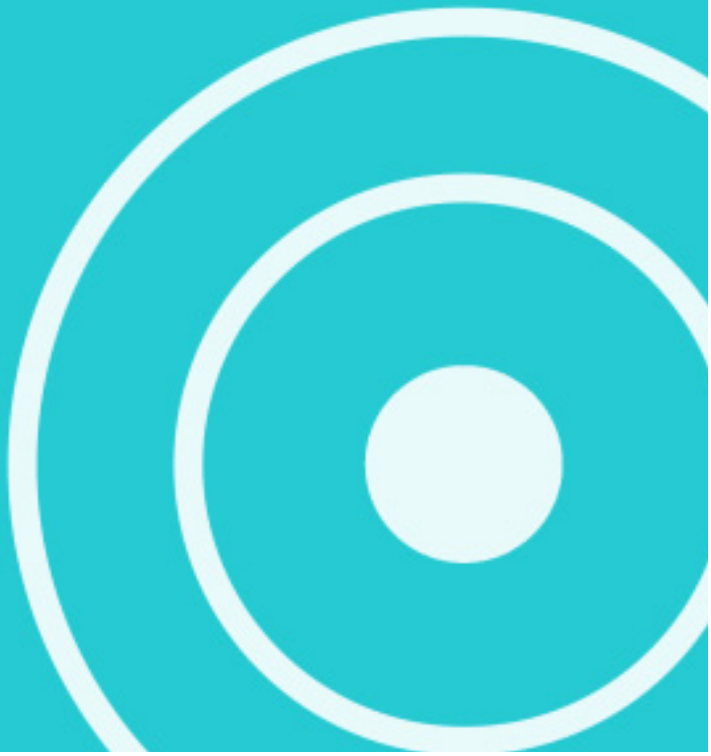
VENUIQ

GDPR

Compliance Bulletin



What is GDPR

The EU's General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring data protection legislation into line with new, previously unforeseen ways that data is now used.

Currently, the UK relies on the Data Protection Act 1998, which was enacted following the 1995 EU Data Protection Directive, but this will be superseded by the new legislation. It introduces tougher fines for non-compliance and breaches, and gives people more say over what companies can do with their data (Personal Data). It also makes data protection rules more or less identical throughout the EU.

'Personal data' 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.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The GDPR is (ironically given its name) a pretty 'general' piece of legislation. It mainly asks for an organisation to prove they are working to industry best practice. The good news is that, in our opinion, having an active and properly managed platform is a key part of that as you are able to demonstrate a central repository and control of personal data of your clients and prospects.

VenuIQ does not offer any advice or warranty any action based on the contents of this document. It is intended to bring clarity to how VenuIQ ensures GDPR compliance but the end responsibility for compliance resides with the customer.

Contract

The data stored in VenuIQ belongs to you, our customers. However, clearly we store and secure the data. VenuIQ is the "data processor" and you are the "data controller".

Under GDPR there are a series of requirements that a data controller has to ensure that all their data processes are compliant with. In order to make this process as easy as possible to our clients, we have immediately added these obligations into our standard contract, In essence we are pro-actively taking these obligations onto ourselves. These can be found in *Schedule 4* of our updated contract at https://venu-iq.com/terms-and-conditions/

Record of Processing Activity

The GDPR requires the "data controller" to keep a record of processing activity for personal data. This is not a record that we can create for you. Below we have created a small list as a starting point but creation and management of this list depends on how you have configured VenuIQ.

Purpose of Processing	Category of Data	Description
Management of Delegate data for event	Standard	Not limited to but most likely includes: - Lastname and Firstname - Email address - Phone number - Address - Questions answered in Q&A - Polling results from within app - Surveys results from app
iBeacon tracking data (where ibeacon devices used)	Standard	When ibeacon name badges are used, location data is stored from within venue. Data can only be obtained from where gateways are positioned. Data used to analyse event attendee behaviour.
Data accuracy & efficient business operations	Standard	VenuIQ APIs can be used to access and update data from other applications via API. However, this can only be created on request from the Data Controller and regulated via a secure API key

VenuIQ only processes data entered by the "data controller". The above is a register of the primary types of data we would expect to be stored in VenuIQ. Typically this does not include any data that is considered Special Category data under Article 9 or 10 of the GDPR. However, it is the responsibility of the "data controller" to ensure a register of any data collected that is covered by Article 9 or 10 is properly adhered to and VenuIQ does not warrant any such collection of data. To check what type of data is covered by Article 9 or 10, please check here https://gdpr-info.eu/art-9-gdpr/.

Provide Assistance

As part of GDPR, we as the “data processor”, must provide all best efforts assistance to the “data controller” in adhering to a data request from an individual.

Our support teams will seek to accommodate occasional support requests from customers relating to these areas.

In the case of ongoing or regular requests, as defined by VenuIQ, our data teams will be available to offer support on a chargeable basis. This can be discussed with your Account Manager in more detail.

Protect Information

Data Deletion & Retention schedules

Once data is deleted by a customer (“data controller”) from the VenuIQ interface, it is soft deleted in the VenuIQ database. There is no way for access to this data by the “data controller” without going through our support teams.

If the setting is enabled as part of your subscription, data can be set to auto hard delete 12 weeks after last access. Also, the same setting allows manual hard delete via the VenuIQ interface. Once hard deleted it cannot be retrieved.

In terms of data that you, as the “data controller”, have sent to us as part of ongoing support, this is also subject to our two-year retention period. It is stored on secure storage and will be deleted during our annual data review if it is over two years since it was last edited or accessed. It is the data accessed date that applies. This review happens once per annum so it can be up to three years after last accessed date that the data is deleted.

Model Clauses

All staff members of VenuIQ are contractually bound to adhere to data protection rules. If as part of our ongoing work, any of our team members outside the EU have to access your data (note it will never physically leave UK/EU) then all appropriate safeguards will be in place including EU Model Clauses.

Staff Awareness Training

All VenuIQ staff members receive ongoing awareness training as to our data policies.

Technical & Organisation safety measures

We follow industry best practice with regard to our infrastructure and software security:

- All your user passwords are saved in a hashed format so cannot be accessed in plain text

- All data is secured in AWS UK based data centres with 99.9% availability
- Data centre is manned by security 24x7
- Perimeter door monitoring and alerts
- Multi-tenanted infrastructure including multiple webservers, databases and file storage
- Data replicated within AWS for disaster recovery purposes
- Extensive digital CCTV system covering internal and external areas. Monitored by on-site security teams
- PAC Integrated card access and biometric access control with full auditing and reporting
- Access to infrastructure is locked down to VenuIQ offices
- All development is managed using Github tools to manage code quality and security access to code
- Password change policies enacted frequently
- VenuIQ has committed to starting the process of becoming ISO27001 accredited which will provide an external audit of all our security policies and systems

These measures are listed for information purposes and don't replace the contractual terms set out in our terms and conditions.

Notify of Breaches

Whilst data breaches are rare, GDPR sets out that we must have a clear policy in dealing with data breaches.

Our infrastructure teams consistently monitor for intrusions and they form part of our ongoing regular proactive checks.

In the case of a data breach being identified, a "Major Data Protection Incident" will be declared. The Delivery & Support Manager and Chief Technical Officer will be notified and will head up an initial investigation to establish what sort of access was obtained and if any data was at risk. Immediate steps would be taken to close any access that caused the data breach.

As early as possible, but certainly within 24 hours, the primary contact at the "data controller" (customer) will be informed and provided with as much information as possible. As our investigation continues, we will update the "data controller" continually. We will do all we can to provide all information to enable the "data controller" to meet their duty under GDPR to notify individuals of a data breach regarding *Personally Identifiable Information* (PII) within 72 hours.

Nominated Person

We are not a large multi-national or a public-sector business so we aren't required to appoint a Data Protection Officer (DPO) who would have certain fiduciary duties.

However, all our staff have undertaken training on the impact of GDPR. If extra help is needed, then the Delivery & Support Manager can assist.

The ultimate contact with relation to GDPR is the Chief Technical Officer

Location of Data

All our data centres are UK based. None of your data will ever be physically stored outside the UK or wider EU.

These data centres are using industry best practice security and access control.

If as part of our ongoing work, any of our team members outside the EU have to access your data (note it will never leave UK/EU) then all appropriate safeguards will be in place including EU Model Clauses.