COMPANY OF OTHERS

Data Protection Policy

Date October 2024

To be reviewed and updated: October 2025

COMPANY OF OTHERS

Contents

COMPANY OF OTHERS

Principles of the UK GDPR

This policy is in place to ensure that the Company of Others Board of Trustees and Staff comply with the following core principles of the UK GDPR at all times. Article 5 of the UK GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

COMPANY OF OTHERS

Summary

Company of Others is committed to operating as a transparent and accountable organisation at all times and is directly informed by the UK GDPR. This policy applies to all staff and the Board of Trustees.

Data Capture and Protection Policy

Company of Others is committed to protecting all personal information that we collect, being transparent about what data we hold and giving people control over how we use it.

Applicable data

For the purpose of this policy 'personal data' means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised, for example key-coded, can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The UK GDPR refers to sensitive personal data as “special categories of personal data”. The special categories specifically include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

COMPANY OF OTHERS

Accountability

The accountability principle in Article 5(2) requires Company of Others to demonstrate compliance with the principles and states explicitly that this is the company's responsibility.

Bases for collection and storage of personal information

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these bases must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for CoO to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract CoO has with the individual, or because they have asked CoO to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for CoO to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for CoO to perform a task in the public interest or for COO's official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for CoO's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Before we collect and store personal information we will consider the following checklist:

Lawfulness

☐ We have identified an appropriate lawful basis (or bases) for our processing.

☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.

☐ We don't do anything generally unlawful with personal data.

COMPANY OF OTHERS

Fairness

☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.

☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.

☐ We do not deceive or mislead people when we collect their personal data.

Transparency

☐ We are open and honest, and comply with the transparency obligations of the right to be informed.

Requests for personal information

In line with the UK GDPR requests for personal information (SARs) will be responded to within 30 calendar days of the request. No fee will apply for this information.

Consent

Consent must be freely given and must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Company of Others will also check that consent is the most appropriate lawful basis for processing.

Gaining consent:

- We will not use pre-ticked boxes, opt-out boxes or other default settings
- Our consent requests will be kept separate from our other terms and conditions
- Withdrawal of consent will be simple and easy to do
- We ensure that individuals can refuse to consent without detriment.
- Clearly name any third-party controllers who will rely on the consent.

Recording of consent

- We keep a record of when and how we got consent from the individual.
- We keep a record of exactly what they were told at the time

COMPANY OF OTHERS

Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed.
- We have processes in place to refresh consent at appropriate intervals, including any parental consents.
- We consider using privacy dashboards or other preference-management tools as a matter of good practice.
- We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
- We act on withdrawals of consent as soon as we can.
- We don't penalise individuals who wish to withdraw consent.

Data relating to Children

Children must be provided with the same information about what happens with their personal data as adults. However, when relying on the consent of their Parent/Guardian/Carer/responsible adult in terms of ensuring that the consent is informed, it is the Parent/Guardian/Carer/responsible adult rather than the child who needs to understand what they are consenting to. However, Company of Other recognises that children do not lose their rights as data subjects to transparency just because consent has been given by an adult. Company of Others will therefore give both the adult and the child clear and accessible privacy information by producing accessible information relevant to both parties.

Third parties

Company of Others will ensure that third parties are named clearly when collecting personal data and requesting consent. Company of Others will carefully consider why the third party wants the information, whether they actually need it, and what they will do with it and will be able to demonstrate that the disclosure is justified. However, Company of Others recognises that it will be the responsibility of the third party to determine their lawful basis for their own processing.

COMPANY OF OTHERS

Personal data stored outside of the UK

Company of Others may use programs or applications that are based and store personal information outside of the UK, for example Patreon and Mailchimp which are both based in the USA. To ensure the security of any data stored outside of the UK we only used companies that comply with the UK GDPR (Patreon and Mailchimp).

Keeping personal data secure

- Paper files will be kept in locked cabinets or locked offices when not being used and stored securely at the end of the day – not left on desks.
- Offices will be locked when left unattended (during meetings and lunch breaks).
- Staff will always log off computers when away from them.
- Password protection will be used for any electronic files/documents containing sensitive personal data.
- Particular care will be taken when transferring personal data onto a memory stick, laptop or any other mobile device – using password protection and encryption where appropriate.
- If CoO ever needs to include sensitive personal data in an email password protection or encryption will be used where appropriate.
- Staff should only use company laptops and phones for work that includes any personal data and all devices must be password protected.
- Never leave devices unattended and store laptops/devices in a secure place (whether you are working on our premises, at home or if travelling). If you are in a public space, do not have personal data visible on your screen or on paperwork.
- Do not write login details or passwords down or store them with your devices.
- Only share personal data with people who really need it (on a need to know basis) and only share the minimum data they need.

The disposal of data

Personal data will not be stored for longer than is necessary. Our standard data retention period will be 6 months following the end of a project, unless retention is specifically required for longer by a grant funder.

Hard copies of personal data will be shredded using a professional and secure shredding company or in house with a UK GDPR compliant shredder.

All data sources of electronic copies of personal data will be identified including on hard drives, individual computers and iCloud storage. Once identified the data will be disposed of permanently.

ICO Notification

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission

When a breach of personal or sensitive data is identified the individual(s) concerned must be **notified within 72 hours**. Notification will include the nature of the personal data breach and:

- the name and contact details of the Operations & Resource Lead (Emma Whitenstall) where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

We will also identify the likelihood and severity of the resulting risk to the individual(s) rights and freedoms. If there will be a risk, we will notify the ICO; if it's unlikely there is a risk, we do not need to report the ICO, however CoO must be able to justify this decision, so documentation of the breach and justification for not notifying the ICO must be made.

The cause of the data breach will be investigated as soon as possible and contained to prevent any further data breaches. We will also determine how a recurrence can be prevented, for example through better processes or further training.

Records will be kept of all personal data breaches.

All data breach investigations and actions will be led by the Operations & Resource Lead, Emma Whitenstall.

Compliance with the UK GDPR

Company of Others will:

- implement appropriate technical and organisational measures that ensure and demonstrate that we comply. Including staff training when appropriate, internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - data minimisation;
    - pseudonymisation;
    - transparency;
    - allowing individuals to monitor processing; and
    - creating and improving security features on an ongoing basis.
    - use data protection impact assessments where appropriate.

COMPANY OF OTHERS

Personal Data collection and storage checklist

☐ We know what personal data we hold and why we need it.
☐ We carefully consider and can justify how long we keep personal data.
☐ We have a policy with standard retention periods where possible, in line with documentation obligations.
☐ We regularly review our information and erase or anonymise personal data when we no longer need it.
☐ We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.
☐ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Cyber Security Measures

To ensure the safety of our data, Company of Others staff will take the following cyber security measures:

- Block, report and delete any suspicious email, do not click on links
- Change Passwords regularly
- Use a Password Manager to create and save strong passwords
- Set Up Multi-Factor Authentication where possible
- Do not share bank card details – different cards are assigned for different budget holders
- Keep Operating Systems up to date
- Only share login details to online platforms/accounts with those who really need access
- Avoid unknown websites
- Ensure anti-virus or malware installed on all company devices
- Keep all company related information on business laptops and mobile devices only

COMPANY OF OTHERS

- Ensure all company devices are secured with password protection
- Ensure company wifi is password protected

Policy Date

This policy was agreed in December 2021 and will be reviewed annually or when there are substantial organisational changes/changes in legislation.

Policy review date: 21 October 2024

Signed:

Chair of the Board – Hilary Knight

Signed:

CEO & Artistic Director – Nadia Iftkhar

Date: 21 October 2024