Microtrading
Your trusted IT partner

GDPR Guide for Sports and Recreation Alliance members

Helping you to understand the new privacy laws and how they affect your organisation.

What is GDPR?

The GDPR seeks to create a data protection law framework across all organisations that manage, process and control data, and aims to give control of personal data back to the individual. The reform imposes strict rules on those hosting and processing this data, anywhere in the world. The regulation presents some challenges to the accepted ways of managing data and makes clear the responsibilities of both the controllers and the processors of any data.

How does it affect sporting bodies?

If you collect, store or process personal data (data that can be identified with an individual—this could be by name or other identifier, such as an IP address) then yes, GDPR will affect you.

As a sports governing body, it's likely that you hold a large amount of personal data pertaining to your staff, your members and many other associated individuals. As a result, the volume of data you store may even be larger than that of most businesses, with your size of staff.

Due to the nature of your organisation, you may also hold a large amount of what is regarded as 'special data'. This can include information, such as the height and weight of individuals, which you must hold and process for the purposes of competition, and health and safety.

Not only this, but you are also likely to be subject to safeguarding legislation, stemming from your younger members. As such, you have perhaps one of the strongest obligations to keep your data safe and using it correctly in accordance with the GDPR.

Five key areas that need to be addressed

1. Governance:

Identify what measures need to be put in place, against what activities and compliances you already maintain and have. You'll also need to determine roles and responsibilities within your organisation.

2. Security:

Protecting the security of your data and providing systems that ensures proper user rights, choice, rectification and erasure correctly and easily is paramount.

3. Processes:

This is probably one of the largest and impacting areas of the regulations, understanding the required changes is key and will allow you to adapt existing processes and implement new ones where needed. Make sure you have the internal resources and processes in place to detect, investigate and respond to breaches.

4. Data:

Understanding where your data is, how it's used and who is interacting with it is a primary requirement. Access to sensitive data should be granted on a need to know basis and reviewed regularly.

5. People:

Educate your staff on GDPR requirements so they understand the risks of improper data use and how to spot a breach if one occurs. You may wish to consider designating a Data Protection Officer (DPO) if applicable.

What if personal data is lost or stolen?

If personal data is lost or stolen then you must inform the Information Commissioner's Office (ICO) of the loss within 72 hours of discovery. If you are found to be in breach of the regulation then the fines are potentially catastrophic. For the most serious breaches the fines are up to 4% of global turnover, or 20 million euros, whichever is greater. There is even the possibility of a custodial sentence for wilful disregard.

How is data loss most likely to occur?

The most common ways for organisations to suffer from data loss and security breaches are:

- Rogue employees
- Ransomware attacks
- Honest mistakes
- Phishing emails
- Technology failures

What should you do now?

The GDPR is in full effect. If you have yet to make changes to ensure your compliance with the GDPR, or if you are concerned that the changes you have made may fall short, it is crucial that you act immediately. it's important that you understand:

- The data your organisation holds and where it is stored?
- How data is shared amongst staff and business partners?
- Where are the potential risks for data loss and how can these be mitigated?

You should also be looking at using technology to help your organisation protect its data and reduce the likelihood of a security breach and data loss.

Microtrading
Your trusted IT partner

How can technology help?

Prevent external hack attacks and malware outbreaks

Emails and websites are by far the most common ways for a virus to enter a system. As an absolute minimum your organisation should be using a recognised and reputable anti-virus and email ltering solution that is updated daily.

Perimeter security should also be put in place, such as a hardware rewall with gateway services, to provide multi-layered protection and prevent hackers from gaining external access to your network. Most firewalls provide web content filtering services too, this stop users from browsing to undesirable websites that may contain malware.

Automated patch management and updates

Nearly all software programs have vulnerabilities and software vendors regularly release updates and patches to fix these. This means all of your software applications and operating systems need to be patched and kept up-to-date to reduce the likelihood of a security breach. Preferably these updates should be deployed as soon as they are released by the vendor, but this can be an onerous and time consuming task. You should look to use an automated patch management system to reduce this burden. A good Managed IT Services Provider (MSP) should be able to take care of this for you.

Minimise data loss

In the event of a malware attack, human error or technology failure your organisation may need to rely on its backups to restore services and minimise data loss.

Critical data and software applications should be backed up at least once a day to a secure off-site location. You'll need to regularly test your backups to ensure they are working as expected and systems can be recovered quickly and comprehensively. We recommend testing your backups at least once every three months.

GDPR imposes a legal requirement to adhere to the following:

- Have a lawful purpose for collecting the data
- Only collect the minimum you require for that purpose
- Store the data for no longer than is necessary
- Processandstorethedatasecurely
- Ensure the data you hold is accurate and up-to-date
- Ensure that you can provide the data subject with the data you hold upon receipt of a legitimate request

Controlled access to sensitive data

Most organisations have devices such as laptops, tablets and smart phones that are regularly taken outside of the office. Often there is sensitive data stored on these, which should be protected to prevent it from falling into the wrong hands. Using encryption technology, such as Bit-Locker, is a must for these devices and will prevent this data from being accessible in the event that the device is lost or stolen.

Additionally, digital rights management solutions can control access to sensitive data to only authorised users. Policies and restrictions can be applied to stop data from going outside of the organisation or reduce the functionality available to the person receiving it. For example permissions can be applied to a file that prevents it from being copied, printed, emailed or screen grabbed.

Technology can be used to help you comply with GDPR, reduce the likelihood of data breaches and protect your organisation's reputation.

Where can you go for help?

Further information on GDPR can be found on the Information Commissioner's Office website at **www.ico.org.uk**.

Microsoft's Secure Productive Enterprise suite offers many of the components needed to help protect your data.

For more information visit,
https://www.microsoft.com/en-gb/microsoft-365.

For more information and advice

You can call **Andrew McLellan, Senior Business Advisor on 0121 784 0077 or email am@microtrading.co.uk** to get help and discuss your needs in more detail. Also, visit our website and news page at **www.microtrading.co.uk** for the latest updates on technology and IT security.

GDPR is a regulation and not a directive. This means it has to be implemented by every organisation and you must continue to adhere to it.

Microtrading
Your trusted IT partner

For more information on GDPR and how Microtrading can help, call 0121 784 0077 or visit www.microtrading.co.uk