health club management

Website: www.healthclubmanagement.co.uk
Date: 16.11.17

DATA PROTECTION

HANDLE WITH CARE

With the implementation of the general data protection regulation (GDPR) fast approaching, Health Club Management explores what the biggest shake up of data protection laws for 25 years means for health and fitness businesses across the UK and Europe

Once the preserve of lawyers, data protection is about to become something business owners and their employees need to understand. The GDPR is a new piece of European legislation, which comes into force on 25 May 2018. Designed to address the sheer volume of data created and collected today, the GDPR will oblige every leisure operator to overhaul the way it handles data.

"Every two days, we create as much data as we did from the beginning of time until 2003," says analyst and author Bernard Marr in his book *Data Strategy: How to Profit from a World of Big Data, Analytics and the Internet of Things*. "Then we do it again. Every two days. Today we have five zettabytes of digital information; by 2020 it's expected to grow to 50."

With this in mind, one thing has become impossible to ignore: the Data Protection Act, which was implemented in 1998, is vastly out of date and is unable to fully address the issues raised by the amount of data generated in society today.

More customer data is being collected by businesses now than ever before

GETTING READY

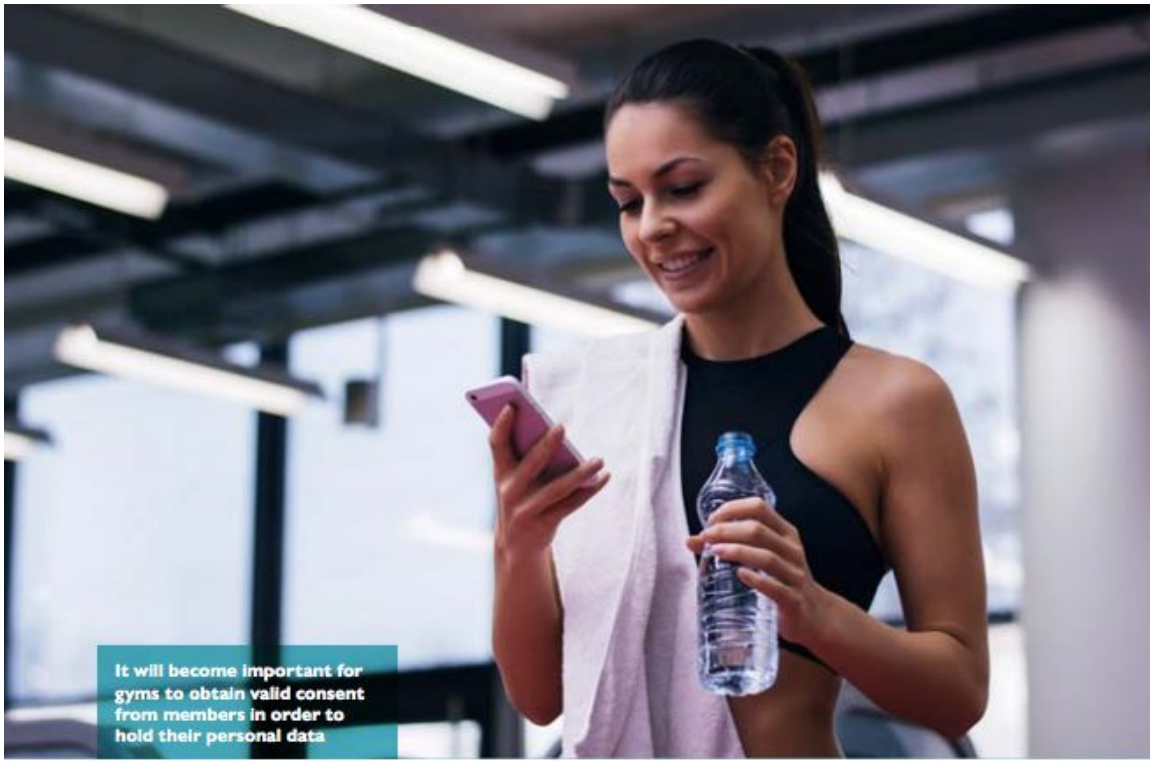
The GDPR has been in development since 2012, yet a vast number of organisations still aren't ready for the change. One survey by IT company Ipswitch found that 52 per cent of firms admit they're not prepared for the changes that the regulations will bring, and 44 per cent of IT professionals are struggling to grasp the new rules. Yet

"If you fail to comply, supervisory authorities like the ICO can issue fines of up to 4 per cent of annual global turnover or €20 million, whichever is higher"

Raoul Lumb, SM&B law firm

health club management

Website: www.healthclubmanagement.co.uk
Date: 16.11.17



It will become important for gyms to obtain valid consent from members in order to hold their personal data

the GDPR will apply to all UK companies, regardless of Brexit. Some additional legislation will be required, but the bottom line is that the nation will be affected, even after leaving the union.

Getting on board is vital, as financial penalties will be high. "If you fail to comply, supervisory authorities like the Information Commissioner's Office (ICO) can issue fines of up to 4 per cent of annual global turnover or €20 million, whichever is higher," explains Raoul Lumb, data protection associate at law firm SM&B. "Previously, the maximum fine was £500,000, which demonstrates just how serious the EU is about instigating an attitude shift."

But is getting on board easier said than done? Paul Simpson, Legend Club Management Systems' chief operating officer says that as safeguarding valuable information is key to the new legislation, organisations must begin by thinking about their information assets. "Operators must be sure about the information their business holds, where this information is located, how up to date it is, if it's still required and if it's in digital or paper format," Simpson explains.

"They should also make sure they know the extent to which employees are accessing this information using their own devices," he adds.

principles of security – confidentiality, availability and integrity – organisations can begin to understand how to best protect their data assets."

THE EXPECTED CHANGES

Particularly relevant for the leisure sector will be changes to what is classified as 'personal data'. Online identifiers like IP addresses and cookies, for example, will now be considered personal data, which means that a vast amount of data that most operators currently capture as a matter of routine will be subject to specific GDPR stipulations. Secondly, an additional definition has been added to data that falls under the 'special category of personal data' classification. Genetic and biometric data is now included, and as such, any data used to measure athletic performance and/or health must be treated according to the rules of this category.

In both instances, the most important factor will be ensuring valid consent is obtained from the owner of the data. A member specifically asking for performance monitoring is likely to be lawful, but operators should stop and question wholesale monitoring, especially if it's carried out without the knowledge of club members.

Also relevant is the 'right to be

right and withdraws consent to the storage or use of their personal data. According to Joanne Barton, product design analyst at Gladstone, software suppliers are already implementing measures to anonymise this type of dataset so they can be validly stored and used after the GDPR's implementation. She says: "We're instigating changes to make adherence as straightforward as possible.

"Compliance with this and many other aspects of the GDPR will be made easier by having a robust software system that's ready for the change. We're adapting our user interfaces to support changes ▶

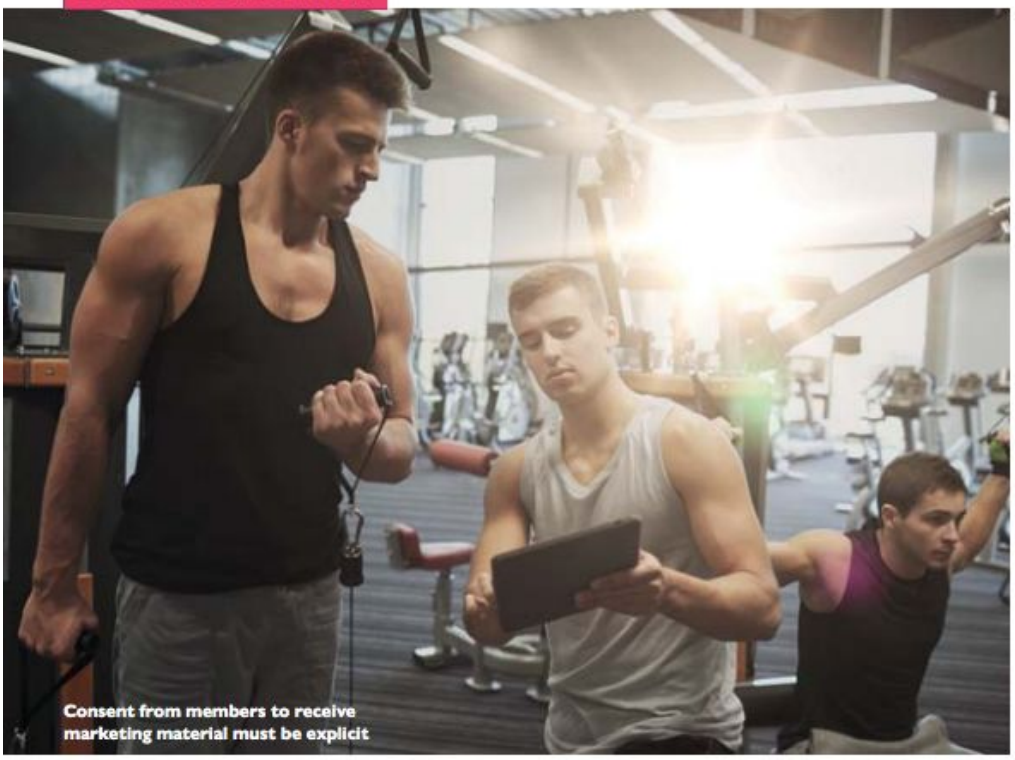
Club members must be told when

© SHUTTERSTOCK.COM

health club management

Website: www.healthclubmanagement.co.uk
Date: 16.11.17

DATA PROTECTION



Consent from members to receive marketing material must be explicit

PHOTOS: SHUTTERSTOCK.COM

"Compliance with many aspects of the GDPR will be made easier by having a robust software system that's ready for the change"

Joanne Barton, Gladstone

affecting consent rules and anonymisation of data, so all personal data is removed from a database but transactional details remain."

THE MARKETING MINEFIELD

Current laws ensure marketers only email people who've 'opted in' to receive correspondence from them. The GDPR toughens this process up considerably.

Consent must be explicit, rather than implied, and freely given after a request has been made in clear and plain language. Hiding consent within small print or bundling it up in terms and conditions that must be accepted to become a member or buy a product will no longer be allowed. Operators will need to explain clearly why they're collecting personal data and how they intend to use it, and as a final hurdle, hold records that prove consent was given.

"The safest option will be to actively seek consent before sending marketing emails and similar," says Lumb. "Tick boxes will need to be presented separately, with their own wording, and a member shouldn't be forced to tick that box in order to purchase services. You must also make it clear that consent can be withdrawn at any time."

Email marketing is an area that companies will need to scrutinise closely to ensure they are operating within the boundaries of the new legislation, and this extends beyond the consent process. Sharing of data obtained with other related services will no longer be acceptable unless the data owner expressly agrees to this.

ON THE RECORD

A clean-up of membership databases will also be important, assessing what data has been collected, how long it has – and will be – stored for and whether it's accurate.

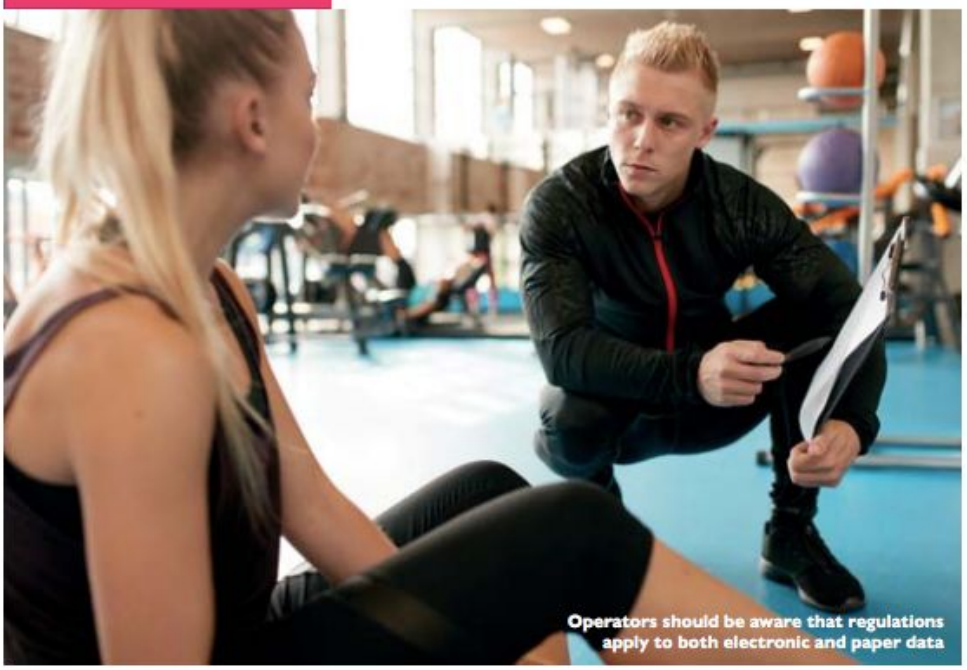
Utku Toprakseven is the director of sports intelligence at 4 global, which runs the DataHub Club – a data sharing community for sport and leisure sector organisations. He says: "Data takes numerous journeys through organisations. It can generate intelligence and inform operational solutions that produce commercial returns, participation outcomes and social value. The GDPR is a hot topic for all DataHub Club members, from operators to data controllers, processors and users. The GDPR makes it vital to know where data will add the most value to your business upfront, as this will inform requirements at the point of capture."

Just complying with the GDPR won't be enough. Operators must also prove

health club management

Website: www.healthclubmanagement.co.uk
Date: 16.11.17

DATA PROTECTION



Operators should be aware that regulations apply to both electronic and paper data

PHOTOS: SHUTTERSTOCK.COM

"Operators must be sure about the information their business holds, where this information is located and how up to date it is"

Paul Simpson, Legend Club Management Systems

they are compliant by keeping a full audit trail, which the ICO can ask for at any time. Most organisations will need someone who owns the data role and is answerable to all data requirements. As such, companies should consider appointing a dedicated data protection officer (DPO). "Getting GDPR-ready isn't a one-off project, it requires rolling management and record-keeping. You wouldn't run your business without an accountant; the same applies to data protection," explains Toprakseven.

Barton advises: "Speak with your software provider about what changes they're making internally. If consent and audit trails aren't captured within your software applications, the onus will still be on your business to put manual processes in place to ensure compliance. But of course, if your processes are manual, then they're open to error."

THE ROAD AHEAD

Don't panic and conclude it's better to take no action, says Lumb. "Start by working out what personal data your organisation collects and how – remember it applies to electronic records and paper records, too." Next, create a list of what you do with that data and, if it leaves your organisation, how it does so. Lumb advises contacting a specialist lawyer to establish what's compliant, what isn't and what steps you'll need to take to make your systems GDPR-ready. He warns, however, that "lots of companies have seen a business opportunity in the GDPR and are trying to turn themselves into experts. Just be wary."

The new rules aren't designed to put operators out of business. "The GDPR will curb invasive uses of personal data by organisations that have no business dealing with that data in the first place," says Toprakseven. "Lots of people think the GDPR will bind us with red tape. It won't. It's simply making sure things aren't happening to people's data without them knowing about it."

The truth is that it's too early to say exactly how this will affect the health and fitness industry, but what is certain is that it will affect the whole sector.

"Despite the lack of clear security guidelines in the industry, GDPR casts a clear spotlight on our legal and moral duty to take a proactive approach to protect and secure customer data," Simpson says. "This is a real opportunity for businesses to embrace the new regulation, to expand our current view of information beyond that held electronically to include all information assets in the business, and to embed best practice within our daily operations. This will ensure that both business and customer data are protected for a very long time." ●

For further information on the GDPR, visit: *https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf*

https://dma.org.uk/gdpr

www.itgovernance.co.uk/data-protection