

GDPR, in summary

The General Data Protection Regulation (GDPR) became effective May 25, 2018.

This regulation is the EU's attempt to provide better protection for EU citizens, and to allow them more control over their personal information while providing businesses a clearer environment within which to operate. This regulation affects events that previously or will involve collection of personal data from an EU citizen who attends events anywhere in the world (EU attendees).

There are seven key requirements of GDPR:

Consent: EU Event participants must consent to the storing and use their personal data. The organizers of the Trade Show or Conference must provide an explanation of how an attendee's data will be used. The attendee must actively opt-in or opt-out of allowing their data to be used.

Breach Notification: EU participants and the governing authorities must be notified within 72 hours of discovering a security breach that impacts their personal data.

Access: EU participants must have access to their data. If a participant requests their recorded data records, the organizer of the Event must provide them and include information on where the records are stored, what they are being used for and provide the attendee an opportunity to correct any incorrect information.

Right to be Forgotten: EU participants have the right to instruct the Event organizer to delete or not share their personal information.

Data Portability: EU participants have the right to ask the Event organizer to provide their personal information to another data controller. The file must be in a commonly used digital format, e.g. CSV or JSON file formats.

Implemented Privacy Design: Event Organizers must have data privacy controls and security processes developed into all data collection and usage systems from the onset. Privacy considerations must be built into all systems that collect personal data, such as registration systems, electronic communication methods (e-mail or SMS) and Contact/Customer Management Systems.

Data Protection Officer (DPO): Organizations that handle large amounts of data must identify an individual within that organization to oversee this data. This person is responsible for ensuring internal data protection policies are updated, staff training is conducted and processing activities are documented.