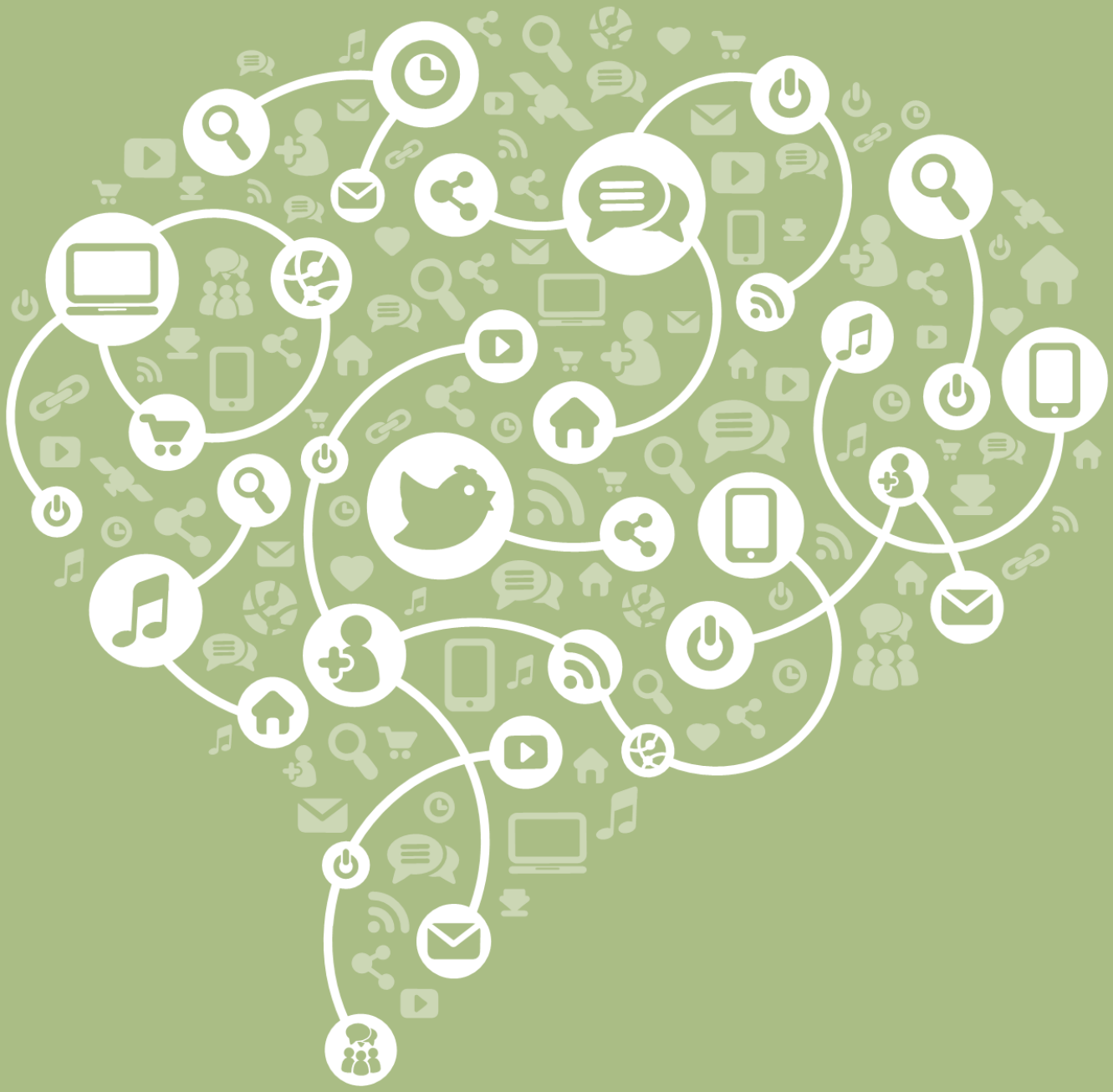

Data protection in the events industry

What you need to know to stay within the law

EventReference

<ref:tech>

Disclaimer

Relevance

This white paper pertains to EU data protection law through its implementation in the United Kingdom. Residents of other EU member states should consult their national data protection authorities for clarification and guidance, as derogations (minor variations specific to local situations) can exist across individual member states.

The data protection authority in the United Kingdom is the Information Commissioner's Office (ICO) at http://www.ico.org.uk.

All URLs are current as of June 2016 and are subject to change.

Disclaimer

This white paper has been written in the summer of 2016 at a time when data protection laws are in transition. The EU has approved the General Data Protection Regulation (GDPR), the new European data protection regime, which will replace the existing 1995 data protection regulation on 25 May 2018.

In addition to GDPR, the Privacy Shield scheme, the transatlantic data protection agreement intended to replace the invalidated Safe Harbor scheme, is currently the subject of ongoing contention between the US and EU. We encourage readers of this white paper to research current developments concerning the Privacy Shield scheme, as they will have changed since publication.

The information provided in this paper is not legal advice and its guidance is offered without prejudice.

Contents

Introduction

For events industry professionals, data is the key to the success of conferences, events, and trade shows. Every event you help to create generates a mountain of data ranging from contact details to dietary requirements to sponsor leads. As the event approaches, that data is typically shared across a variety of roles from exhibitors to advertisers to hotels. The nature of our industry means that this data also moves across international borders. Put simply, a lot of information moves around a lot of different people in a lot of different countries.

In our privacy-conscious times, it is important for members of the events industry to understand their legal obligations to this data and to the people behind it. European law requires careful stewardship of personal data regardless of industry, content, or nationality. The legal framework governing those standards is set to be extensively modernised and strengthened over the next two years. While we will all face increased obligations for data protection, we must view this time as an opportunity to better serve the profession, and the people who attend our events, through stronger data protection standards.

There is a great deal of detailed information in this white paper. It can seem daunting but, as with health and safety regulations, every organiser of every conference or exhibition needs to understand the subject. This white paper is not an expert guide to data protection law. It is, however, a means of informing and inspiring you on your data protection journey. We start by examining the current state of data protection law. We then move on to typical dilemmas faced by events industry professionals, ranging from USB sticks to passwords to web hosts. In doing so we will also examine the lessons learnt by organisations who failed to take data protection seriously. We close by learning about the imminent future of our data protection obligations. At the end of this white paper you will have a greater understanding of the questions you need to ask to ensure robust data protection standards across all levels of your events business.

Our objective is to answer many of the questions you may already have about data security in the conference and exhibitions industries. If you don't have any questions, we hope that this white paper will convince you that you need to think about whether you are taking the proper steps to protect the personal information that you gather about your registrants.

If you need any more information, please email us on datasafety@eventreference.com. We'll do our best to provide answers and I promise that it won't cost you anything.

Simon Clayton
Chief Ideas Officer
RefTech and EventReference

The eight principles of data protection law in Europe require personal data to be:

- Stored fairly and lawfully;
- Stored only for a specific purpose;
- Relevant, adequate, and not excessive for that purpose;
- Accurate;
- Kept for no longer than it is necessary;
- Kept in accordance with the individual's rights;
- Protected by technical and organisational security measures; and
- Not transferred outside the EU, unless the recipient country ensures an adequate standard of data protection.

What is the state of play now?

The current law covering data protection in Europe is the EU Data Protection Directive of 1995. It is transposed into UK law through the 1998 Data Protection Act (DPA). This law applies to all personal data within EU member states regardless of sector.

Data protection deals with what is known as personal data - information relating to identifiable individuals. For example, a conference attendee's registration details contain personal data. The form a trade show attendee fills out to request more information from an exhibitor contains personal data. A dinner attendee's special dietary requests contain personal data.

The eight data protection principles do not impose universal rules, such as a list of specific data which qualifies as relevant. Each principle's interpretation is unique to each organisation and, indeed, to each event. However, the criteria you should use to determine your organisation's compliance with each standard has been set forth by data protection authorities across Europe, including ICO.

What can you do?

In this section we will look at typical data protection dilemmas within the events industry. Many of these scenarios are based on the actual experiences of event organisers and professionals.

As you review these questions, take time to reflect upon your own compliance within both the existing data protection standard and the forthcoming General Data Protection Regulation (GDPR).

Data transfers outside the EEA

"The registration system we are using is based in the US and the data is hosted there. Are we doing anything illegal? Am I doing anything wrong by emailing a spreadsheet containing my event data outside Europe?"

Sharing data within Europe is legal provided that all requirements of the DPA have been met. While it is not necessarily illegal to move data outside Europe, you do need to check a few things. Start by looking at the terms and conditions of the supplier. This should tell you very clearly in which country and under which legal jurisdiction the data is stored. Once you know that, you can check that the country has a bilateral agreement such as Privacy Shield[1] in place. The acceptable standard of adequacy can also be achieved through your existing service contracts with service providers, or through intra-company transfers which may be allowed under certain bilateral agreements. You can also assess a recipient country's adequacy yourself using guidelines provided by ICO, though you must be prepared to document and explain your reasoning to an acceptable legal standard.[2]

Major service providers you may use frequently, such as Dropbox, OneDrive, and Google Drive, are keen to serve their European customers and take frequent steps to adhere to changing EU data protection standards. You can verify this in each service's terms and conditions statement. Smaller service providers, however, may not be aware of the evolving data protection landscape. Many non-European firms are not aware of their EU data protection obligations at all, despite being required to be compliant.

The legal ownership of events data has no bearing on its data protection obligations. An event registration system which maintains ownership of personal data regarding European service users must be in full compliance with EU data protection principles.

If you suspect that your service provider is not located within Europe, check their terms and conditions. Look for evidence of where your data is stored and under what legal jurisdiction. Does the service provider certify adherence to EU data protection principles, and how do they demonstrate it? Do they pass data onto third parties, including social networks, which may aggregate the data with personally identifiable information? If they do not make clear statements on these subjects, you need to be very careful. It may be better to choose an alternative supplier.

1) As of this writing the agreement has not been finalised. Please visit https://ico.org.uk for the latest updates.
2) https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

Consent for data transfers outside Europe

"Most people have no way of knowing where their event registration data is stored. Why is this a problem?"

It's probably fair to say that most registrants won't even think about where their data is stored. Those that do will be well aware that the technical realities of web hosting and cloud storage mean that the data is likely to be transferred outside the European Union at some point. They will also be aware of a series of high-profile European court rulings which have created more stringent notification obligations for international data transfers.

For that reason, your registration processes should advise users that their data will be transferred outside the European Union to a country which complies with the DPA standard. You must demonstrate how you have confirmed that the country of transfer compiles with EU data protection requirements as well as any data protection laws of that country. If the country of transfer is the US, the statement should discuss compliance with the Safe Harbor/Privacy Shield regime.

Microsoft provides a good example[1] of an international data transfer statement, which we have included below. However, it is not enough to bury this notice in a lengthy terms and conditions page. An indication of the international transfer, linked to the full statement, should be visible to users at the time of registration.

"Personal data collected by Microsoft may be stored and processed in your region, in the United States or in any other country where Microsoft or its affiliates, subsidiaries or service providers maintain facilities. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located.

"When we transfer personal data from the European Economic Area to other countries, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data. Microsoft also adheres to the principles of the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of data from the European Economic Area and Switzerland. To learn more about the Safe Harbor program, and to view our certification, please visit http://www.export.gov/safeharbor."

1) https://privacy.microsoft.com/en-us/privacystatement

Encryption

"Are we doing anything illegal by keeping events data on a USB stick or laptop? Does the law require us to encrypt that data? What happens if it gets stolen?"

Encryption is not legally required, and in fact, many politicians with a feeble understanding of technology have humiliated themselves by calling for encryption to be banned. However, encryption is the foundation of a responsible data protection strategy. It is also increasingly expected as the standard required to meet the data security requirement of the DPA.

We strongly recommend encryption of all personal data regardless of whether it is stored on physical or virtual media. This must include data on laptops, CDs, cloud storage, and USB sticks; the data contained in email attachments; data stored on web sites; and the data contained in backup files and archives.

Encryption is critically important during your event, where USB sticks are easily lost and devices are easily stolen. If you utilise data on physical media, ensure that the data is encrypted and that hardware is as locked down as far as practicality allows.

If a data breach or theft occurred within your events business, unencrypted data would be available to anyone. This would greatly increase your legal and financial liabilities to those whose data was lost - as the TalkTalk ISP learned the hard way.

Encryption is a strategy and a business process, not a feature or an add-on. There are many factors to consider in creating your encryption strategy:

- What data will be encrypted;
- The kind of encryption you will use;
- How you will choose the right key size, algorithm, and software;
- What guidelines will be established, for example, mandatory encryption of all outgoing emails;
- How staff will be trained on the new standards; and
- Whether the industry or sector-specific guidelines of the organisations you provide events for require specific or additional encryption standards.

These issues should be clarified with an experienced information security professional.

In 2015 the TalkTalk ISP was the victim of a data breach after hackers accessed the accounts of an estimated 1.2 million customers, including bank details. The data was apparently not encrypted. Rather than apologising for that oversight, TalkTalk's CEO told the Sunday Times "[Our data] wasn't encrypted, nor are you legally required to encrypt it. We have complied with all of our legal obligations in terms of storing of financial information". This box-ticking attitude to data protection caused TalkTalk to incur an estimated £35 million in one-off costs.

How EventReference protects your data

EventReference uses as many protection mechanisms and procedures as possible to ensure your data stays secure and our systems remain available. We have:

- Replicated databases and multiple web servers to provide high availability services;
- Overnight backups of databases to servers hosted in our secure data centre;
- Two-factor authentication (2FA) to provide the strongest possible protection for your admin users;
- Brute force login protection to thwart hackers who might try to attack your account by guessing thousands of passwords;
- Total data isolation between events;
- Full HTTPS encryption which provides security for you and your registrants;
- The highest grade of firewall and network security;
- Constant scans of our systems for security vulnerabilities with a military-grade tool;
- Extensive physical security at our premises including high-grade locks, high-definition CCTV, and smoke cloaks in sensitive areas.
- Encrypted hard drives on all RefTech computers, so even if a machine is lost or stolen, no-one can access the data it contains.

These are just some of the factors that have enabled us to earn ISO27001:2013 accreditation for our whole organisation. We believe that it provides absolute proof that we take the security of your data very seriously indeed.

EventReference

Data security

"We use an online registration service provider. Surely it's their responsibility to keep our event data safe?"

As an organiser, it is likely you will have a website to promote your event. It will be on located on a server which is operated by a web host. The recent loss of data - including *entire web sites* - by a UK web host demonstrated that it is *not* the web host's responsibility to protect or backup your data. It is very clearly your responsibility to keep the data on your website secure and to regularly back it up. You should ensure that there are regular backups of your data from the web site to a DPA-compliant cloud storage account.

Online registration is usually a different matter because many organisers use off-the-shelf online registration systems. These are referred to as Software as a Service (SaaS) because you rent the software rather than owning it. SaaS vendors tend to be responsible for creating and storing backup files, and the best SaaS registration systems will invest significant time and money to ensure that their systems are as secure as possible. Look for ISO27001:2013 accreditation through the whole organisation, an indication that they follow international information security best practices to keep your data safe.

Some conference badges now feature a QR code which contains that attendee's personal information. Conference attendees love to post pictures of themselves and their colleagues on social media. However, a photo of an attendee's QR code can be read by a scanner. If that code contains personal data, anyone seeing the photo has access to that data. Ensure that QR codes do not contain any personal data or information which is not relevant to attendance at the event.

Protection against hacking and external attacks varies widely between different SAAS registration systems. You should choose your service provider based on their security standards as well as their ability to understand your evolving data protection obligations. You should also ask the provider how they monitor their system against vulnerabilities and how they keep up to date with current best practices. Regard your registration system provider as a critical business relationship, not as a faceless utility.

It is worth remembering that a number of reports have shown the primary reason that data is lost from SaaS sites is because of poor admin passwords, which is no fault of any system. Education about good password choices should be part of your data security policies.

The BPAS hack

In 2012 the web site of BPAS, a British charity offering pregnancy and sexual health services, was hacked into by an anti-abortion activist. He was able to download the contact form submission records of nearly 10,000 individuals who had contacted the charity over a period of five years. These records included names, home addresses, and pregnancy and sexual health status. Religions could be derived from many women's surnames. Many of the women requesting help were from Ireland, where strict anti-abortion laws made their contact form submissions a criminal offence. The hacker threatened to publish the dataset on an anti-abortion forum, but was found and arrested before he could.

The investigation into the data breach carried out by ICO found that the charity had not audited the web site for its processing of personal data, they did not store administrative passwords securely, and they had not conducted any security testing. It almost goes without saying that the content management system was outdated and unpatched.

Worst of all, the charity had no idea that a copy of public contact form submissions were stored on the web site. This meant that thousands of data files containing the most sensitive personal data imaginable were on a public web server up to five years after the initial contact. (The data retention period should not have been any longer than a few weeks for the purposes of medical and emotional follow-ups.)

The charity was fined £200,000 on the grounds that their lack of knowledge about how their web site worked did not mitigate the fact that they had been a *victim* of a hacking. It was no exaggeration, ICO rightly said, that women could have been killed as a result of this data breach.

There was simply no excuse.

Passwords and data protection

"Is our event data protected because it has a password? Do poor passwords constitute a data breach? Can password protection help to protect us from a legal perspective?"

Where passwords are concerned, there are two things to take into consideration: the passwords themselves, and the ways they are stored. Poor passwords and strategies can be construed as a failure to meet the DPA data security requirement.

Lists of compromised passwords constantly show that people are using bad passwords like "password" or "123456". Likewise, we have all seen passwords written on sticky notes stuck to monitors. All of these are preventable data breaches waiting to happen. User accounts and passwords should never be shared between multiple users. Passwords should also be difficult to break and impossible to guess. Never use one password for multiple systems.

Password storage is of vital importance to both prevent and mitigate data breaches. For that reason, passwords should never be stored in an easily retrievable way. A password reset option should never send you your password by email. Passwords should never be stored encrypted because encryption can be reversed. If you allow people to log in to your website to register for an event, make sure the site stores their passwords securely.

ICO recommends using a security technique called salted hashing for maximum password security.[1] Ensure that any systems you use for event organisation use this technique, and document this in your organisation's data security policy.

Your password strategies must also be noted in your organisation's data security policy. In the event of a data breach, your password standards will form part of the investigation. In addition to explaining what kind of passwords you use, explain how you ensure passwords are kept safe. Your strategy must also contain a plan of action for the unfortunate event of a data breach: how would you reset all passwords in bulk, how would you inform registrants, and what options would you give them regarding the loss of their data?

The most secure systems support Two Factor Authentication (2FA), where a user account is protected with a second password which changes frequently. In EventReference, these 2FA passwords change every 30 seconds and are generated by a mobile app, meaning an attacker would need to have your username, password, and unlocked access to your smartphone in order to access your account. You should always enable 2FA if it is available as it helps demonstrate that you are taking data safety seriously.

1) https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf.

Data retention and length

"How long should event organisers keep data? What can we keep? How do we determine what's safe to retain?"

Two of the core principles of European data protection law, under both the old and new regimes, are that the data you collect must be *relevant* to the ways you are using it and that it must not be *retained* for longer than is necessary. Event organisers should consider these two standards together.

Because every event's circumstances are different, there is no set rule on the length of data retention. Some data is only relevant for the duration of your event, while other data can be relevant for years. You can, however, devise an acceptable policy by asking these questions about your data:

1. Why do we need this data?
2. What value might it have in future?
3. How much will it cost us to keep this data?
4. What risks are there in keeping it?

Under the GDPR you will need to explain your data retention rationale in your privacy notices and terms and conditions. It is not enough to simply guess what a good data retention policy, or its length, should be. You have to prove that you have created a valid policy through the appropriate evaluation process.

Event organisers wishing to retain data for future use should remove sensitive personal data - information pertaining to health, disability, ethnicity, or religion - from those records. For example, you may retain the contact data for this year's attendees in order to invite them back next year. However, you should not retain data such as requests for a kosher meal, a wheelchair ramp, or a prayer room, as associating these requests with individuals is retaining sensitive personal data.

The retained data must be also be used solely for its original intended purpose. For example, the list of attendees should not be sold to advertisers after the conference if this was not explicitly consented to at the time of registration.

What should you do with data concerning a Code of Conduct violation at an event? Unless litigation ensues, the identifying details of both the victim and the perpetrator should be deleted after a reasonable period of time. For example, it is acceptable for the organisers of an industry conference to maintain a secure list of individuals banned from future conferences for unacceptable behaviour at previous conferences, but it is not acceptable for the details about those incidents, or who they were directed against, to be retained with that list. Following the deletion of personal data, an account of the incident, anonymised to persons X and Y, can be retained securely and indefinitely for the purposes of institutional memory.

Data deletion

"If we ask a company hosting our events data to delete it, how can we be sure they've carried out the request? What if your event's data was breached because of a stolen backup file?"

When the time comes to delete personal data, ask your data processors to confirm in writing that your data has either been deleted or "put beyond use." Deletion must mean that the data genuinely no longer exists. It should not, for example, have been dragged to the trash, remain visible behind a URL, or reside on cloud storage as part of the organisers' archive.

The concept of data being "put beyond use" covers situations where, for example, data on physical media has been deleted and overwritten with new data, or paper files are in a secure warehouse awaiting shredding. "Put beyond use" means no one outside the data controller has access to the data, and no one, including the data controller, is actually processing it.

If a data processor failed to delete your data as promised, having written evidence that you believed in good faith that your data had been deleted or "put beyond use" would afford you some protection.[1]

HMRC's internal data protection manual, at the time of the 2007 data breach, was restricted to civil servants; the junior staff who, as in any organisation, did the actual grunt work had only been given slogans about respecting confidentiality. The lesson here is to ensure that all of your events staff, including zero-hours contractors and volunteers, have training on data protection procedures and are given access to vetted guidelines.

Data theft from backups is always the result of preventable human error. In 2007 HMRC famously lost two CD-ROMs containing the backup data of all UK families claiming child benefit. The records contained information on an estimated twenty five million individuals - nearly half of the UK's population. The CDs were sent through HMRC's internal courier service without proper encryption and using only easily broken password protection. While the CDs were never located and the data apparently never compromised, the damage was done. Every family in the UK had to be put on fraud alert.

1) https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

What is changing in 2018?

In Spring 2016 the European Parliament approved the final text of the General Data Protection Regulation (GDPR), the successor law to the Data Protection Directive. It will take effect across Europe on 25 March 2018, after it has been transposed into all European member states' national legislation.

The GDPR will update and modernise the principles of the 1995 law to reflect today's practical data protection issues.

Compliance with the current DPA is a starting point for compliance with the new regulation, but it is not compliance itself. Events industry professionals should start thinking about new obligations right away.

ICO, other European data protection agencies, and industry bodies will be working together to support businesses in the lead-up to implementation, but you must take the initiative to begin learning about your new obligations as soon as possible.

RefTech recognises that now is the time to get to grips with our increased data protection compliance obligations under the GDPR. While we are already fully compliant with the existing Data Protection Directive, we have already begun reviewing our systems, processes, and service provision to ensure that we will be fully compliant with our GDPR obligations well before the May 2018 deadline. We are also actively monitoring developments in the ongoing Privacy Shield debate to ensure that we remain compliant with changing legal requirements for data transfers between the EU and US.

GDPR in a nutshell

1. You will need to be more accountable for data. You should be prepared to document what personal data you hold, where it came from, and who you share it with.
2. You will have to provide clear, easily understood privacy notices containing certain standardised information.
3. Individuals will have greatly expanded rights over their data which you must be prepared to meet.
4. Subject access requests - the right to ask an organisation to show you all the data it holds about you - are also strengthened.
5. You will need to justify and document your legal basis for processing all personal data.
6. Consent is everything under the new regulation. You will have to seek it, confirm it, and document it.
7. Data about children will require extra safeguards and levels of consent.
8. There are new obligations about detecting, investigating, and reporting data breaches.
9. Privacy and data protection by design *are the new defaults.* In many cases this will require privacy impact assessments to be carried out.
10. It is likely that you will need to designate a data protection officer (DPO) for your business - a named individual holding professional accountability for your data protection compliance.
11. You will need to identify which national data protection authority governs your work. This is a response to evidence that companies working internationally have engaged in "jurisdiction shopping" to choose the lightest-touch data regulatory environment.
12. Finally, you need to be aware of GDPR's teeth. Penalties for data breaches can be as high as €20M or 4% of an organisation's annual global turnover – whichever is higher.

RefTech is an acknowledged technological leader in the areas of Badging and Registration systems for exhibitions, conferences and events where we have expertise in:

- Online, paper and on-site registration services
- Automated appointment setting
- Pre-event badge production and despatch
- On-site badge production including payment processing
- Lead retrieval systems for exhibitors
- Attendance reporting

EventReference

EventReference, the simple, easy and effective online registration system

- Event Registration
- Event Management
- Event Reporting
- Paid Registration
- WebBadging
- WebScanning

Reference Technology Ltd
1-3 The Pavilions, Amber Close,
Tamworth, Staffordshire, B77 4RP

Telephone: +44 (0)1827 61666
Email: enquiries@reftech.com

www.reftech.com
www.eventreference.com

We are a Living Wage Employer