Get ready for GDPR:

Your events management strategy

EventReference

<ref:tech>

Disclaimer

This 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 guidance and URLs are current as of November 2017 and are subject to change.

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

Contents

A note from the Chief Ideas Officer

Last year RefTech released our white paper, “Data protection in the events industry: what you need to know to stay within the law”, to encourage a culture of best practice within the events industry.

We are continuing to work towards that mission with this new paper, “Get ready for GDPR: Your events management strategy,” which has been written specifically with next year’s compliance deadline in mind.

The 25th of May 2018 is approaching fast and now is the time to get serious about the General Data Protection Regulation. It will bring a raft of new obligations regarding privacy and the protection of user data. The level of difficulty of those obligations will bring depends entirely on your perspective towards on the task.

At RefTech, we began our GDPR compliance journey in the spring of 2016, as soon as the finalised text of the Regulation was released. While we have always placed the highest priority on compliance with existing data protection law, we immediately began reviewing our systems, processes, and service provision to meet our new obligations well before the May 2018 deadline.

This guide shares what we learned on the way.

As with last year’s guide, this paper is not an expert guide to data protection law, nor is it legal advice. You will not emerge from this as an expert in data protection.

You will, however, be empowered and equipped to kickstart your compliance process, to know what can be comfortably handled internally, and to recognise what steps may need outside assistance.

Our objective is to inspire your own questions above and beyond the prompts we have offered here. If you don’t have any questions, we’d be delighted to chat with you about how to develop a healthy view of data protection and privacy practice within your events industry business. Simply email us on datasafety@eventreference.com. We’ll do our best to start you on your journey and I promise that it won’t cost you anything.

Simon Clayton
Chief Ideas Officer
RefTech and EventReference

GDPR is a culture shift

So we know what you're thinking: "Oh no, another GDPR white paper!"

After all, you have no doubt have been bombarded by offers for GDPR "compliance solutions," applications, and software platforms which promise to make you fully compliant overnight – some of which are little more than advertorials.

What's more, those who want to sell you these products and services are doing so with dire warnings about the catastrophic penalties and fines that await you if you don't part with your money right away. Others scream that GDPR will stifle innovation, kill businesses, and destroy livelihoods.

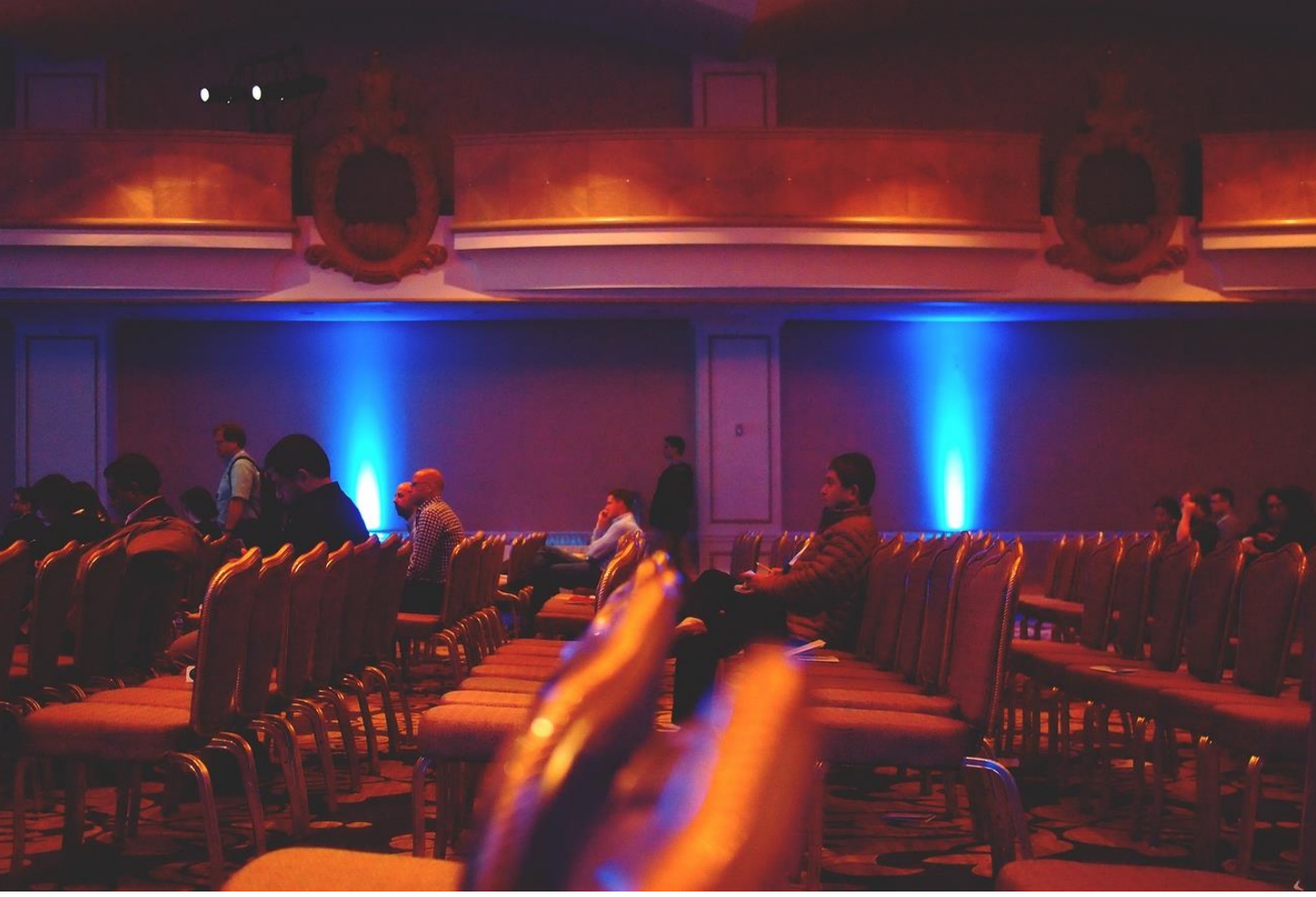
That is absolutely not what GDPR is about, that is not what data protection means, and that is certainly not the focus of this paper.

Our aim today is to encourage you to view GDPR compliance *as a culture shift*. We want you to get on board with GDPR as your once-in-a-generation opportunity to improve your events, streamline your in-house processes, and even renew your business models.

> *We want you to get on board with GDPR as your once-in-a-generation opportunity*

Healthy GDPR compliance is not about avoiding fines, it is not about ticking legal boxes, and it is absolutely not about leaving these processes to an automated "solution". Nor is it about approaching the task from a perspective of fear and dread: comply or die. GDPR compliance is about *doing the right thing*.

As events industry professionals, we cannot pretend that the users of our services are not affected by the changing world around us. Organisers are moving conference locations, or even threatening to cancel events altogether, when politicians openly threaten the safety of attendees based on race, religion, sexual orientation, or even their country of birth. Attendees are leaving their laptops and smartphones at home rather than risk of having their customers' data downloaded into a database at border control. And many event attendees, sadly, are skipping events altogether rather than travel to countries which demonstrate hostile behaviour towards people like them.



"Internet Engineering Task Force moves meeting from USA to Canada to dodge Trump travel ban - 15 per cent of potential attendees don't fancy trying to make it to San Francisco"

-The Register, 16 July 2017

This is why meaningful GDPR compliance is so important. By *reducing* the data that we collect, *protecting* the information that we have, and *responsibly stewarding* the data that we share, we can play a small but important role in safeguarding our users and their data.

That, in turn, can help us all to keep our industry a safe place to do business. It can also help to position you as safe people to do business with.

We hope that this paper will encourage you to view GDPR compliance as a cultural shift to a proactive, protective, and permanent norm of "privacy first".

Who and what does GDPR affect?

Many people are surprised to learn that GDPR is already in force. It *becomes enforceable* on 25 May 2018. This lead-in time has been granted to give you plenty of time to get to grips with the new and upgraded requirements.

GDPR replaces the existing data protection regime, 1995's Data Protection Directive. In the UK we know it as the Data Protection Act of 1998.

GDPR, and the EU's principles of data protection and privacy in general, pertain to *personal data*. Personal data, for our purposes, means information about a living individual who could be identified from that data, either on its own or when combined with other information. GDPR officially defines personal data as "any information relating to an identified or identifiable natural person."

The 1995 data protection principles established that personal data must be

1. Processed in a manner which is fair and lawful;
2. Used only for the manner in which it was intended to be used;
3. Processed in a manner which is adequate, relevant, and not excessive;
4. Accurate and kept up to date;
5. Not kept for longer than its intended purpose;
6. Processed in accordance with the rights of the people the data is about;
7. Protected by technical and organisational security measures;
8. Not transferred to third countries outside the EU which do not guarantee an adequate measure of data protection.

Sensitive Personal Data

Beyond personal data there is also *sensitive personal data*, which is defined as any information concerning an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life or sexual orientation
- Past or spent criminal convictions

Sensitive personal data requires stricter curation, and the loss or breaches of such data rightfully carries stricter punishments.

GDPR expands the definition of personal data from the 1995 standard to include an individual's:

- Genetic data
- Biometric data
- Location data
- Online identifiers

What if your events business is not in Europe?

European data protection law is universal and extraterritorial. It applies to all personal data about individuals collected or processed in Europe regardless of those individuals' nationality or citizenship. It also applies across all sectors, industries, and situations.

If you do business with people located in Europe, GDPR applies to you. This means that you must apply GDPR rules to the personal and sensitive personal data you collect and process about Europeans even if your business is not based in Europe and/or has no physical or incorporated presence there.

In the event of a privacy concern or data breach, claiming that EU data protection law does not apply to you, or that you cannot have been expected to be aware of the requirements, will be seen as exactly what it is by Europe's strict data protection regulators.

Awareness and compliance is the price of doing business in Europe.

But what about Brexit?

There are many misconceptions and inaccuracies about GDPR, but one of them is particularly dangerous. It is the belief that GDPR will no longer apply in the United Kingdom after we have left the European Union.

In fact, several polls have suggested that many UK businesses have ceased preparations for GDPR on the belief that Brexit means they are off the hook.

Not only is this an *incorrect* assumption to make - it is a potentially catastrophic one.

The UK government has confirmed that the UK will adopt GDPR and go into it regardless of Brexit.

In September 2017 Parliament introduced the Data Protection Bill, a piece of legislation which is intended to act as the bridge between GDPR and any post-EU data protection framework. Everything GDPR requires will be included within the Bill.

This will ensure that GDPR will remain the standard of data protection law for at least a few years after the UK leaves the European Union.

It is that 2018 standard, not the 1998 Data Protection Act, which you should be working to achieve.

> *"It is imperative that any post-EU UK data protection regime remain fully equivalent to European data protection standards*

As for the Data Protection Bill itself, it is imperative that any post-EU UK data protection regime remain fully equivalent to European data protection standards. Without equivalence, the most basic data flows will become contentious, cumbersome, and expensive. Events industry professionals should be prepared to make our industry's needs clear to government in the years to come.

Developing your strategy

GDPR compliance, as with all data protection and privacy initiatives, is a journey and a process. To that end, our journey began with broad, open-ended questions.

This section contains the questions that *we asked ourselves* about what we needed to do to get ready.

We are happy to share these questions with you and, even if you are not responsible for your organisation's compliance, these questions will help you understand what your organisation needs to do.

We hope that these questions form a bridge from the in-depth information offered by the ICO to the everyday practicalities of implementation in your workplaces and at your events.

Awareness

The most basic step involved in GDPR compliance is awareness. You can encourage a culture of healthy data protection by making everyone in your organisation aware of the ways the law is changing and how these changes will impact your work.

Questions you need to ask

❑ Do you understand what GDPR continues from the old Data Protection Act, and what is new?
❑ Are you confident that you are compliant with the existing Data Protection Act?
❑ Have you devised a GDPR awareness and implementation plan for all employees, ranging from senior management to zero-hours events staff?
❑ Are you providing your Board with regular updates about your GDPR implementation progress?
❑ Have you allocated appropriate human and technical resources to GDPR implementation both before and after May 2018?
❑ Have you spoken with your contractors and suppliers about their own GDPR implementation plans?
❑ Have you used the ICO's self-assessment toolkit to assess where you are?
❑ Can you distinguish good, accurate, and helpful GDPR advice from the marketing hype, scaremongering, and snake oil?

Questions you should ask

❑ Have you reviewed your organisation's risk register?
❑ Have you refreshed your new employee induction information to include their new obligations under GDPR?
❑ Have you set up a training session for all staff on GDPR?
❑ Do you keep an eye on the news and industry periodicals for stories about data protection, privacy, and data breach issues which could have been prevented?
❑ Likewise, are you keeping an eye the UK government's intentions for data protection law after Brexit?
❑ Have you contacted the ICO for a supportive, non-adversarial on-site audit of your existing data protection compliance?
❑ Have you shared this paper with a colleague?

Information you hold

The next step in your data protection journey is assessing what information you hold, where it is stored, what kinds of data it comprises, and whether it is still needed. Events professionals should be mindful of the notion that this data often resides in very different physical places. For example, it might be that data is stored on various servers either in your office or online, there may be copies of that data on some laptops, or it may even be printed and stored in filing cabinets.

If your organisation has more than 250 employees OR your data collection and processing is regular (meaning it is a core part of your business), if it includes sensitive personal data, or if it could threaten people's rights and freedoms, you must keep a full record of all of your data collection and processing activities.

Questions you need to ask

❑ Have you conducted an audit of the information you hold online?
❑ Have you conducted an audit of the information you hold offline?
❑ Have you determined whether you must keep a full record of your data collection and processing activities?
❑ Does your audit contain record of all processing activities?

Questions you should ask

❑ Have you conducted an audit of how information is shared during events?
❑ Have you conducted an audit of how information is retained, re-used, and shared after events?
❑ Have you reviewed the ways that your partners and third party suppliers audit the data you share with them?
❑ Have you read the ICO's code of practice for conducting privacy impact assessments?

Audit questions

- The purposes for which you are collecting and/or processing personal data;
- A description of the categories of individuals you are processing data about;
- A description of the categories of data you are processing;
- A description of the recipients of personal data you transfer out of your organisation;
- A description of non-EU transfers of personal data, including safeguards;
- Any data protection impact assessments you have carried out;
- A description of your data retention procedures;
- A description of what technical security measures you have taken;
- A description of your organisational security measures, including training and HR documentation; and
- A record of the policies you have put in place to deal with a data breach.

Individual Rights

Users have always had rights over how organisations use their information under the existing data protection regime. Under GDPR these rights are greatly expanded. For your events, this means respecting those rights, implementing them into your planning structures, and being prepared to meet users' invocation of these rights in an open and fast way.

Individual rights

- The right to be informed about what you are doing with data through privacy notices;
- The right of users to access a copy of the data you hold on them;
- The right to correct any data that you hold;
- The right to erasure, meaning the right to request that you delete certain kinds of data that you hold;
- The right to restrict processing, or the right to ask you to stop using their data in certain ways;
- The right to data portability, or the right to take the data you hold about them to another service provider;
- The right to object to your uses of their data; and
- Their rights in relation to automated decision making and profiling, where there are legal implications.

Questions you need to ask

❑ Are you aware of the rights that individuals have over their data?

❑ Do you understand how these rights work in practice?

❑ Are you aware that these rights are granular, meaning the user can invoke any one at any time over any aspect of their data?

❑ Are you aware that you cannot charge users an administrative fee for invoking these rights, or any costs for the time you require to meet them?

❑ Are you aware that in certain circumstances, there are legal grounds for rejecting the invocation of these rights?

Questions you should ask

❑ Have you reviewed your current provisions for meeting individual rights?

❑ Have you reviewed how you publicise individual rights in your privacy notices?

❑ Have you determined which data you hold could be subject to these rights?

❑ Have you unbundled individual rights over data used for automated decision making and profiling from the data which is strictly necessary for the provision of your services?

Subject Access Requests

One way that people can invoke their individual rights is known as a subject access request (SAR). The people whose data you store or process can file a SAR with you to receive confirmation that you are processing their data; to gain access to a copy of the personal data that you hold on them; and to gain other information you hold on them, such as details of the data you have passed to third parties.

Questions you need to ask

- ❑ Have you created a SAR process?
- ❑ Is your SAR process detailed in your privacy notices?
- ❑ Is your internal SAR process documented in a way that would meet your data protection regulator's approval?
- ❑ Do you have a central point of contact for handling subject access requests?
- ❑ How are SARs tallied in your organisation? Who is informed of their receipt, their progress, and their completion?
- ❑ Do you have the technical and staffing capability to respond to SARs within one month?
- ❑ Are your systems equipped to generate the data required under an SAR?
- ❑ Does your documentation ensure that no uses of data would be overlooked when responding to an SAR?

Questions you should ask

- ❑ If you anticipate receiving many SARs, have you looked into creating systems which will allow users to access their own data without a formal SAR process?
- ❑ Do you have a process in place that would allow a fair and reasonable charge only for SARs which are excessive or "manifestly unfounded"?
- ❑ Would you be able to document and justify your process for defining an SAR as excessive or "manifestly unfounded"?
- ❑ Do your third party subcontractors and partners have a documented and visible SAR process?

Privacy Notices

Data protection law has always required you to inform your users about the ways you are using their data. Under the previous data protection regime, however, those notices become long, lazy, and legalistic. GDPR reclaims privacy notices as concise, transparent, and intelligible dialogues with your users. Going forward, your notices need to be written in plain English. They need to contain certain kinds of information in a cleanly formatted manner. And everything you are doing with your users' data - everything - needs to come out into the open.

Questions you need to ask

- ❑ Review the privacy notices on your web sites, apps, and online services, as well as any printed literature you display at events, for currency, accuracy, and compliance with the 2018 (not 1995) guidelines;
- ❑ Ensure that your privacy notices are:
  - ❑ Written in plain English, not "legalese";
  - ❑ Broken down into clear sentences and short paragraphs;
  - ❑ Provide a clear description of what data is collected, how long it will be stored, how it is processed, how it is used, and who it is shared with;
- ❑ If not based on consent, explain your lawful basis for processing user data;
- ❑ List all third party partners and services providers with whom you share data, and note what that data is and how it is used;
- ❑ Inform users of their individual rights;
- ❑ Provide clear granular opt-in options for consent, individual rights, and SARs;
- ❑ Provide clear contact details for your company, your point of contact for SARs, and your Data Protection Officer if applicable.

Questions you should ask

- ❑ Check with your data protection regulator to ensure that you are providing all of the information they require, which can differ by country;
- ❑ Check with your data protection regulator to see if they have developed templates with standardised icons for privacy notices, as some countries are doing in the lead-up to 2018;
- ❑ Ensure that you have provided an email address as the point of contact for privacy queries, and not only a postal address;
- ❑ Ask a friend to read your privacy notices. Do they make sense to someone "on the outside"?
- ❑ Read your own privacy notices as if you were a sceptical potential client. Would you do business with your own company?
- ❑ Separate your privacy policies from general terms and conditions, particularly on your web sites and apps.

Consent and Legal Basis

Under GDPR, in most circumstances, your use of data must be grounded in a legal justification. Where there is no legal justification, the data collection and processing you perform must be done with the consent of the people that data is about.

This applies to your in-house processes as well as to the data you collect on the events floor.

Whether your data processing takes the shape of a site visitor filling out a form, a trade exhibition visitor entering a prize draw, or a new client hiring you to provide a service, the consent and legal basis you use to perform those tasks must be clear, documented, and verifiable (see next page).

Questions you need to ask

❑ Have you determined which aspects of your data collection and processing are grounded in consent, and which aspects are grounded in a legal basis?

❑ Have you ensured that your consent processes are valid? (See next page)

❑ If not grounded in active consent, can you document and prove that your collection and processing of data is grounded in a legal basis? (See next page)

❑ Are you able to document proof of consent or legal basis for the data you collect and process? (See next page)

❑ Are you aware that if the data subject is under the age of consent then you will need parental consent to store their data?

❑ Have you applied these processes to the ways you collect and process data before, during, and after events?

Questions you should ask

❑ Have you reviewed your existing consent mechanisms and records to ensure that your consent processes meet the above criteria?

❑ If any aspect of the new criteria is missing, are you prepared to alter your consent mechanisms to refresh and secure GDPR-level consent?

❑ If you are not able to re-establish consent under the GDPR requirements, does your data processing have a legal basis?

❑ Are you prepared to cease data processing and delete records for cases where you cannot secure consent and have no legal basis?

The Rules for Consent

Consent must be:

- ❑ **Active**: consent is freely given, specific, and unambiguous;
- ❑ Active consent is also **positive**, meaning you have not presumed consent from a pre-ticked box, inactivity, or not selecting any option;
- ❑ Privacy must be presented as **granular** multiple choices, and not a single in-or-out option for multiple elements. For example, if you have determined that you need consent for the data you are collecting, then it cannot be automatic opt-in during a registration process;
- ❑ **Unbundled**: users cannot be forced to grant consent for one thing in order to receive another;
- ❑ **Named**: the user must be made aware of all specific third parties who will be receiving their data and why they will be receiving it;
- ❑ **No imbalance in the relationship**: consent must not create an unfair relationship between the user and the data processor, such as requiring excessive data collection in an employer-employee relationship;
- ❑ **Verifiable and documented**: you must be able to prove who gave their consent, how consent was given, what information they were given, what they agreed to, when they consented, and whether or not the user has withdrawn their consent.

If not grounded in *consent*, your data processing must be done within a *legal basis.* This means that your collection and processing of the data is:

- ❑ Necessary for the performance of a contract or in order to take steps at the request of the data subject prior to entering into a contract;
- ❑ Necessary to comply with a legal obligation;
- ❑ Necessary to protect the person's vital interests (for example, providing someone with emergency medical help);
- ❑ Necessary for the performance of a task in the public interest or in the exercise of official authority;
- ❑ Necessary for the purposes of the "legitimate interests" pursued by the controller or third party.

Whether grounded in consent or legal basis, you must be able to document proof. That proof must indicate

- ❑ Who gave their consent;
- ❑ How consent was given;
- ❑ What information they were given, and what they agreed to;
- ❑ When they consented (ideally a timestamped record); and
- ❑ Whether or not the user has withdrawn their consent.

Childrens' data

If your events collect data from or about children, there are new requirements under GDPR that you will need to pay extra attention to in your processes.

Whether you're creating an app for kids to use or running a trade show for expectant mothers, no one wants to be accused of misusing information about children.

Questions you need to ask

❑ Are you aware whether you collect information about or from underage individuals at your events?
❑ If so, have you documented the processes you use to protect this information?
❑ Have you documented your additional data minimisation, storage, and deletion processes for underage individuals' data?
❑ Do children provide their information directly? If so, have you written a privacy notice for children in language they can understand?
❑ Are you documenting evidence that you have parental consent for any data processing for underage individuals?

Questions you should ask

❑ Do you protect documentary evidence submitted through any age verification processes in full accordance with data protection principles?
❑ How do you verify parental responsibility when being asked to delete childrens' data records by a parent or guardian?
❑ How do you re-establish consent once the child reaches the age of consent and the parental consent is no longer valid?
❑ Do you delete data that a child generated if that child is now an adult and requests that you do so?

Data Protection by Design and Default

GDPR requires the adoption of a culture of data protection by design and default. This means that all your processes, services, and applications must be designed with optimal privacy and data protection built in from the start, not bolted on as an afterthought or made contingent on the user activating a series of options (assuming they had any at all.)

Your obligations here are both internal and external. Internal obligations include conducting data protection impact assessments (DPIAs), ensuring technical safeguards, and making staff aware of their legal obligations. External obligations include publishing privacy notices, engaging in data minimisation and deletion, and providing users with granular privacy options.

Questions you need to ask

❑ Have you familiarised yourself with the basic principles of data protection by design and default?
❑ Have you reviewed your existing sites, apps, and processes to verify data protection by design and default?
❑ Have you run a DPIA on your data-intensive projects in development?
❑ Have you developed a DPIA template unique to your events business's needs?
❑ Have you reviewed your current points of data input for ways that data could be minimised? These could include "required" form fields, outdated marketing information, and customer records.
❑ Have you developed a data retention and deletion policy for the different kinds of information you hold?

Questions you should ask

❑ Have you reviewed the ICO's useful guidance on DPIAs?
❑ Have you run retrospective DPIAs on existing projects?
❑ Have you reviewed the DPIAs of your partners and third party service providers?
❑ Have you reviewed your process for verifying that data has been deleted?
❑ Are you confident that you could share your data protection by design and default processes with the general public?
❑ Are you confident that your documented data protection by design and default processes would pass muster with a regulator?

Data Breaches

GDPR defines a data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data." Note those distinctions quite carefully, because they matter: data breaches can be *internal* and they can involve data being changed, not necessarily lost.

GDPR requires you to do everything you can to prevent data breaches from happening. That said, it also requires you to prepare for data breaches in advance. This process should include discerning what sort of breaches, depending on the nature of your events process, will be reportable to your data protection authority. It also includes developing a process to document the evidence behind a data breach, and to also document the technical and security measures that were in place to prevent it.

Another important definition to note is that of a high risk data breach: this is a loss of personal data which could threaten "rights and freedoms," or what we might call life and limb. High risk breaches must be reported to both the data protection regulator and the data subjects within 72 hours of discovery.

Questions you need to ask

- ❑ Have you conducted a postmortem of data breaches you may have experienced in the past?
- ❑ Do you regularly audit your systems and processes for potential data breach issues?
- ❑ Do you know the criteria for a "high-risk", reportable breach?
- ❑ Have you created a template for GDPR's data breach reporting requirements?
- ❑ Does this template reflect your new processes to document and report:
  - ❑ Details about the nature of a breach, such as what category of data was breached, how many individuals were affected, and how many data records were involved;
  - ❑ Information on how you were alerted to a breach, and by whom;
  - ❑ Any available information on who is responsible for a breach, or how it happened;
  - ❑ What consequences are happening as a result of a breach;
  - ❑ What measures you are taking to deal with a breach, such as contacting customers or resetting all passwords;
  - ❑ What measures you are taking to deal with the consequences, such as unauthorised charges to customers' accounts;
  - ❑ The name and contact details of your DPO or the individual taking the lead on data breaches.

Questions you should ask

- ❑ Do you have an internal reporting mechanism in place to report potential data breaches before they happen?
- ❑ Can staff report an issue, either technical or human, which could lead to a data breach, without fear of reprisal?
- ❑ Is your data breach procedure extensible to the events floor?
- ❑ Have you studied the lessons learnt from past data breaches committed by others, such as the ones we discussed in our white paper on data protection in the events industry? Jot down some observations here.

Data Protection Officers

GDPR introduces the concept of the Data Protection Officer, or the DPO. For organisations engaging in certain kinds of processing of personal data, the DPO is a named individual who carries legal and professional responsibility for that organisation's GDPR compliance.

Events businesses are only required to appoint a DPO if they engage in large-scale data processing. "Large-scale" is a subjective term determined by:

1. The number of data subjects;
2. The volume of data and/or the range of data processing;
3. The length or duration of the data processing;
4. The geographical reach of the data processing.

That being said, those businesses which do not strictly *require* a DPO may wish to consider appointing one voluntarily all the same.

What better way to ensure that good data protection practice remains an everyday part of your work?

Questions you need to ask

- ❑ Have you determined whether you need a DPO by law?
- ❑ If not required, have you considered appointing a DPO voluntarily?
- ❑ Are you prepared for your DPO to:
  - ❑ Be informed of all data protection issues in a transparent and timely matter;
  - ❑ Be made available to any user who has a concern over your use of their data;
  - ❑ Maintain secrecy and confidentiality at all times;
  - ❑ Be provided with all the resources necessary to do the job;
  - ❑ Report directly to, and be in contact with, your highest level of management;
  - ❑ Not be given any instruction (that is, coercion) on how to do their job;
  - ❑ Not be punished or fired for doing their job;
  - ❑ Not be given other tasks or responsibilities which could cause a conflict of interest with their obligations as a DPO.
- ❑ Have you publicised your DPO's details in your privacy notices?
- ❑ Have you submitted your DPO's details to your data protection regulator?

Questions you should ask

- ❑ Are you aware that a DPO does not require any specific, formal, or legal qualifications?
- ❑ Are you aware that a DPO should, nevertheless, have a track record of hands-on data protection and privacy experience?
- ❑ If your potential DPO is claiming a qualification or accreditation, have you verified its authenticity?
- ❑ Are you aware that a DPO can be contracted-in, part-time, or an existing member of staff?
- ❑ While your DPO can be part-time or contracted in, have you chosen a DPO who is located within easy physical access of your premises?
- ❑ Have you drawn up a list of what qualities would be desirable for a DPO within the specific needs of your events business?
- ❑ Are you prepared to give your DPO a regular spot on your Board's agenda, if applicable?
- ❑ Is there anyone within your organisation essentially doing the job already?

Working Internationally

One of the fundamental principles of EU data protection law, both past and future, is that personal data cannot be transferred outside of the EU to third countries unless that country ensures an equal and adequate level of data protection. This creates two issues: the safeguarding of your data at its origin and its destination, and the legal means by which that data moves between them.

To safeguard data, you must ensure that your non-EU partners and service providers have implemented a data protection system equal and adequate to GDPR for the European data you are sending them. To create a legal basis, you must ensure that your data is being transferred either under a framework agreement or through specific alternatives.

Questions you need to ask

- ❑ Are all of your partners and third party service providers in non-EU countries familiar with the new requirements under GDPR?
- ❑ Are they already in compliance or is remedial work required?
- ❑ Are your US-based partners and third party service providers Privacy Shield compliant?
- ❑ Are you including and requiring GDPR compliance in your contracts with partners and service providers?
- ❑ Are all international transfers of data, and the uses of that data, made clear in your public-facing privacy notices?
- ❑ If you work across European borders, have you identified your main country of establishment and lead supervisory authority in your privacy notices?

Questions you should ask

- ❑ If Privacy Shield is not an option for your US partners and service providers, have you looked into other means of legal data transfers under GDPR, including
  - ❑ Binding corporate rules;
  - ❑ Data protection clauses in your contracts;
  - ❑ Data protection clauses adopted by a supervisory authority, such as an industry regulator;
  - ❑ Compliance with an approved code of conduct approved by a supervisory authority, such as an industry regulator;
  - ❑ Certification under an approved transfer mechanism.
- ❑ Are you monitoring the often contentious developments on Privacy Shield, including possible threats to its integrity caused by the Trump administration as well as UK domestic surveillance law?

For more information

United Kingdom

In the lead up to 25 May 2018 the Information Commissioner's Office is publishing helpful, plain-English guidance on many aspects of GDPR compliance. Bookmark their page at https://ico.org.uk/for-organisations/data-protection-reform/ and visit it often.

The ICO also offers free, constructive, non-adversarial advisory visits. ICO staff will visit your office, speak with you and your staff, and identify areas for improvement. You can request a visit at https://ico.org.uk/for-organisations/resources-and-support/advisory-visits/.

Europe

The European Commission has published a plain English introduction to GDPR at http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm

Because European member states are permitted to legislate additional data protection requirements over and above GDPR's baseline, it is important that you check with your national data protection regulator for information on your country's GDPR compliance requirements. A list of regulators is available here: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

Outside the EU

We recommend using ICO's English language guidance for basic compliance information.

For information on specific data protection agreements your countries may have with the European Union, and for a list of regulators and agencies which work with the EU on data protection matters, visit this page: http://ec.europa.eu/justice/data-protection/bodies/authorities/third-countries/index_en.htm

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, the simple, easy and secure 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

http://www.reftech.com

http://www.eventreference.com