Info paper
14
July 2017

europe active
MORE PEOPLE | MORE ACTIVE | MORE OFTEN

The New European Union's General Data Protection Regulation (GDPR)

The GDPR is a new EU Regulation governing how organisation should handle, protect and use personal data. It applies to EU citizens' personal data, regardless of where it is collected, stored, or processed and whether it is inside or outside of the EU;
*The regulation becomes enforceable from **25 May 2018**;*
There are increased penalties for non-compliance.

Summary of the GDPR

The primary objective of the GDPR is to give control of personal data back to individuals, and to simplify the regulatory environment for international business by unifying the regulation within the European Union. The GDPR covers any organisation if it holds, or controls, processes, applies or stores any data about EU subjects, even if the organisation is not located in the European Union.

Simply put, GDPR requires companies to implement entirely new processes and procedures around the collection and storage of personally identifiable information (PII). The focus of GDPR is on ensuring that PII is stored with a person's permission, used for the specified purpose for which it was obtained, and for a duration that is consistent with the initial reason for obtaining the data.

Because the new Regulation comes into effect in May 2018 it is important for organisations, such as fitness clubs to start thinking about what processes and procedures may have to be changed or amended to be compliant with GDPR.

The notable changes of the new regulation (from the 1995 Directive)

Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; some of the key points of the GDPR are noted here:

Stricter Consent Rules: The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of "legalese", as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. The GDPR requires that individuals give unambiguous, informed consent before their data may be processed. Consent cannot be assumed from inaction.

Enhanced rights for individuals: Individuals have more rights under the GDPR, including rights to have their personal data erased, have inaccurate data corrected, and to be removed from digital marketing, etc.

Data breach notification: Under the GDPR, breach notification will become mandatory in all Member States where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach.

Increased accountability measures: There are a number of new governance requirements for organisations, including conducting privacy impact assessments and appointing a data protection officer.

Substantial fines: Maximum penalties for non-compliance and or breaches are €20 million or 4% of annual global revenue, whichever is greater, and can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

What to do?

As a first step it is recommended to undertake a comprehensive data audit to understand:

- What personal data you hold and process?
- Where it is stored across your organisation?
- Who has access to it?
- What consent has been provided, and where is it documented?
- Where data has been transferred from, and what is it being used for, and how is it being protected?
- How is personal data secured throughout its "lifecycle"?
- What is the policy and process to dispose of personal data?

This will take time to complete, so it's better now, before implementation in May 2018. Due to the wide-ranging application of GDPR full compliance may take time so it may be necessary to take expert advice. Some of the key considerations include:

- **Evaluate your internal policies** relating to data protection and identify what needs to be reviewed, addressed, and updated.

- **Identify what changes and upgrade**s are needed to your **IT systems.**

- Decide how you will **word your new privacy notices** to ensure they adhere to the enhanced rights of EU subjects (your customers and clients).

- **Review your data collection procedures** to ensure you let consumers know why you're requesting their data. This moves to an opt-in process rather than opt-out approach.

- **Assess your data security** and identify the enhancements necessary to ensure compliance with the new regulations.

- Determine the origin of your data and ensure you have compliant systems in place to **capture consent**.

- Check your **procedures for reporting data breaches** as per the new guidelines.

- Determine whether or not you need to employ a **data controller** to help you comply with these new regulations.

Check **your websites and marketing information** – *even details of who works in your clubs, their photographs, qualifications, contact details*, etc. should have **their consent** before publication in the future.

More information is available on:
http://ec.europa.eu/justice/data-protection/reform/index_en.htm

EuropeActive
Avenue des Arts 43 - 4
1040 Brussels, Belgium
tel: +32 (2) 649 90 44
thesecretariat@europeactive.eu
www.europeactive.eu