Barefoot Law

Data Retention Policy

2019

1. Introduction

1.1. This Policy sets out the obligations of BAREFOOTLAW, a non-profit Organization registered in Uganda, whose registered office is at P. O. Box 25431, Plot 1, Muwafu Road, Ministers' Village, Ntinda, Kampala herein after referred to as ("the Organization"), regarding retention of personal data collected, held, and processed by the Organization in accordance with the "DATA PROTECTION AND PRIVACY ACT".

1.2. The Data Protection and Privacy Act defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.3. The Data Protection and Privacy Act also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

1.4. Under the Data Protection and Privacy Act, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and Organizational measures

required by the Data Protection and Privacy Act to protect that data).

1.5. In addition, the Data Protection and Privacy Act includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

1.5.1. Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

1.5.2. When the data subject withdraws their consent;

1.5.3. When the data subject objects to the processing of their personal data and the Organization has no overriding legitimate interest;

1.5.4. When the personal data is processed unlawfully (i.e. in breach of the Data Protection and Privacy Act);

1.5.5. When the personal data has to be erased to comply with a legal obligation; or

1.5.6. Where the personal data is processed for the provision of information society services to a child.

1.6. This Policy sets out the type(s) of personal data held by the Organization by the Information Technology and Digital Strategy Team, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

1.7. For further information on other aspects of data protection and compliance with the Data Protection and Privacy Act, please refer to the Organization's Data Protection Policy.

2. Aims and Objectives

2.1. The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Organization complies fully with its obligations and the rights of data subjects under the Data Protection and Privacy Act.

2.2. In addition to safeguarding the rights of data subjects under the Data Protection and Privacy Act, by ensuring that excessive amounts of data are not retained by the Organization, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1. This Policy applies to all personal data held by the Organization **OR** by the I.T Department & Digital Strategy of the organization **OR** for beneficiaries follow ups, creation of data bases on all cases for further assessment and general data for internal purposes and by third-party data processors processing personal data on the Organization's behalf.

3.2. Personal data, as held by the Organization **OR** the above is stored in the following ways and in the following locations:

3.2.1. The Organization's servers;

3.2.2. Computers permanently located in the Organization's premises at is at P. O. Box 25431, Plot 1, Muwafu Road, Ministers' Village, Ntinda, Kampala;

3.2.3. Laptop computers and other mobile devices provided by the Organization to its employees;

3.2.4. Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Organization's Bring Your Own Device ("BYOD") Policy.

3.2.5. Physical records stored at the Organization's physical office;

4. Data Subject Rights and Data Integrity

4.1. All personal data held by the Organization is held in accordance with the requirements of the Data Protection and Privacy Act and data subjects' rights thereunder, as set out in the Organization's Data Protection Policy.

4.2. Data subjects are kept fully informed of their rights, of what personal data the Organization holds about them, how that personal data is used, and how long the Organization will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.3. Data subjects are given control over their personal data held by the Organization including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Organization's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling , as set out in Parts 14 to 20 of the Organization's Data Protection Policy.

5. Technical and Organizational Data Security Measures

5.1. The following technical measures are in place within the Organization to protect the security of personal data. Please refer to Parts 22 to 26 of the Organization's Data Protection Policy for further details: https://barefootlaw.org/data-policy/

5.1.1. All emails containing personal data must be encrypted;

5.1.2. All emails containing sensitive personal data must be marked "confidential";

5.1.3. Personal data may only be transmitted over secure networks;

5.1.4. Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

5.1.5. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

5.1.6. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

5.1.7. Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient.

5.1.8. All personal data transferred physically should be transferred in a suitable container marked "confidential";

5.1.9. No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the Data Protection Officer.

5.1.10. All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

5.1.11. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Organization or not, without authorisation;

5.1.12. Personal data must be handled with care at all times and should not be left unattended or on view;

5.1.13. Computers used to view personal data must always be locked before being left unattended;

5.1.14. No personal data should be stored on any mobile device, whether such device belongs to the Organization or otherwise without the formal written approval of the Data Protection Officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

5.1.15. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Organization where the party in question has agreed to comply fully with the Organization's Data Protection Policy and the Data Protection and Privacy Act;

5.1.16. All personal data stored electronically should be backed up monthly with backups stored onsite **OR** offsite. All backups should be encrypted;

5.1.17. All electronic copies of personal data should be stored securely using passwords and encryption;

5.1.18. All passwords used to protect personal data should be changed regularly and should must be secure;

5.1.19. Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff shall not have access to passwords;

5.1.20. All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

5.1.21. No software may be installed on any Organization-owned computer or device without approval; and

5.1.22. Where personal data held by the Organization is used for marketing purposes, it shall be the responsibility of Head of Comms to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.1.23. The following Organizational measures are in place within the Organization to protect the security of personal data. Please refer to Part 27 of the Organization's Data Protection Policy for further details:

5.1.23.1. All employees and other parties working on behalf of the Organization shall be made fully aware of both their individual responsibilities and the Organization's responsibilities under the Data Protection and Privacy Act and under the Organization's Data Protection Policy;

5.1.23.2. Only employees and other parties working on behalf of the Organization that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Organization;

5.1.23.3. All employees and other parties working on behalf of the Organization handling personal data will be appropriately trained to do so;

5.1.23.4. All employees and other parties working on behalf of the Organization handling personal data will be appropriately supervised;

5.1.23.5. All employees and other parties working on behalf of the Organization handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

5.1.23.6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

5.1.23.7. The performance of those employees and other parties working on behalf of the Organization handling personal data shall be regularly evaluated and reviewed;

5.1.23.8. All employees and other parties working on behalf of the Organization handling personal data will be bound by contract to comply with the Data Protection and Privacy Act and the Organization's Data Protection Policy;

5.1.23.9. All agents, contractors, or other parties working on behalf of the Organization handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Organization arising out of the Data Protection and Privacy Act and the Organization's Data Protection Policy;

5.1.23.10 Where any agent, contractor or other party working on behalf of the Organization handling personal data fails in their obligations under the Data Protection and Privacy Act and/or the Organization's Data Protection Policy, that party shall indemnify and hold harmless the Organization against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

NB: *any conflicts with the Data protection policy in this part are settled by the data protection policy. *

6. Data Disposal

6.1. Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1.1. Personal data stored electronically (including any and all backups thereof) shall be deleted securely using the High Security (7 runs) method.

6.1.2. Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely using the High Security (7 runs) method;

6.1.3. Personal data stored in hardcopy form shall be shredded to at least the BS EN15713:2009 standard

This is the main standard that is adhered to as it is specifically designed for use by customers and suppliers of regular outsourced secure shredding on a commercial level.

6.1.4. Special category personal data stored in hardcopy form shall be shredded to at least BS EN15713:2009 standard, this is the same as above in 6.1.3.

7. Data Retention

7.1. As stated above, and as required by law, the Organization shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2. Different types of personal data, used for different purposes, will necessarily be retained for different periods (**(**and its retention periodically reviewed), as set out below:

7.2.1. When establishing and/or reviewing retention periods, the following shall be taken into account:

7.2.2. The objectives and requirements of the Organization;

7.2.3. The type of personal data in question;

7.2.4. The purpose(s) for which the data in question is collected, held, and processed;

7.2.5. The Organization's legal basis for collecting, holding, and processing that data;

7.2.6. The category or categories of data subject to whom the data relates;

7.2.7. Any other considerations that may be updated from time to time.

7.3. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.4. Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Organization to do so (whether in response to a request by a data subject or otherwise).

7.5. In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and Organizational measures to protect the rights and freedoms of data subjects, as required by the Data Protection and Privacy Act.

Data Ref.	**Type of Data**	**Purpose of Data**	**Review Period**	**Retention Period or**	**Comments**

				Criteria	
01	Text	Data used to store user details and case data.	Yearly	2 years	This included names, addresses, messages between BFL and beneficiaries, case details and more.
02	Audio Messages	This is a communication channel with beneficiaries	Yearly	2 Years	These are voice recordings made by beneficiaries
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data	<<describe purpose of data>>	<<insert review date or	<<insert retention	<<add additional information as required>>

	type>>		period>>	period>>	
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>

8. Roles and Responsibilities

8.1.1. The Organization's Data Protection Officer is Timothy Kakuru, C/o P. O. Box 25431, Plot 1, Muwafu Road, Ministers' Village, Ntinda, Kampala; kakuru@barefootlaw.org.

8.1.2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Organization's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the Data Protection and Privacy Act and other applicable data protection legislation.

8.1.3. The Data Protection Officer **AND** the Director of Information Technology and Digital Strategy shall be directly responsible for ensuring compliance with the above data retention periods throughout the Organization.

8.1.4. Any questions regarding this Policy, the retention of personal data, or any other aspect of Data Protection and Privacy Act compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of <<insert date>>. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: <<insert full name>>

Position: <<insert position>>

Date: <<insert date>>

Due for Review by: <<insert date>>

Signature: