DataHub

The GDPR

A new reality for the sport and leisure sector

datahubclub.com

Introduction

Data can take numerous journeys through an organisation. It can inform operational solutions, play a vital role in generating intelligence and be used to help produce commercial returns, influence participation outcomes and create increased social value.

The GDPR is a hot topic for all the members of the DataHub Club, from sports clubs, leisure operators and activity providers to software companies, data capturers, processors and users. Our role at the DataHub is to bring together the very best experts in the sector and share their know-how about the subject.

Getting GDPR ready isn't a one-off project, it will require rolling management and record-keeping. It going to become vital for all businesses to know where data will add most value from the outset, as this will inform data protection requirements at the point of capture.

With this in mind, we have prepared this White Paper together with the DataHub's Legal Partners, Simon Muirhead and Burton LLP as well as the DataHub's Research and Insight Partners, ukactive.

It is designed to inform the DataHub Club Members and Partners about data protection changes the GDPR will bring about and the impact they will have on sports and leisure sector organisations. It provides guidance on what we should start doing as a sector in order to comply with this changing environment.

Data comes to the fore

In the last few months, the subject of data protection has gone from being a niche concern, usually left to lawyers and IT personnel, to something that's being discussed, at length, in boardrooms across the country.

The reason for this sudden sea change? The impending implementation of the General Data Protection Regulation (GDPR), new European legislation, which obliges everyone to overhaul the way they think about and manage data.

About SM&B

DataHub's Legal Partners, Simon Muirhead and Burton LLP is a full service law firm located in the heart of Soho in Central London. The firm acts for a wide range of sports, leisure and technology clients and has particular expertise in broadcasting and data protection matters. The firm is currently helping many of its clients prepare for the impact of GDPR, ensuring that they are able to seamlessly transition into the new regime on 25 May 2018.

So what is the GDPR?

The technological landscape has changed immeasurably in the last 20 years – cloud computing, social media, artificial intelligence technologies, to name but a few – and there has also been a significant shift in the sheer volume of data created and collected.

Data protection legislation hasn't kept pace with this change. Currently, the collection, processing and use of personal data is governed by the Data Protection Directive, which was implemented by all 28 EU Member States in the late 90's; in the UK as the 'Data Protection Act 1998'.

The European Union has chosen to replace this directive, to bring data protection law in line with technological developments. The new GDPR will become law in the UK (and across the EU) on 25 May 2018.

The GDPR is a Regulation, so it will affect all EU Member States without the need for any national legislation – it's designed to apply to all EU businesses, no matter where in Europe they're based (and even businesses outside of the EU, if they collect data about EU citizens). Additional UK legislation will likely be needed from Parliament, however, to retain the effects of the GDPR after Brexit.

What you need to know

The scope of the GDPR is vast – it covers a huge variety of data-related subjects in immense detail. For sport and leisure businesses there are a number of headline changes to be aware of.

First up, the GDPR obliges you to act in a particular way when dealing with data from which any living individual could be identified. So, for example a record of their name, address or telephone number. As under the Data Protection Act, organisations will not be permitted to handle and or process such data without satisfying a relevant 'condition for processing', which are set out in the GDPR and which are not optional.

Heavier fines

This is the game changer. From 25 May 2018, data supervisory authorities such as the UK's Information Commissioner's Office (ICO) will be able to issue fines of up to four per cent of your annual global turnover, or €20 million (whichever is higher) for GDPR breaches.

This is an enormous increase from the previous level where the maximum fine the ICO could issue was a 'mere' £500,000.

This change considerably increases every organisation's data protection risk profile. If you decide to take a relaxed or boundary-pushing approach to data protection, you're putting your business at considerably higher risk.

The reason for this dramatic change? To hopefully push data governance issues much higher up boardroom agendas than they have traditionally been.

Wider definition of 'personal data'

The definition of what information counts as 'personal data' is also being expanded.

Firstly, online identifiers (things like IP addresses and cookies) will be regarded as 'personal data'. This change may seem minor, but it's highly significant for any organisation with an online presence. Why? Because it brings a vast amount of data that most website operators routinely capture (often without even knowing it's being done) inside the scope of data protection regulations.

Secondly, there is a wider definition of what counts as 'special category' personal data – in other words sensitive data such as information relating to someone's racial or ethnic origin, their political opinions, religious or philosophical beliefs, their sex life or sexual orientation.

The key change for the sport and leisure industry is that, for the first time, genetic and biometric data will be considered 'special category'. So, any data used to measure athletic performance and/or health has been brought into the higher risk 'special category' data protection fold.

Getting personal...

Personal data under the GDPR means *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

A note for personal trainers and organisations that employ/engage with them – PT's records are likely to contain personal data and may well even include sensitive personal data. Day to day, this means if a personal trainer is going to record data about their clients on their own technology, and then take that laptop or phone out of a gym, their data protection responsibilities must be made clear to them and an effective contract (backed by insurance) needs to be put in place to manage the risk.

Leisure operators would be wise to review their contracts with service providers like personal trainers / consultants in order to ensure that those agreements comply with the GDPR's requirements for data-related agreements and to make sure that they have adequate warranties and indemnities to protect themselves financially in the event of a data breach. Individuals (especially those who are self-employed contractors) should also take care to ensure that mobile devices that they use to store personal data are properly encrypted. A laptop stolen from a public place (or left on a train) that is not properly encrypted and secured against third party access would be considered a breach of the GDPR the individual/organisation responsible would be duty bound to report that breach to the ICO.

New definition of 'consent'

The GDPR will oblige you to change the way you collect and use data about your customers, and potential customers. When gathering personal data, you'll need to satisfy a 'condition for processing' – one of the most common will be the collection of consent.

This process will be made more difficult than under the DPA as 'consent' has been given a new meaning. For consent to be considered valid, it must be *"freely given, specific, informed... [and made] by a statement or by a clear affirmative action".*

In practice, this means it will no longer be acceptable to bury consent deep inside the small print or in your terms and conditions, or to collect it as part of a mandatory tick-box that must be clicked on before your product or service is delivered. As an added hurdle, you'll also need to keep records that clearly show consent has been given.

The GDPR's effect on the 'hard' opt-in

The new definition of consent is particularly important for email marketeers. Email marketing is governed not only by the Data Protection Act (and, soon, the GDPR), but also by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

As email marketeers will already know, the PECR restricts you from sending marketing emails unless individuals have 'opted in' to receiving them. From 25 May 2018, the PECR will draw its definition of 'consent' from the GDPR.

It may seem like a small, technical change, but all organisations in the UK will need to review the way they collect email marketing consent going forwards, and have previously, to ensure they can show consent has been validly collected.

By far your safest option will be to actively seek consent from each individual before sending them new or further marketing emails. Because of the changes, email marketing tick boxes will need (generally speaking) to be presented as separate elements, with their own wording, and a user should not be forced to tick that box in order to purchase a product or service. The wording must also state individuals can withdraw their consent at any time.

New rights for data subjects

Individuals already have a right to access their own personal data, rectify any inaccuracies, challenge automated decisions about them and object to direct marketing – the GDPR largely preserves these rights. There are, however, a number of complex but potentially significant new rights, which aren't entirely clear yet. What is clear, and you'll need to be aware of, is:

Subject Access Requests (SAR)

You'll will no longer be able to charge £10 to individuals who request information about what (if any) data you hold about them. You'll will be obliged to respond to these requests for free, within one month. If you don't, you may be fined.

Data Portability

Individuals will have the right to be given a copy of their data in a machine readable (easily processed by a computer) format – so they can either process it themselves or provide it to an alternative processor. So for example, your members can ask for their data to be transferred directly from your gym to their new one. You'll have no right to charge for this service.

Right to restrict processing

You'll be obliged to cease processing personal data where, for example, an individual contests its accuracy or says processing of their personal data is no longer necessary and its determined that no overriding legitimate grounds for continued processing exist.

This right may be more difficult to apply in practice than it sounds, as technical solutions must be found to isolate individual items of personal data and to freeze their processing, without halting your overall data processing activities. Your software provider should be able to help in this matter.

Object to automated decision making and profiling

Individuals will be able to object to automated decision making and profiling. Not all automated processes will be included, but if you rely on large-scale automation and/or 'AI' processes in dealing with your customers, this issue needs consideration.

Accountability and governance

Just complying with the GDPR won't be enough, under the new regime it is also a requirement that organisations are able to demonstrate that they do so. Essentially, these obligations add up to a duty to put in place data 'book-keeping' processes, keeping regularly updated records of how your data is collected, processed and stored. You'll be obliged to show these records to the ICO on request.

Organisations with more than 250 staff will have to record all of their data processing activities. These reports, known as 'Article 30' reports, will require lists of all data processing activities conducted by an organisation to be made and kept. So, any organisation that acts as a controller of personal data must keep a record of the purposes for which it processes that data, what measures it takes to keep it secure, how that data was originally collected, and details of any transfer of that data to third parties.

In addition, all organisations, regardless of size, will be required to carry out privacy impact assessments where a type of processing that they carry out *"in particular using new technologies... is likely to result in a high risk"* to individuals. At present, there is little guidance on what processing may be considered "high risk".

It's vital you take a highly sensitive approach to these data impact assessments; it's far safer to perform them where they're not technically necessary than it is to fail to perform one where it is.

> "The GDPR also states that you must aim to design data protection controls into all that you do. Practically speaking, this means setting up a clear compliance structure, carrying out staff training, auditing your firm and reviewing technical measures for securing all data that's collected, used and processed. One way in which the ICO suggests that organisations could demonstrate compliance would be complying with industry led 'Codes of Conduct' or obtaining 'Certification' as envisaged under Articles 40-43 – though as yet no such code of conduct exists for the sport and leisure sector."

Privacy by default means you must ensure only personal data necessary for specific identified purposes is processed. You'll therefore need to consider the amount of personal data you collect and how long it's stored for. This will, by definition, raise questions as to whether you genuinely need to retain and store all of the datasets you currently have.

Lastly, some organisations will need to formally appoint a 'Data Protection Officer' to manage and oversee their data processing. This is not mandatory, but if you collect large quantities of data, or routinely handle special category personal data, you should seek legal advice on whether this is required.

What do these changes mean for the sport and leisure sector?

It's easy to feel intimidated by the GDPR's requirements and conclude it's better to take no action than it is to achieve compliance, but this isn't the case. Often, compliance will be achieved by making relatively modest changes.

First things first, don't panic. There's lots of work to be done but this isn't designed to 'kill' businesses. You've got until 25th May 2018, so there is still plenty of time for change.

Start by establishing what personal data your organisation collects. Anything that's filed is in scope. The GDPR isn't just about electric data in databases – it applies to your paper records, too.

Next come up with a list (a 'data map', in ICO terms) of all the personal data you're gathering and what you do with it. So that's what data you collect, how you get it, what you do with it and – if it leaves your organisation – how it does so and where exactly it goes. If you can create that list, you're already in excellent shape.

Now is the time to contact a specialist lawyer to work through your map with in order to establish what's compliant, what isn't and what steps you need to take to bring your data systems up to date to become GDPR ready. Most organisations will need to change at least some aspect of the way they collect and store data, and seeking legal advice is recommended.

A word of warning. Lots of companies have seen a business opportunity in the GDPR and are trying to turn themselves into 'experts' overnight. Before engaging any services, whether that's legal advice or software products, be wary and ask for examples of GDPR and data protection work they've done in the past 12 months. Any competent provider ought to be able to tell you about their track record of advising on (and/or solving) data protection issues under the old Data Protection Act regime, not just about their recent GDPR engagements.

Finally, consider carefully if you need a Data Protection Officer. The sports sector is heavily regulated, and regulators like the ICO may require organisations such as professional sporting clubs to regularly disclose data. It's worth considering a DPO to assist with such requests.

DPO or not, most organisations will need someone who owns the data role – who is responsible for all of your your data requirements. Getting GDPR ready isn't a one-off project, it will require rolling management and record-keeping going forwards. You wouldn't run your business without an accountant. The same will apply to data protection.

Finding the right DPO

The GDPR states that a DPO must have sufficient data protection expertise and have direct access to senior management. They must be able to exercise their role free from undue influence or pressure, operate without conflicts of interest and be involved in all aspects of the organisation's data management of data.

The specifics

Example 1: Members Records

A clean-up of your member database will be particularly important – assessing what data you've collected, how long it has and will be stored for, and whether it's accurate.

For example, many sport and leisure organisations monitor members' performance. It will be important to assess whether you've validly obtained consent from the members concerned. If a member has specifically asked for monitoring, this kind of processing is likely to be lawful, but you'll need to question wholesale monitoring, especially if it is carried out without your members' knowledge. More difficult still will be justifying the ongoing processing of a member's data after they've left your organisation.

There are ways to manage these kind of data risks. Providers of sports data technology services are already implementing measures to anonymise and aggregate this type of dataset so they can be validly stored and used after the GDPR's implementation. And 'cloud' based technologies enable a data controller to delegate the secure holding and processing of members' records to a third party, whose business model will already ensure GDPR compliance.

Example 2: Marketing to members

At present, many leisure and sports organisations market to large databases, usually via email, using data acquired either directly or from third parties.

Existing direct marketing rules require either consent or a 'reasonable indication the individual would expect to receive marketing' before that marketing can begin.

As mentioned above, the GDPR rules mean collecting consent to email marketing on an 'all or nothing' basis will no longer be sufficient. Nor, in most circumstances, can giving consent to email marketing be an obligatory part of subscribing to receive a particular service.

With this in mind you'll need to consider how your collect email marketing data and also how you'll record and demonstrate consent has been given.

The GDPR is designed to make life particularly difficult for organisations selling lists of potential customers, such as email marketing lists. If you deal with such companies, ensure their data is GDPR compliant, ideally seeking professional advice – ignorance of a third party's data processing practices is no defense. By receiving and processing data collected non-compliantly it is likely that you will be breaching the GDPR yourself.

Email marketing is one area that organisations should give greatest scrutiny to, simply because its public-facing nature means non-compliant conduct is more likely to trigger a complaint to the ICO and attract a fine.

Final word

The GDPR represents a huge change for all organisations that process data – the sport and leisure sector is by no means alone in being affected by it.

If you're worried about having enough time, start with any data that's public facing, such as email marketing and online web forms. Next focus on your privacy policy, which is again very easy to spot. As are activities where you send or sell personal data to third parties, or buy it in. Collecting anything that could be health data is also worth promoting to the top of your priority list.

While all data processing that you conduct must be compliant by 25 May 2018, it is best to prioritise remediating your public-facing activities first, as their publicly visible nature makes them far higher risk than internal processes. They can be a lower priority, as you're highly unlikely to be fined on day one.

The GDPR needn't induce panic – remember the new rules are not designed to put you out of business or to prevent organisations from dealing fairly with personal data, they're designed to curb unfair or invasive uses of personal data by organisations that have no business dealing with that data in the first place.

Lots of people believe the GDPR has been initiated to bind us with red tape. It hasn't. It' simply making sure that data about individuals is being handled fairly and not without their consent.

Where to go for help?

For advice on any of the matters set out in this paper, please contact:

Raoul Lumb
(Associate–Technology and Data protection) **raoul.Lumb@smab.co.uk**

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