The Care Experienced Movement
GDPR Policy 2024

CXM GDPR Policy 2024

CEM data privacy and GDPR guidance for processing personal data of external stakeholders

Last updated June 2024
To be reviewed June 2025

Background

This guidance sets out the key principles of how the Care Experienced Movement will use and process the personal data of external stakeholders in line with GDPR regulations, and what this means for your day-to-day work.

Key terms and principles

The guidance and privacy notice refers to our process of the personal data of external stakeholders.

- **Personal data/information** refers to all the information we store about a person, including name, email address, job role, and any other personal information.
- **Processing of data** covers pretty much anything we do with the information; how we store it, how we use it and how we share it. That includes, for example, collecting email addresses in a spreadsheet, setting up a mailing list, sending someone an email, or passing somebody's details on to somebody else.

In a nutshell, GDPR regulations for the UK are telling us to make sure that:

- We carefully think through the personal information we are collecting, where we are storing them and how we process them.
- We make sure that we have an adequate lawful basis (i.e. a legally approved reason) for processing personal information.
- We inform our stakeholders how and why we process their information. The Privacy Notice linked above is our main way of doing that.

The **lawful basis** is important. There are four possible lawful bases (see Privacy Notice for more detail) but two of them are most relevant for our work:

- **Consent**: We have informed our stakeholders how we are using their data and they have actively consented. For example, when we ask people to consent when signing up to our mailing list.
- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The CXM ensures that consent mechanisms meet the
- standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.

- **Legitimate Interest**: It is not always practical or appropriate to ask for consent. In this case we can still process personal information if it is reasonably necessary for our legitimate activities. But it is important that this use is fair, balanced and does not unduly impact an individual's rights. It is useful to ask yourself whether the person would be expecting us to process their data in that way, or whether they would disagree with it. For example, it is ok if we obtain an email address of someone whose work is relevant to ours and send them an invite to be a speaker at an event or to have a meeting with us. But it would not be appropriate to add them to our mailing list without asking them.

What does this mean in practice for my work?

Collecting and using personal data

- If you want to add somebody to a mailing list you have to ask for their consent and provide them with the link to the Privacy Notice for external stakeholders.
- In other cases of collecting and using external personal data, you should ask for consent and share the Privacy Notice whenever possible and practicable. If it is not possible or practicable, make sure that the use of the data is part of our legitimate activities and is not unduly inflicting on their rights to data privacy.
- You should only collect sensitive personal data (e.g. health information, ethnicity, trade union membership, religious beliefs, sexuality, and political opinions) where absolutely necessary, and always ask for consent when you do.
- If somebody tells you to delete their data or update a specific piece of information, please do so and also let the rest of the team know, so that we can make sure that the information is updated across the organisation.

Storing personal data

- You have to store any personal data securely. Physical copies of personal data should be kept in a locked filing cabinet, drawer, or safe.
- Electronic personal data should be coded, encrypted, or password protected either on a local hard drive or on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Sharing of personal data

- It is fine to share personal data within CXM (although, in case of sensitive data, it should be avoided).
- It is also acceptable to share any personal data with a partner organisation if that is necessary for organising a jointly run project. But, if possible, stakeholders should be informed that this is the case and should be provided with the Privacy Notice from all organisations involved.
- In any other cases, you should obtain the consent of stakeholders if you are planning to share their information with others.
- You have to make sure that there is no accidental sharing of data with third parties. For example
- Check the access rights of documents containing personal data that are stored in the google drive to make sure they are limited to CXM.
- Use the 'bcc' function when emailing lots of stakeholders at once (e.g. event participants).

Right of access

- Individuals have the right to obtain confirmation that their data is being processed.
- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- All SARs must be made using the organisation's template SAR form. If the initial request does not clearly identify the information required, then further
- enquiries will be made.

Right of Erasure

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Individuals have the right to erasure in the following circumstances:

1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
2. When the individual withdraws their consent where consent was the original legal basis for processing the data
3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
4. The personal data was unlawfully processed
5. The personal data is required to be erased in order to comply with a legal obligation

Data breaches

- Should you become aware that any C data has been compromised or that there has been a "data breach" you should report this to the Development Leads without delay (by the next working day at the latest).

If you have any questions at all, please get in touch with us!
info@careexperiencedmovement.com