Ideas for managing stakeholders' contact details in advocacy campaigns

Last updated: June 2021

Software can be used to build a contacts database, which maps and manages relationships with a range of stakeholders, including targets, allies, opponents, supporters and activists.

Types of information to collect

The scope of a contacts database is vast. However, it can be useful to include the following types of information for each person, group or organisation:

- Their contact information, such as phone number, email address or postal address
- Their position on the issue, including their level of agreement with us and their level of influence to bring about change, whether positive or negative
- Strategies for influencing them
- Their correspondence with us, including phone calls and meetings with them or people who work for them
- Their membership of influential committees, groups, coalitions, alliances or networks
- Any relevant news stories

This information is important because it:

- enables our advocacy to focus on the most appropriate, influential, and supportive people
- ensures that information is not lost if a key relationship-holder leaves our organisation
- helps ensure that our advocacy is coordinated and is not duplicated

Only collect the data that you really need. Too much data can be overwhelming and hard to manage, so always question the purpose of that data before you gather it. Do you need an email address and a postal address? How will you analyse data on membership of groups and networks? Adopting a systematic, transparent approach to gathering data helps cut down unnecessary collection.

Storing stakeholder details

When you gather personal data about stakeholders, from their phone numbers and addresses to their personal interests, you need to have a plan to keep that information safe. This helps build stakeholder trust and guards against data breaches that may incur fines under data protection legislation.

However you choose to store your data, it needs to be secure.

The best way to build a contacts database is with Customer Relationship Management (CRM) software like CiviCRM, which has been specifically designed to map and monitor relationships and store that information in a secure database.

Alternatively, a simple contacts database can be created in a spreadsheet programme. This should be stored behind a firewall and password-protected to keep the information safe.

Consider creating a backup of your data, so that if it gets corrupted or lost in any way, you can still recover the information rather than having to start gathering it again.

However the contacts database is set up, it is vitally important that the information in it is kept up to date. Validate and update information such as email addresses, phone numbers and home addresses. Remove duplicates, and delete contacts who are no longer relevant. This kind of data cleansing enhances the value of your current data in order for it to function effectively.

Training and access

Once you have decided what data you want to collect and the best way to store it, make sure that you train your staff and volunteers in how to handle and interpret that data. Accidentally deleting hundreds of stakeholder records when trying to clean up the database will create a headache for everyone, so it is a good investment of time to properly train those who will be accessing the data.

Think about who needs to access your stakeholder data and why. Only give people access to information that they actually need. For example, a volunteer may need to know how many stakeholders there are in a particular town or city, but is unlikely to need their names or contact details. Use permission settings, reporting tools and filters in your CRM or database to only share what is needed.

Data protection and GDPR

It is important that you manage all stakeholder details and engage with data in a way that complies with the data protection legislation in your country, and that you have consent from all the stakeholders to process their data.

If you hold any data of European citizens then you must also comply with General Data Protection Regulations (GDPR) legislation. GDPR provides citizens of the European Union (EU) with greater control over their personal data and assures that their information is being securely protected across Europe, regardless of whether the data processing takes place in the EU or not.

For information on how GDPR applies outside of Europe, please see this article[1].

Examples of personal data include names, emails, addresses, dates of birth, personal interests, and any other information by which someone might be uniquely identified.Typically, this is the kind of data you might store about your stakeholders.

---

[1] gdpr.eu/companies-outside-of-europe

Regardless of whether GDPR legislation applies in your context, the citizens' rights that underpin this legislation are still a good starting point for considering best practice in managing your stakeholder details. These are:

1. **The right to access:** This means that individuals have the right to request access to their personal data and to ask how their data is used by you after it has been gathered.

2. **The right to be forgotten:** If stakeholders no longer wish to be involved, they can withdraw their consent for you to use their personal data, and you must then delete it.

3. **The right to data portability:** Individuals have a right to transfer their data from one service provider to another.

4. **The right to be informed:** Stakeholders must opt in for their data to be gathered, and consent must be freely given rather than assumed.

5. **The right to have information corrected:** You need to make sure that processes are in place to enable stakeholders details to be updated if it is out of date, incomplete or incorrect.

6. **The right to restrict processing:** Individuals can request that their data is not used for processing. This would mean you could still have their details but you don't contact them.

7. **The right to object:** This includes the right of individuals to stop the processing of their data.This right should be made clear to individuals at the very start of any communication.

8. **The right to be notified:** If there has been a data breach which compromises any stakeholder's personal data, they have the right to be informed.

Also in this series
This guide is part of a series of resources on **Advocacy in the digital age**.
Other titles include:

- Using the internet and mobile phones to identify advocacy issues
- Using the internet for research and analysis in advocacy
- Using the internet and mobile phones to mobilise people for advocacy
- Using the internet and mobile phones to advocate in difficult political contexts

Download the series for free from Tearfund Learn:

learn.tearfund.org/en/resources/series/advocacy-in-the-digital-age

The Advocacy toolkit
The **Advocacy in the digital age** series is designed to complement the Advocacy toolkit.
This comprehensive guide to the theory and practice of advocacy contains teaching notes, tools and exercises that will enable any individual or organisation to integrate advocacy into their programmes, in order to bring sustainable, positive change.

Explore the Advocacy toolkit on Tearfund Learn:

learn.tearfund.org/en/resources/series/roots-guides/advocacy-toolkit--a-roots-guide

tearfund