October 2021

The event organiser’s perspective on data ownership

The power of interaction

The ability to connect people and facilitate information sharing is at the core of the exhibition industry. Formally and informally, being able to bring the right people, thinking, and businesses together is what this industry has always been about. Historically, this capacity may have been spoken of as 'industry insight,' garnered within the minds of, and materials generated by, a show team. Today, the industry is more reliant on digital tools and platforms to capture and analyse 'industry insight,' and with a rapidly developing digital landscape, interaction data is now integral to enabling useful business connections.

The exhibition industry business model centres on our ability to facilitate customer interactions by gathering the right data, in terms of connections and information, and delivering it to the right customers, at the right time. Organisers have been successful at acquiring and delivering these connections, which are underpinned by organisers' custody of personal data, because of the long-standing, trust built, relationships with customers. For a customer, the value of sharing personal data with a trusted organiser is to become connected, or to get information directly related to their individual business needs. From an organiser perspective, the value of understanding that data exchange is to help uncover and understand interactions between customers, enabling organisers to tailor events and ancillary products/services to the specific needs of the community. There is an established and transparent relationship between the organiser, acting as a data controller, and the customer, as to the uses and benefits of that data exchange.

The digitisation of the exhibition industry, accelerated by the COVID-19 pandemic, has given rise to new types of events and digital offerings and more ways to obtain personal data linked to customers. Organisers are often doorkeepers for attendees, open access directories for exhibitors, and concierges to both. To meet the wide-ranging needs of the various categories of customers, organisers have turned to third-party technology providers for solutions. However, in some cases, the standard operating procedures for suppliers, acting as data processors, may not have been implemented as quickly as the technologies themselves, which, if left unremedied, could potentially lead to governance gaps. This has led to challenges of trust between organisers and suppliers, as well as organisers and their customers.

A notable example is the emergence of more virtual and hybrid event platforms and event organisers' increased use of these services. It is of critical importance that any organiser, as a data controller instructing third-party suppliers to act as data processors, understands and defines the supplier's terms of trade and operation. This includes clearly articulating the parties' respective responsibilities with regards to data, both acquired directly from customers (for example, during the event registration process) and generated throughout the course of the supplier providing services on the organiser's behalf (for example, interaction data gathered during sessions). The trust of the customer relies on the conscientious treatment of this data, for their benefit, and therefore our industry relies on protecting and being transparent about data.

Definitions

For the purposes of this paper, we refer to "data ownership" in the context of liability and responsibility for the personal data entrusted during the course of event hosting. In addition, we utilise these definitions for roles within the context of data ownership.

Data Controller: The organisation that determines the purposes for which and the means by which (the 'why' and 'how') personal data is processed is defined as the 'Data Controller'. Data Controllers are usually event organisers. It is possible to have Joint Controllers, for example in the case of a JV partnership.

Data Processor: The organisation that processes personal data on behalf, and under the instructions, of the Data Controller is a Data Processor. The Data Processor is usually a third party service provider, such as event registration providers or general services contractors. Data Processors may contract out parts of their service provision to other service providers, who are defined as 'sub-processors'.

Topics for organisers to consider

The below are critical areas that must always be considered in any data relationship.

Is the goal of the customer at the forefront? The goal of the customer is to exchange personal data, often in the form of business contact information, with other customers. The industry's role is to use the data entrusted to it to help individuals and businesses find what they need, helping the customer fulfil their goals. The sharing and exchanging of data, and the facilitation of that exchange, relies on transparency and trust.

What data is being created? The utilisation of digital platforms to stage online events or components of events offers opportunities to learn more about our customer interactions that would otherwise not be available at a purely face-to-face event. This provides greater insights into our customer networking and event needs, which in turn enables better connections and business opportunities and experiences for our customers.

However, there are times when third-party suppliers engaged by organisers may offer services over and above the original intent of the event, and therefore it is key to define the scope of services from the outset. Some of these services may fit the commercial strategy of the organiser, whereas others may not and thus could lead to the collection of far more data than is needed. Furthermore, some suppliers may process more data than others to deliver the same service. Therefore, it is important the organiser fully understands what data is being gathered and processed by each supplier and that appropriate contractual parameters are agreed.

Historically, digital interaction data is not a class of data that has been widely available to the organiser as it typically was not captured in full. From the organiser's perspective, the emerging availability of such interaction data is a valuable asset and so data policies and operating procedures should take this development into consideration.

What data does an organiser send/receive from the supplier in the relationship? When partnering with service providers, such as virtual event platforms, an organiser should establish what data is needed to create and maintain the platform, as well as who owns the raw interaction data after an event, and whether it can be used by the supplier (e.g. to train artificial-intelligence models). Organisers need to be exceptionally clear on who owns this information and how, if at all, suppliers can use it, whether that's via a singular ownership or co-ownership structure.

The simplest, and most critical, question your supplier should give a clear response to is **"will the supplier be using the data for its own commercial purposes?"**

If the answer is "yes", it is key for organisers to understand why that needs to be the case and for organisers to determine if they are comfortable with that position (taking into account factors such as whether or not customers would expect the supplier to have this right). Further, it is crucial to determine if a supplier's intended use of data involves the capturing of anonymised, aggregated data, used solely for the purposes of improving platform functionality, or whether a supplier believes it is a data controller and can utilise the data for anything it wants, including using the interaction data to facilitate business connections within that community, replicating the services and business aims of the organiser.

Question guide

You and your supplier should be able to answer questions such as:

- Who decides what data is collected, how it will be used and why?
- Will our customers expect their data to be processed in this way? Will there be any surprises?
- Is the processing fair, lawful and secure?
- Are we prepared to tell our customers their data will be processed in this way and is it reflected within an accessible privacy notice?
- Is there a contract in place clearly stating the responsibilities, requirements and liabilities of each party related to the data collected or used?
- If / when something goes wrong (i.e. a data breach) who will take responsibility and be liable for any violations or breaches?
- How long will data be retained by the supplier and why?
- Who can access the data or use the data?
- Who can download a copy of the data or disseminate the data, in any format, and at any time?
- Who can restrict access to the data?
- Who can ask for data to be deleted?
- What can potentially happen with the data?
- Who is responsible for responding to customers' complaints/requests?
- From a customer's perspective, who can contact them/use their information and on what terms?
- Whose terms and conditions apply to the individual's use of the system, platform, service etc?
- Who will be responsible for complying with legal data collection and dissemination requirements for personal data under applicable laws, whether they be foreign or domestic (i.e. the EU's General Data Protection Regulation or the California Consumer Protection Act)?
- On what legal/consent basis will a supplier, as a Data Processor or Data Sub-Processor, be processing data?

Appendix

What is Personal Data (sometimes referred to in the U.S. as "personally identifiable information" or "PII")?

There are many laws globally that define personal information in various ways, but for the purposes of this paper, we define Personal Data as *"any information relating to an identified or identifiable living individual".*

The difference between whether an individual is identified or identifiable is whether the individual can be directly or indirectly identified from the information regardless of intention.

For example, an identified individual would be *"Kai Hattendorf, Managing Director and CEO of UFI".* From this information Kai is quite clearly identified. An identifiable individual would be *"Managing Director and CEO of UFI".* Whilst we do not include Kai's name, this information is quite clearly about him, so he is identifiable.

The most obvious identifier is a name. However, an individual may be identified through other factors including but not limited to combinations of other identifiers such as: home address, IP address, email address, browsing history, GPS data, job title, physical characteristics or likeness.

Personal Data does not include anonymous or de-identified data.

What do we mean by "Processing"?

''Processing'' is anything we do with personal data, from the initial collection to the amendment, alteration, transfer, deletion, archiving, storage, sharing, dissemination, distribution, analysis, etc. of the personal data

What do we mean by ''Data Ownership''?

The term 'data ownership' varies and very much depends upon the context in which the term is applied and the applicable legislation.

For the purposes of this paper, we refer to ''data ownership'' in the context of liability and responsibility for the personal data entrusted during the course of event hosting. In this context there are 3 main roles:

Data Controller: The organisation that determines the purposes for which and the means by which (the 'why' and 'how') personal data is processed is defined as the **'Data Controller'**. Data Controllers are usually event hosts.

Joint Controller: Some event organisers work together with other organisations to jointly determine the 'why' and 'how' personal data is processed. In such cases both organisations are considered as **'Joint Controllers'** of the personal data. Joint Controllers may include JV partnerships.

Data Processor: The organisation that processes personal data on behalf, and under the instructions, of the Data Controller is a **Data Processor**. The Data Processor is usually a third party service provider, such as event registration providers or general services contractors. Data Processors may contract out parts of their service provision to other service providers, who are defined as 'sub-processors'.

Appendix

Why are specific data roles important?

There are two main reasons why it is important to understand the "data ownership" role, and what role your organisation undertakes when processing personal data:

1. **Legal compliance and liability:** There are many privacy and data protection laws globally that speak to the need to be clear on organisational responsibility, accountability and liability when processing personal data. It is critical that you are clear on the roles and liabilities your organisation undertakes whenever processing personal data. It is important to stress, in many jurisdictions you cannot 'contract out' your legal responsibility when handling personal data – just because the contract may stipulate an organisation is the liable party, the applicable legislation and the circumstances of the particular processing activity may dictate otherwise.
2. **Transparency and customer trust:** Transparency is one of the most common requirements of the majority (if not all) of the privacy and data protection laws globally. Whenever organisations are processing personal data it is generally a requirement that individuals must be informed who is processing their personal data, and therefore, who is responsible for the fair, lawful and secure handling of this data. Whilst this is a legal requirement, transparency also speaks to building and maintaining customer trust.

How can we ensure that we, and suppliers acting on our behalf, are processing Personal Data fairly, lawfully and securely?

To process personal data fairly, lawfully and securely, we recommend the below listed **Privacy Principles:**

1. **Accountability** – Act as a responsible steward of personal information, ensuring that privacy is a 'board level issue', a culture of privacy is established within the organisation and an appropriate privacy programme is implemented.
2. **Design** – Embed privacy protections into the design of our products, services and business practices, including the implementation of Privacy Impact Assessments.
3. **Purpose** – Collect and use personal information only for legitimate business purposes.
4. **Transparency** – Be open on why and who will be processing personal data.
5. **Choice** – Offer individuals a choice, as required by applicable law, over the use and disclosure of their personal information for marketing and sales purposes.
6. **Rights** – Provide individuals, upon their request, with access to their personal information and amend / delete / restrict as required by applicable law.
7. **Accuracy** – Maintain reasonable procedures to keep personal information accurate, consistent with legal requirements.
8. **Security** – Seek to protect personal information from unauthorised access, use, modification, disclosure and loss through appropriate organisational and technical measures and ensuring that all service provider relationships are covered by contract.
9. **Disposal** – Dispose of (render it useless) personal information appropriately when it is no longer needed.
10. **Lawfulness** – Ensure there is a lawful basis to process personal information collected whether that be a relevant ''legal basis'' or the individual's consent.

Disclaimer

Contributors

Bill Charles, Chief Information Officer, Emerald

Merilyne Davies, Global Director of Privacy / Data Protection Officer, RX

Sinead Davies, Head of Legal, EMEA, Informa Markets

Douglas Emslie, Group Chief Executive Officer, Tarsus

Fernando Fischer, President of the Americas, RX

Adam Ford, Chief Operating Officer, Clarion Events

Stephan Forseilles, Chief Digital Officer, Easyfairs

Lisa Hannant, Group Managing Director, Clarion Events

David Holmes, Privacy & Compliance Manager, Informa Markets

Stuart Ledden, Group Marketing Director, Tarsus Group

Baris Onay, Co-Founder and CEO, Precision Communities

Mark Parsons, Director, Events Intelligence

Herve Sedky, President & Chief Executive Officer, Emerald

Mark Temple-Smith, Chief Operating Officer, Informa Markets

David Audrain, CEO, SISO

Kai Hattendorf, CEO, UFI

Caitlin Read, Content, UFI