Security & privacy:

Do's & don'ts for event professionals

When you organise events, and ask your visitors to register, you are officially processing personal data. This implies that, from a legal point of view, you have certain responsibilities regarding privacy and security. We will point out some things you as an event manager should consider - and give you 5 tips to prevent a data breach.

Text Rutger Bremer, Momice - www.momice.com

As event manager you are continuously collecting and processing personal data. Think about it: how many registration lists are on your computer? Are these data secured? Do you share lists with suppliers, agencies, registration or software partners? Make sure your policy is in line with all parties involved - as most data breaches are caused by human mistakes. As from May 2018, a European regulation will be in force, holding managers (directors) of a company responsible for a data breach. In other words: if something happens to your data, it is not only unpleasant for your clients, but your organisation will risk a (big) fine.

STORAGE: INSIDE OR OUTSIDE THE EU?

It is important to know where the registration data are stored: inside or outside of the EU. The European Union has strict privacy laws that secure the privacy of your data. The US regulations, however, are less strict. This means the American government can easily access your data. This can be highly inconvenient!

A DATA BREACH IS A SERIOUS MATTER

Since 1 January 2016, Dutch companies have an obligation to report each data breach. This implies that organisations (companies as well as governments) must immediately report a (serious) data breach to the Dutch Authority Personal Data. We speak of a data breach when a person or organisation loses control of the destination of large numbers of sensitive personal data, regarding health or religion, but also financial or login information. This is a serious matter: it can cause serious damage to the people involved - and in some cases even lead to dangerous situations. Apart from that, it can result in considerable reputation damage for your organisation (or your event agency's client)!

LIMIT THE AMOUNT OF PERSONAL DATA

You can't avoid asking certain data from your visitor, like first name, last name and an email address. However, always try to limit yourself to the necessary data. Avoid collecting passport, creditcard and medical information: these data are extremely sensitive and require a higher level of security. In any case, always protect your personal data well! Here are some tips to keep your data safe:

5 TIPS FOR SAFE DATA STORAGE

1. Protect your lists with a (strong) password

If you keep the event data in an Excel file, always secure the document with a password. Particularly when you email these lists to a supplier. Send the password separately (preferably in a text message) to make sure only you and the supplier can access the data.

2. Work with trusted event software (partners)

If you work with event software or registration partners, ask them about their security policy. Are the registration data encrypted, when sent between website and server? Where and how are the data stored? Become familiar with the policy of your partners, so you know whether you can trust them with your data!

3. Be careful with free software

Free software is never really free. Commercial products that don't demand payment for their services, always have a different business model. There is a chance that they sell your data on to third parties: client data are worth a lot of money! Carefully consider whether you want to share your valuable database with a free service.

"Without proper awareness you can not comply with privacy laws. Make sure, therefore, that you always know which personal data you process and why"

Legal advice bureau ICTRecht

4. Don't save your passwords in the browser

If you use online software to store your event data, never save the log-in data in your browser. Suppose someone gets hold of your computer, then this person can access your valuable data with just one click. Of course, saving your passwords might seem efficient, however, remember why you needed a password in the first place.

5. Close a processing agreement with your supplier(s)

As from 25 May 2018, the new General Data Protection Regulation (GDPR) will be effective. According to this new law, you have the obligation to close a processing agreement with every person or organisation that processes personal data on your behalf (for instance an external marketing agency or a web developer). This agreement determines how certain data should be processed - and what the consequences are if an incident occurs.

CONCLUSION

As event manager, you are responsible for the personal data of your relations. New regulations (like GDPR) make the careful handling of data more relevant than ever before. If you make sure to involve your suppliers early in the process and secure your own data well, the data of your valuable contacts will remain in safe hands!

Rutger Bremer is founder and managing director of Momice. His company develops all-in-one software for event professionals. Respond to this article? Send an email to rutger@momice.com.