order to perform their role. The secretary may need full names and addresses for sending post. An ad hoc dinghy instructor may only need an emergency contact number and basic medical information.
- Regular volunteers:
  - Use generic email addresses which can move to a new volunteer or be switched off.
  - Have a policy regarding use of personal devices/handling of personal data.
  - Tell volunteers of their obligations - basic training.

Volunteers

- Occasional volunteers/ Contractors:
  - Consider what data they actually need. An occasional volunteer may well be working alongside a more regular volunteer and so may not actually require access to members personal data.
  - Consider what they are doing with the data. Are they acting as a data processor? If so a written data processing agreement should be put in place. This must include certain prescribed provisions covering topics such as the permitted use of the data, what happens when the agreement comes to an end, and what happens if a data subject exercises their rights as a data subject.

.

Data Processing Agreements

- Data Controller
  - Natural or legal person e.g. individuals, organisations, unincorporated or incorporated bodies of persons.
  - Responsible for determining the purposes and means of processing data.
  - Responsible for taking appropriate technical and organisational measures for the protection of data subjects and their rights and for demonstrating compliance with this.
- Data Processor
  - Natural or legal person (as above).
  - Responsible for processing data on behalf of a Data Controller pursuant to a contractual relationship.
  - Responsibilities under the GDPR limited compared to those of DCs.
  - Responsible for processing in accordance with the data processing principles and protecting the rights and freedoms of data subjects and demonstrating compliance with this.

Data Processing Agreements

- Whenever a Controller engages a Processor to process data on its behalf, there should be a formal agreement in place.
- There are two way to achieve this:
  - A GDPR compliant data processing clause contained within a more general service contract. (These will become more common as organisations update their standard contracts and the GDPR becomes more widely accepted).
  - A stand alone data processing contract.

Data Processing Agreements

- In either case, the following must be included:
    - The following compulsory details:
        - the subject matter and duration of the processing;
        - the nature and purpose of the processing;
        - the type of personal data and categories of data subject; and
        - the obligations and rights of the controller.

Data Processing Agreements

- Must contain the following compulsory terms:
  - the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
  - the processor must ensure that people processing the data are subject to a duty of confidence;
  - the processor must take appropriate measures to ensure the security of processing;
  - the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
  - the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;

Data Processing Agreements

- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

- As a matter of good practice, contracts should:
  - state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR; and
  - reflect any indemnity that has been agreed.

Data Protection Compliance Folder

- Data Protection Privacy Policy;
- Record of Processing Activity (if applicable – see below);
- Data retention policy;
- Procedure for a response to a Subject Access Request;
- Procedure for a response to a Data Breach;
- Impact Assessment Template for Legitimate Interest purposes;
- Details of contractual arrangements with third party processors**;**
- Record of staff/volunteer training;

Insurance Cover

- It is possible to obtain cyber insurance to cover data protection breaches and resultant fines.
- Cover, at present, is not incorporated as part of the RYA Club Policy with Gallagher, although it is hoped to be added to as an optional extension in near future, in the meantime it can be arranged separately.
- Gallagher contact Ben Bennett Tel: 01384 500283 or ben_bennett@ajg.com

Resources

Further Information:

- We have produced Guidance on the GDPR, Subject Access Requests, Data Time Period for Clubs, Data Audit Template, Data Privacy Policy and suggested wording for Membership Application/Renewal Forms
- Information Commissioners Office website
- GDPR helpline - **0303 123 1113**
- Can be obtained from the Legal Team –
  Email: legal@rya.org.uk Tel: 023 8060 4223

OPEN LEGAL FORUM