

GDPR

General Data Protection Regulation



MEETINGS & EVENTS

What your event tech provider
can do for you.



etouches

soors.it

Table of contents



This guide is by no means a legal document. It is a vulgarization guide with the editor's interpretation of the law. Please read disclaimer carefully.

Why another guide on GDPR?

The new General Data Protection Regulation (GDPR) law will take effect May 25, 2018, which is quickly approaching. Event teams have already started to work on events for next year, thus compliancy starts today. We've spent hundreds of hours to fully understand the implication of the new law and what it means for our industry. While there is tons of documentation out there, we found them very difficult to understand from one standpoint in particular: what is the vendor responsibility versus the client responsibility in the context of meetings and events? Many event professionals are asking themselves the same question in regard to GDPR.

While this guide focuses primarily on meetings and events, it will also discuss the basic requirements needed for GDPR and examples throughout our industry.

We did the research for you, so that you can set yourself up for success when the regulation is enforced in May 2018.

1	Introduction	2	2	What are the key principles of GDPR	6
	Important definitions to start	3		Who is the DPO	8
	Meetings and events, a first statement:	4		Penalties that can hurt	9
	Was GDPR created to annoy event organizers (and everyone else)?	5		Event data in a global world	10
				What about Brexit?	10
3	How does GDPR affect your event technology vendor?	11	4	GDPR also requires getting your participant's consent	17
	Why it matters	12		Additional notes on consent	18
	GDPR reinforces the risk of managing multiple point solutions	13		Other key aspects of GDPR	20
	GDPR, it's all about data. But what is event data?	14		Road to compliance	22
	What is the event planner's responsibility?	15		Meetings and events use cases – Q&A	24
	GDPR, let's kill some rumors	16			
5	etouches' commitment to client GDPR compliance	26			
	External resources about GDPR	27			
	Our view on GDPR for organizations running meetings and events	28			

Introduction

Planners, this is not boring!

The goal of this eBook is to provide you with information on how GDPR will impact meetings, events and your organization in an enjoyable and easily digestible manner.

We did tons of research, and collected some of the best material out there to bring you this eBook. All of our material can be found in our research section for future use. Finally, to make it more tangible, we will share some real life situations that may arise with GDPR in meetings and events.

GDPR is not something new, it mostly consists of strengthening the existing laws and increasing penalties for offenders. That's why it is key that planners and event stakeholders understand their roles and how the new regulation will work.



AS OF JUNE 2017

61%

of companies
have not
started GDPR
implementation

Source TrustArc-IAPP

Disclaimer

This document is intended to convey general information only, and should only be used as a starting point in your understanding of issues relating to GDPR. This is not intended as legal advice, nor is it meant to convey legal facts or opinions. The contents of this document should not be relied upon in any particular situation, and the information presented here is not guaranteed to be correct, complete or up-to-date. No action should be taken in reliance on the information found here, and etouches disclaims all liability with respect to any acts or omissions based on the contents of this document. You should consult a licensed attorney or regulatory expert to discuss your specific legal, compliance and GDPR-related issues.

Important definitions to start:



The Data Processor +

This is etouches, or any other vendor in your software ecosystem (CRM, marketing automation, accounting, etc.). While both parties must align on compliance, the burden of compliance rests with the controller. To manage this burden, the data controller is responsible for building procedures with their data processor to ensure compliance. The role of the processor is to assist the controller in this regard, as a controller will often have a GDPR compliance process that involves multiple processors across its ecosystem.



The Data Controller

This is you! Whether you are a corporation, an association, etc., you own the data and the responsibility of your customers' data, regardless of the technology you use to handle it (CRM, event software, survey tools, etc.). This software and their vendors are the data processors.

= A Simple Rule

The data controller is the one that needs to ensure its GDPR compliance by defining its requirement to the data processor.

A good data processor is one that has documented policies and state of the art practices on data management, privacy and security, and proactively offers tools like data purge and data queries to the controller.

On a side note, etouches, as a corporation is also a controller, working with an ecosystem of processors (all the software that we use) and we must be GDPR compliant too. So we feel the pain and have taken the steps as a processor to help you comply!

Meetings and events,* a first statement:

**This includes tradeshows, conferences, roadshows, networking meetings, training events, association meetings, and more.*

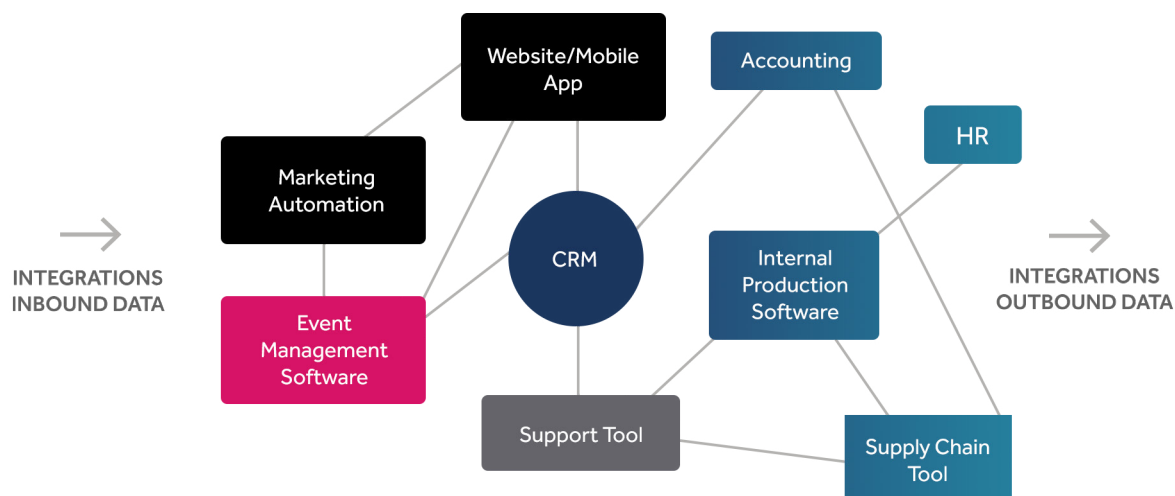
If there's one business that is about exchanging contact info, most would agree our industry ranks pretty high. But the GDPR dimension goes beyond our industry. For some corporations, events are just one component of a larger chain. This chain involves complex workflows where the data originates from an ecosystem that is transformed and pushed into another cycle. One example occurs when data moves from a marketing automation tool, like Hubspot or Marketo, to an event management software solution like etouches, and then onward to your CRM, like Salesforce.

This means that the data doesn't live in silos and can be quite pervasive in the ecosystem. The impact of GDPR does not affect just one software solution, but your company's entire ecosystem and workflow.

An example of a company's data and software ecosystem:

This is the reason why planners need to understand the broader impact of the information they collect before, during and after events; they need to inform the EU participant (consent) on how the data will be utilized.

GO TO MARKET > SALES AND SUPPORT > PRODUCTION OF SERVICE > MANAGEMENT OF SERVICE



Finally, it is key that the planner (on the controller side) engages with the Data Protection Officer, IT and legal departments to map out all the tools within the event ecosystem, and correlate the policies with each event tech vendor (the processors) to ensure full alignment and acquire and maintain compliancy.

Was GDPR created to annoy event organizers (and everyone else)?

It is fair to say that we are living in a connected world. Like any fast growing science or technology that impacts humans holistically, hyper-connectedness can lead to excesses, and regulations such as GDPR are an attempt to control the excess. Just as road signs and speed limits were introduced to reduce car accidents, this is not a preventive law, rather a reactive law. That's why you shouldn't need to implement a whole new process here; rather, make sure existing procedures are enforced!

By design, GDPR focuses on ONE thing: giving any EU citizen the right to access and control the private information that anyone may hold on them, obviously with some restrictions. For example, while Mr. Smith may demand that his personal demographic information is erased, he cannot ask for his financial transactions to be deleted. That is why a company needs to understand:

- What information can be viewed
- What information can be altered
- What information can be deleted
- How to host/maintain/archive information

GDPR should really be called the "Data Transparency Act"

The law is always subject to interpretation, and companies that may be negatively impacted by GDPR will find a way to bypass it. The law is never perfect, but the intention is laudable, and the regulator will look at companies performing risky practices and try to make examples out of them.

Depending on the nature of your business, GDPR can impact your organization a lot or almost not at all, but in any case you should not ignore it.

The regulator will often be more accommodating if you have a track record of good processes, but the law is very clear and you must ensure that your policies have been implemented by your tech vendors, and that they have bullet proof security standards. Historically big lawsuits happen around data breaches.



Planners must be ahead of the May 2018 deadline. Event registrations will start way before!

What are the key principles of GDPR:


GDPR is set to go into effect on May 25, 2018, and this represents a landmark change for EU data privacy regulations. It replaces and improves upon existing regulations – namely, the EU Data Protection Directive of 1995 (Directive 95/46/EC) – by giving individuals more insight into, and control over, how their personal information is collected and used. In particular, GDPR addresses developments in mobile internet technology and cloud computing that have transpired in the years since the directive was implemented. GDPR also transforms what was a patchwork system of differing regulations across the EU into one cohesive, harmonized and simplified set of rules that applies across-the-board to all EU nations. Lastly, GDPR adds “teeth” to existing data protection regulations, by implementing significant fines and penalties for non-compliant data controllers and processors, thereby raising the stakes for any business that collects, stores, or processes the personal data of its customers.

The law is a multilayer framework to ensure a company has developed the tools and the processes to comply with the following principles:




SECURITY

Data security becomes paramount and has to be built into products and processes. It must demonstrate that all the tech systems that help you gather and manage data on your event attendees are secured according to industry standards. Any security breach must be reported within 72 hours.



CONSENT

Event organizers are required to obtain their attendees' consent to store and use their data, and explain how it will be used. Consent must be an active and traceable action by the individual, rather than passive acceptance through pre-ticked boxes or opt-outs.



PORTABILITY

The new regulation states that individuals will have the right to transmit their data from one data controller to another. You should always be ready to provide attendee data in a commonly used digital format.




PRIVACY

EU citizens at any time will be able to ask you to not only delete their personal data (except legal archive obligations, payments, etc.), but to also stop sharing it with third parties – who will also be obliged to stop processing it. Make sure processes are implemented to track data.



ACCESS

You need to provide EU citizens, within 30 days and for free, access to their data in a common digital format. You also need to provide how you are using or planning to use this information.



DATA PROTECTION OFFICER

You must appoint a Data Protection Officer if your business carries out large scale systematic monitoring of individuals (for example, online behavior tracking). You can also contract out the role of DPO externally.

soors.it

SOURCE THE RIGHT TECHNOLOGY FOR YOUR BUSINESS



Today, soors.it offers a range of senior consultants, with a particular focus on CRM, marketing automation, event software and social media automation.

soors.it

Soors.it is a new platform allowing companies of all sizes to source their technologies.

Stay tuned for our platform launch

info@soors.it

Who is the DPO?

The DPO is the Data Protection Officer. While it is unlikely going to be you, the event planner, you must identify who will be your organisation's DPO. Below, we detailed the context and role of a DPO. Get to know them!

WHO

- You may appoint a single Data Protection Officer (DPO) to act for a group of organizations.
- The DPO can be an existing employee (with no conflict of interest) or an external contractor.
- GDPR doesn't specify the credentials a DPO needs to have, but generally they will have a technical background (security, data management, etc.).

ROLE

- To inform the organization and its employees about their obligations to comply with GDPR.
- To monitor compliance, including managing internal data protection activities, security, and risk assessment.
- To document and review all GDPR related policies and data workflows with legal and IT.
- To be the point of contact for supervisory authorities and for individuals whose data is processed (employees, customers, etc.).

CONTEXT

- The organization must provide adequate resources and bandwidth to the DPO for him to meet GDPR requirements.
- The DPO reports to the highest management level of your company/association.
- The DPO remains an independent party and cannot be penalized for performing their task.

RISK MGT.

- The DPO reduces the risk of non-compliance. Evidence of roadmap input from DPO will limit the risk of getting fined.
- The DPO role must be documented and their activity logged in case of a dispute; it will reduce the risk of getting fined.

OBLIGATIONS

Any organization is able to appoint a DPO. Regardless of whether GDPR obliges you to appoint a DPO, you must ensure that your organization has sufficient staff and skills to discharge your obligations under GDPR.

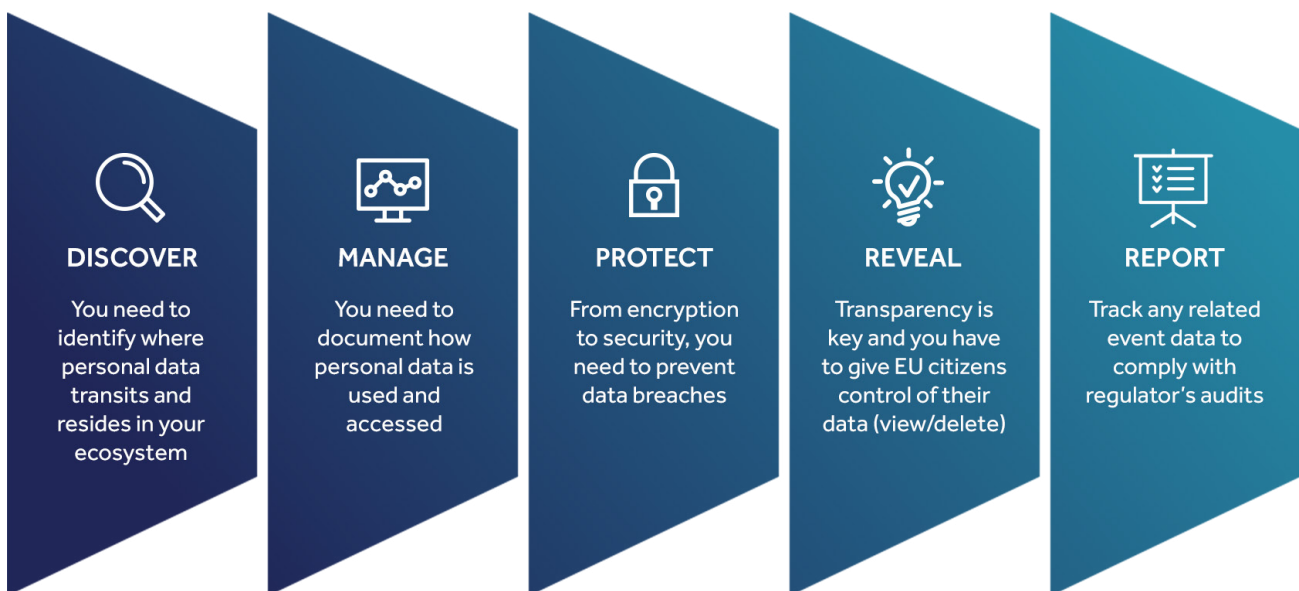
Penalties that can hurt:

This says a lot about how serious the EU is about GDPR: companies dealing with data need to be aware that there are going to be huge penalties if they aren't GDPR compliant when it's enforced in May 2018.

“The fines would be of up to 20 million Euro or 4% of annual global turnover, whichever is greater.”

The EU is definitely a complex engine with several governance layers. It is interesting to note that GDPR is not a directive (EU commission) but an enforceable law voted on by the EU Parliament.

Make no mistake, they will make examples of companies. You don't want to be one of them, so pay attention to avoid fines!



How do you avoid penalties?

Along with the key principles of GDPR, you need to understand the philosophy of the law. While it can be very difficult to comply, you must build your policies and process around a good rationale like the amount of technology, the volume of data collection, the size of your organization, etc.

Common sense and best business practices will help prevent you from being fined.

It is also important that you seek advice from technical and legal consultants. Many organizations have now built a standard checklist and practices to minimize the cost. Ask your peers, benchmark the market!

Event data in a global world

What is the difference between GDPR and Privacy Shield/ Safe Harbor?

While the EU has a "Super Administrator" (the EU parliament), each country has its own set of regulators like the CNIL in France, ICO in the UK, and BFDI in Germany. Europe also has its own instance, the EDPS (European Data Protection Supervisor). See the resource page for direct links.

In the late 90s, Europe started to strengthen its centralized policies with the idea that it will reinforce its economical weight in an ever more global world. Make no mistake, economy is the driver not ethics, so that is why many treaties have been dealt among large geo-influencers (USA, Europe, China, etc.).

From a data standpoint, the EU implemented Safe Harbor, which became Privacy Shield. This applied to the transfer of personal data from the EU/ Switzerland to the United States. This has little to do with data privacy and more with data exchange. We live in a world where data means business and competitive intel. Large industry consortiums or sensible verticals were created by each country's ability to access their data. While some data could also be legally owned in region A, it may not be in region B, etc.

Thus, the Privacy Shield was not so much about data privacy but data transfer. While GDPR has a data transfer component its focus is data security, integrity, collection, use and ownership.

What about Brexit?

Our take is that Brexit won't impact GDPR for a couple of reasons. First, the UK will still be in the EU when GDPR takes effect so it will be implemented there. Second, given the benefits and the cost for implementation, it is unlikely that UK regulators will modify the legislation especially if you consider that downgrading is pointless as it will only impact UK residents. British companies (or any company regardless of their location) that have business with EU citizens have to abide by the GDPR regulation to operate.

It is only if you are a company dealing with only non-EU citizens, that you won't have to comply. The question in the future may only be, will British citizens be entitled to the same level of rights for their own data once the UK leaves the EU?

Did you know?

etouches has taken the steps to go beyond compliancy with data privacy by offering customers three different cloud hosting locations to increase speed, data security and compliance with client's enterprise policies. This also helps prevent the transfer of EU citizens' data outside of the EU.

etouches offers three state-of-the-art cloud instances:

Europe
North America
Asia Pacific



Controls regarding data transfers:

As noted above, etouches offers data hosting and storage solutions at server locations within the EU. We have put in place approved contractual and legal safeguards to meet the data transfer requirements of GDPR.

Data transfers of EU personal data to the US are permissible with a Privacy Shield certification your vendor should provide you with.

Data transfers outside of the EU (for example, to customer support centers in foreign locations that for provide 24/7 support) are addressed through use of our etouches Data Processing Addendum containing Standard Contractual Clauses (SCCs). The SCCs were enacted and approved under the EU Data Protection Directive. The SCCs have been deemed effective and may continue to be used post-GDPR implementation.

How does GDPR affect your event technology vendor?

At etouches, we see GDPR as a positive development and an important opportunity to differentiate ourselves from the competition.

With respect to etouches' client services, etouches serves as a "data processor" while its clients are considered "data controllers" under the GDPR regime. Essentially, a controller is the one making decisions about data collection and processing activities; a processor is the one contracted by the controller to carry out the processing. While the burden for personal data protection under the GDPR is mainly with controllers, etouches' clients will be looking to etouches to help ease that burden by providing clients with GDPR-focused tools and solutions.

We want to reassure our clients that we embrace the most up-to-date data protection standards, and take our role seriously as guardians of personal data belonging to clients and those people who attend their events.

Event tech vendor compliance on data transfer

In order to transfer personal data from the European Economic Area to other countries, the processor can use a variety of legal mechanisms to help ensure the integrity and safety of personal data:

- Adhesion to the EU-US Privacy Shield certification program.
- Adoption of Standard Contractual Clauses into its form of Data Processing Addendum. These clauses are approved by the EU regulator, and will permit data transfers under the GDPR regime.

Customers and attendees will now be able to access the personal data stored on or processed through the etouches system. etouches pledges to promptly and efficiently respond to data access requests. etouches aims to provide functionality to facilitate and manage requests from registrants and clients who want access to their personal data.

Here are some of the ways in which your tech vendor must prepare for GDPR data security requirements:

In compliance with GDPR standards, the data processor or technology vendor must appoint a dedicated [Data Protection Officer \(DPO\)](#).

The tech vendor should provide **staff training** in principles of data protection, including subject access and deletion requests, verifying subject consent, detecting and reporting data breaches, and recognition of sensitive personal data.

The tech vendor employs a variety of **encryption** technologies. For example, at etouches all data collection takes place under a secure protocol (HTTPS/TLS), data in transit is encrypted using AES with 128bit Rijandel keys, and primary account numbers (PAN) and cardholder data (CHD) remains encrypted in the same way at rest and in backups. In the unlikely possibility of data breach, the encrypted data will be useless to the thief.

Why it matters

When properly managed, things like technology certifications and processes help alleviate the risk of noncompliance, preventing data breaches, security failures or lack of reactiveness.

As an example, data controllers (our clients) must also have a process for responding to access requests within 30 days, and for validating the identity of the people who request personal data.

Our DPO can assist in the management of these requests, and we can provide our clients with tools to manage data access requests from their event registrants.

Additional policies and data security standards for technology providers to consider under GDPR:

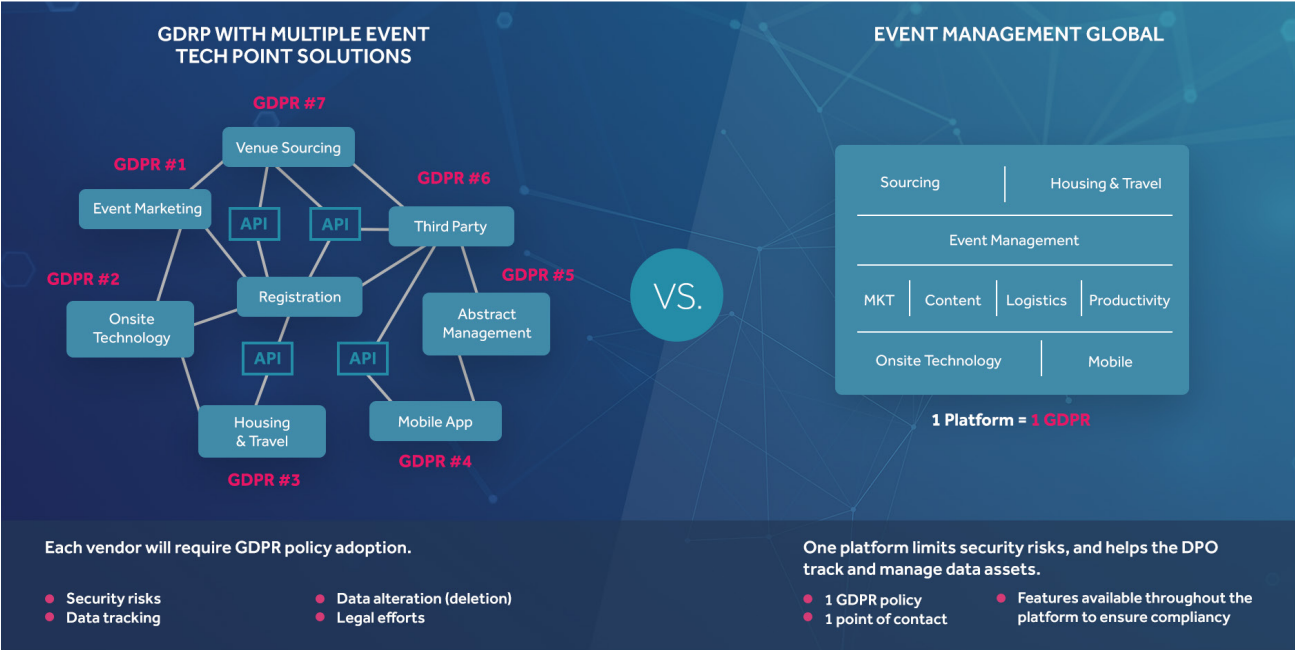
- PCI DSS
- Written privacy and password policies
- Encryption at rest for API and database
- Single-sign on (SAML 2.0 standard)
- Hosting policies
- Penetration test and vulnerability scan reports
- ISO certification
- Incident response plans
- Risk assessment policy

As a client/data controller, make sure your tech vendor has those items above ready and updated. It is a strong sign if the processor is taking the right step to ensure your compliance. Your DPO/legal/IT teams need to have access, make a thorough review and perform a gap analysis versus your GDPR requirements.

GDPR reinforces the risk of managing multiple point solutions

The chart below outlines a new challenge for companies using multiple event technology solutions. Each vendor you contract with is supposed to align with your GDPR requirement. This obviously increases the effort to achieve compliance as not all vendors can provide the same level of security, process, and data control. The data transfer is always considered as the weakest point in terms of data security. Not only can this risk increase as you need to connect multiple point solutions (ex: registration, mobile app, abstract management and onsite check-in) it also makes the individual data tracking tedious with multiple repositories; the data becomes more resilient. If you are asked to delete a record, you need to make sure it is done across the entire ecosystem, including each vendor's archives.




Benefits of event platforms versus point solutions under GDPR







Large platforms offering end-to-end meeting and event technology not only minimize the risks around GDPR compliance, but also significantly reduce the burden of implementing the compliancy.

GDPR, it's all about data. But what is event data?

Events were often considered as an offline mediums. This is no longer true. Meetings and events are now part of the digital marketing workflow. Let's review the data component of the event cycle.

PRE-EVENT		PRE- (+ DURING EVENT)
SALES-MARKETING DATA	INTEGRATION	EVENT DEMOGRAPHIC DATA
 <p>Client Ecosystem Client Data</p>	 <p>REST API</p>	 <p>EMS etouches Back End</p>
<p>Your entire ecosystem is subject to GDPR. As data often transfers from CRM or marketing automation to event software, you need to ensure alignment and continuity. A good question for a planner to ask is: where does participant consent begin and how is it applicable throughout the event lifecycle?</p>	<p>What goes into your event management software, what goes out? Help your DPO understand your event data workflow.</p>	<p>Whether data comes from an integration or not, from registration to session attendance and matchmaking, there is an important number of data assets tied to an individual. The demographic data is, of course, subject to GDPR compliance, starting with participant consent. Your vendor must allow access to their entire dataset.</p>

DURING EVENT			POST- (+DURING) EVENT
EVENT BEHAVIORAL DATA			BUSINESS INTEL
 <p>Mobile App</p>	 <p>IoT</p>	 <p>Onsite Technology</p>	 <p>etouches Data Analytics, Automation</p>
<p>Mobile Apps: As soon as participants log in, you start to capture hundreds of data points, from session voting, messaging, etc.</p> <p>IoT: Smart badge technology, like Loopd, by definition is a multitasking data exchange device with the ability to track session attendance, booth traffic, information exchanges, etc.</p> <p>Badge & Scan: Even a paper printing solution can be subject to GDPR regulations based on your storage policies. It is also important to understand the implications of lead generation and consent if you have sponsors or exhibitors.</p>			<p>Most systems will allow cross event reporting across all data points. Business intelligence analyzes behavior based on patterns, usually not directly linked to an individual, rather profiles. If asked, you have to disclose though if an individual is associated with a specific profile.</p>

What is the event planner's responsibility?

You are not likely to be the only one in charge of GDPR compliance. As we demonstrate, GDPR goes beyond events and meetings. It actually impacts the entire workflow and ecosystem: data collection, data management, data protection, and data storage.

Your role as a planner is to understand your ecosystem and the implication of your events:

GDPR shines a spotlight on personal data – that is, information concerning an individually identifiable person. In the context of an event planner, marketer or technology suppliers' products and services, this spotlight is most likely to fall upon a conference attendee's registration details and other personal information that may be contained in event registration and attendance data.

Data collection plays an increasingly important role in the events industry. The more personal data event managers can collect regarding a person who attends their events, the better they can customize the event experience, as well as future products and services aimed at that individual. Since event professionals collect and store a wide variety of personal data, it is especially critical for etouches and its clients to understand what we can and can't do with that data under the GDPR, and implement the appropriate controls to comply with new regulations, aimed at protecting the personal information of event attendees.

Some of the planner's responsibilities:



Collaborate actively with your GDPR group or DPO
(Data Protection Officer)



Make sure your registration form complies
(opt-in, disclaimers, access links to private policy, etc.)



Understand what participant "consent" means at all stages of the event



Make sure your vendor offers a level of security matching your GDPR requirements



Be cautious with exports and data transfers



Don't manipulate the data in a manner that can impact compliance
(example: mass imports)



Map the functional event areas for your DPO
(travel, PNR, housing, survey, mobile, etc.)

Meeting and event planners often deal with various event technologies and manual processes; thus the planner and their organization become more exposed. Therefore, it is beneficial to work with one global platform, limiting the number of technologies and policy assessments.

GDPR, let's kill some rumors

6 common misconceptions about GDPR

False

While it is enforceable in May 2018, the law has already been put in place. Also, 2018 events may already have opened registration and they still need to comply.

I have up until May 2018 to comply

False

GDPR applies to businesses of all sizes as long as you own EU citizen data.

I am a SME, GDPR is only for large companies

False

Regardless of your headquarters' location, as long as you capture EU citizen data, you need to abide by GDPR.

My business is not located in EU, so GDPR does not apply

We have excellent data security, the regulator will give us a warning without a fine

False

While security is a key aspect, they are many more requirements to meet in order to have a compliant regulator.

False

Most personal records can be deleted, and the law requires you to keep track of certain transactions (payments, invoices, etc.) for audit and tax purposes. However, you need to inform the demander."

I have to delete all information about an EU citizen if asked

I only have internal meetings, GDPR does not apply

False

GDPR applies to all EU citizen private data, including employee information. Internal meetings data against an individual are subject to GDPR compliance.

GDPR is not a completely new law, rather a reinforcement of many existing policies. Like every law, while it is subject to interpretation, there are clear facts that cannot be ignored. Meetings and events are highly exposed to complex data collection and management. While it is not directly the planner's responsibility, it is important to understand (and certainly not ignore) its fundamentals.

GDPR also requires getting your participant's consent

Businesses that collect personal data from EU-based individuals must now get express consent to collect and use that data.

- How we get a data subject's consent is context-specific (depends on the type of data, or type of consent being sought), but it must be "specific, informed and unambiguous" no matter the context.
- Silence does not constitute consent.
- Opting out is not permitted when seeking initial consent. As a matter of best practice, we should always assume that a data subject needs to opt-in rather than opt-out.
- "Unambiguous" means the registrant must opt in. Pre-checked boxes or consent terms buried among other legal terms, are no longer acceptable. Previously, the directive largely allowed data controllers to rely on implicit consent and opt-outs. GDPR requires the data subject to provide "freely given" consent by "a statement or a clear affirmative action."
- Under GDPR, a request for consent must be in "an easily accessible form, using clear and plain language."
- Controllers and processors may also need to provide separate consent language for different types of data.

Disclosures

Under the GDPR, data controllers must make certain disclosures to data subjects before collecting their personal information, including:

- The identity of the controller
- The purpose for processing
- Any recipients of the data
- How long the data will be stored
- If the data is being transferred to another country; where it is going and which transfer safeguard is being relied upon
- The ability to withdraw consent at any time
- The right to request access to data, correction of data or limitation of processing
- The right to lodge a complaint with a supervisory authority

These disclosures need to be written in plain language.

Additional notes on consent

- Separate consent language may need to be provided for different types of data usage and processing – for example, for different formats (e.g., emails vs. texts), and types (e.g., one consent for marketing emails, another for event updates) of communications.
- Additionally, consent may now need to specify who will be receiving or sharing the information. Merely saying that a registrant's information may be shared with "event venues" or "corporate sponsors" will no longer be sufficient. Recipients of personal data must be named with some specificity.

How can etouches help with requirements for consent?

In preparation for May 2018, clients may need to have registrants "re-opt-in" for data collection, and etouches can provide the tools to help them do so. etouches can also develop tools to offer different consents, record the consent statement itself, and evidence that consent was obtained (including when and how the consent was received). Ideally, these tools can be customized to be as granular as a client requires, depending on the ways in which they intend to collect and use the data.



IMPORTANT TO REMEMBER:

1. **GDPR now gives data subjects the right to withdraw consent at any time, and doing so must be as easy as giving consent in the first place.**
2. **Consent must be specific to each type of data processing activity or operation.**
3. **GDPR has enhanced parental/guardian consent requirements for the processing of any personal data relating to children (including use of reasonable efforts to verify parental consent).**



Event management is evolving,
so should your software.



One integrated solution to create, manage
and optimize every aspect of your events.

When it comes to event management
platforms, you have a choice.

try.etches.com/evolve



cloud-based enterprise event software

Other key aspects of GDPR

Restrictions on Data Profiling and Targeted Marketing

New GDPR regulations address the development of technologies that allow data controllers to analyze personal data in order to draw conclusions about data subjects and take certain actions based upon those conclusions, including targeted marketing efforts. GDPR contains many restrictions on "profiling" - the automated processing of personal data, use of that data for purposes of predicting or analyzing a person's preferences, interests, location or movements, and the making of decisions based upon those predictions or analyses.

A data collector must notify the data subject at time of data collection that profiling will occur, the analysis and logic involved, and the consequences of this profiling. Data subjects must then have the right to object to profiling for direct marketing purposes, or any circumstance where they are subject to decisions based solely on automated processing.

A processor or controller may not be subject to profiling requirements if the data being analyzed is anonymous. It's still a bit vague what activities qualify as profiling, and we can expect additional regulatory guidance to be issued

Privacy by Design

Companies such as etouches must demonstrate that privacy considerations are a driver in designing and implementing event management technology and solutions, and are not just an afterthought. etouches will reassure clients that any changes, enhancements, and updates for the etouches ecosystem are undertaken with an eye to potential privacy and security risks; security measures are not just tacked on after the fact.

Pseudonymization is an important feature of privacy by design. This entails giving clients the ability to break up personal information so that it is no longer identifying. For example, date of birth, zip code and gender - each on its own can't be used to identify a specific person, but all three combined could be enough.

Data Portability

GDPR regulations now require data controllers to provide personal data to the data subject in a commonly used and "machine readable" format, and to transfer that data to another controller (even a competitor) at the request of the data subject.

Detecting, Investigating, and Reporting Data Breaches

Previously, US companies had data breach notification obligations primarily in instances of leaks involving sensitive personal data such as social security numbers, or financial account information. Under GDPR, all personal data is subject to breach notification requirements.

GDPR defines a "data breach" as "the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Under GDPR, our clients, who are the "data controllers" with respect to event registrant data, will have only 72 hours to provide the data subjects and applicable authorities with notice of data breaches. Clients will look to etouches to help them comply with that requirement.

Right to Be Forgotten

Under GDPR, data subjects have greater rights to withdraw consent for the use of their personal data, and to request that it be deleted. etouches may need to provide clients with the ability to accurately locate and delete a registrant's personal information in response to a registrant's request for deletion. This process must be prompt and efficient. According to the "Right to Be Forgotten" under the GDPR, data controllers must erase personal data "without undue delay" if the data is no longer needed, or if the data subject objects or requests it. A request to delete need not be granted in every instance. Exceptions apply, and requests can be denied for a number of legitimate reasons.

etouches already appointed a designated individual (e.g., the Data Protection Officer) to handle all such requests.

Road to Compliance

Here is an example of a check list to get you on the right track. Note, this list is not exhaustive and does not represent an official check list for compliance, the purpose is only to illustrate the type of tasks you need to consider or that you want your tech vendor to achieve. This is not legal advice by any means. Each GDPR policy is tied to a specific controller/processor context.

Key GDPR principles:

- Diligence
- One stop shop analysis (for the regulator)
- Data controller analysis
- Legal basis for processing
- Notices
- Inventory of data
- Appointing a Data Protection Officer (DPO)
- Privacy impact assessments
- Rights of data subjects
- Breach
- Security
- Vendor relationships
- Cross border transfers
- Training and awareness

- Confirm the relevant legal entities in the EU and the locations where key data decisions regarding EU data processing take place.
- Identify all instances in which personal data is processed by a non-EU entity or service provider that offers goods or services to individuals in the EU or monitors the behavior of individuals in the EU.
- Collate all notices and consents used by processor-controller.
- Confirm the personal data that is processed by processor, the purposes for which such data are processed, the categories of persons to whom the data relate, and the persons to whom the data may be disclosed.
- Collate all data processing and service agreements to which the processor is a party.
- For each processing activity identified from the diligence, determine who acts as a data controller or data processor.
- Ensure the data processor is processing personal data only in accordance with controller's instructions.
- Confirm cognizable legal basis to be relied upon for each processing activity (e.g., contractual performance, consent, compliance with law, legitimate interests).
- Update policy documents as needed to contemplate legal bases for processing personal data.
- Update internal procedures as needed to contemplate legal bases for processing personal data.
- Review and update consent language and mechanism to reflect GDPR requirements where legal basis for processing is consent.
- Update process to allow for withdrawal of consent.
- Ensure processor and controller have evidence to prove that consent has been validly obtained.
- Review existing privacy notices against GDPR requirements.
- Draft new or update existing notices.
- Roll out of new notices to individuals.
- Create data processing inventories for controller and processor activities that document all data processing requirements and meet requirements of GDPR.
- Implement a process to ensure data processing inventories are kept up to date.
- Determine whether a DPO is required.

Road to Compliance (cont.)

- If required, determine the appropriate DPO structure (a single DPO office, regional, country or business unit DPOs reporting to a lead DPO).
- Select and appoint DPO, ensuring that they have adequate independent reporting lines to a person of sufficient seniority within the organization, and determine budget and other resources the DPO will require to fulfil the obligations of the role.
- Create Data Protection Impact Assessment (DPIA) process and templates that reflect the GDPR requirements.
- Create internal processes to ensure DPIAs are conducted when required.
- Consider leveraging a technology platform to allow scalability in the Data Protection Authorities program.
- Update or draft access request procedure to reflect new GDPR requirements.
- Update or draft policies for handling a request for erasure or correction.
- Develop process to inform any third party of the request to erase data.
- Draft policies for handling a request for data portability.
- Adjust data processing file format as needed to comply with the right to data portability.
- Develop process to ensure the processor can cease processing personal data in response to an objection to data processing.
- Draft breach notification policy and procedure, including means of documenting personal data breaches for inspection by supervisory authority.
- Ensure that appropriate technical and organizational security measures are implemented and can be demonstrated, having regard to risk.
- Review all data processing or service agreements to ensure that they meet the minimum requirements of GDPR.
- Negotiate required changes with vendors as necessary. Review existing cross border data transfer mechanisms in place at etouches.
- Develop a training and awareness program to raise awareness of GDPR within specific areas of business. In particular, provide training on:
 - Maintaining inventories of data processing activities
 - Data subject rights and how to respond appropriately when those rights are exercised
 - Breach notification procedure
 - Using DPIAs

Meetings and events use cases – Q&A

If at the end of a potential contract we choose not to continue with your system, who is the legal holder of data? Does it belong to us or to you?

By design, we are a data processor, not a data controller (you are). The data belongs to you. Our built-in policies will define the means to access data during and post contract. Based on your GDPR internal policies, you have at any time the ability as an administrator to export all data of your own using existing functionality through report exports. Data backup scrub is part of identified items in our road to compliance.

In terms of data management, we can overwrite the data in the database with one-way hashes. The fields to be overwritten are selected by the client so you can implement your own PII classification policies.

My company uses your event management software to plan internal meetings: it means the only information that is transferred or enriched is employee information. Are we impacted by GDPR in regards of these events?

Yes. GDPR is about EU citizen data, regardless of who/why you own it. As a company, you have obligations toward data management in relation to your employees under GDPR. More internal meetings often bring external speakers, contractors, etc.

When I scan a lead at an event, do I need to get consent from the individual?

Technically yes. Especially since the scan data is not solely used by the controller, but for example by many exhibitors. If you resell this data, make sure you have a thorough policy opt-in process disclosing it. Your exhibitors are entitled with the same constrains. Seek legal advice on how best formulate opt-in process and privacy policy disclaimer.



Meetings and events use cases – Q&A (cont.)

We are hosting an event in the EU, but none of the participants are from the EU and our company is headquartered in APAC. Do we need to comply?

Based on that description the answer would be no. However, you may want to make sure you capture your attendees' citizenship! Technically, one EU citizen in your attendee database is enough to bind you to the GDPR regulation. Based on citizenship, you may refuse to register an EU citizen, depending on your country's regulation (eg: discrimination).

Is the fine a real risk, who is entitled to claim it?

Yes, the risk is real. This is not specific to events. The recent fines have been issued by the country regulator. Most fines resulted from data breach, reinforcing the importance of data security. Recent examples involved Equifax, HSBC, Talk-talk, and Sony. These last two were fined nearly 400,000 GBP by ICO. This does not just happen to big multinational companies. Staysure.co.uk, a mid market insurance firm, was fined 175,000 GBP for a data breach.

Exhibitors and sponsors collecting attendee data: who needs to comply?

Everyone! You have to get consent from your participants as much as your exhibitors or sponsors do. The challenge is rather the traceability of this consent: business cards, scan, check-in, and mobile lead retrieval. Regardless of your means of collection, throughout the collection process each party needs to inform the participant about the use of its data. Remember that GDPR promotes marketing opt-out by default.



Meetings and events use cases – Q&A (cont.)

How does the etouches data purge function work and is it possible to automatically schedule personal attendee data to be purged after X amount of months?

The purge data, once applied to an account, is a one click manual purge per event.

We did think about adding a timeframe trigger to automatically purge events after X dates, but the negative implications against this outweigh any positive effect. If you set to purge events after X days, it would mean that all events would then be purged after X days, even perhaps events you did not want to purge.

The second issue we came across was event status; for an event to be purged it needs to be "closed" or "archived".

Creating an automatic purge could lead to scenarios where clients may not close events and expect the purge to still happen after X days; which would not be the case – this user error could potentially yield to data protection policy not being followed/respected.

Due to the examples mentioned above, we decided to maintain a manual process to purge data.

Is the GDPR clear on how long data can be stored when being collect for an event?

GDPR does not set out any specific minimum or maximum periods for retaining a client's personal data. Rather, it simply states that personal data must be kept "no longer than is necessary for the purposes for which the personal data is processed."

How long you keep your client's personal data will depend on the business needs for which you collected that data in the first place, and the nature of that personal data. You will also want to weigh the benefits of retaining the data (e.g. to keep a business record and be able to address any future contract claims, financial liabilities, and other future issues to which that information may be relevant) against the potential costs and risks of retaining that information for long periods of time.

Also note that certain kinds of personal information may need to be retained, even after the client relationship may have terminated, to meet audit or other legal or regulatory requirements. As GDPR implementation becomes more widespread, industry-specific standard data retention periods will begin to emerge. For now, each company will need to evaluate and carefully consider what retaining client information "no longer than is necessary" means in their particular context.



etouches' commitment to client GDPR compliance

etouches is aware that our clients, as data controllers, are required by GDPR to engage data processors that provide "sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement appropriate technical and organizational measures which will meet GDPR's requirements for the protection of the personal information of data subjects. etouches must therefore be able to provide our clients with those guarantees.

etouches understands that our clients will rely on us to facilitate their own GDPR compliance programs, and we commit to supporting clients in our role as processors of their event and registrant data.

Road to compliance

As the data controller, you will be designing your compliancy not just around etouches but your entire ecosystem. We are prepared as the data processor to work with your team and help them leverage our GDPR infrastructure, ranging from tools to policies or implemented processes.

MAY 2018 IS TOMORROW

We have already started to work on GDPR certification with numerous clients.

Some events for 2018 will launch their registration in the last few months of 2017. The data, consent, and process must be locked down by then!

gdpr@etouches.com

External resources about GDPR

Creating content has a lot to do with thorough research. While this ebook aims to provide a best of GDPR with a focus on meetings and events, the following links are additional resources we found useful.

Official GDPR regulation

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

<http://www.eugdpr.org/>

Data protection instances

EDPS (Europe)

http://ec.europa.eu/justice/data-protection/bodies/supervisor/index_en.htm

List of data protection authorities by country

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

ICO practical guide of data compliance

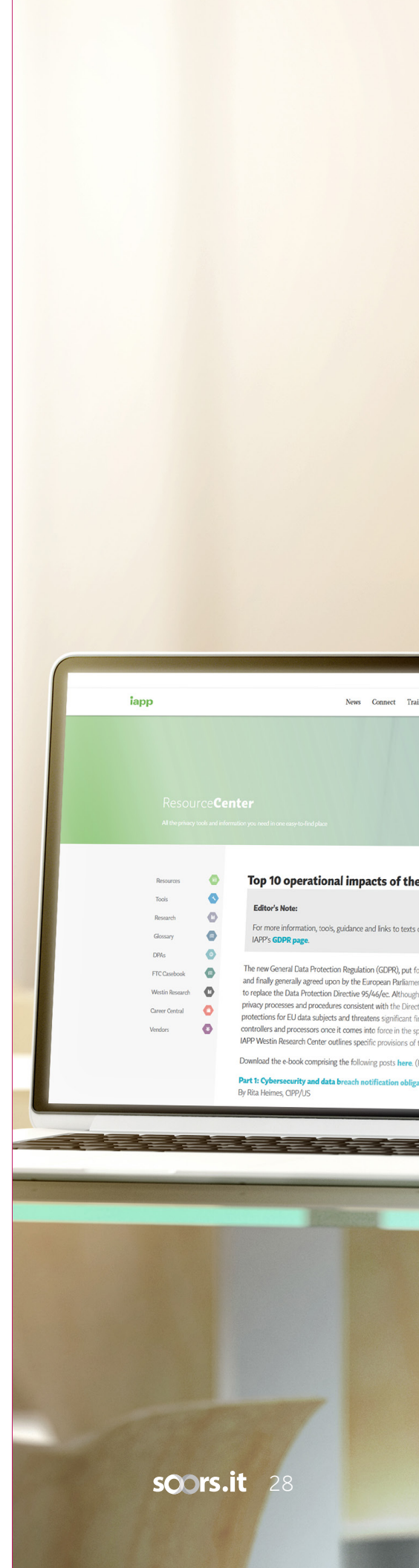
<https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/>

IAPP top 10 operational impacts of the GDPR

<https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/>

APSCo GDPR toolkit

<http://www.apsco.org/apsco-gdpr-toolkit.aspx>



Our view on GDPR for organizations running meetings and events

GDPR is 90% a business initiative, where technology becomes in fact a means. We hope this eBook gave you a better understanding on what the law and the regulator is looking to achieve. If you start with the granularity of the technical impact, you'll get overwhelmed and you will lose sight of the goal. Take a step back and follow the necessary steps: nominate a DPO and document their role, write processes, make sure you map your ecosystem and its data, and give access to that data. Of course your level of effort will differ based on the nature of your business whether you are a multinational company, SMB, association or agency. Unfortunately, there is a cost associated with GDPR and you need to take it seriously: get on it, work with your vendors, but state exactly what it is you expect from them based on your interpretation/legal advice.

The good vendor is not the one that will tell you what to do, it is the one that has the tools ready for you to comply based on your specific context and expressed needs.

At etouches, we've built a myriad of assets between security layers, EU hosting, compliances, reporting and data access to provide you with the arsenal you need, not in May 2018, but today.

We are here to team up with your organization and ensure you can rely on us for GDPR, but also for successful events that positively impact your business.

Want to know more about how etouches can help you achieve your GDPR compliance?

gdpr@etouches.com



About etouches



etouches is a global end-to-end event management software solution. The success oriented and cloud-based platform delivers innovative technology solutions to streamline the event process and increase ROI. Founded in 2008, etouches has assisted over 20,000 event professionals in planning, executing and measuring their events. With a focus on event sourcing, registration, marketing, logistics, engagement, mobile and data, the software solution has been able to serve more than 1,200 customers in corporations, associations, agencies and educational institutions. Headquartered in the United States in Norwalk, CT, the company has a second office in Orlando, Florida and five global offices in the United Kingdom, Belgium, Australia, UAE, and Singapore. Learn more at etouches.com.

About Soors.it



Soors.it is a new platform allowing companies of all sizes to source their technologies. Today, soors.it offers a range of senior consultants, with a particular focus on CRM, marketing automation, event software and social media automation. Founded in 2016, soors.it is headquartered in Paris, France with representation in U.K. learn more at soors.it.

Contact us

For questions or enquiries about GDPR contact us at:
gdp@etouches.com

CONCEPTION: Soors.it

EDITORIAL MANAGEMENT: Nicola Rossetti

EDITORIAL CONTRIBUTION: Soors.it content team, Karin Wichman

COPY-EDITING: Lauren Williams, Kristen Carvalho

DESIGN: Tamsin Hatton

COPYRIGHTS SOORS.IT 2017 – ETOUCHES 2017

GDPR

MEETINGS & EVENTS

We've got you covered.

etouches

soors.it