C40 Data Protection Policy

Table of Contents

Introduction

Scope

- Personal Data is any information about an Individual that can be linked to them, such as name, personal details, photos or even comments.
- All C40 Staff must understand and follow this policy if working with Personal Data.
- C40 staff must have completed training on this policy before working with Personal Data Training Slides are available here.
- Staff can use this Checklist to make sure they are complying with this policy.

Key Points: Everything you need to know in 10 Points

1. **Lawful Basis:** C40 must only work with Personal Data where we have a **(i) good reason** to do so and a **(ii) lawful basis** for the work.
2. **Special Category Data:** Certain types of Personal Data can cause harm or embarrassment to the individual. Be careful working with Personal Data about political opinions, health, race, trade union membership, health sex life or sexual orientation.
3. **Inform People how we use their Data:** Staff must **(i)** inform individuals how their Personal Data will be used and **(ii)** share the C40 Privacy Notice.
4. **Reduce the Risk of Working with Personal Data:** To reduce the risks when working with Personal Data staff must **(i) minimize the amount of Data** we collect and work with, and **(ii) build privacy controls** into the project.
5. **Data Privacy Impact Assessment:** Where staff are planning to work with Personal Data in a way that is new or risky, or could cause harm to an individual, a Data Privacy Impact Assessment (DPIA) needs to be completed. Contact Legal@c40.org for advice.
6. **Keep Personal Data secure:** Where C40 collects Personal Data, we must keep it **secure** - even if people's names have been removed from the record.
7. **Keep Personal Data accurate:** C40 must record personal data accurately and correct or delete inaccurate data.
8. **Deleting Personal Data:** Records containing personal data should be kept only as long as they are needed and deleted when it isn't necessary any more.
9. **Working with Third Parties:** Any Third Party we share Personal Data with must sign a Data Sharing Agreement.
10. **Data Breaches and Requests:**. All actual, suspected or potential **Data Security breaches** should be reported immediately to legal@c40.org. Also contact legal if anyone questions how we use their data.

1. Lawful Basis

1.1. C40 must only work with Personal Data where we have a (i) good reason to do so and a (ii) lawful basis for the work.

1.2. **Lawful Bases** that C40 can use are:

- Consent
- Legal Requirement
- Contractual Agreement
- Legitimate Interest

1.3. **Consent** is the best lawful basis and the only one that is acceptable for promotional and campaigning activities (e.g. adding someone to your mailing list).

1.4. Consent must be positive and explicit rather than implied and should be able to be withdrawn by at any time.

1.5. If you are relying on Consent as your lawful basis for working with data you must keep a record of that consent.

1.6. If you receive a request to be opted out of being contacted (for example removing them from your mailing list) you should comply with the request immediately - it is best if you can automate this process (for example by including an opt-out button.)

1.7. If you are relying on consent as your reason for working with Personal Data and want to use that data in a different way you will need to get people to consent to any new use of their information.

1.8. Alternatively, you may be able to rely on **Legitimate Interest** as a lawful basis. This applies when the data processing 1) carries little risk of infringing on the privacy of individuals and when it 2) is conducted in a way they should reasonably expect.

1.9. If you are unsure whether you have a Legitimate Interest basis for using Personal Data, you can complete a Legitimate Interest Checklist and keep it on file in case of any questions.

1.10. Contact legal@c40.org if you have any questions on completing the Legitimate Interest Checklist.

1.11. If you are working with Special Category Data you will find it harder to establish legitimate interest and it would be better to rely on consent.

Example:

❓ Mohinder is running an event. He receives City Officials' IDs and their consent to use them for registration. His manager suggests keeping them for future events.

✔ Even if Mohinder obtained the attendees' consent to collect and process their IDs, keeping them for the future is a different purpose. Mohinder should delete the IDs rather than keep them.

2. Special Category Data

2.1. Certain types of Personal Data can cause harm or embarrassment to the individual.

2.2. You should be especially careful when working with Personal Data about:

- Political opinions
- Religious beliefs
- Race or ethnic origin
- Trade union membership
- Genetic or Biometrics
- Health
- Sex life
- Sexual orientation
- Criminal Records

2.3. Work with Special Category Data will usually require a Data Privacy Impact Assessment before it begins. Contact legal@c40.org for support with this process.

2.4. Staff should also be aware of the C40 Safeguarding Policy when gathering information about children and adults at risk.

3. Informing People How We Use Their Data

3.1. When a C40 member of staff works with someone's Personal Data, they need to tell them:

- What information we collect about them
- What their information is used for
- Who we share their personal data with

3.2. You cannot get people's consent to one use of their personal data and then use it for something else without telling them.

3.3. If the Personal Data is collected directly from people, for example via a website form or a paper based form, include a link to the C40 Privacy Notice - which explains how C40 will use their information.

3.4. If the C40 Privacy Notice does not cover your proposed use of the Personal Data this will usually be identified as part of a Data Privacy Impact Assessment - Legal will help you draft a notice as required.

4. Reducing the Risk of Working with Personal Data

4.1. The best way to reduce the risk of working with Personal Data is by minimizing the amount of personal data C40 collects in the first place (‘**Data Minimization’**) and building privacy controls into the project from the start (‘**Privacy by Design’**).

Practical Tips to Build Privacy by Design Principles into Your Project:

- When you are thinking about working with Personal Data, try and find a way to achieve the same goal without collecting Personal Data.
- Never collect Personal Data you do not really need. Only collect the minimum amount necessary to achieve the goal.
- Limit access to any Personal Data to people who really need it.
- Remember, Personal Data is any information that can be linked to an individual. Removing names from a record is not always enough to stop individuals being identified, but it can help.
- A safer way to store records without creating Personal Data risk is to aggregate information so that it covers a range of people rather than any one identifiable individual.

4.2. Keep the reason you collected the Data for under continuous review, and if that purpose no longer exists delete the data in line with Section 8.

4.3. It is never justified to keep personal data forever, if data is more than two to three years old we should delete it unless we can confirm with the original data subject they are still happy for us to keep it.

4.4. It is very easy to collect data for one reason in the first place and then find other uses for it, make sure any data we use is only used for the original purpose - watch out for **‘function creep.’**

4.5. If you have consent to one use of Personal Data, you would need to get a new consent for additional uses.

4.6. Whenever you record personal data about an individual, remember this must be provided to them if they make an access request. To reduce the risk of harm or embarrassment to individuals, always record facts and opinions in a professional manner.

Example:

❓ Yousef is working on a project to reduce health inequities by routing traffic away from low-income neighborhoods. He plans to

survey residents on how busy traffic has impacted their health. He thinks this is probably ok as he won't collect names, only ages and addresses.

✔ Health is special category data so Yousef needs to be very cautious. The age and address of a respondent would allow them to be identified. He can do this project without working with personal data by ensuring that no information he collects is attributable to any one individual - only recording aggregated examples like 'one third of residents reported shortness of breath on busy days.'

5. Data Privacy Impact Assessments

5.1. Where C40 is planning to work with Personal Data in a way that is new or risky, or could cause harm to an individual, a **DPIA** needs to be completed. Contact legal@c40.org for guidance on whether a DPIA is required and support completing the form.

5.2. The DPIA will be kept under review and a timetable for checking progress on mitigation measures will be agreed as part of sign-off.

6. Keeping Personal Data Secure

6.1. When we work with Personal Data we need to make sure it is held securely at all times to avoid unauthorized access to, alteration or loss of Personal Data.

6.2. Staff should not grant third parties access to secure C40 systems containing Personal Data until they have signed a Data Sharing Agreement in line with Working with Third Parties below.

6.3. Staff should never provide Personal Data to anyone - including C40 staff - without checking that they need to access that Data for the original purpose.

6.4. Unauthorized access to C40 Systems or Personal Data Records could be a Data Breach.

Practical Steps you Can Take to Increase Data Security:

- Keep hard copies of data in locked cabinets
- Store electronic data using C40's systems and use the cloud to share data wherever possible.
- Avoid using devices like a USB drive as these can be lost or stolen.
- If we have to use email to send files containing personal data password protect them.
- Send passwords and password protected files in separate emails.

7. Keeping Personal Data Accurate

7.1. If C40 Staff are working with Personal Data they need to take reasonable steps to make sure that the Data is accurate.

7.2. If C40 discovers that Personal Data we hold is wrong, it should be corrected as soon as possible.

7.3. If we have shared the C40 Privacy Notice this should give people options for correcting us if we have made a mistake.

7.4. We cannot use data we know to be inaccurate. If it isn't possible to correct inaccurate data, it must be deleted as soon as possible.

8. Deleting Personal Data

8.1. C40 should keep the Personal Data we hold under continuous review, keep it up to date and delete data we no longer need.

8.2. If the Personal Data is no longer needed for a specific use but there is a legal reason to retain it, then it should be securely archived with access limited to people who need it to ensure legal compliance.

8.3. C40 Staff should be familiar with the Records Retention Policy and follow any requirements on retaining information.

Example:

❓ Aisha keeps a mailing list with contact information that they collected explicit consent for. They have not updated the data in this list for 5 years.

✔ After five years the data in this list is probably out of date. Aisha should assess whether this information is still needed and delete it if it is not. If we do still need it Aisha should take steps to ensure the old information is updated.

9. Working with Third Parties

9.1. When we work with Third Parties - including Member Cities, Suppliers, Grantees, Partners and Funders - we could be responsible for their use of Personal Data.

9.2. Any Third Party who works with Personal Data on our behalf must sign a 'Data Sharing Agreement' - this will describe:

- The approved uses of the Personal Data
- The applicable security measures

9.3. Third Parties can either be 'Data Controller' or 'Data Processors.'

9.4. A Data Controller makes decisions about how Personal Data is used - this will usually be C40.

9.5. A Data Processor works for the Controller and will only work with the Personal Data as they are instructed to by the Data Controller. This will usually be our Suppliers or Grantees.

9.6. The Data Sharing Agreement will make it clear who is the Controller and who is the Processor.

9.7. Data Sharing Agreements are usually between C40 as the Controller and a Supplier as the Processor but can also be between two Controllers - for example where we are co-organising an event.

9.8. If C40 is the Data Processor in the Agreement we must comply with any requirements in the agreement.

9.9. Contact legal@c40.org if you need a Data Sharing Agreement.

10. Data Breaches and Requests

10.1. A Data Breach is the:

- Destruction
- Loss
- Unauthorized Alteration
- Unauthorized Disclosure
- Unauthorized Access

Of Personal Data.

10.2. A data breach may include the loss or destruction of a device containing personal data such as a laptop or mobile phone.

10.3. All actual, suspected or potential Data Breaches or Access Requests must be reported immediately on discovery to legal@c40.org who will assess the applicable local law and how to respond to the request.

10.4. Also contact legal if anyone asks:

- What data we hold about them,
- Why we hold it, or
- Complains about how we use their Personal Data

Example:

❓ Sinead receives an email from an individual who previously worked for a C40 Supplier. They ask for a copy of all the information C40 holds on her client including where he is mentioned in emails and online chats between the C40 and his employer.

✔ Sinead should not respond to the email but note the date of the request and forward it to legal@c40.org for advice. Sinead should not delete the data.

Annex 1: Checklist for Staff Working with Personal Data

Can you do this WITHOUT COLLECTING PERSONAL DATA?	
What is your LAWFUL BASIS for using this data?	
How do we make sure the DATA IS ACCURATE?	
For HOW LONG do you need TO RETAIN the data?	
HOW will you check the PURPOSE STILL EXISTS?	
How will you PREVENT FUNCTION CREEP?	
How will you MINIMIZE DATA COLLECTION?	
Where will the DATA BE STORED?	
Is Hard Copy Data LOCKED AWAY?	
Will Electronic Copies be PASSWORD PROTECTED?	
Will Passwords and Links be SENT SEPARATELY?	
Will users USE THE CLOUD rather than Downloading?	
How will we make PROCESSORS AWARE of their obligations?	
Will you have A DATA SHARING AGREEMENT with any third parties?	

Annexe 2: Records Retention

C40 is committed to ensuring we keep the necessary records to comply with our legal, tax, and auditing requirements and to meet our operational and organizational needs.

General principles:

- Records containing Personal Data should be stored securely, kept up to date and deleted when no longer needed in line with *Sections 6-8* of the Data Protection Policy.
- If records containing Personal Data do not need to be accessible on a daily basis, Staff should archive them in a way that means they cannot be immediately accessed going forward.
- Data subjects have the right to revoke their consent at any time. Once consent has been withdrawn, Staff should delete the data in question as soon as possible - unless it can be processed on another legal ground (e.g. if necessary to fulfill a contract).

Retention periods:

- Records containing personal data older than **5 years** should automatically be deleted, with the following exceptions:
    - HR records such as personnel files, termination of employment and redundancy information will be kept for **7 years** and retirement and pension records will be kept for **12 years**.
    - All Zoom cloud recordings, Slack messages, or emails older than **5 years** are automatically deleted unless otherwise agreed with C40 IT.

The above retention periods may be revisited if there is an ongoing rationale to retain records for longer, e.g. in case of any investigation, audit, claim, litigation or as otherwise deemed appropriate for continuous use.