Data Protection Policy

C40.SOP/OPS/001, Issue 1 - April 2018

Table of Contents

1. Introduction

This document sets out C40 policy regarding data protection in respect of all Personal Data held or otherwise processed by C40, such as the Personal Data of city mayors and their teams, staff, funders, suppliers or any others, whose data C40 controls. This policy, as a global policy, identifies the obligations imposed on C40 by the General Data Protection Regulation ("GDPR") in respect of the Processing of Data Subjects' Personal Data. This policy is in addition to other requirements which may be necessary for specific operations, or relevant local data protection laws.

If any individual feels uncomfortable or unsure about anything in this policy or related to data protection at C40, they should contact C40's Director of Corporate Services.

Please familiarise yourself with the important definitions in Appendix 1.

2. Responsibilities

Ultimate responsibility for data protection compliance lies with C40's Directors. Day-to-day responsibility for administration and compliance is delegated to the Director of Corporate Services.

All employees and Directors of C40 have a duty to observe the principles of GDPR and the procedures referred to in this document and to comply fully with this policy and the principles of GDPR.

Disciplinary action may be taken against any employee who breaches any of the instructions or procedures set out in this policy. Most individuals will handle Personal Data in the course of their work, even indirectly. For example, unauthorised disclosure of data might occur by passing

information over the telephone, communicating information contained on a computer print-out or even inadvertently by reading a computer.

3. What is data protection and how does it apply to C40?

The basic principles of the GDPR are designed to:

- Safeguard the handling and use of personal information;
- Protect individuals' data protection and privacy rights over their personal information; and
- Enable organisations, such as C40, to legitimately use personal information to operate its business.

C40 needs to process certain Personal Data in relation to the people and organisations that we work with when carrying out our activities to enable us to, amongst other things:

- Carry out and promote our educational and charitable mission;
- Monitor and evaluate our reach and impact;
- Hold C40 events and facilitate participation by arranging flights and travel accommodations for attendees;
- Keep and update a relationship database consisting of partner and city contacts;
- Inform others of the work we are doing that may benefit them; and
- In respect of C40 staff and directors and volunteers' data, process data in the course of the employment or director or volunteer relationship (e.g. recruitment, training, promotion, payroll, employee benefits, disciplinary and grievance, retirement, provision of a reference).

C40 recognises the importance of the correct and lawful treatment of Personal Data and that the failure to do so can cause real harm and distress to the individual to whom the information relates and also cause harm to C40's reputation and trust. A breach of GDPR can also lead to regulatory sanctions being imposed on C40, such as a fine.

4. When does GDPR Apply?

GDPR applies whenever there is Processing of Personal Data belonging to a Data Subject in the European Union or the United Kingdom, or in the context of the activities of a Controller or Processor in the EU or UK (e.g. C40 UK) regardless of where the Processing takes place.

Whilst GDPR governs the Processing of Personal Data for Data Subjects within (or in the context of an organisation within) the European Union and the United Kingdom, this policy will govern how C40 treats ALL Personal Data, to ensure a consistent framework and standard of compliance. Where Personal Data does not fall under the jurisdiction of GDPR and this policy calls for the involvement of a Supervisory Authority or other GDPR specific measure, the Director of Corporate Services will be responsible for determining the most appropriate course of action, taking into account local data protection legislation, where necessary.

4.1 When does GDPR Apply?

C40 must comply with the data protection principles listed under the GDPR, which require that Personal Data shall be:

a) Processed fairly, lawfully and in a transparent manner (lawfulness, fairness and transparency)

The first data protection principle requires that Personal Data is obtained fairly and lawfully and Processed for purposes that the Data Subject has been informed of.

Legal basis

Processing will only be lawful where C40 can rely on at least one of the following lawful bases for each instance of Processing:

- The Data Subject has given Consent;
- The Processing is necessary to perform a contract with the Data Subject;
- The Processing is necessary to comply with a legal obligation on C40 (under EU or Member State law only);
- The Processing is necessary to protect the "vital interests" of a Data Subject – vital interests means essential for the Data Subject's life and so is likely to be relevant only in emergency medical situations;
- The Processing is necessary for the performance of a task carried out in the public interest – this is unlikely to apply to the day-to-day work of C40;
- The processing is necessary for the purposes of C40, or a third party's, legitimate interests – provided those interests are not overridden by the interests or rights and freedoms of the Data Subject.

Most of the Processing C40 undertakes will be on the basis of legitimate interests. This requires C40 to balance our interest against the rights of the individual, taking into account their reasonable expectations as to how their Personal Data will be Processed. For Processing that is particularly intrusive or unexpected, this may not be lawful.

In some cases, particularly where we are communicating with Data Subjects electronically, C40 may specifically require Consent.

Transparency

To ensure transparency, C40 will provide all Data Subjects whose data it receives with "fair processing information" through a Privacy Notice. The Privacy Notice will include the following, and be provided in the following timescales where possible:

To do this, C40 will provide all Data Subjects whose data it receives with "fair processing information" through a Privacy Notice. The Privacy Notice will include the following:

	Where Personal Data obtained directly from Data Subject	**Where Personal Data obtained from other sources.**
What information must be supplied	**Not required when the Data Subject has the information.**	**Not required when the Data Subject has the information. Not required when derogations in article 14(5)(b) to (d) apply.**
C40's contact details (e.g. privacy@c40.org)	x	x

The Purposes and the legal basis for the Processing	x	x
Legitimate interests of the C40 or third party, where applicable	x	x
Categories of Personal Data		x
Any recipient or categories of recipients of the Personal Data	x	x
Details of transfers to third country and safeguards	x	x
Retention period or criteria used to determine the retention period	x	x
The existence of each of Data Subject's rights	x	x
The right to withdraw Consent at any time, where relevant	x	x
The right to lodge a complaint with a supervisory authority	x	x
The source the Personal Data originates from and whether it came from publicly accessible sources		x
Whether the provision of Personal Data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the Personal Data	x	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	x	x
When should information be provided?	At the time the Personal Data are obtained	Within a reasonable period of having obtained the Personal Data (and latest within one month) If the data re used to communicate with the individual, at the latest, when the first communication takes place; or I disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

Additionally, C40 seeks to ensure that it has legitimate reasons for using the Data Subject's information and that the use of such information is in line with what that person would expect.

a) Obtained for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes (purpose limitation)

C40 must process Personal Data in a way which is compatible with the original purposes for which the data was obtained and was notified to the Data Subject (i.e. these should be the purposes contained in the Privacy Notice). If it becomes necessary to Process Personal Data for a new (incompatible) purpose, the Data Subject should be informed beforehand.

b) Adequate, relevant and limited to what is necessary for those purposes (data minimization)

C40 seeks to ensure that the volume and extent of the Personal Data it holds on a Data Subject is the minimum amount of data required for the specific purpose(s) for which is it Processed and which have been notified to the Data Subject.

c) Accurate and kept up to date (accuracy)

Reasonable steps are to be taken to ensure the accuracy of Personal Data. The Privacy Notice shall set out means for Data Subjects to request this. If Personal Data is found to be inaccurate, it is to be corrected or deleted.

d) Kept for no longer than is necessary for those purposes (storage limitation)

C40 will review the nature of the information being collected and held on an annual basis to ensure there is a valid business reason for requiring the information to be retained. C40 takes steps to remove Personal Data that is no longer needed for the purposes for which it was obtained. Out of date data or any information deemed unnecessary may be destroyed (or in some cases, archived).

e) Kept secure

C40 will put in place adequate procedures and technological measures to prevent unauthorised or unlawful Processing of Personal Data and to prevent accidental loss, destruction or damage. All Personal Data is stored in secured and encrypted systems. C40 takes reasonable and proportionate steps to ensure that:

- Unauthorised access to systems containing Personal Data is prevented;
- Any doubt about a person's authorisation to be in any of C40 workplaces is reported;
- Computers and phones are password protected and encrypted;
- Data is exchanged securely;
- Personal Data is not disclosed either orally or in writing or otherwise to any unauthorised third party; and
- All relevant IT policies or other local security policies (which will contain more detailed requirements to assist C40 in satisfying these obligations) are followed.

The following, whilst not principles, are also important obligations under the GDPR:

f) Personal Data shall not be transferred to countries or territories outside the European Economic Area ("EEA") without adequate protection

C40 may only transfer Personal Data to countries which are outside of the European Economic Area, provided that one of the following conditions applies:

- The country to which the Personal Data is transferred has been determined by the European Commission to ensure an adequate level of protection for the Data Subject's rights and freedoms (known as "white listed countries")1;
- The Data Subject has given their Consent to the transfer;
- The transfer is necessary (this is a high bar) for one of the reasons set out in GDPR, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject;
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;
- The transfer is to an organisation in the US which is approved under the EU-US Privacy Shield framework;
- We have entered into a European Commission-approved contract with the third party.
- The transfer is authorised by the relevant data protection authority (for instance in the UK, this would be the Information Commissioner's Office (ICO)) where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

g) Processed in accordance with the Data Subject's rights

Personal Data will be Processed in accordance with an individual's rights under GDPR. GDPR gives Data Subjects specific rights which they may seek to exercise in relation to their Personal Data that C40 controls. This means that C40 will consider each reasonable request of an individual to access, rectify, erase, stop Processing, port out, object to the Processing of, their Personal Data, under a "Data Subject access request"; and C40, where appropriate, will provide individuals with the opportunity to express preferences relating to receiving marketing material and will honour those preferences. Those rights are expanded on in Appendix 2

.

All requests will be responded to within one month of its receipt except in exceptional circumstances.

GDPR imposes specific obligations in respect of 'automated decision making', including automated profiling. C40 does not currently engage in this kind of activity. If C40 engages in automated decision making and profiling, it will do so in accordance with GDPR guidelines and requirements.

5. Access to Personal Data

GDPR gives individuals specific rights. In particular all Data Subjects have the right (known as "subject access rights") under GDPR on request to be:

- Told whether any of their Personal Data is being processed; and, if so

- Given a description of the Personal Data, the reasons why it is being processed and whether it will be given to any third party organisation or other person/s;
- Given a copy of the Personal Data (subject to certain exceptions and redaction under GDPR, such as to comply with C40's GDPR obligations to other Data Subjects whose Personal Data might be included);
- Other supplementary information;
- Given details of the source of the data if available.

A Data Subject may exercise these rights by making a valid request in writing. All such requests should be directed or promptly forwarded to privacy@c40.org.

C40 will validate the identity of the requester using reasonable means.

C40 will aim to comply with any subject access request as quickly as possible, but must ensure that it is provided within one month of a written request. If a request is complex or numerous, the access request may be completed in two months, so long as the Data Subject is made aware of the delay within the initial one month response period.

C40 will not charge Data Subjects for access request, unless a request is determined to be manifestly unfounded, excessive or repetitive, at which point, a reasonable fee may be charged or we may refuse the request.

If a request is denied on such grounds, C40 will inform the Data Subject of the reason for the denial and inform them of their right to complain to a Supervisory Authority.

6. Sensitive Personal Data

Special rules apply to the Processing of Sensitive Personal Data.

In most cases, in order to process Sensitive Personal Data, we must obtain explicit Consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use it.

It is not always necessary to obtain explicit Consent. There are a limited number of other circumstances in which GDPR permits organisations to process sensitive Personal Data. If you are concerned that you are Processing Sensitive Personal Data and are not able to obtain explicit Consent for the Processing, please speak to the Director of Corporate Services.

7. Disclosure of Personal Data

7.1 Sharing with Data Processors

C40 is required to take particular security precautions when it uses third parties to Process Personal Data on its behalf (for example, IT contractors, providers of web hosting services, professional fundraisers, payroll providers or other outsourced service providers).

- These third parties are data Processors. Staff who are responsible for the selection or appointment of data Processors must:

- select only Data Processors who provide sufficient guarantees in respect of the technical and organisational security measures they will use in relation to the Processing of Personal Data (i.e. we undertake proportionate due diligence);
- ensure that C40 enters into a written contract with each data processor before the Processing actually begins (see Section 9 below for what those contracts must contain);
- where the data Processor is located outside the EEA, consider the restrictions to transfer personal data internationally (set out above);
- in particular, each data Processing contract will make it clear that data Processors must only act on instructions from C40. The law makes C40 responsible as Controller for the Processing of all Personal Data, even if it is carried out on its behalf by a data Processor. It must, therefore, maintain control over such Processing at all times, and such instructions must be documented.

Personal Data may only be disclosed outside of C40 to a third party Controller (i.e. another organisation which may use the Personal Data for its own purposes, as opposed to a Processor that will carry out the purposes of C40) when we are legally able to do so (for example, where we have the Consent of the Data Subject, or where subject to a legal obligation to which we are subject such as reporting to regulators). C40 will occasionally share anonymised information with our funders (for reporting purposes) and with other agencies that we consider might benefit our work. GDPR does not apply to data which is sufficiently anonymised, as it will no longer be Personal Data (i.e. it will no longer be possible to identify an individual from the data).

8. Contracts

Where C40 uses a third-party Processor, it will require that a contract be signed that requires the Processor (amongst other things, and as a minimum) to:

- only act on the documented instructions of the Controller;
- ensure that people Processing the data (e.g. its staff) are subject to a duty of confidence;
- take appropriate measures to ensure the security of Processing and of the data;
- only engage sub-processors with the prior consent of the Controller and where it does so, under a written contract containing the same data protection obligations as set out in the principal contract – with the Processor remaining fully liable to the Controller for the performance of the sub-processors' obligations;
- assist the Controller in providing subject access and allowing Data Subjects to exercise their rights under the GDPR;
- assist the Controller in meeting its GDPR obligations in relation to the security of Processing, the notification of Data Breaches and data protection impact assessments;
- delete or return (at the Controller's option) all Personal Data to the Controller at the end of the contract or the Processing; and
- submit to audits and inspections, provide the Controller with whatever information it needs to ensure that they are both meeting their Article 28 GDPR obligations, and tell the Controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

9. Privacy by Design

Privacy by design is the concept of taking an approach to projects/ systems to ensure that data privacy compliance is built-in from the start. Where appropriate and proportionate, C40 will ensure data privacy by design by requiring it to be factored into internal processes and programme design wherever C40 will act as a Controller.

10. Accountability

C40 must be accountable and able to demonstrate its compliance with GDPR principles at all times.

C40 must keep a record of the following and keep that record up to date:

- are not occasional (e.g., are more than just a one-off occurrence or something done rarely); or
- are likely to result in a risk to the rights and freedoms of individuals (e.g., something that might be intrusive or adversely affect individuals); or

involve special category data or criminal conviction and offence data (as defined by Articles 9 and 10 of the GDPR). In addition, the following must be documented:

- Data Protection Impact Assessments
- Data Breach investigations; and
- Where we Process on the basis of Consent, those Consents shall be documented (so that we can evidence the Consent if challenged).

11. Data Protection Impact Assessment

A data protection impact assessment ("DPIA") must be done where we have identified or suspect that proposed data Processing is likely to result in a High Risk to Data Subjects.

If a DPIA indicates that a Processing activity is High Risk, then it will take appropriate measures to mitigate the Processing risk. If the risk cannot be mitigated, then C40 will contact the appropriate local Supervisory Authority to seek advice/ authorisation on how to proceed.

C40 will always carry out a DPIA if it plans to do the following and this might result in a High Risk:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- Process special category data or criminal offence data on a large scale;
- Systematically monitor Data Subjects on a large scale;
- Use new technologies which may have an impact on privacy;
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- Carry out profiling on a large scale;
- Process biometric or genetic data;
- Combine, compare or match data from multiple sources;
- Process Personal Data without providing a privacy notice directly to the individual.
- Process Personal Data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's Personal Data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process Personal Data which could result in a risk of physical harm in the event of a Data Breach.

C40 will consider carrying out a DPIA if it plans to carry out any other:

- Evaluation or scoring;
- Automated decision-making with significant effects;
- Systematic Processing of sensitive data or data of a highly personal nature;

- Processing on a large scale that is not usual to the work and activities of C40;
- Processing of Personal Data concerning vulnerable Data Subjects;
- Innovative technological or organisational solutions;
- Processing involving preventing Data Subjects from exercising a right or using a service or contract.

12. Data Breaches

At all times, C40 will maintain systems to detect Data Breaches and maintain investigation and internal reporting procedures.

If a Data Breach has been identified, in tandem with ensuring the Data Breach is contained and its effects (including on the business) are mitigated, C40 will investigate the Data Breach and determine the likelihood and severity of the risk to the affected Data Subject's rights and freedoms, under GDPR.

If a Data Breach investigation determines that it is unlikely the affected Data Subjects will be at risk, then the decision not to report the incident and its justification will be documented.

If the investigation determines the affected Data Subjects are likely to be at risk it will report it the appropriate Supervisory Authority (e.g. the ICO) within 72 hours after becoming aware of the Data Breach. If more than 72 hours is needed to investigate the Breach, the Director of Corporate Services will notify the appropriate Supervisory Authority with an interim report based on the current information, and explaining the cause for the delay. The following information will be provided to the Supervisory Authority:

- a description of the nature of the Data Breach including, where possible:
  - the categories and approximate number of individuals concerned;
  - the categories and approximate number of Personal Data records concerned;
  - the name and contact details of the Director of Corporate Services;
- a description of the likely consequences of the Data Breach; and
- a description of the measures taken, or proposed to be taken, to deal with the Data Breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If the Data Breach investigation determines that affected Data Subjects' rights and freedoms are at High Risk, then C40 will inform the affected Data Subjects as soon as possible in order that they may take measures to protect themselves from the effects of the Data Breach. The following information will be provided to the affected Data Subjects:

- the name and contact details of our Director of Corporate Services;
- a description of the likely consequences of the Data Breach; and
- a description of the measures taken, or proposed to be taken, to deal with the Data Breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects (including any appropriate advice to the Data Subjects to, for example, change passwords).

All incidents and investigations of a Breach will be documented. The documentation for each investigation will include the facts of, effects, and actions taken regarding the Data Breach.

13. Monitoring and Review of This Policy

This policy is reviewed periodically by the Directors of the Boards to ensure that it is achieving its objectives and may be amended from time to time.

This policy was adopted by the Directors of the Boards on: April 2018. This policy will next be reviewed by: April 2019

[1] At May 2018, this includes Andorra, Argentina Canada (commercial organisations only), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.