conrego

Event Attendee Personal Data Processing in Compliance with the GDPR

A guide for event managers and organizers of conferences, congresses, workshops, as well as other events

Authors: Łukasz Krawczuk (CONREGO),
Przemysław Kilian (rodoszczecin.pl)

2nd edition, 2021.01

Interactive table of contents

conrego

From the authors

Writing this guide, I assume you are an event manager or event planner. If you are not, there's still a lot of valuable and relevant information in this guide and it most likely concerns you as well.

My aim is to present you the stipulations of GDPR and how to comply with them. In this case, compliance is a group effort and every party that collects, stores, or processes personal data in any way, needs to take necessary actions to ensure data protection. I will explain each party's duties in the **Compliance step-by-step** section. If you already know what is GDPR, realize it concerns you, and know that you need to comply, feel free to skip to page 6.

What is GDPR?

GDPR, or General Data Protection Regulation, is a regulation issued by EU authorities to unify, modernize, and strengthen personal data protection. It becomes enforceable as of May 25, 2018.

The way it differs from previous regulations is that it was created with the intention to issue a lasting solution to data protection. This is achieved by ignoring technological means. As a result, GDPR is more strict and requires data controllers and processors to undertake additional means and exercise extra caution gathering and processing data; at the same time, it gives us more freedom as to technological solutions we employ to ensure compliance.

Who does it concern?

In short, every organization that stores or processes personal data based in the EU and organizations that store and process personal data of EU citizens. Pretty much everyone. In particular:

Data controllers

Data controller is an entity that stores or processes personal data and controls it. This entity decides which pieces of data are to be stored, removed or processed.

This means end users of collected data - you. You use this data to provide service to your attendees. Before and during the event, you probably access it on a daily basis and that's what you need to do. Booking accommodation, sending reminders, marking attendance, printing ID badges, last-minute changes - all this is data processing. This is fine as long as you have the attendee's active and explicit consent. I listed these to show you why the GDPR concerns you.

Data processors

Data processor is an entity that stores or processes personal data on behalf of the data controller. However, the data processor does not decide which pieces of data are to be stored, removed, or processed.

This means providers of technological solutions - developers of event registration software and mobile event applications - us. We store it in databases, we make sure it's properly protected and you have means to easily comply with the GDPR. And we sometimes process the data on your behalf.

Why you should care?

Image

Let's face it - it feels good to do good. And while the GDPR might pose some technical and organizational challenges, it's designed to empower persons to control their personal data processed by organizations. In a way, it forces you to respect your attendees' privacy. It promotes transparency and convenience. You do want your customers (end users, i.e. attendees) to feel comfortable using your services. Satisfied attendees will trust and like your client or yourself, making them more likely to attend again. The main point of this section, however, is you. Most of us want to be liked, not only because of financial issues. You don't want your brand to be seen as an evil, scheming corporation, do you? Honesty will get you a long way.

Profit

I somewhat related to this point in the previous section but that's not all. The common idea is that a well-perceived, honest, and transparent brand increases revenue. It does that because:

- attendees are more likely to trust this brand again;
- your employees and staff will feel better working for that brand and will work more efficiently.

The other point I'd like to touch on is your contact list and the contact lists of your clients and vendors. You see, under GDPR, you need to gather separate expressions of consent to add personal data to marketing lists and to transfer them to other organizations. This implies that you will probably be able to gather fewer marketing contacts, and even fewer of them can be added to the vendors' lists. However, once you have a contact that has consented to all of the above, that lead is really interested in the offer. This will let you build healthy lists without sending communication to people who are not interested. Instead, you can focus your resources on the contacts that are likely to generate revenue.

Penalties

Last but not least, we are simply forced to comply. I know it's not the most pleasant point and that's why I put it last. Just in case you're still not convinced. This one can really hurt you. If you fail to comply to any of the GDPR's stipulations, you are subject to fine of up to **€20 million** or **4%** of your global annual turnover of the previous financial year, whichever is higher. The amount depends on the risk created by non-compliance and the scope of non-compliance.

But that's only the fine. If your non-compliance caused damage to persons whom the data you process concerns, they can sue you for damages.

Compliance step-by-step

You know you have to comply and why you need to. But how do you go about it? I will describe all the key changes you need to take into account and then show you what you need to do and what we have done to comply.

Consent

You obviously need consent. But some things have changed:

- **consent needs to be active** - no more pre-ticked checkboxes or opt-out clauses;
- **be transparent about what you need the data for** - to you it's obvious that you need to give some data to the venue staff or a hotel but still, your attendees need to be informed about it. And you need to name the organizations that will access the data - it's no longer enough to state the industry, you need to specifically state organizations and purposes;
- **you need separate clauses for different data processing purposes** - consent for marketing purposes now needs to be a separate clause and it cannot be a mandatory one. When registering attendees for an event, the main purpose of data processing is to handle the event. Marketing is a separate matter and needs to be treated as such;
- **personal data transfer to third parties** - if you want to transfer data to your vendors, you need to list them by names in a separate clause. If you want to determine consent based on ID badge code reads at vendors' booths, such information needs to be explicitly presented at the booth.

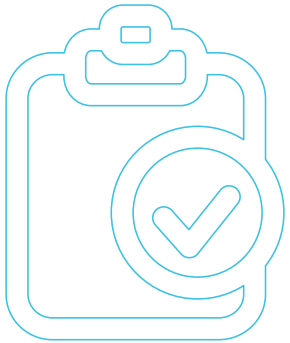
What do you need to do to comply?

Make sure your clauses are precise, specific, and properly divided. Formulate their content according to the requirements above and you'll be fine.

What did we do to comply?

We allow you to add any number of clauses to the registration form and link them to documents with terms and conditions. For every integration with external data processing services, you can make a condition that only attendees who ticked an adequate clause will be automatically exported to other services.

Moreover, every clause selected by an attendee becomes a part of that attendee's record. You will be able to prove you have appropriate consent and from which IP consent was given.



Mandatory Breach Notification

In case of a security breach that puts the privacy of your attendees at risk, you need to report such event to data protection authorities within 72 hours from that event.

What do you need to do to comply?

Well, monitor your registration records.

What did we do to comply?

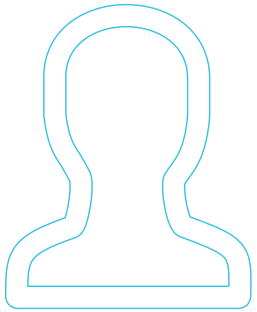
We can't do much about that as successful attacks cannot be automatically detected by their very nature. Detected attacks are blocked without any harm to the data. All the personal data we store and process is stored on a server located in the EU. Non-personal data, like pictures and documents, is stored in the Amazon cloud, which is also compliant.

Right to Access

Every attendee (or any person whose personal data you store or process) has the right to demand that you give them a complete set of their personal data you have gathered. You are bound to provide that data in a commonly used, machine-readable format within 30 days.

What do you need to do to comply?

React to such request. It would be a good idea to have a process ready for such events and have it documented. You should also verify that person's identity before sending the complete set of data. You know, you don't want to be held liable for personal data disclosure. What is a commonly used, machine-readable format? PDF or .XLS is your best bet. The former looks better, should the attendee want to print it out, while the latter is easier to read and import to other systems (more on that below).



What did we do to comply?

You will be able to let your attendees use a contact form to request a full set of their personal data. When you receive such a request, you can easily download a PDF file with the attendee's full set of data and send it to them.

Right to be Forgotten

The rule sounds simple. The attendee demands to be forgotten so you forget about them. Delete all the data you've gathered on them and that's it, right? Right. However, you need to **delete all their data**. This means event registration software, CRM, mailing lists, and any other location they could be stored. Paper guest lists - erase. XLS files - delete the row.

What do you need to do to comply?

I don't think it needs any additional clarification. The most important thing is to be diligent, thorough, and timely. I cannot tell you in particular what to do because every organization has its own data network. And if you have had consent to give data to third parties and have done so, remember to remove data from these third parties - they need to stop processing it as well.

What did we do to comply?

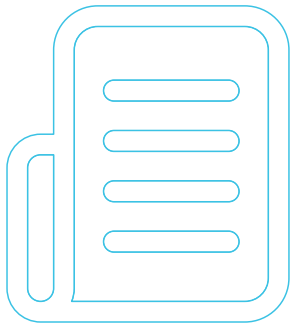
The contact form can also be used by the attendee to demand data deletion. After logging in and provided that you have permission to view this data, you can decide whether to remove the data or not. Mind you, you do have the right to keep the data if and only if it is necessary to carry out your part of the agreement. In this case, if you need the data to provide the service of participation in your event.

Data Portability

In essence, you have to make it possible to easily transfer personal data to other organizations. Most data processing systems accept CSV and XLS files for data import. Hence, it's a good format to have personal data exported from your system.

What do you need to do to comply?

Make sure you're able to withdraw all personal data of an individual on demand and that it can easily be imported to most external systems. As in every case of transferring personal data, do make effort to verify the identity of the person requesting such transfer.

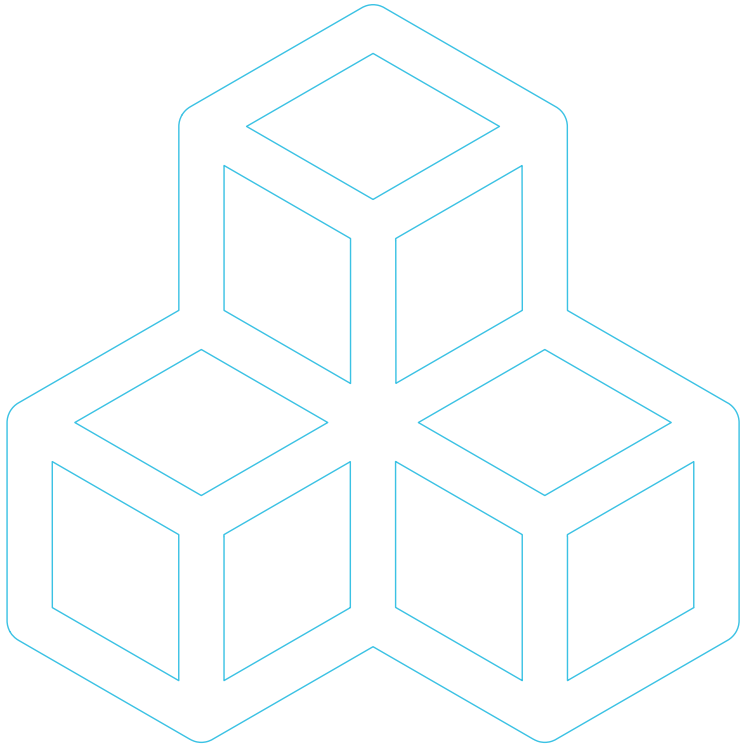


What did we do to comply?

You can easily download a set of personal data onto your disk from the administration panel.

Privacy by Design

This means that data protection is neither a feature nor an option. It should be an underlying principle of any system and process related to personal data. Vague, isn't it? But by adopting this mindset, you are almost sure to comply with the GDPR. It's really reasonable and if you make personal data protection a part of your organization's agenda, you will meet at least most of these requirements.



What do you need to do to comply?

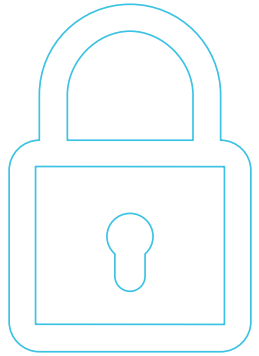
Revise all your processes, tools, and the entire system as a whole, asking the questions:

- does it protect my contacts' privacy?
- are there any points where personal data could be disclosed?
- does it create a risk of disclosure?
- is it fair how I gather and process this data?

Should you find a conflict with GDPR, change and innovate! It's in your best interest to comply
- not just because of the fine. And no, this content
is not sponsored by the EU.

What did we do to comply?

If you create additional system user accounts, you can limit their access to sections containing attendees' personal data. Your browser session is terminated after 30 minutes of inactivity so if you leave your computer unattended, there is a smaller chance of someone accessing the data. We also provide our customers with subdomains of conrego.com that are all protected with an SSL certificate. As for external domains, you can purchase your own SSL certificate and we'll help you install it or we can install a free **Let's Encrypt** certificate courtesy of https://letsencrypt.org.



Data Protection Officers

Some organizations will be required to hire a DPO. This most likely includes us all because having one is a must for:

- organizations that engage in large scale systematic monitoring or,
- organizations that engage in large scale processing of sensitive personal data.

For some conferences, you will gather data like dietary requirements, allergies, or passport number, which constitute sensitive personal data. "Large scale" here is far from precise. Hundreds of registrations is a lot but is it large scale when compared to corporations like Google Inc? It's not clear but I'd stay on the safe side and appoint a DPO.

What do you need to do to comply?

Appoint a DPO and have them train your staff about personal data processing, document your personal data related processes, and report any failures in compliance to authorities.

What did we do to comply?

We have a DPO. The staff that deals with personal data is periodically retrained and we have documented processes in place regarding personal data processing and security breaches.

Conclusion

GDPR is coming into effect soon and we all must prepare for it. I hope this guide was useful and eased your mind a little. As long as you make personal data protection your business and really put your mind into it, you will be fine. Fortunately, the regulation is really rational. On the other hand, it's pretty vague and that could be alarming. After all, what you consider enough may be considered lacking by authorities. We don't like uncertainty and therefore I wrote this guide taking into account extreme caution. This means that I even included elements that I consider a slight overkill.

All in all, it's better to be overly prepared than to try and justify your choices when your compliance is questioned.

Good luck!

Your Event Registration Software should simplify event management for in-person and virtual events.

Congratulations! Your search is over.

https://conrego.com

conrego