Bloomberg Philanthropies DATA FOR HEALTH INITIATIVE
Global Grants Program

Kiribati

Data Protection Policy

Rev.1

January 2022

Index

Data Protection Policy

Government of Kiribati

Last updated	13/01/2022

1. Definitions

Responsible Person	means [insert name of person responsible for data protection within the Government.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Government.

2. Data protection principles

The Government of Kiribati is committed to processing data in accordance with its responsibilities under this document.

Data shall be:

processed lawfully, fairly and in a transparent manner in relation to individuals;

a. 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 incompatible with the initial purposes;

b. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

c. 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;

d. 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 in order to safeguard the rights and freedoms of individuals;

e. 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; and

f. not be transferred outside the Government of Kiribati unless that country or territory also ensures an adequate level of protection.

3. General provisions

a. This policy applies to all personal data processed by the Government of Kiribati.
b. A Responsible area (or the **data protection officer**) shall take responsibility for the Government of Kiribati's ongoing compliance with this policy.
c. This policy applies regardless of whether data is stored electronically, on paper or on other materials.
d. This policy shall be reviewed at least annually.

4. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Government of Kiribati shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed periodically.
c. Individuals have the right to access their personal data and any such requests made to the Government of Kiribati shall be dealt with in a timely manner.

5. Lawful purposes

a. All data processed by the Government of Kiribati must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The Government of Kiribati shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Government's systems.

6. Data minimisation

a. The Government of Kiribati shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7. Accuracy

a. The Government of Kiribati shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

a. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Government of Kiribati shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The Government of Kiribati shall ensure that personal data is stored securely using modern software that is kept-up to date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted, this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Government of Kiribati shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach.

10. Responsibilities

Everyone who works for or with Government of Kiribati has some responsibility for ensuring data is collected, stored and handled appropriately.

Each area that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

a. The **data protection officer,** is responsible for:

- Keeping the Government official updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Government holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the Government's sensitive data.

b. The **ICT area** is responsible for:

   - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
   - Performing regular checks and scans to ensure security hardware and software is functioning properly.
   - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

11. General staff guidelines

a. The only people able to access data covered by this policy should be those who need it for their work.

b. Data should not be shared informally. When access to confidential information is required, staff can request it from their line managers.

c. The Government shall provide training to all staff to help them understand their responsibilities when handling data.

d. Staff should keep all data secure, by taking sensible precautions and following the guidelines below.

e. Strong passwords must be used, and they should never be shared.

f. Personal data should not be disclosed to unauthorised people, either within the Government or externally.

g. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

h. Staff should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

12. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the ICT manager or data protection officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

a. When not required, the paper or files should be kept in a locked drawer or filing cabinet.

b. Staff should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

c. Data printouts should be shredded and disposed of securely when no longer required.

d. When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

e. Data should be protected by strong passwords that are changed regularly and never shared between staff.

f. If data is stored on removable media (like a flash drive, external HDD, CD or DVD), these should be kept locked away securely when not being used.

g. Data should only be stored on designated drives and servers and should only be uploaded to an **approved** cloud computing service.

h. Servers containing personal data should be sited in a secure location, away from general office space.

i. Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

j. Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

k. All servers and computers containing data should be protected by approved security software and a firewall.

13. Data use

When personal data is accessed and used it can be at the greatest risk of loss, corruption or theft:

a. When working with personal data, staff should ensure the screens of their computers are always locked when left unattended.

b. Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.

c. Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.

d. Personal data should never be transferred outside of the Government.

e. Staff should not save copies of personal data to their own computers. Always access and update the central copy of any data.

f. It is strongly recommended the use of an access log to track government personnel access to data.

14. Data accuracy

The Government should take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Government should put into ensuring its accuracy.

It is the responsibility of all staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

a. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

b. Data should be updated as inaccuracies are discovered.

15. Subject access requests

All individuals who are the subject of personal data held by the Government are entitled to:

a. Ask what information the Government holds about them and why.

b. Ask how to gain access to it.

c. Be informed how to keep it up to date.

d. Be informed how the Government is meeting its data protection obligations.

If an individual contacts the Government requesting this information, this is called a *subject access request*.

Individuals could be charged per subject access request. The data protection officer will aim to provide the relevant data within a reasonable number of days.

The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

16. Disclosing data for other reasons

In certain circumstances, personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Government will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the board and from the Government's legal advisers where necessary.

END OF POLICY

17. References

1. Data protection in the EU - The General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and other rules concerning the protection of personal data - https://ec.europa.eu/info/law/law-topic/data-protection_en

2. ICO. Information Commissioner's Office - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals - https://ico.org.uk/