



GOLDSRING
— CONSULTING —

Are You Ready for The General Data Protection Regulation (GDPR)?

Introduction of Presenter

2



Kevin Iwamoto

Senior Consultant, GoldSpring Consulting

Author: Strategic Meetings Management
Handbook: From Theory to Practice

&

Your Personal Brand, Your Power Tool to Build
Career Integrity

What's GDPR? When Does it Go Into Effect?

3

- The new General Data Protection Regulation (GDPR), which replaces the current 1995 EU Data Protection Directive, will provide a completely new framework to the way we collect, process and protect the personal data of citizens and residents from the European Union (EU) and will include the UK pre Brexit.
- The new EU General Data Protection Regulation (GDPR) will be directly applicable from May 25, 2018.

What Constitutes PII & Personal Data?

- “Any information related to a natural person or ‘Data Subject’, that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, traveler loyalty programs, medical information, or a computer IP address.” – GDPR site definition
- Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Why is GDPR happening?

- The legislation that is currently in use (the EU Data Protection Directive) was put in place before the Internet and cloud technology completely changed the way companies use data, and the GDPR aims to address that.
- The U.S. has the least rigor and regulations around data governance; previous exemptions allowed to the U.S. via Safe Harbor and currently Privacy Shield have been opt in for a payment to gain an exception to the stricter EU data governance standards. GDPR will eliminate this loophole and bring all countries into the same EU governance standards.

Who Does GDPR Impact?

6

- Any organization that collects and processes data on European citizens and/or residents falls under the new regulation.
- If you're using any technology (e.g. GDS, on-line booking tools (OBTs), registration software, mobile apps, etc.) which helps you capture and process personal data around your programs, then GDPR will also apply to your technology and program support providers (even if they're based outside of the EU).

Three Main Reasons Why GDPR Legislation Should Matter Companies Worldwide

7

- Responsibility for GDPR compliance will extend to marketing, travel, meetings and event operations – not just IT and legal departments. It will apply to every organization collecting data on EU citizens and residents – regardless of the trip, meeting or event location.
- Travel and events deal with high volumes of personal data collected through GDS and OBT bookings, on-line registration forms, newsletters, mobile apps, surveys, etc. However, current practices around getting and documenting consent in using this information and sharing it with other parties can now land organizations into big trouble under GDPR.

Three Main Reasons Why GDPR Legislation Should Matter to Companies Worldwide

8

- Travel managers, event planners (TMCs and meeting-event management agencies) now have to play a bigger role in securing their travel and event data; ensuring that third party suppliers (e.g. Tech suppliers, event registration suppliers) are also GDPR compliant. Not doing so can result in hefty fines* and lost business.

*Up to 4% of their global annual turnover of the preceding financial year or up to €20 million (whichever is higher) – that's in addition to any personal damage that may be claimed by individuals whose personal data has been compromised.

What Are Some of the Major Changes?

9

- Classification of data handling roles: Controller & Processor
- Appointment of Data Protection Officers (DPO)
- Enhanced individual privacy and consent rights – (Article 17 – The Right to Erasure aka Right to be Forgotten)
- Large fines

What is a data processor and a data controller?

10

- A controller is the entity that determines the purposes, conditions and means of the processing of personal data (Your Company)
- The processor is an entity which processes personal data on behalf of the controller (Your Third Party Suppliers)
- GDPR compliance from all supplier partners rolls up to the travel and meeting buyers who would serve as the Controller.
- Because GDPR defines obligations and liabilities based on the roles of Controller or Processor, the million dollar question is who will be the one penalized when something goes wrong.

The Controller Role Is...

11

- Fully liable for damages caused by noncompliant processing unless the controller can prove that it is not in any way responsible for the event giving rise to the damage.
- Data controllers are also responsible for reporting data breaches to appropriate authorities and affected individuals within 72 hours of discovery.
- In the case of travel it's feasible that a TMC or MMC partner could be a co-controller.

The Processor is...

12

- Handles data on behalf of the data owner, or controller, and should handle information only according to the written instructions of the controller.
- GDPR requires minimum contract terms between the controller and the processor, also referred to as the data processing agreement. These agreements:
 - Assure data confidentiality and require documentation of GDPR-compliant data processes include written consent from the controller to pass data to a subcontractor, (also called a sub processor) and assure the processor will assist the controller in executing the requirements of GDPR, such as adhering to individual rights requirements to access, correct or delete data and disclosing data breaches to the controller within 72 hours

The Processor is...

13

- If the processor and/or sub processor acts outside the terms of the written contract, it could be liable for fines.

Data Protection Officer (DPO)

14

- GDPR references the hiring of a DPO; does this apply to all companies?
- “DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data (Art. 37). If your organization doesn’t fall into one of these categories, then you do not need to appoint a DPO.”

Individual Privacy Rights Under GDPR

15

Travelers and 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 permit reuse their personal data
- Ask for errors to be rectified
- Request the deletion of their data and documentation of the deletion (Article 17 – The Right to Erasure aka Right to be Forgotten)

2017 The Event Planner's Guide to GDPR Compliance by Eventsforce

What's the Impact to Travel Programs

16

- Do we run and/or provide reports that contain PII?
- Do a process & policy audit to understand when and where PII is being collected and how it is used
- Schedule and review findings for alignment with all suppliers that support and execute your travel program and policies
- Ensure that you are only using data as it was intended and that you are purging it when it's no longer needed
- Evaluate your use of encryption, password protected document transfers and plan for pseudonymization.)"; consider anonymization of reporting data
- Be ready for Article 17 - the "right to erasure (right to be forgotten)"
- What if a EU resident and/or citizen doesn't want to receive the travel newsletter or partner offers?

What's the Impact to Event Management

17

- Using pre-ticked consent boxes and vague opt-outs within registration forms will require changes
- Not having the proper processes and systems in place that store consent as well as delete consent
- Sharing delegate lists freely with venues, speakers and other attendees (encryption, password protection)
- Not paying attention to the data freelancers and temp staff who have access to attendee and registration data
- Emailing unsecure spreadsheets
- Leaving printed registration lists unattended on-site
- Re-usage of mailing and registration lists

Best Practices to Get GDPR Ready

18

1. Have an internal discussion with your company officials who are preparing for GDPR on an enterprise basis; leverage the work already done and customize for your meetings/events
2. Understand the definition and roles of Controllers and Processors, have appropriate alignment discussions with your supplier partners and amend all SOW and SLAs to include GDPR regulation adherence
3. Conduct a data and current process audit; resolve all identified gaps
4. Update your Privacy Information & Consent Boxes on forms
5. Understand individual's rights under GDPR

It's Not All Bad News

19

- GDPR will standardize personal data definitions, guidelines and regulations across the 28 member countries (including the UK).
- GDPR will pressure the U.S. to get more serious about individual data privacy regulations.
- SMMP leaders can use GDPR compliance to gain visibility into global rogue spend and supplier agreements.
- You will stop receiving or get much less annoying marketing ads and solicitations!

GDPR Resources

20

The EU web portal for GDPR: www.eugdpr.org/

GoldSpring Consulting: <http://www.goldspringconsulting.com/strategic-meetings-management/>

The Event Planner's Guide to GDPR Compliance by Eventsforce: <http://www.eventsforce.com/ebooks>

GDPR for Meetings and Events by etouches: <https://get.etches.com/gdpr-meetings-events-ebook/>

Glisser: <https://www.glisser.com/gdpr/>

Stay Connected

21



GoldSpring Consulting LLC
www.GoldSpringConsulting.com

Kevin Iwamoto

kevin@goldspringconsulting.com

- Twitter: @KevinIwamoto
- Industry Insights Blog – Meetings & Conventions:
<http://www.meetings-conventions.com/blogs/industryinsights>
- LinkedIn:
[linkedin.com/in/kevin-iwamoto-glp-gtp-18a1348](https://www.linkedin.com/in/kevin-iwamoto-glp-gtp-18a1348)
- Amazon Author Page:
<https://www.amazon.com/author/keviniwamoto>



GOLDSPRING
— CONSULTING —