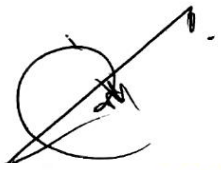
GONOSHASTHAYA KENDRA

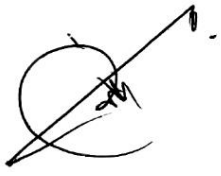
DATA PROTECTION POLICY

January 2024



Dr. Manzur Kadir Ahamed
Senior Director
Gonoshasthaya Kendra
Cox's Bazar.

Table of Contents



DATA PROTECTION POLICY OF GONOSHASTHAYA KENDRA (GK)

1. Introduction

Gonoshasthaya Kendra (GK) is a non-profit, non-political organization that was established in 1972. Since its inception, GK has been operating a variety of institutions, hospitals, and projects across different regions of Bangladesh.

Independent, private, and non-profit, GK respects strict political, social, cultural, and religious impartiality and operates following the principles of neutrality, non-discrimination, and transparency, according to its core values: responsibility, impact, enterprising spirit, and inspiration.

A data protection policy outlines how Gonoshasthaya Kendra (GK) will collect, use, store, and protect personal data to comply with relevant laws and regulations. It establishes the principles and procedures for handling personal information, ensuring transparency, security, and accountability.

1.1. Gonoshasthaya Kendra is committed to protecting the personal data of our employees, customers, beneficiaries, patients, partners, and stakeholders in compliance with applicable data protection laws and regulations.

2. Scope

2.1. This policy applies to all employees, beneficiaries, patients, customers, contractors/vendors, and third parties who handle personal data on behalf of the Organization.

2.2. It covers all personal data collected, processed, stored, or shared by the Organization, whether in electronic or physical form.

3. Data Collection and Use

3.1. The Organization collects personal data only for legitimate services/business purposes, including but not limited to employee administration, beneficiary/customer service, marketing, and regulatory compliance.

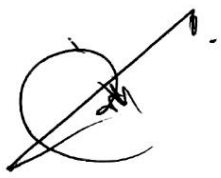
3.2. Personal data is processed lawfully, fairly, and transparently in accordance with applicable laws.

3.3. We ensure that the data collected is relevant, accurate, and limited to what is necessary for the intended purpose.

4. Legal Bases for Processing

4.1. The Organization processes personal data based on one or more of the following legal grounds:

- Consent from the data subject
- Contractual necessity
- Legal obligation
- Legitimate service/business interests
- Protection of vital interests



5. Date Storage and Retention

5.1. Personal data is stored securely using appropriate technical and organizational measures.

5.2. Date is retained only for as long as necessary to fulfill the purposes for which it was collected, unless otherwise required by law.

6. GK's sets of data and definitions

6.1. GK's Data Protection Policy applies to all sets of personal data, currently stored, maintained, and handled by GK, and more specifically to the following identified sets of personal data:

- GK's personnel, including national and international staff, interns, and volunteers,
- GK's direct and indirect beneficiaries, including interviewees,
- GK's individual donors and sympathisers,
- GK's contractors, suppliers, consultants, and implementing partners are currently under contract with GK.

6.2. Personal data herein referred to means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. This can include, in particular:

- Name of individuals
- Postal or living address
- Identification of relatives
- National ID/MRC Number or Passport Number
- Date and place of birth
- Telephone Numbers
- Email ID
- Fingerprints
- Business reference

Processing of personal data means any operation or set of operations in relation to such data, whatever the mechanism is used, especially the obtaining, recording, organization, retention, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction.

7. Principles for Processing Personal Data

7.1. Fairness and Lawfulness

- When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.
- Collected data shall be adequate, relevant, and not excessive in relation to the purposes for which they are obtained and their further processing.
- Individual data can be processed upon the voluntary consent of the person concerned.

7.2. Restriction to a specific purpose

- Personal data can be processed only for the purpose that was defined before the data was collected. Personal data shall be obtained for specified, explicit, and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require justification.

- However, further data processing for statistical, scientific, and historical purposes shall be considered compatible with the initial purposes of the data collection if it is not used to make decisions with respect to the data subjects.

7.3. Transparency

- The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be made aware of, or informed of:

  - The purpose of data processing
  - Categories of third parties to whom the data might be transmitted

- Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: compliance with any legal obligation to which GK is subject; the protection of the data subject's life; the performance of a public service mission entrusted to GK.

7.4. Confidentiality and Data Security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification, or destruction.

7.5. Deletion

Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed. There may be an indication of interests that merit protection or the historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

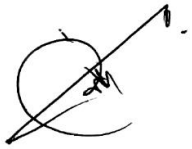
7.6. Factual Accuracy and Up-to-datedness of Data

Personal data on file must be correct, complete, and if necessary kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

8. Data Processing

8.1. Consent to Data Processing

Individual data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. In certain exceptional circumstance, consent may be given verbally.



8.2. Data processing Pursuant to Legitimate Interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of GK. Legitimate interests are generally of a legal (such as filing, enforcing or defending against legal claims), audit or financial nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the individual merit protection. Before data is processed, it must be determined whether there are interests that merit protection. Control measures that require processing of personal data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the organization in performing the control measure (e.g. compliance with legal provisions and internal rules of the organization) must be weighed against any interests meriting protection that the individual affected by the measure may have in its exclusion, and cannot be performed unless appropriate.

8.3. Telecommunications and Internet

- Telephone equipment, e-mail addresses, intranet and internet along with interna social networks are provided by GK primarily for work-related assignments. They are a tool and an organizational resource. They can be used within the applicable legal regulations and internal GK communication policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

- There will be no general monitoring of telephone and e-mail communications or intranet/internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the network used by GK that block technically harmful content, or that analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be blocked for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of policies and/or procedures of GK. The evaluations can be conducted only by investigating committee while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the GK regulations.

8.4. Confidentiality of Processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The “need to know” principle applies. Duly-authorized employee may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, ad well as implementation, of roles and responsibilities.

8.5. Processing Security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must

be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification). The technical and organization measures for protecting personal data are part of GK's ITC management and must be adjusted continuously to the technical developments and organizational changes.

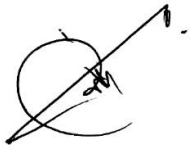
9. Data Protection Control

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of GK's Sr. Director/CEO or appointed representative. The results of the data protection controls performed by appointed representative must be reported to the Sr. Director/CEO. GK's Board of Director must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

10. Violation, sanction and reporting

- Any failure to comply with the current policy or to deliberately violate the rules set in the policy will result in the launch of an appropriate investigation by GK.
- Depending of the gravity of the suspicion or accusations, GK may suspend staff or relations with other stakeholder during the investigation. This will not be subject to challenge.
- Depending on the outcome of the independent investigation, if it comes to light that anyone associated with GK has deliberately violated the rules set in the policy for its personal profit or any other usage of personal data, or has systematically and deliberately contravened with the principles and standards contained in this document, GK will take immediate disciplinary action and any other action which may be appropriate to the circumstances. This may mean, for example, for:
    - Employees – disciplinary action/dismissal;
    - Trustees, Board of Directors, Officers and Interns – ending the relationship with the Organization;
    - Partners – withdrawal of funding/support;
    - Contractors and Consultants – termination of contract.

- Depending on the nature, circumstances and location of the case and violation, GK will also consider involving authorities such as the police to ensure the protection of personal data and victims.
- The reporting of suspected or actual violations to this policy is a professional and legal obligation of all staff and partners. Failure to report information can lead to disciplinary action.



- GK encourages its staff and stakeholders to report suspected cases which involve any GK staff, consultants, board members, guests or staff of GK's partner organizations, their board members, staff and or suppliers.

GK encourages its staff and stakeholders to report suspected cases through the following means:

- Staff and interns can report contacting
  - Standard lines of hierarchy (contained in staff Terms of Reference);
  - The Head of Human Resources.
- Beneficiaries and their representatives can report using the Complaints and Feedback Mechanism (CFM); Hotline Number:+88 01894 419218
- Suppliers and contractors can use the confidential email address
  Email ID: complaint@gkcox.org
- Individual donors and sympathizers can refer to the confidential email address
  Email ID: complaint@gkcox.org
- All reposts will be treated as confidential in line with GK's Code of Conduct and GK's Human Resources Guidelines.
- GK will not tolerate false accusations which are designed to damage a member of staff's reputation. Anyone found making false accusations will be subject to investigation and disciplinary action.

11. Responsibilities

- Management staff are responsible for ensuring that organizational, Human Resources, and technical measures are in place so that any data processing is carried out in accordance with data protection. The Coordinator(s)/Managers/Supervisors must ensure that their employees are sufficiently trained in data protection compliance with these requirements is the responsibility of the relevant employees.

12. Implementation of the Policy

This policy has been approved by GK's Appropriate Authority on January 2024 and comes into effect immediately. It could be reviewed regularly.

****