GDPR

General Data Protection Regulation

Compliance Information Guide - May 2018

eventgenius

About this document

Ticket Arena & Event Genius Disclaimer

DISCLAIMER: This is a brief presentation for information purposes only and is general and educational in nature. The guidance does not intend to constitute legal advice for any specific situation or a definitive or complete statement of the law on any subject. The guidance may not reflect or include all recent legal developments and may not apply to all the specific facts and circumstances. Ticket Arena & Event Genius does not undertake any obligation to consider whether the information provided in this guidance is sufficient or appropriate for any particular circumstances. You shall seek separate legal advice where necessary.

Ticket Arena & Event Genius are not responsible for your GDPR compliance.

What is GDPR?

GDPR stands for General Data Protection Regulation and is a **new piece of legislation** surrounding data management that comes into effect on May 25th 2018. This will **replace the current Data Protection Act (DPA)**. This law **increases Europeans rights** when it comes to how their data is used. This gives regulators greater powers to **take action** against businesses that breach the new law.

Firm Fines

4% of annual gross turnover, or

€20 million, whichever the greater

Data Protection Act

The GDPR is **an extension of the Data Protection Act that came out in 1998 –** many policies may already be in place

Who the law covers

The law applies to non-EU companies that offer services to **EU Citizens** – this does not affect non-EU customers

eventgenius

GDPR, PECR & Direct Marketing

- GDPR does ***not*** cover direct marketing. This is governed by the Privacy and Electronic Communications Regulation, (or **PECR**) which sits alongside the current DPA and will continue to be in place when GDPR becomes enforceable on May 25th.

- **Consent** under the GDPR relates to gaining consent for ***processing*** the personal data, not consent for receiving direct marketing from companies.

- Whilst GDPR does not cover direct marketing, GDPR is still relevant as it regulates the processing of the personal data, including the personal data contained in a marketing database. Prior to May 25th, if you created or obtained your marketing database in a lawful way pertaining to the PECR and the Data Protection Act, then you should be able to use it for marketing purposes, but it must be used now in compliance with GDPR and PECR. If your database was purchased from a third-party supplier, then please seek legal advice on the best way to approach this so you can continue to utilise the data.

- From May 25th, **new** customers can opt-in to receive marketing communications from *both* ourselves and *you* as the event organiser at the point of purchase; these individuals will be clearly marked on our systems. Please be aware that you could be breaching the laws if you send **electronic marketing communications** to end users that are not marked in our systems as an "opt-in", so please consider if you have any legal grounds before doing so (and seek legal advice if required).

- You will still be able to see customer aggregated/anonymised information for event management and analytical purposes.

- You can find out more about PECR and GDPR by clicking here

eventgenius

Key Definitions

Personal Data: The GDPR applied to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Data Subject: The data subject is a living individual to whom the data relates.

Data Controller: A data controller is a person or organisation (either alone or jointly or in common with others) who determines the purposes for which and the manner in which any personal data are, or are to be processed.

Data Processor: A data processor is a person or organisation who processes the data on behalf of the data controller.

Many of the obligations described in this presentation apply to controllers, however processors also have obligations under the GDPR.

The Rules of GDPR

Field	Before GDPR	After GDPR
Fines for failed compliance	Max £500 (UK)	Max 4% of the company gross annual turnover, or €20 million, whichever is the highest
Authorities enforcement	Governing bodies had limited enforcement powers	The ICO will have a wider range of enforcement tools available to them such as raids and audits. They can stop a business transacting if necessary.
Who is it relevant for?	Companies based in the EU	Processing carried out by controllers or processors operating within the EU and organisations established outside of the EU (when offering their goods or services to EU individuals or monitoring their behaviour).
Data subjects rights	Data subjects had the right to access and correct their information.	There are now 8 data subjects rights that each individual has in relation to the processing of personal data by a conroller
Consumer consent	Implied consent was acceptable. For example 'By continuing with this purchase you agree to abide by the terms & conditions...'	Much greater onus on companies to document and prove consent from individuals and being transparent enough to validate that consent. Positive consent (e.g opt-in).
Breach notifications	Not compulsory under the DPA 1998	There is now a mandatory requirement to have the regulating body (ICO) notified within 72 hours notice of the breach taking place. Have to prove documentation and securities that are in place to show due diligence.
Accountability	No real explicit accountability	Companies must prove their compliance. Documentation is not enough. Procedures, policies and systems in place must be documented and if needed, demonstrated to the governing body (ICO) should an audit be carried out.

What does it mean?

The GDPR is about the personal data of our consumers, promoters and staff, ensuring it is managed appropriately, effectively and securely. Transparency and accountability is key. You can look at the **principles** and **data subjects rights** that underpin the regulation in more detail during using the hyperlinks below.

Six Principles of GDPR:

a. Lawful, fairly & transparent
b. Specified, explicit & legitimate
c. Adequate, necessary & relevant
d. Accuracy
e. Data Timeframes
f. Security

Data subjects rights:

1. To be informed
2. To access
3. To rectification
4. To erasure
5. To restrict processing
6. To data portability
7. To object
8. To automation & profiling

eventgenius

What are WE doing?

Event Genius is in the process of the following actions:

- An **internal audit of our current process, policies and data flows** relating to personal data, ensuring that the basis of our data use is lawful
- A **gap analysis (GA)** in conjunction with the new GDPR compliances and policies
- **Research & training:** GDPR compliances have been documented and training sessions implemented for our staff
- **Deploy any changes** that need to be made to the system and/or processes as a result of the GA
- Ensure **systems are able to track, audit and manage data** as expected
- Ensure **systems are robust and secure** by conducting tests with our IT infrastructure supplier
- **Work with our legal team** to ensure all legal documents are up to date, including our Privacy Policy, & Event Genius Terms & Conditions

eventgenius

What should YOU be doing?

We have outlined some steps that should help you get started on your GDPR journey. Remember, your GDPR compliance for your company, is your responsibility.

- **Understand the changes to GDPR** – remember, this is an extension from the 1998 DPA so you may well have many policies & processes in place
- **Review your Privacy Policy** and any other policies to ensure they are up to date
- **Review any contracts you have in place with third party suppliers** and ensure they are updated to be GDPR compliant – if they aren't, then you may also be liable
- **Appoint someone to manage your GDPR process** and be accountable – do you need a Data Protection Officer?
- Ensure your **websites are updated as applicable**
- **Build a paper shield** – document and detail all of your processes
- **Create a flow record of your data** – what data do you keep? Where does it go? Who is it shared with? How is it shared?
- Ensure that you have a **lawful basis in place for data processing**
- **Research & training:** Make sure your GDPR compliances have been documented and training sessions implemented as applicable to your staff

eventgenius

Further reading & useful resources

- ICO Getting Ready for GDPR Checklist
- ICO Website
- ICO GDPR Main Page
- ICO GDPR Key Definitions
- ICO GDPR Lawful Basis for Data Processing
- ICO GDPR Individual Rights
- ICO Guide to Legitimate Interest under GDPR
- ICO Guide to Privacy and Electronic Communications Regulations

Contact Us...

@ support@ticketarena.co.uk

0113 350 4114
Our office is open Monday – Friday 10:00am – 5:00pm
should you wish to speak with a member of the team

eventgenius