

# EVENT REGISTRATION AND PARTICIPANT DATA

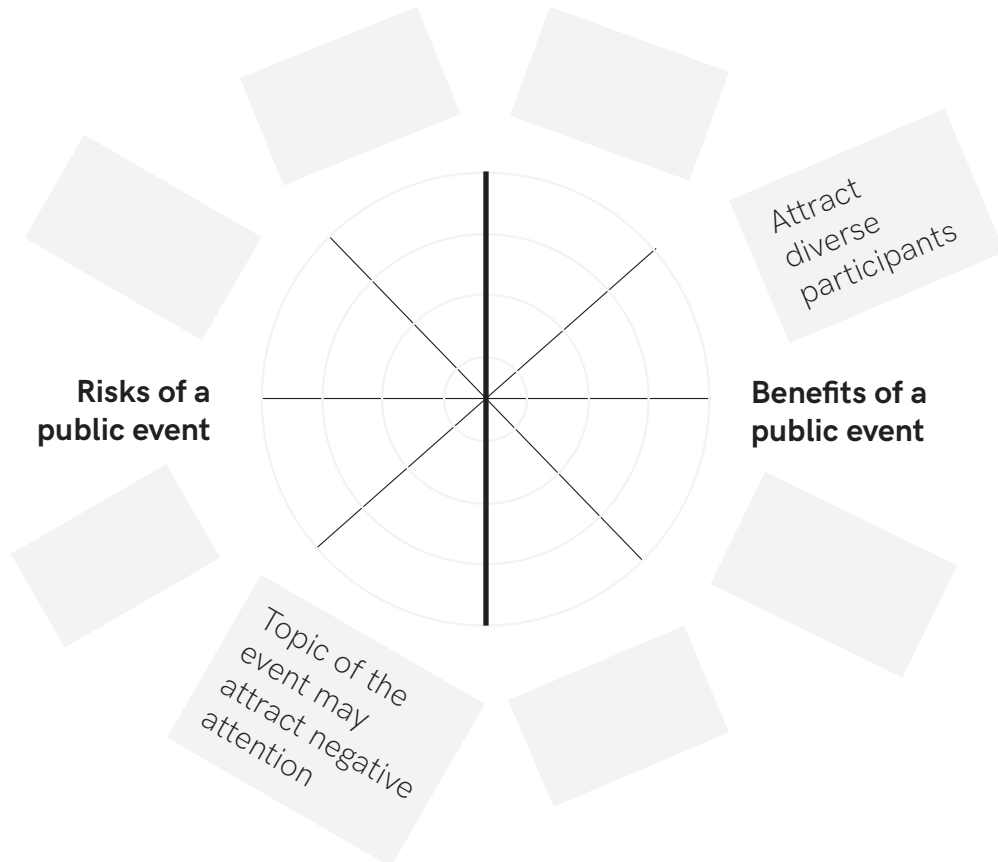
The **Organiser's Activity Book** is a series of activities to help you explore when, where and how personal information is created and shared, what alternatives there are and how to balance the benefits and risks for you and the people you work with. At the end you have the opportunity to make **Your Data Policy**, a context specific data policy for your events.

In this chapter you will discover:

- Public and Private invitations**
- Tools for registration and event apps**
- Tools for communication with participants**
- How to help participants facing higher risks**

# INVITING YOUR PARTICIPANTS

There are many approaches to inviting participants to attend, or apply to attend, your event. Some of the options are listed in the box to the right showing how they fall on a spectrum from private to public methods. There are risks and benefits across this spectrum. First, fill in the boxes around the edges of the ring below with the benefits of a public event, such as publicity or a diverse audience, and the risks, such as putting participants at risk either due to their background, or to the topic of the event. Then, rank how important these are to you by colouring in the rings - the more rings you colour the more important you feel this benefit or risk will be to take into account when organising the event.



## Private invitation

- Invitation only
- Word of mouth between in your network
- Open call - Ticketed event with application process
- Ticketed event, first come, first served
- Public announcement - anyone can attend in person or by watching online without ticket or application

## Public invitation



If you aren't sure, for inspiration return to the chapter **Introduction to Personal Data and Events**, found on <https://ourdataourselves.tacticaltech.org/projects/data-and-activism/> to consider what you might need to take into account to make the decision.

Once you've filled in your rings, choose from the options in the box above what invitation method you will use.




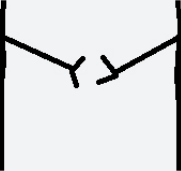


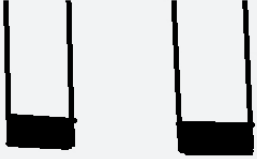

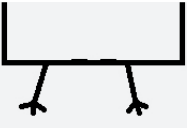
# MONSTER APP MATCH

**Organisers can use different websites and apps to register participants for events. However, the company who owns the website or app might not have the same data policy as the event organiser. Use a pen to draw a line to connect the three different monsters' head, body and feet to discover which software collects what data and with whom they might share it.**



Because these tools are easy and accessible, you may still decide to use them, but now you can do so with more awareness of the risks. You may consider asking for less information from participants at the registration stage. If you want to learn more check out the "Research" tab at <https://ourdataourselves.tacticaltech.org/projects/data-and-activism>

Make your app-monster come to life with colour or extra eyes, arms and legs.

Name of website or app			
Data collected	 <p>1. Eventbrite</p> <p>4. Location, photos/media/files, storage, network connections and full network access</p>	 <p>2. Sched.com</p> <p>5. Identity, calendar, contacts (name, work email, organisation, phone number, zip code) runs at start up</p>	 <p>3. CrowdCompass</p> <p>6. Name, email address, address, IP address, access device or browser, type of event registration, interest in events from website browsing</p>
Data shared with	 <p>7. U.S. Federal Trade Commission. May be required to disclose personal data in response to lawful requests by public authorities.</p>	 <p>8. Political parties for profiling potential supporters such as Donald Trump's 2016 presidential campaign team.</p>	 <p>9. Facebook, Twitter, Umbel, Foursquare, Madrill, Intercom, Google Analytics</p>

Answers:  
 Monster A : 1, 6, and 8;  
 Monster B : 2, 4, and 9;  
 Monster C : 3, 5, and 7

# WHAT OTHERS HAVE TO SAY

**Read the following real life stories about previous events. On the next page, reflect on how these stories make you feel, and what they prompt you to think about, while doodling, colouring, or taking a break.**

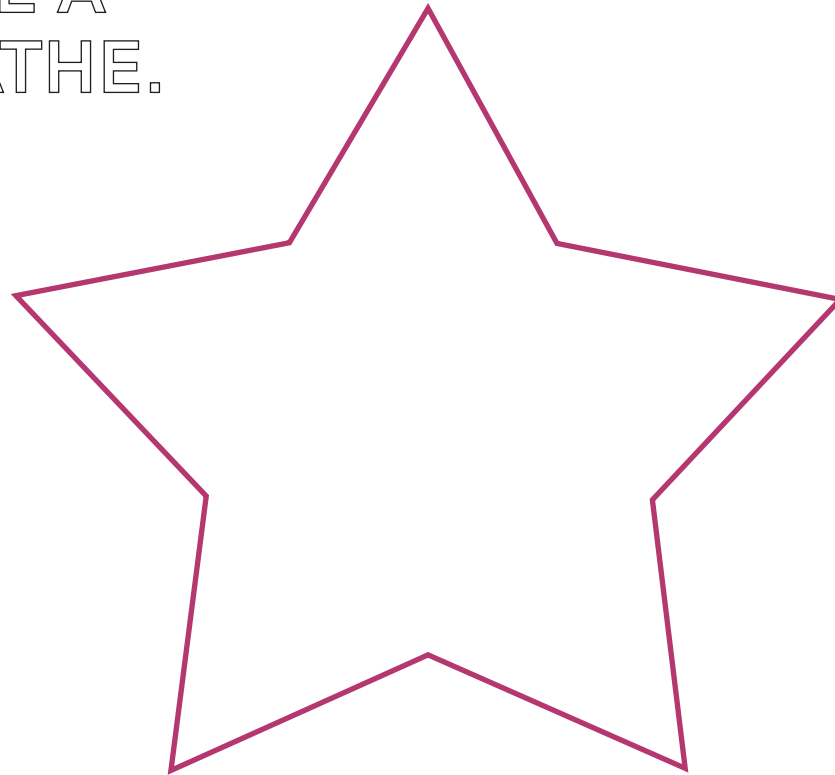
*In certain countries, merely attending an event, be it a workshop or a conference, can put a human rights defender at risk. In Egypt, for example, the Cairo Institute for Human Rights Studies canceled its annual training program on human rights, which it had held for the past twenty-two years. Explaining the decision in a published statement, the institute wrote, 'It has become impossible to find a safe space for youth for learning and creativity. Prisons have become the fate of all those who care about public matters.' Smear campaigns against NGOs in pro-government media outlets have made public outreach more difficult and dangerous: activists report threats of violence from ordinary Egyptian citizens during public activities." This is just one example of the way, for multiple reasons, states and corporations alike are interested in obtaining your information. From security to marketing, we are reduced to data that is used beyond your control and your knowledge. This makes attending an event yet another threat vector, especially when your data is not secured by those who plan the event or the platforms it is outsourced to.*



Both of these stories are excerpts from our research which can be found at [https://ourdataourselves.tacticaltech.org/posts/24\\_events\\_conferences\\_1](https://ourdataourselves.tacticaltech.org/posts/24_events_conferences_1)

*In September 2011, two iPads were stolen from an Eventbrite employee which contained data collected at one of their customer's events. Eventbrite describes itself as the "world's largest event technology platform," building "technology to allow anyone to create, share, find and attend new things to do that fuel their passions and enrich their lives." Kevin Hartz, Eventbrite's co-founder and CEO at the time, wrote in a blog post on the company's website that the "potentially compromised data included full credit card information for 28 people who bought tickets for the event; names and email addresses for some customers who bought tickets online for the event; and the names, email addresses and last four digits of credit cards for some fans who bought tickets at the event. The full credit card information was erroneously stored due to a glitch in the iPad app that has since been fixed." Though the company notified the attendees whose email addresses were potentially exposed, and immediately alerted authorities and initiated a remote password-lock and a wipe of the data on both devices, Hartz went on to say that he knows that having one's personal data compromised is a violation of the trust put in Eventbrite, and expressed his apologies to the people affected.*

DOODLE WHILE YOU  
THINK ABOUT THE  
STORIES, WRITE DOWN  
ANYTHING THAT COMES  
TO MIND, OR TAKE A  
BREAK AND BREATHE.  
YOU'RE A STAR!



# CONNECTING WITH YOUR PARTICIPANTS

**There are different platforms you can use to collect initial information from your participants such as their name, contact details or reasons for interest in the event. However, the company who owns the platform can also collect, store, and analyse not only the data you collect on your participants but also extra data that the platform requests. In the bubbles, highlight the information that you use the platform for and note to yourself how much more the software can see.**

Apps like EventBrite

- IP address
- name
- email ID
- any form data:
  - name,
  - phone,
  - travel/arrival date,
  - health conditions,
  - affiliated organization,

Online Google form

- IP address
- any form data:
  - name,
  - phone,
  - travel/arrival date,
  - health conditions,
  - affiliated organization,

E-mail (unencrypted)

- e-mail ID
- event name if mentioned
- contents of the email
- time of e-mail

E-mail (encrypted)

- e-mail ID
- subject line
- time of e-mail
- (note: avoid putting sensitive information like the event's name in the subject line!)

By Phone

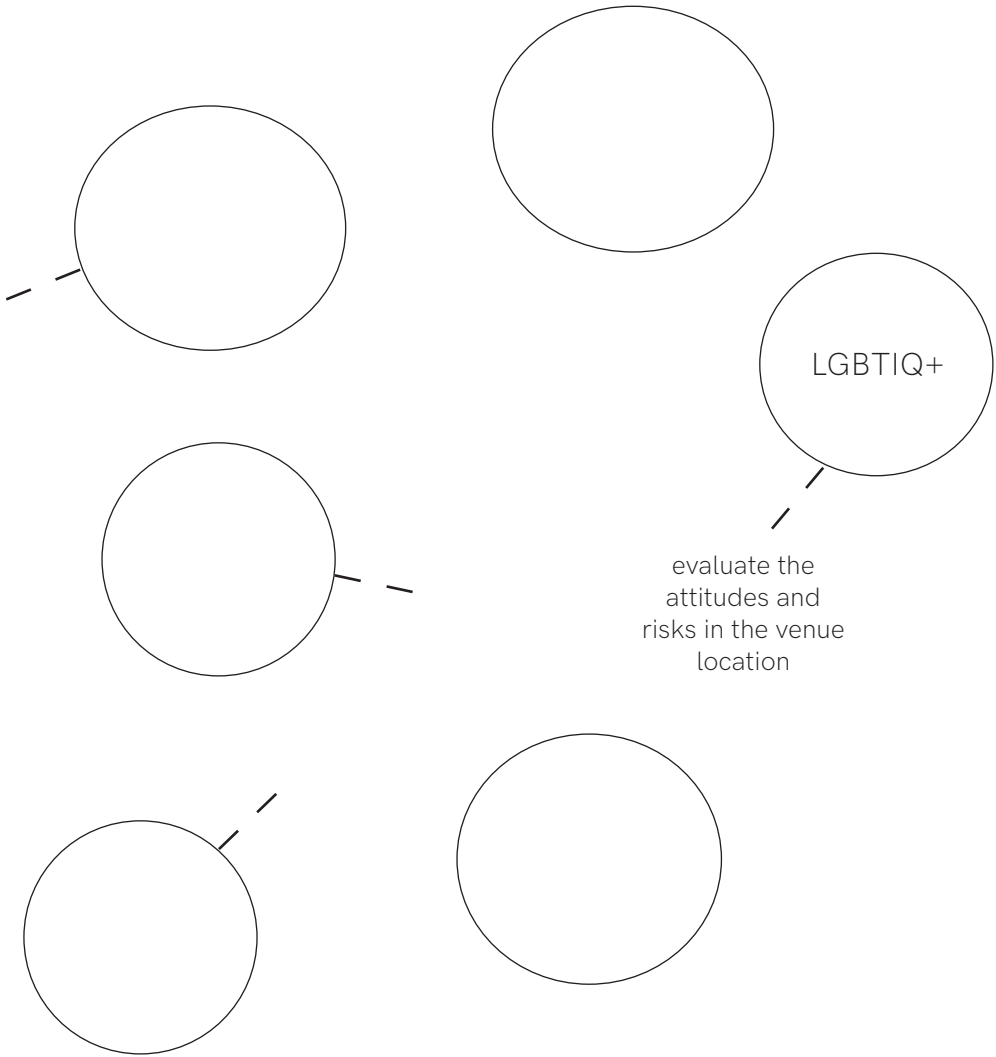
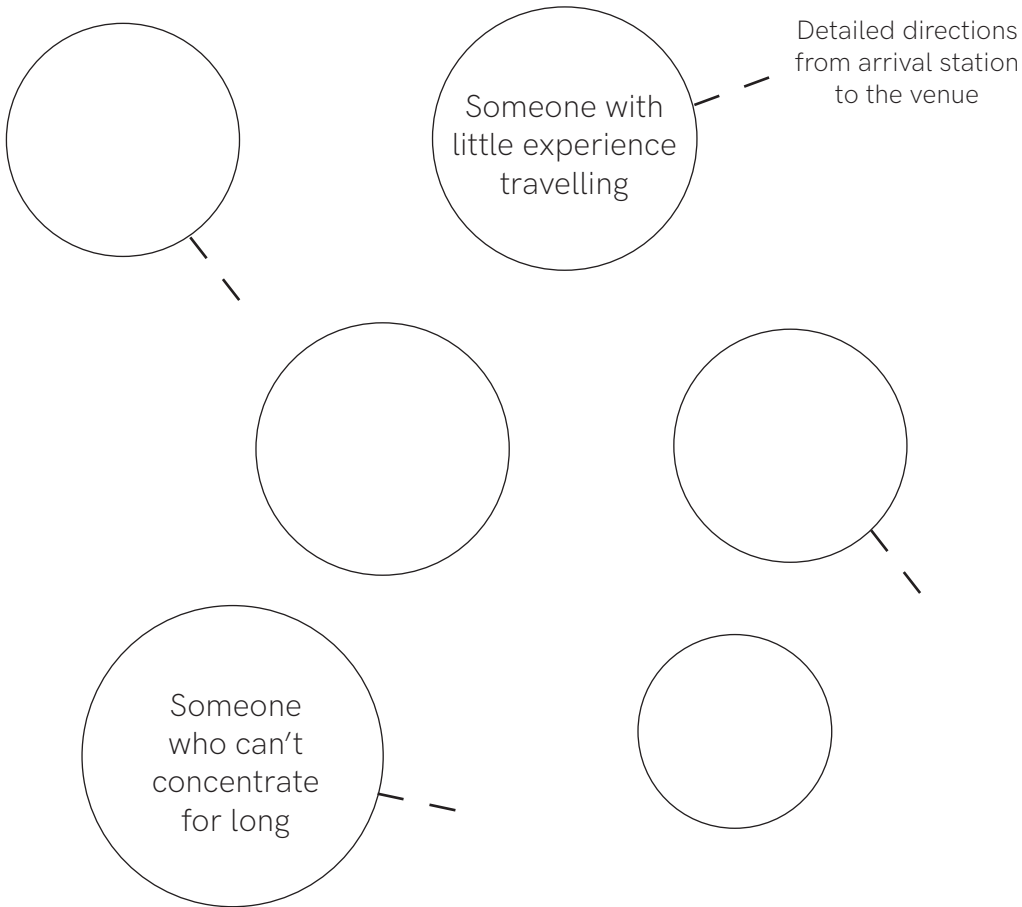
- phone number
- phone location
- time of call
- (note: risk of the whole conversation being recorded through phone tapping)



Some of these tools are the most accessible to you and your participants, but it is important to check out the relevant risks and how you will mitigate for them. Think about whether any of the information could put any of your participants at risk if it were compromised.

# PUT YOURSELF IN THEIR SHOES

When organising an event, you might need to mitigate for risks and put in place logistics that can support a diverse group of participants. Fill in the empty circles with information about your participants that may require you, as an organiser, to consider risks or provide specific resources. Around each of the circles, add how you might mitigate these risks or deliver the requirements.



▶ Now you've filled in this page, consider whether you could keep this information anonymous by planning for these eventualities without asking the participants for the information. For example, ask if they have specific requirements, rather than for their personal information. Once you collect this data, decide how you will store it safely and when you will delete it. Remember, whilst this data is helpful to an organiser to improve the participants' experience, in the wrong hands it could be used to make things more difficult for the participants.

# YOUR DATA POLICY

Now that you've completed **Event Registration and Participant Data**, you can begin to create your own data policy. You can keep Your Data Policy on hand for your own reference and to share with attendees and partners so they can make their own risk assessments. To start making your data policy, answer the questions in the boxes. Don't worry about covering everything straight away, just add anything you can think of from big to small.

**1: Write a list of all the data you might collect such as: participant names, participant travel data, participant dietary requirements, the speakers' details, financial details.**

**2: Write a list of everyone you share need to share it with such as: partners, cloud providers, funders, other participants.**

You might want to create a new box for each individual bit of data from question 1. From here, ask yourself what risks are involved with everyone who you choose to share it with. This can dictate what software you choose to use, what you decide is not worth the risk, as well as what data you might decide not to gather. Note the risks involved with any you choose to work with.

**3: For the data you decide to keep, when will you delete the data? If it is shared with someone else, when will they delete the data?**



Once you're done, look back at the last exercise **Put Yourself In Their Shoes**, is there data you might need but would be too risky to collect? How will you collect and store that data? Can you be transparent about this within your data policy?

Now head back to the list on the first page of what you will discover in this chapter. Do you feel you began to learn what you wanted to? What's missing? What would you like to learn more about? Heading to the rest of the chapters, which all have their own data policy section, at <https://ourdataourselves.tacticaltech.org/projects/data-and-activism>.

**1** What personal data do you need?

---

---

---

---

---

---

**2** Who will you share the personal data with?  
Who else can access the data?

---

---

---

---

---

---

**3** When will the personal data be deleted?  
When will those listed in 2 delete the data?

---

---

---

---

---

---

**TACTICAL TECH**

The Organiser's Activity Book