P&B Guideline: People-oriented meeting organisation for Beginners

People-orientation
Be excellent to each other! Always transparently inform people and consider different needs when planning a meeting.

Privacy-preservation
Respect people's privacy. Only collect data that you really need.

Bureaucracy-prevention
Avoid unnecessary work, stick to the rules!

Benefit of provided tools
Use tools provided by your institution. For those, paperwork is already done.

Introduction

In science, many of us have to organise a workshop or other meetings at some point. The organisation of such meetings can present certain challenges, particularly in the context of the management of participants' personal data. Consequently, the primary course of action would be to consult the data protection office of one's own institution. In this department, personnel are available to provide information and assistance on data protection matters. Nevertheless, it is often useful to have a list that is easily comprehensible in order to provide a rapid overview of the points that should be considered when planning a meeting according to data protection. For this purpose the P&B Guideline was developed to support ourselves and others with smooth meeting organisation. The guideline is meant as a supportive tool.
Disclaimer: Legal assurance, however, can only be given by legal personnel and should therefore not be assumed to be fully covered when adhering to the guideline. Nonetheless, adhering to the guideline will give you a good direction for making your meeting organisation privacy-oriented.

Your Notes

Workshop:

Further Notes:

In brief

Think first
A good preparation reduces the risk of data incidents and time-consuming reporting to the authorities.

Less is better
The less different tools you use, the less effort it is to setup and communicate the data protection implications.

Have a plan
Treat the personal data of your meeting participants similar to data from a scientific project, i.e., have a "data management plan", including which data you collect, how you store and use the data, and when they will be deleted.

Specify the purposes
When planning to collect data of your meeting participants you need a data protection information that includes a purpose for every data usage ("purpose limitation").

Clean up
Delete the personal data collected after it served its purpose.

Checklist

Note: The checklist is not linear. You may have to come back to earlier points later in the process.

In General

- [ ] Know the responsible person according to GDPR

  This is not necessarily the person who is organising the meeting.

  Example: The data protection officer of your institution.

- [ ] Name a contact person

  This helps the participants to know whom to contact in case of questions, problems or if they want to exercise their rights.

  Example: The person organising the meeting. Or the secretary of your institution.

- [ ] Data processing justification according to GDPR Art.6

  What kind of data will be processed and for what purpose?
  List all purposes for every item on your data collection list (see below), including optional data.

  Example: names and email addresses for meeting organisation and information provision; research field to plan an interdisciplinary meeting and prepare for expertise brought in by the participants; optional age for statistical analysis

- [ ] Provide a process for the data handling

  Data handling includes not only to define which data to collect and where to store it (see below), but also to define how to delete it after the meeting is over.

- [ ] Define handling of requests

  Be aware of the "Rights of the data subject", Chapter 3 GDPR, especially Art. 15-21.
  Important rights are to object (Widerspruch), to access (Auskunft), to rectification (Berichtigung), to delete (Löschung).

Which data is involved and what is it used for

☐ List the data to be provided by participants

This is data that you explicitly collect by asking the participants to provide information to you.

Examples: name, mail address, job description

☐ List the data that will be collected automatically

This is data that you implicitly collect during the process of getting information from participants.

Examples: IP-address, browser fingerprint by visiting a website, registration form

☐ List where the data is stored

Here, you should define where the collected data (from the previous two points) technically ends up.

Examples: On a server of your institution, written down on paper and stored at your file cabinet, in email inboxes, on third-party-servers

☐ List the tools that are planned to be used

Define tools to be used and check what data they process (e.g., check whether it is required to add personal information into a tool).

- *Communicate usage of such personal data processing tools beforehand.*
- *Think about providing an alternative solution for participants who do not agree to the usage.*
- *Also the IP-address is considered personal data, so just using a website must be listed as well.*
- *Include links to external privacy agreements and terms of use if applicable.*

☐ In-house tools

These are tools that are provided by your institution. Usually, the legal requirements should be already covered by your institution. However, in case of insecurity, it is recommendable to check for the respective information.

☐ External tools

Tools that are not provided by your institution.

Access to data

☐ List who has access to the data and for what reason

Examples: working group organising the meeting, your team, your institution, the data centre, third-parties, external tool-providers and data processors, e.g., providers offering tools or services

☐ List with whom else is the data shared

Examples: other participants through group emails

Recordings (audio, video, photo)

Think carefully about whether recordings are necessary at all.
Participants should have the option to decline any recordings of themselves.
Consider making areas available where recordings are not allowed.
Please be aware that automatically uploading recordings to a cloud (as many smart devices automatically do with EU-external providers) can lead to data incidents. People can be held personally responsible for such an incident.

Examples: usage of no-photo-stickers or badges that allow easy identification of people who do not want to be recorded; provide recording-free tables or spaces

☐ Define what is recorded and on what basis

The storage, use, and processing of personal data must always be linked to a specific purpose. Inform about what will be recorded, which device will be used, where recordings will be stored.

Examples: Promotion/advertisement on social media

☐ Clarify where the recordings will be published

Publish recordings only according to the defined terms and purpose.

Examples:

- *On social media, website of the institution*
- *Photos are taken with the purpose of writing a report of the event for the organisation website. Photos can therefore not be uploaded on social media for advertising of the event.*

Transparent communication

☐ Share the collected information above transparently with the participants who plan to register for your meeting

In general, be approachable to participants. Provide the comprehensive data protection information to the participants before collecting their data! You could provide these information directly with all the other advertising infos for your meeting or latest during the registration process.
Ways how to simplify contacting participants: Use a central automated system to contact participants and deliver materials, set up a mailing list to contact participants and avoid manual adding of email addresses, always put email addresses in BCC and yourself as visible recipient.

What to do in case of a data incident

- Whenever something goes wrong with personal data, please do not panic!
- At first, document what exactly happened as any incident must be reported without delay and requires proper documentation.
- Delete data that is stored/processed not in accordance to your data protection information and data management plan, e.g., any data that could be leaked.
- Stick to your organisation's incident response standard operating procedure (SOP) and report to your data protection officer (who should be able to tell you how to proceed from here).

Enjoy your meeting, don't stress yourself, and after the meeting delete the data. :)

About

Created as part of our efforts to promote young talent, supported by the GMDS PK Nachwuchs.

Authors

ORCID	Name
0000-0001-5504-5108	Lea Gütebier [1]
0000-0001-9691-2677	Lea Michaelis [1]
0000-0001-9008-1868	Christina Schüttler [2]
0000-0002-8349-6798	Hannes Ulrich [3]
0000-0002-9902-6459	Joshua Wiedekopf [4]
0000-0003-1632-4328	Benjamin Winter [1]
0009-0009-9712-060X	Judith Wodke [1]

[1] Medical Informatics Laboratory, Institute for Community Medicine, University Medicine Greifswald, Germany
[2] Medical Centre for Information and Communication Technology, Uniklinikum Erlangen, Germany
[3] Institute for Medical Informatics and Statistics, Kiel University and University Hospital Schleswig-Holstein, Germany
[4] Institute of Medical Biometry and Statistics, Section for Clinical Research IT, University of Luebeck and University Hospital Schleswig-Holstein, Germany

Version: ***2025.1***
Pictures from cocomaterial.com

https://www.medizin.uni-greifswald.de/medizininformatik/pnb