RULES ON PROTECTION OF PERSONAL DATA

Approval:	Director-General	**Date Approved:**	25 October 2021
Effective Date	Date of Approval	**Responsible Office:**	Assistant Director-General and Head of Operations Enabling Division
Version	2		

Table of Contents

1. Background and Purpose

GGGI is committed to respecting the privacy of individuals and ensuring that any information collected, stored, used or otherwise processed by GGGI is done so in accordance with recognized international practices and standards. In order to adequately protect the personal data of all individuals, including GGGI personnel, governance officials, service providers, applicants, and individuals involved in GGGI's programmatic activities or outreach, while at the same time ensuring that GGGI can carry out its mandate and mission and efficiently execute required administrative actions, these Rules on Protection of Personal Data (the "Rules") set out the requirements to be followed by GGGI when handling personal data.

These Rules apply to Personal Data processed by GGGI. It applies to all staff members of GGGI, consultants, contractors, interns, volunteers, secondees, or other GGGI stakeholders, regardless of location or whether in the Headquarters or in county offices, to the extent that they are Processing Personal Data under the name of GGGI as a Data Controller or Data Processor with respect to Personal Data relating to Data Subjects.

2. Definitions

The following definitions apply for the purpose of these Rules:

"Consent" means any freely given informed indication of an agreement by a Data Subject to the Processing of his or her Personal Data, which may be given by a written or oral statement or by a clear affirmative action;

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;

"Data Controller" means the natural or legal person or body determining the purposes and the means of the Processing of Personal Data;

"Data Transfer" or "Transfer" means any act that makes Personal Data accessible, whether on paper, via electronic means or any other method, to a third party;

"Personal Data" shall mean any information relating to an identified or identifiable natural person ("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;

"Process" means any operation which is performed involving Personal Data such as collection, recording, organization, structuring storage adaptation or alteration, use, disclosure, restriction, erasure or destruction;

"Processor" means the natural or legal person which processes Personal Data on behalf of the Data Controller; and

"Sensitive Personal Data" means Personal Data revealing racial or ethnic origins, political opinions, trade union membership, religious or philosophical beliefs, health or sexual life, genetic or biometric data, or criminal convictions of a Data Subject.

3. Principles relating to Processing Personal Data

3.1 GGGI, as Data Controller or Processor, shall be guided by the following principles in relation to all actions relating to Personal Data:
Personal Data shall be

a) Processed lawfully, fairly and in a transparent manner in relation to the Data Subject;
b) Collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed;
d) Accurate and where necessary, kept up to date;
e) Kept in a form which permits identification of Data Subjects for no longer than necessary for the purposes for which the data are Processed; and
f) Processed in a manner which ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage using appropriate technical or organizational measures.

4. Purpose for Processing of Personal Data

4.1 Any Processing of Personal Data should be proportionate to the purpose for which it is being Processed. The Personal Data collected and Processed should be adequate and relevant for the identified purpose and should not exceed that purpose.

4.2 GGGI as Data Controller shall ensure that Personal Data shall be Processed only if and to the extent at least one of the following applies:

a) The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps necessary prior to entering into a contract;
c) Processing is necessary for compliance with a legal obligation to which the Data Controller is subject, including compliance with GGGI's legal framework;
d) Processing is necessary to protect the vital interest of the Data Subject or another natural person;
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the authority vested in GGGI; or
f) Processing is necessary for the purpose of the legitimate interests pursued by GGGI or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the Data Subject which require protection of the Personal Data.

4.3 Processing of Sensitive Personal Data is not allowed, unless:

a) the Data Subject has given Consent;
b) the data have been made public by the Data Subject;
c) it is necessary to protect vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving Consent;
d) it is necessary to carry out investigative procedures; or
e) it is necessary to carry out obligations under the Staff Regulations and Staff Rules, including those relating to health and social care.

4.4 Consent Management

a) GGGI will consider Consent as a legal basis for Processing only when Data Subjects have a real choice and control over the Processing of their Personal Data.

b) When GGGI is relying on Consent as legal basis for Processing Personal Data, GGGI personnel processing the Personal Data must clearly establish the Data Subject's Consent and monitor Consent usage. Consent must be obtained in writing or electronically and is valid only if given voluntarily. To establish Consent, there should be a positive opt-in (no pre-ticked boxes or default consent) by the Data Subject. GGGI personnel shall keep a record of when and how it obtained Consent, together with the Personal Data.

c) Data Subjects shall be provided with the possibility to withdraw their Consent at any time.

5. Data Processing by Third Parties

5.1 GGGI may Transfer Personal Data to third parties only on the following conditions:

a) The Data Subject is informed of the Data Transfer;
b) The third party, as Processor, ensures data protection on at least the same level as GGGI and such level of data protection is established by a contract or other legally binding documentation;
c) The Data Transfer is made for one more or more legitimate purposes, as set out in paragraph 4.2 above; and
d) The amount of Personal Data transferred is strictly restricted to the data the third party needs to have for the specific purpose the third party receives the data.

6. Information to be provided

6.1 At the time the Personal Data is obtained, GGGI shall provide the Data Subject the following information:

a) GGGI's contact details;
b) The type of Personal Data related to the Data Subject Processed by GGGI;
c) The purposes of the Processing;
d) Legal basis for the Processing;
e) The recipient or categories of recipients (third parties) that the Personal Data are to be disclosed to;

f) The period for which the Personal Data will be stored; and
g) How to exercise the Data Subject's rights set out in Section 7.

7. Rights of Data Subject

7.1 Right to Access. The Data Subject has the right to obtain confirmation as to whether Personal Data relating to the Data Subject has been collected, stored or Processed, and, where that is the case, how the Personal Data was collected and Processed and for what purpose, and to have access to copies of such Personal Data.

7.2 Right to Rectification. The Data Subject has the right to request rectification of Personal Data relating to the Data Subject if such data can be established to be inaccurate or incomplete.

7.3 Right to Erasure and Restriction. The Data Subject has the right to request that GGGI delete or restrict (i.e. GGGI may only store the data without further Processing) the Personal Data relating to the Data Subject or refrain from sharing such data with third parties in case the data is clearly excessive, no longer necessary in relation to the purposes for which it was collected or the Data Subject withdraws Consent, if Consent is the basis for Processing in accordance with paragraph 4.2.

7.4 Right to Object. The Data Subject has the right to object to the Processing of Personal Data relating to the Data Subject, unless GGGI can establish that there is a legitimate ground for the Processing.

7.5 Right to Data Portability. The Data Subject has the right to request that that their Personal Data be transmitted to the Data Subject or others designated by the Data Subject, in a structured, commonly used and machine readable format, where technically feasible.

7.6 Right against automated individual decision-making including profiling. The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

7.7 A Data Subject may contact GGGI regarding any requests in relation to the exercise of these rights under this Section 7 through the dedicated email address dataprotection@gggi.org, indicating that the request concerns personal data. Such request will be forwarded to the GGGI personnel responsible for Processing the Data Subject's Personal Data. The identity of the requester must be verified before complying with the request. The responsible GGGI personnel should provide a response within one month of the receipt of such request, which can be extended by another month depending on the complexity of the request. The response shall be in writing and explain the action to be taken or provide reasons if the request cannot be met. Templates for responses will be developed as needed.

7.8 The Data Subject whose request was not acted upon by GGGI has the right to raise a request for review of alleged violation of his or her rights under this Section 7 in accordance with GGGI's Compliance Review Mechanism (the relevant rules available on gggi.org/policy-documents/).

8. Storage

8.1 Personal Data shall be kept only as long as it is necessary for the relevant purposes or for the periods GGGI has notified to Data Subjects under Section 6. After these periods, the personal data shall be either deleted or kept in a form which does not permit identification of Data Subjects.

8.2 GGGI shall take appropriate technical and organizational measures to ensure a level of security appropriate to the risks and nature of the Personal Data to be Processed and to ensure protection against accidental or unlawful destruction or accidental loss, and to prevent unlawful forms of Processing, in particular unauthorized disclosure, dissemination or access or alteration of Personal Data.

9. Privacy by Design and Privacy by Default

9.1 GGGI will implement appropriate technical and organizational measures which are designed to implement these Rules, both at the time of the determination of the means for Processing and at the time of the Processing.

9.2 In particular, while designing a database and drafting procedures for collecting Personal Data, the principles of Processing of Personal Data and the rights of Data Subjects stipulated in these Rules must be taken into account and reflected accordingly.

9.3 GGGI will also implement appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are actually Processed.

10. Data Protection Impact Assessment

10.1 Where the Processing of Personal Data is likely to present high risks for the rights or freedoms of Data Subjects e.g. due to the type or amount of data or the number of Data Subjects or the purposes of the Processing, GGGI shall, in advance of the Processing, carry out a data protection impact assessment (DPIA) and address any issues such assessment may reveal. Examples of high-risk Processing include (i) systematic and extensive Processing activities (including profiling) where decisions have legal effects or similarly significant effects on Data Subjects; or (ii) large scale Processing of Sensitive Personal Data.

10.2 A DPIA should include: (i) a description of the envisaged Processing and the purposes of the Processing; (ii) an assessment of the need for and proportionality of the Processing and the risks to Data Subjects arising; and (iii) measures envisaged to mitigate those risks and ensure compliance with these Rules.

10.3 If an assessment indicates that the Processing may indicate a high risk, the Assistant Director-General and Head of Operations Enabling Division (ADG-OED) must be consulted.

11. Data Breach Management Procedure

11.1 GGGI personnel are required to inform ADG-OED as soon as possible upon becoming aware of an actual or suspected Data Breach.

11.2 GGGI will take the following measures to address an actual or suspected Data Breach:

a) Assessment consisting of: (i) data records and type of Personal Data affected; (ii) date, time, duration and location; (iii) cause of the Data Breach; (iv) list of affected Data Subjects; (v) risk of serious harm to Data Subjects; and (vi) risk of other adverse consequences (operational, security, financial, reputational); and

b) Measures taken or proposed to be taken to mitigate and address the possible adverse impacts of the Data Breach.

11.3 ADG-OED may appoint a Data Breach response team who will carry out the assessment as described above. Such team may include members from TSU, Legal Unit and other GGGI personnel and external experts as appropriate. The response team will submit a report to ADG-OED which includes the results of the assessment and recommendation on the measures to be taken in response to the Data Breach.

11.4 If a Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, ADG-OED shall inform the Data Subject on the results of the assessments and take appropriate measures without undue delay. In such case, the Director-General shall be also informed.

12. Data Transfer

External Data Transfer

12.1 GGGI will ensure that Personal Data is only transferred under Section 5 to jurisdictions or international organizations that ensure adequate level of protection. Should it be necessary to transfer Personal Data to a third country or an international organization that does not provide adequate level of protection, GGGI will ensure that it maintains appropriate safeguards such as entering into appropriate contractual clauses in order to safeguard Personal Data.

Data Transfer within GGGI

12.2 Data transfer within GGGI carried out between different GGGI offices or between different components of GGGI are permitted to the extent that the data transfers are in accordance with these Rules and that all offices, staff, interns, volunteers, secondees, individual consultants, and individual contractors involved in the internal data transfers strictly comply with these Rules. Strict adherence to these Rules is included in the obligations of staff under the GGGI Code of Conduct. Contracts with interns, volunteers,

secondees, consultants, and contractors shall specifically include provisions requiring compliance with these Rules. Violations of these Rules will result in appropriate disciplinary measures for staff, while those involving contractors, consultants, interns, secondees, and volunteers will result in appropriate action under the terms and conditions of their respective contracts.

13. Implementation

13.1 These Rules may be complemented by guidelines as appropriate to provide further guidance on the implementation of these Rules.

13.2 The Assistant Director-General and Head of Operations Enabling Division (ADG-OED) shall act as the data protection contact and is responsible for overseeing the application and implementation of these Rules throughout the organization.

13.3 A committee comprising of ADG-OED, representatives of the Legal Unit and Technology Services Unit and other relevant stakeholders as determined by ADG-OED shall convene at least once a year to discuss and assess the needs regarding data protection issues.

13.4 Regular audits will be conducted with a focus on data protection and security measures to monitor, assess and improve data protection practices/documentation.