Phone Credit for Refugees
Data Protection Policy Statement

Introduction

Phone Credit for Refugees (PC4R) has a legal requirement to comply with the requirements of the General Data Protection Regulation (GDPR) as a data controller. We'll follow procedures that aim to ensure that all volunteers who have access to personal data held by PC4R are fully aware of and abide by their duties under the GDPR.

Responsibilities

All volunteers must comply with this policy and with the related policies outlined in this document.

Data Protection Principles

PC4R needs to collect and use personal information in order to operate and carry out its functions. This personal information must be handled and dealt with in accordance with the principles below.

PC4R shall ensure that personal data is:

1. Processed fairly and lawfully and, in particular, not process data unless these principles and the rules set out here are followed
2. Obtained only for specified and lawful purposes, and not processed in any manner incompatible with that purpose or those purposes
3. Adequate, relevant and not excessive
4. Processed for a specific purpose or purposes
5. Accurate and up to date
6. Kept for no longer than is necessary (See Data Retention Policy)
7. Processed in accordance with the rights of data subjects under the General Data Protection Regulation (GDPR)
8. Take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage.

9 Not transferred to another country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What is Data Protection?

The GDPR aims to protect individual's fundamental rights and freedoms, notably privacy rights, in respect of personal data processing.

The GDPR applies to paper and electronic records that contain personal data, meaning data that relates to living individuals who can be identified from the data.

Data protection operates by giving individuals the right to gain access to their personal data. This is done by making a subject access request in which they are entitled to:

- a description of their personal data
- the purposes for which they are being processed
- details of whom they are or may be disclosed to

For more information, please refer to our Subject Access Request policy.

Individuals can also prevent processing of their data in certain circumstances. This includes:

- opting-out of having their data used for direct marketing and automated decision making processes
- applying to the courts for inaccurate data to be corrected
- applying to the courts to claim compensation for damage and distress caused as a result of any data protection breach
- opting-out of using our services

Data Protection Officer

The Data Protection Officer (DPO) is responsible for ensuring that PC4R meets its legal obligations. The DPO is responsible for:

- keeping the Board of Trustees updated about GDPR responsibilities, risks and issues
- Develop, implement and review the organisation’s Data Protection Policy.
- Advising on best practice
- Advising and working with volunteers to ensure everyone is compliant with GDPR

- Overseeing all requests for information from data subjects including subject access requests

Data Controllers

PC4R is a data controller. This is defined as: *any person (or organisation) who (either alone, jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.*

Data Subjects

Any living individual who can be identified, directly or indirectly, via an identifier such as name, address or email. For PC4R this may include any of the following:

- Service users
- Volunteers
- Correspondents and enquirers
- Donors

Data Classes

Data classes are the types of data which are being processed, such as:

- Personal Details
- Financial transactions
- Goods or services provided
- Correspondences

Recipients

Recipients are individuals or Organisations to whom PC4R may wish to disclose data. This list does not include any person to whom PC4R as a data controller may be required by law to disclose in any particular case, for example if required by the police under a warrant.

This list should not be read as a list of those to whom data ***will*** be disclosed - PC4R is required to make clear all of the possible categories of 'recipient' to which they might need or wish to disclose data.

- Data subjects themselves
- Current volunteers
- Healthcare, social and welfare advisors or practitioners
- Vendors or technical partners

Purposes

The purposes to which PC4R as a Data Controller may put the data held are described here. This list does not represent the purposes to which all data held will always be put to.

PC4R holds a wide range of data types relating to diverse data subjects. At various times the data held in respect of these subjects may be used in relation to some or all of the following purposes:

Accounting and auditing

The provision of accounting and related services; the provision of an audit where such an audit is required by statute.

Administration of complaints processes

The administration of complaint and grievance processes of all kinds, including professional disciplinary processes.

Administration of data relevant to volunteering roles

Internal administration of data relevant to volunteering roles

Advertising marketing and public relations for others

Public relations work, advertising and marketing

Quality Assurance

Ensuring donations are dispersed fairly and equally in line with our rules

Safeguarding

To alert the relevant health or social care authorities if someone is at risk

To provide services

Assessing eligibility for our services, providing top-ups, running our online shop, or responding to requests or queries

Data storage

All data must be kept securely, and where data is stored electronically, it must be stored in a GDPR compliant database. Please see our Data storage policy for more more information.

Duration of data retention

As a data controller PC4R will not hold data for longer than two years. For further information please refer to our data retention policy.

Sensitive personal data

PC4R will comply with the terms of the GDPR when handling sensitive personal data. The GDPR refers to sensitive personal data as “special categories of personal data”.

Security

PC4R will respect confidentiality and will keep information confidential. We store it securely and control who has access to it.

We will only share such information as necessary, and where we are satisfied that a third party is entitled to receive it and they will keep the information confidential and secure.

Other relevant documents related to this policy

Subject Access Request
Data Retention
Data Breach Reporting
Data Protection

Review of this Policy

This policy will be reviewed annually by the Board of Trustees.