What Virtual Event Planners Need to Know About GDPR

The new General Data Protection Regulation (GDPR) law goes into effect 25, May 2018. GDPR will apply to every organization organizing/hosting events where any EU citizen attends regardless of the event hosting location or the organizers location.

GDPR will change the way we arrange, market, attend and follow up events and how we collect data right from registration through to attending an event.

Data collection has an increasingly important role in the events industry as the more personal data event organizers can collect about the people who attend their events, the better they can customize the event experience. But, there is risk associated with the collection and handling of all that data. That is why the EU approved the General Data Protection Regulation (GDPR), which goes into effect on 25 May 2018.

For event planners, this means the personal data of EU citizens who attend their events must be handled in compliance with GDPR. Some companies think they are too small, or ignore GDPR because they do not have European operations. However, GDPR applies to companies of all sizes no matter where they are located. As long as one or more attendee joins an event from Europe, GDPR applies.

What is GDPR and Why Does it Matter?

GDPR replaces and improves upon existing regulations, notably, the EU Data Protection Directive of 1995, and addresses developments in mobile and cloud technology. GDPR also combines various existing regulations into one harmonized and simplified set of rules for all EU nations.

Non-compliance to GDPR can lead to some very serious financial consequences (up to 20 million Euros). People aren't fully aware of their rights yet, but they will be. And once they are, the enquiries will start to come. As will the lawsuits.

Collecting Data Before and After Events

- Purchasing data lists for marketing purposes: Clean data lists are the key to successful events, yet where do event organizers stand when it comes to buying a data list once the new regulations come into force? Before purchasing any data lists, organizers must make sure their supplier has proof and permission that the contacts have given their consent to be marketed to.
- Data Retention: The data can be retained for future use, there is no black and white stipulation regarding how long you can hold the data for, but all sensitive personal data should be removed (dietary, political, religious, etc.) and if the data is used again, it must be used solely for its original intended purpose and cannot be used to promote other events or sold to a third party unless explicitly consented to at the time.
- Consent: To process data, organizers don't always require consent, however, for things like profiling (behavioral advertising), they need to go back and get consent to use the data. Similarly, if they're using the data to send marketing emails, the recipients must opt-in.
- Event Registration: When it comes to registration, the process should be as streamlined as possible. Organizers must only collect the vital data needed for registration and have the ability to demonstrate the necessity of the data collected. This includes collecting event feedback. Data that is not being used for profiling shouldn't be stored by event organizers.

  Systems must be in place to ensure data has been collected in a GDPR compliant way and if event organizers can prove their existing data collection procedure was compliant there is no need to re-validate the data.

- Removal: For data that was not collected in a GDPR compliant way, those customers must be contacted and they must give opt in consent in order to keep their data. Customers who do not give explicit consent have to be removed from the list and this should happen before May 25th 2018 when the regulation comes into effect.
- Collecting Data at Virtual Events: An integral part of any exhibitor's strategy while attending a virtual conference is to engage with attendees in a live environment and inevitably follow up with an email. Once GDPR regulations come into force, traditional methods of collecting booth visitor data will take a new direction for exhibitors.

  Events deal with high volumes of personal data collected through registration forms, mobile apps and surveys. However, current practices around getting consent in using this information and sharing it with other parties can now land organizations into big trouble under GDPR.

  Exhibitors must obtain consent to use customer data from virtual events for marketing purposes, which can only be done by email contact after the event. There must be a system in place during registration to prove consent whenever data is received.

The Role of Technology Vendors in GDPR Compliance

Data processors (i.e., virtual conference platform providers) – the technology vendors that process the data owned by the event planner – play a significant role in GDPR compliance.

Under GDPR, data controllers appoint a Data Protection Officer (DPO), responsible for ensuring compliance with GDPR. Vendors are also required to provide adequate staff training in principles of data protection and must employ a variety of encryption technologies to alleviate the risk of noncompliance, data breaches, security failures or lack of reactiveness.

While a good data processor will support adherence to GDPR standards, it's worth noting the more solutions and vendors an event planner uses, the higher the risk to data security and non-compliance. Comprehensive technology platforms and end-to-end solutions can help alleviate the burden of compliance.

Disruption in the Technology World is Positive and GDPR Should Be Viewed in this Light

A great example is the taxi company Uber, who didn't have proper procedures in place to safeguard a data breach. The company's reputation has been seriously tarnished in the process.

A more positive example is from accommodation company Airbnb which took additional steps (procedurally and financially) to secure its customer's private data and while there certainly was a monetary cost associated with this change, the brand power gained was immeasurable.

Avoiding hefty fines is the main reason for event planners to comply with GDPR. However, organizations that organize virtual events can set themselves apart from competing events and gain tremendous brand with attendees and sponsors power by complying with GDPR.

GDPR Compliance is a Must

Meetings and events are highly exposed to complex data collection and management, which makes compliance with GDPR a must. The responsibility for compliance with GDPR ultimately resides with the organization organizing the event. This makes choosing the right virtual conference technology partner more critical than ever.

What are the GDPR Requirements?

- Consent: Event organizers will be required to obtain their attendees' consent to store and use their data, as well as explain clearly how it will be used. Consent must be active, affirmative action by the attendee, instead of passive acceptance through pre-ticked boxes or opt-outs.
- Right to be forgotten: EU citizens and residents at any time will be able to ask you to not only delete their personal data but to also stop sharing it with third parties that they have previously given consent to (ex. suppliers, hotels, venues etc.) – who will also be obliged to stop processing it.
- Breach Notification: GDPR makes it compulsory to notify both users and data protection authorities within 72 hours of discovering a security breach. This is a problem as most of the time, breaches can happen and no one will know about it for a while. But failure to report a breach in this timeframe can result in heavy fines. Make sure that you choose virtual conference platform provider that:

    a) Has security parameters in place to mitigate the chances of a data breach

    b) Has processes in place to quickly notify the event organizer of a breach

- Data Portability: Individuals will now have the right to ask your organization to give them back a copy of all the personal data they previously provided or, send this data to another organization – which may be a competitor. The data has to be provided in a commonly used and machine-readable format so that the new organization can readily import and make use of the data.
- Access: Event organizers must always be prepared to provide digital copies of private records to attendees that request what personal data your organization is processing, where the data is stored and what it's being used for. You need to be able to provide this for free within 30 days of the request. Make sure that you choose virtual conference platform provider that processes in place to quickly help provide this information.
- Privacy by Design: GDPR requires that organizations have to have data security built into products and process from the very start – this particularly applies to all the technology systems (e.g., virtual conference platforms) that help you gather and manage the personal data you have on attendees, as well as any other company systems that hold the same information (ex. CRM systems).
- Data Protection Officers (DPO): Some organizations that frequently monitor large amounts of data or deal with data will also be obliged to have a DPO, who will be in charge of GDPR compliance. That means ensuring internal data protection policies are updated, staff training is conducted and that processing activities are always documented.

The Impact of GDPR on Events

It's easy to look at GDPR compliance as a technology initiative and not a business one. But the reality is that even though it may be the responsibility of the IT, legal or operations team to sort it all out; many of the day to day things event planners do today can put organizations under serious financial risk with GDPR:

- Using pre-ticked consent boxes and vague opt-outs within registration forms
- Not having the proper processes and systems in place that store consent
- Sharing delegate lists freely with venues, speakers and other attendees
- Not paying attention to freelancers and 3rd party organizations that have access to attendee data
- Emailing unsecure spreadsheets

What Will Change with GDPR?

Event attendees will now have the right to:

- Access the personal data you hold on them for free
- Stop or restrict the processing of their data
- Know exactly how the data is being used
- Obtain and reuse their personal data
- Ask for errors to be rectified
- Request the deletion

Event planners will have to demonstrate that:

- They are keeping attendee data safe and secure
- They have the appropriate data management processes and controls in place
- They can respond to data access requests within 30 days at no charge
- They have ways of minimizing errors, correcting inaccuracies and deleting data

- They use data in a transparent, appropriate, fair and permitted way
- They can respond within 72 hours in the event of a data breach

Data Security under GDPR

Data security is another issue that becomes more of a priority under GDPR. Organizations will have to show that they're doing their best to protect the personal information of individuals to minimize the chances of it getting into the wrong hands.

Responsibility for GDPR compliance goes through the entire supply chain – from the organization that is hosting the event all the way through to the third-party vendors that stores and process data on their behalf. Virtual conference organizers are ultimately responsible (in this case, the organization that's hosting the event). This is why it is absolutely critical to choose a virtual conference provider that meets GDPR compliance.

Checklist for Getting Attendee Consent under GDPR

Use this checklist to make sure you're following the right guidelines when it comes to managing consent correctly under GDPR:

- Unbundled - Consent requests (individually) must be separate from other terms and conditions.
- Active Opt-Ins - Pre-ticked opt-in boxes are no longer valid.
- Granular - Give options to consent separately for different types of processing wherever appropriate.
- Named - Name your organization, subsidiaries and any third parties who will be relying on consent (industry sectors will no longer be acceptable under GDPR).
- Easy to withdraw - Tell people that they have the right to withdraw their consent at any time and how they can go about doing this.
- Keep records - You need to maintain records of the consent you got, what users were told and how they gave consent and when.

Five Questions to Ask Event Technology Suppliers about GDPR

GDPR regulations require compliance both by the company organizing an event and by the event technology companies that host, store and process data on their behalf (ex. registration systems, virtual conference platform providers, mobile apps, surveys, networking tools etc.).

The requirements clearly state that data controllers must show how they are complying with the new regulations. And part of that responsibility is making sure that all the vendors and suppliers they are also dealing with are also fulfilling their legal responsibilities.

With this in mind, it is important you ask your event tech suppliers how they're planning to fulfil their obligations around your events and GDPR compliance:

1) Where is my data hosted? Hosting and sharing data within the EU is legally not a problem – as long as your event technology providers meet the requirements of GDPR. *What can create issues*

and a much heavier burden on you, however, is if the data in these systems is stored in servers outside of the EU. Remember, it is your organization's responsibility to ensure that data transfers outside the EU still meet GDPR standards. If your data is hosted in servers outside the EU, then you need to ask your providers what steps they're taking to make sure your data transfers are compliant. They also need to explain clearly what contractual and legal safeguards they have in place to look after your data at all times.

2) Who has access to my data? It is not enough meeting GDPR requirements with just data storage and the location of servers. You also need to find out how your data is being used while it's being processed by their organization. Find out whom from their organization has access to your data and where are these people located. For example, the support center of your event management solution provider will have remote access to your attendees' personal data. If the support team is based outside the EU (event if data is hosted within the EU), then you will need to ensure that they're also complying with GDPR standards.

3) How does your system allow us to obtain and store consent? As we mentioned earlier, one of the key changes that GDPR will bring is ensuring you have the right processes in place to store, access and erase the data and consent you get from individuals when collecting their personal information. For example, if you're using an event registration system, you would want it to store the date and time an attendee ticked a particular consent box, along with the IP address that was used. That way, if the person complains or there's an investigation by authorities, your organization can prove what consent was given, when it was given and how.

4) How does your system help my delete personal data? Similar to the earlier point, GDPR gives individuals the right to be forgotten – which means you need to have a process in place that allows you to quickly 'erase' any personal information you hold on people. Remember that under the new regulations, you will also need to do this if you no longer have the adequate consent in using their information in the first place. So, if someone attended one of your virtual events but wants you to remove all their information from your database, you need to make sure that your systems have the proper processes in place to help you do that - quickly and at little cost. Ask your providers how their system will help you delete the information, whether this data is also deleted in back up servers and how quickly this is done. Make sure they confirm in writing whenever they do this as this will give you protection if they've failed to delete as promised. It's also worth asking them what their general policy is around data retention: how long do they keep your data on their servers, whether it is moved to other locations and whether or not they delete it after a defined period of time.

5) How does your organization comply with GDRP? Ask your tech suppliers how they themselves comply with GDPR. Having a virtual conference provider that has hosting/data centers located in the Europe will ensure that they're also subject to the new regulations, which will limit your own risk of non-compliance. Do they have a GDPR compliance letter from a 3rd party auditor? How will they help you meet your own obligations? Do they follow best practices for data security? How do they monitor vulnerabilities? Who has access to your data, how do they handle authorization and what happens when someone leaves. Having the answers to these questions will protect you from any unpleasant surprises in the future.

Event organizers need to re-look about how your events are collecting data on EU citizens, how you're storing consent and how you're incorporating data security into your event planning and management

processes. You also need to find out what your event tech providers and third-party agencies are also doing in preparation for GDPR – especially if their data centers are based outside of the EU. Finally, implementing changes will be a team effort where everyone is aware of the new requirements, along with the new processes that you'll need to put in place.

While this article contains information about the GDPR and how it might affect your business, it is not intended as and should not be used in place of legal advice. Consult an attorney for guidance specific to your business.