Policies and Procedures

Data Protection Policy

Refugee and Migrant Forum of Essex and London

Responsible Officer:	*James Tullett*
Latest Update:	*March 2019*
Review Date:	*March 2021*
Approval:	*JT*

1. Introduction & Background

RAMFEL is committed to compliance with all national UK laws in respect of personal data, and to protecting the rights and privacy of individuals whose information the organisation collects in accordance with the General Data Protection Regulation and Data Protection Act 2018. The purpose of the Data Protection Legislation is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge.

This Data Protection Policy is designed to ensure that Ramfel complies fully with Data Protection Legislation and that personal data is fairly, lawfully and transparently processed.

RAMFEL is registered with the Information Commissioner's Office.

2. Scope

The Data Protection Legislation applies to all personal data throughout its lifespan, from the point of collection to its eventual destruction. Personal data includes any piece of information which enables the identification of a living individual, such as a name, contact details and/or images/recordings. For the purposes of this Policy, references to personal data shall include sensitive personal data such as information about an individual's health, ethnic origin, sexuality or criminal offences.

The format in which the information is held is in most instances not relevant. If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by the Data Protection Legislation.

The Policy applies to all staff and volunteers of the organisation and third party contractors. You should familiarise yourself with this Policy, the Confidentiality Policy and Ramfel's other policies and comply with their terms when processing personal data on our behalf.

3. Purpose and aims of this Policy

To protect the rights and privacy of living individuals who access RAMFEL services, work for, or support RAMFEL. To ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

4. Policy Statement

When processing personal data in the context of your work with us, you must comply with the six principles of good practice identified in Article 5 of the GDPR. They say the following:

1. **Lawfulness & Fairness:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;

2. **Purpose Limitation:** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

3. **Data Minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date;

5. **Storage Limitation:** Personal data shall be 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; and

6. **Security:** Personal data shall be processed in a manner that ensures appropriate security of the personal data.

In simple terms, this means we must collect and use personal data fairly, tell people how we will use their personal data, store it safely and securely and not disclose it unlawfully to third parties. We need to be careful that the information we collect is relevant and that we do not collect more information than we need for the stated purpose.

There are restrictions on the transfer of personal data outside the EEA and information should not be transferred outside of the UK unless it meets the requirements of the Data Protection Legislation.

Partners and any third parties working with or for the organisation, and who have or may have access to personal data, will be expected to comply with the principles of this Policy and this should be agreed in writing before any personal information is shared.

4.1 Data Collection

In order to process personal data, there mu Under the GDPR there are 6 lawful bases for processing non-sensitive personal data as follows;

1. Consent (which must be informed and can be withdrawn)
2. Necessary as part of a contract (e.g. processing data about employees)
3. To comply with a legal obligation (e.g. processing Gift Aid)
4. To protect the vital interests of an individual (e.g. where someone is at risk in a safeguarding situation)
5. To fulfil a public task (unlikely to be relevant)
6. As part of the organisation's legitimate interests (provided the latter is balanced against the rights of the individual).

Stricter rules apply to sensitive personal data (or special categories of personal data), such as information about a person's race, ethnic origins, religious/political beliefs, health data, disabilities, sexual life, genetics, biometrics or trade union membership as well as information about criminal offences. We can only collect this information where an individual has given their explicit consent or this is necessary to protect their vital interests.

4.2 How does it affect me?

The Charity could be fined if you use or disclose information about other people without their consent or reliance on other lawful grounds. In order to help keep personal data secure, you should take particular care when using the Internet, e-mail and the internal network or talking on mobile or landline telephones. You could be committing an offence if you steal or recklessly misuse personal data.

Any breach of the Data Protection Legislation or this Policy will be dealt with under the Charity’s disciplinary policy and may also be a criminal offence.

4.3 Individuals' Rights

Individuals have the following rights regarding data processing, and the data that is recorded about them:

1. The right to be informed about how we process their personal data
2. The right to access their personal data
3. To right to rectify their personal data
4. To right to have their personal data erased
5. The right to restrict processing
6. The right to have a copy of their personal data
7. The right to object to direct to marketing and profiling
8. Rights in relation to automated decision making and profiling.

If you receive a request, you should inform the CEO immediately as there is a short timeframe to respond (usually within one calendar month). When processing an individual rights request, guidance from the ICO should be reviewed as there are complex exceptions and requirements which must be followed.

Where a person requests access to their information, this is called a data subject access request:
 RAMFEL must usually respond within one month.
 Unintelligible terms must be explained.
 The data must not be changed between receipt of a subject access request and sending the information to the applicant, except for routine amendment of the data which would happen in any case.

4.5 Consent & Transparency
Personal data should not be obtained, held, used or disclosed unless the individual has given consent or there is another lawful basis that allows us to do so. The organisation understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified (by an affirmative action) their freely given agreement preferably in writing, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

All RAMFEL services should display or make available adequate privacy notices to clients explaining how RAMFEL processes their information. We must provide privacy notices even if we do not need to ask for consent.

4.6 Security of Data

All staff are responsible for ensuring that any personal data which the organisation holds and for which they are responsible, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by the organisation to receive that information and has entered into a confidentiality agreement.

You must not remove personal data from RAMFEL’s premises either in electronic or paper form unless it is really necessary – for example, in cases where staff have to attend external meetings, etc. In instances where data is taken out of RAMFEL’s premises, such data must be fully encrypted and password protected. If data is in a paper format, the staff member handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transported and stored securely.

Personal data pertaining to RAMFEL’s beneficiaries should be stored securely on the database or in a locked filing cabinet.

4.7 Disclosure of Data

RAMFEL must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

All third party requests to provide data must be supported by appropriate paperwork and specifically authorised by the CEO or a senior member of staff.

4.8 Retention & Disposal of Data

Personal data should not be retained for longer than is necessary and it must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with RAMFEL's Record Retention Procedure.

Personal data may need to be kept for a certain period of time under other legislation such as accounting or tax laws. In such cases reasonable measures must be taken to ensure it is kept securely in accordance with industry standards.

4.9 Data Protection by Design

Data Protection Impact Assessments (DPIA) must be completed for any significant changes to how personal data is processed at RAMFEL that are likely to result in a high risk to individuals and where any new technologies or systems are used.

4.10 Working with partner organisations

RAMFEL's clients should be informed and give their consent before their personal data is shared with other organisations.

4.11 Personal Data Breaches

If a Personal Information Breach occurs – for example, loss of a memory stick or accidental disclosure of personal data to a third party, this should be reported to the CEO or deputy and immediate steps taken to minimise any potential harm to individuals. Where the breach is likely to result in a risk to individuals, this may need to be reported to the Information Commissioners Office at the soonest possible time and within 72 hours of RAMFEL becoming aware of the breach. If the risk of the breach is high the individuals who are affected must be informed directly and without undue delay.

4.12 Anonymisation

Anonymisation is the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual). Personal data should be anonymised whenever it is practical and appropriate to do so. Anonymised data is not subject to this policy or to data protection legislation.