Affiliated Club Conference

2017

Communicating with members – data protection considerations

RYA LEGAL

John Dyke

Legal Advisor

Today's aims……

- Overview of the General Data Protection Regulation
- How it applies to clubs
- What your club needs to do
- What does it mean in practice
- Resources – where to get help

Overview

- Why did we need new data protection legislation?
- What has changed?
- When does it take effect ? – 25th May 2018.

What has changed?

- Definition of personal data has been expanded
- New rules/terminology around when and how you are permitted to process data – "**legal basis for processing**"
- Opt out/deemed consent can't be relied upon
- No longer a requirement to register with ICO, but may still be a cost.
- "**accountability**"
- New "**right to be forgotten**"
- The fines may be substantial!

Definitions…

- **Personal data**
  - Any information relating to an identified or identifiable natural person (referred to as the **Data Subject**). A person is identifiable if they "*can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors, specifically the physical, physiological, genetic, mental, economic, cultural or social identity of that actual person*".
- **Processing**
  - "A*ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, determination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

The legal basis for processing..

- You can only process (and therefore collect) personal data in certain circumstances
  - *Consent of the Data Subject**.***
  - ***The legitimate interests of the data controller.***
  - ***Necessary for the performance of the contract with the data subject.***
  - *Compliance with a legal obligation to which you are subject.*
  - *Necessary to protect the vital interests of the data subject or of another natural person; or*
  - Necessary for performance of a task carried out in the public interest.

GDPR - Accountability

- The GDPR requires you to show **how** you comply with the principles – for example by documenting the decisions you take about a processing activity.
- You will have significantly more legal liability if you are responsible for a breach. These obligations are a new requirement under the GDPR.

The GDPR - Principles

The principles are broadly similar to those under the DPA:

- Fair, lawful and transparent processing
- Purpose limitation - Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.
- Data minimisation - Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed
- Accuracy - Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay
- Data retention periods - Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Data security - Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- **Accountability** - The controller is responsible for, **and must be able to demonstrate**, compliance with the Data Protection Principles. (NEW)

Right to be forgotten

A request to be forgotten can be made:

- When the use of the data is no longer necessary.
- Consent is withdrawn and there is no other legal basis for processing.
- Data unlawfully processed.
- To comply with legal obligations.

How the GDPR applies to clubs

- All clubs are processing personal data
- Most, if not all, the information you request on your membership application forms, event entry forms and information you collect from coaches, instructors, visitors, suppliers, staff and volunteers will be personal data.
- This includes names, addresses, dates of birth, telephone numbers, e-mail addresses and emergency contact details..and other personal identifiers eg boat names, sail numbers.
- Personal data can also include opinions held about someone and can include references to them in emails or other communication.
- Information about health and physical disabilities will be sensitive personal data to which additional safeguards apply.

What your club needs to do

- **Scope the size of the issue (do an audit)**
  - What data do you collect
  - What do you use it for
  - Who do you share it with
- Review your data management processes
  - How are you managing personal data?
- Marshal your resources/technology
  - Competencies within your club
  - Software solutions?
- Consider insurance

What is it likely to mean in practice (post audit)?

- **Prune/de-personalise/get consent for existing personal data**
- **Amend privacy notices and consents requested at point of data collection**
- **Amend or create a privacy/data policy**
  - Needs to cover: Collection of Data, Using Data, Storing Data,Data Retention Periods Access to Data (Subject Access Requests) , Individuals Rights, Data Breaches
- Review constitutional documents (remove deemed consents)
- Understand subject access requests
- Adopt a process for consent changes/request to be removed
- Adopt data retention policy
- Make sure you have written agreements in place (covering the prescribed areas) with those you share personal data with.
- Document everything!

The GDPR – Insurance Cover

- It is possible to obtain cyber insurance to cover data protection breaches and resultant fines.
- Cover is not currently incorporated as part of the RYA Club Policy with Arthur J Gallagher, although it is expected to be added to as an optional extension in near future, in the meantime it can be arranged separately.
- Arthur J Gallagher contact Ben Bennett Tel: 01384 822279 or ben.bennett@ajg.com

Resources to call upon

Further Information:

- Can be obtained from the Legal Team –
  Email: legal@rya.org.uk Tel: 023 8060 4223
- We have produced Guidance on the GDPR, Subject Access Requests, Data Time Period for Clubs, Data Privacy Template and a Data Audit Template, .
- Information Commissioners Office website
- GDPR helpline will go live on November 1 2017 - **0303 123 1113**
- Look around web at what others are doing
- https://www.ageuk.org.uk/help/privacy-policy/
- https://www.facebook.com/about/privacy/

facebook Sign Up

Join or log in to Facebook

- What kinds of information do we collect?
- How do we use this information?
- How is this information shared?
- How can I manage or delete information about me?
- How do we respond to legal requests or prevent harm?

Data Policy

We give you the power to share as part of our mission to make the world more open and connected. This policy describes what information we collect and how it is used and shared. You can find additional tools and information at Privacy Basics.

As you review our policy, bear in mind that it applies to all Facebook brands, products and services that do not have a separate Privacy Policy or that link to this policy, which we call the "Facebook Services" or "Services".