PERSONAL DATA PROTECTION POLICY

BY RWANDA NETWORK OF PEOPLE LIVING WITH HIV / AIDS (RRP+)

This policy outlines RRP+'s commitment to protecting personal and sensitive data, especially HIV-related information, by ensuring all collection, use, and storage comply with Rwanda's Law No. 058/2021 and uphold the highest standards of confidentiality, accountability, and respect for human dignity.

Version No 1

October 15, 2025

P.O. Box 6559 Kigali-Rwanda
Tel.: + 250 789 287 395
Email: rrp.rwanda@gmail.com
Website: www.rrpplus.org

Board Approval and Signature Page

Document Title: RRP+ Personal Data Protection Policy

Version: 1.1

Date of Approval: 15 October 2025

Review Cycle: Every three (3) years or earlier if required by law or organizational changes.

This policy has been reviewed and approved by the **Board of Directors (BoD)** of the Rwanda Network of People Living with HIV/AIDS (RRP+), in accordance with the organization's governance and compliance framework.

The Board confirms that this policy aligns with **Law No. 058/2021 of 13/10/2021 on the Protection of Personal Data and Privacy** and commits RRP+ to upholding the dignity, confidentiality, and privacy of People Living with HIV (PLHIV) and all data subjects whose personal information it handles.

Role / Position	Name	Signature	Date
Data Protection Officer (Policy Author)	Jean Berchmans TUGIRIMANA		15/10/2025
Executive Secretary (Policy Owner)	Dr. Deo MUTAMBUKA (PhD)		16/10/2025
Chairperson, Board of Directors	Sylvie MUNEZA		16/10/2025

Foreword

The protection of personal data and the privacy of People Living with HIV (PLHIV) are central to the mission and values of RRP+. Beyond being a legal requirement under Rwanda's Law Nº 058/2021 of 13/10/2021, relating to the protection of personal data and privacy, safeguarding data is a matter of human dignity, trust, and respect for every individual we serve.

This **Personal Data Protection Policy** provides a clear framework to ensure that all personal and sensitive data, including HIV-related information, is handled with the highest standards of confidentiality, integrity, and accountability. It defines the roles, responsibilities, and commitments expected from every member of the RRP+ community, including staff, peer educators, volunteers, contractors, and partners.

Through this policy, RRP+ reaffirms its unwavering commitment to building and maintaining the trust of our members, partners, and the broader community. I urge every team member to internalize the principles and procedures outlined here and to act as a guardian of confidentiality and ethical conduct in all aspects of their work.

Together, we will continue to uphold the rights, dignity, and privacy of all individuals whose lives we touch.

Dr. Deo MUTAMBUKA (PhD)

Executive Secretary,

Rwanda Network of People Living with HIV/AIDS (RRP+)

Contents

List of Acronyms

Acronym	Full Meaning
Ann.	Annex
BoD	Board of Directors
CEO	Chief Executive Officer (if applicable to partner organizations)
CSO	Civil Society Organization
CSV	Comma-Separated Values (file format for data exports)
DBMS	Database Management System
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ES	Executive Secretary
HIV	Human Immunodeficiency Virus
HR	Human Resources
HRM	Human Resource Management
ICT	Information and Communication Technology
ID	Identification / Identity Document
IT	Information Technology
M&E	Monitoring and Evaluation
NCSA	National Cyber Security Authority (Rwanda)
NGO	Non-Governmental Organization
PDMS	Personal Data Management System
PDP	Personal Data Protection
PII	Personally Identifiable Information
PLHIV	People Living with HIV
RBC	Rwanda Biomedical Center
RRP+	Rwanda Network of People Living with HIV/AIDS
SMT	Senior Management Team

POLICY MANAGEMENT INFORMATION

Item	Details
Title	Personal Data Protection Policy
Author (Responsible)	Jean Berchmans TUGIRIMANA, Data Protection Officer (DPO), RRP+
Owner (Accountable)	Dr Deo MUTAMBUKA (PhD), Executive Secretary, RRP+
Division	Civil Society Organizations (CSOs) / Non-Governmental Organizations (NGOs)
Contact	DPO – jbtugirimana@rrpplus.org
Version Number	1.1
Status	Approved by Board of Directors
Reviewed by	Senior Management Team, RRP+
Approved by	Board of Directors, RRP+
Date of Original Approval	15-October-2025
Applicability (Informed)	Applies to RRP+ Chairperson, Executive Secretary (ES), employees, contractors, sub-contractors, advisors, temporary staff, volunteers, peer educators, and any other persons performing a function for RRP+ or who have access to personal data under RRP+ supervision and control.
Communicated on	15-October-2025
Last Reviewed	15-October-2025
Summary of Key Changes	Not Applicable (First Issue)
Frequency of Review	Every 3 years, or earlier if required by law or organizational changes
Date of Next Review	October -2028
Related Policies & Procedures	- RRP+ Personal Data Privacy Policy
	- RRP+ Procedures Manual

DECISION MAKING IN RELATION TO THE POLICY

Role	Entity / Position	Responsibilities
Responsible (Author)	Data Protection Officer (DPO)	Drafts and maintains the policy; ensures alignment with Law No. 058/2021; monitors implementation and compliance.
Accountable (Owner)	Director of Finance and Administration	Holds ultimate accountability for ensuring that the policy is implemented across RRP+; provides resources for compliance; reports to the Board of Directors.
Consulted	Board of Directors	Provides oversight, governance input, and approval of the policy; ensures it aligns with organizational strategy and statutory obligations.

Informed	Senior Management Team (Executive Secretary, Director of Finance and Administration, Program Managers, Communication Officer, Field Officers), all staff, volunteers, peer educators, and any other persons with access to personal data	Receive communication and training on the policy; expected to comply fully with its requirements.

KEY MESSAGES

Question	Key Message
Why do we have this policy?	To ensure RRP+ complies with Rwanda's **Law No. 058/2021 of 13/10/2021** on the Protection of Personal Data and Privacy, and to safeguard the dignity, rights, and confidentiality of People Living with HIV (PLHIV) and all other data subjects whose personal data RRP+ handles.
Who does this policy apply to?	It applies to **all RRP+ staff, volunteers, peer educators, consultants, contractors, sub-contractors, field officers, and any other persons** who process or access personal data on behalf of RRP+.
What are the key things I need to know?	- HIV-related data is classified as **sensitive personal data**.
	- Processing must always have a **lawful basis** (e.g., consent, legal obligation, vital interest).
	- Data subjects have enforceable **rights** (access, rectification, erasure, objection, etc.).
	- Breaches must be reported and handled promptly.
What are the key things I need to do?	- Collect only the **minimum necessary data**.
	- Keep all data **secure** (lock paper files, password-protect devices, restrict access).
	- Obtain **informed consent** where required.
	- **Do not disclose** HIV status or other sensitive data without authorization.
	- Report any **suspected data breach** immediately to the DPO.
Where can I find more information?	- This **Personal Data Protection Policy**.
	- The **RRP+ Procedures Manual**.
	- Rwanda's **Law No. 058/2021**.
	- Contact the **Data Protection Officer (DPO): jbtugirimana@rrpplus.org**.

1. Purpose/ Introduction

The Rwanda Network of People Living with HIV/AIDS (RRP+) is committed to protecting the personal data and privacy of all individuals whose information it collects, processes, and stores in the course of its work. This includes data relating to People Living with HIV (PLHIV), their families, staff, volunteers, peer educators, partners, and other stakeholders.

The purpose of this policy is to:

- Ensure RRP+ complies with the requirements of **Rwanda's Law No. 058/2021 of 13/10/2021 on the Protection of Personal Data and Privacy**, and with international best practices in data protection.
- Safeguard the **dignity, confidentiality, and rights** of PLHIV and all other data subjects.
- Provide a **framework of principles, rules, and responsibilities** for how personal data is collected, used, stored, shared, and disposed of within RRP+.
- Reduce the risks of **unauthorized access, disclosure, or misuse** of personal data, particularly HIV-related and other sensitive information.
- Build and maintain **trust with members, communities, partners, and regulators** by demonstrating accountability and transparency in handling personal data.

This policy applies to **all forms of personal data**, whether held in electronic systems, paper registers, or any other format, and to **all persons working for or with RRP+** who have access to such data.

1.1. Purpose of the Personal Data Management System

The Personal Data Management System (PDMS) of RRP+ is designed to provide a **structured and accountable framework** for managing all personal data collected, processed, and stored by the organization. Its purpose is to:

1. **Ensure Legal Compliance**
   - Align all RRP+ practices with **Law No. 058/2021 of 13/10/2021 relating to the Protection of Personal Data and Privacy**, and other applicable regulations.
   - Provide documented evidence of compliance for audits, donor requirements, and oversight by the National Cyber Security Authority (NCSA).
2. **Protect Sensitive HIV-Related Data**
   - Guarantee confidentiality of information relating to People Living with HIV (PLHIV), including HIV status, treatment details, membership in support groups, and key population data.
   - Apply strict safeguards to minimize risks of stigma, discrimination, or harm caused by data misuse.
3. **Standardize Data Handling**
   - Define consistent rules for data collection, classification, processing, storage, sharing, transfer, and disposal across all RRP+ programs and partners.
   - Ensure both **paper-based systems** (registers, forms, files) and **digital systems** (databases, emails, devices) are covered.
4. **Strengthen Accountability and Transparency**
   - Clarify the roles and responsibilities of staff, volunteers, peer educators, contractors, and partners in protecting personal data.
   - Establish procedures for responding to data subject requests (access, correction, deletion, objection, etc.).
5. **Manage Risks and Breaches**
   - Provide mechanisms for reporting, investigating, and mitigating data breaches.
   - Require regular risk assessments and, where appropriate, Data Protection Impact Assessments (DPIAs).
6. **Promote Trust and Organizational Integrity**

- Build confidence among PLHIV, communities, partners, and donors that their personal data is handled responsibly and ethically.
- Reinforce RRP+'s commitment to human rights, dignity, and non-discrimination.

1.2. Purpose of this Document

The purpose of this document is to set out the **RRP+ Personal Data Protection Policy** in a clear, accessible, and practical format that guides all staff, volunteers, peer educators, contractors, and partners in the responsible management of personal data.

Specifically, this document aims to:

1. **Translate Legal Obligations into Practice**
   - Provide RRP+ with a written framework for compliance with **Law No. 058/2021 of 13/10/2021 on the Protection of Personal Data and Privacy**.
   - Ensure that all provisions of the law — particularly those relating to **sensitive personal data** such as HIV status and treatment information — are reflected in organizational practice.
2. **Define Standards and Expectations**
   - Set out the principles, commitments, and procedures that govern the handling of personal data within RRP+.
   - Establish clear expectations for how staff, peer educators, and other actors must protect confidentiality and data security.
3. **Provide a Reference Tool**
   - Serve as a **reference guide** for day-to-day decisions on data protection.
   - Include annexes with checklists, breach procedures, and quick-reference tools for practical application.
4. **Strengthen Accountability**
   - Clarify who is responsible, accountable, consulted, and informed in relation to data protection.
   - Provide a documented basis for audits, monitoring, and oversight by the **Board of Directors** and the **National Cyber Security Authority (NCSA)**.
5. **Promote Trust and Safeguard Rights**
   - Ensure that PLHIV, staff, and partners can trust RRP+ to manage data ethically and responsibly.
   - Reinforce the protection of data subject rights, including the right to access, rectify, erase, or restrict the use of personal data.

1.3. Policy Review, Approval & Continuous Improvement

RRP+ recognizes that the legal, technological, and organizational environment in which personal data is processed is dynamic. To ensure ongoing compliance and effectiveness, this policy will be subject to regular review, approval, and continuous improvement as follows:

1.3.1 Review Cycle

- This policy will be reviewed at least **every three (3) years** or earlier if required by:
  - Amendments to **Law No. 058/2021** or other relevant legislation.
  - Changes in RRP+ operations, technology, or data management practices.
  - Lessons learned from audits, risk assessments, or personal data breach investigations.

1.3.2 Approval

- The **Data Protection Officer (DPO)** is responsible for preparing updates to the policy.
- The **Director of Finance and Administration** (Policy Owner) ensures organizational alignment and resource allocation.
- The **Board of Directors** approves the policy and any subsequent revisions.

1.3.3 Communication of Updates

- Updated versions of the policy will be formally communicated to all staff, volunteers, peer educators, and contractors.
- Training or refresher sessions will be provided where significant changes are introduced.

1.3.4 Continuous Improvement

- RRP+ is committed to continuous improvement of its Personal Data Management System (PDMS) by:
    - Conducting **regular risk assessments and Data Protection Impact Assessments (DPIAs)**.
    - Incorporating **feedback from staff, peer educators, PLHIV communities, donors, and regulators**.
    - Benchmarking against international standards and best practices in data protection and information security.

2. Definitions

For the purpose of this policy, the following terms shall have the meanings ascribed to them below, in alignment with **Law No. 058/2021 on the Protection of Personal Data and Privacy**:

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person ("data subject"), including but not limited to names, contact information, identification numbers, health information, and HIV-related data.
Sensitive Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information (including HIV status), or sexual orientation. Processing sensitive personal data requires additional safeguards.
Processing	Any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, alignment, combination, restriction, erasure, or destruction.
Data Subject	Any natural person whose personal data is collected, stored, or otherwise processed by RRP+ in the course of its operations.
Data Controller	The entity (RRP+) that determines the purposes and means of processing personal data and is responsible for ensuring compliance with data protection obligations.
Data Processor	Any person or entity, internal or external to RRP+, who processes personal data on behalf of the Data Controller.

Consent	Any freely given, specific, informed, and unambiguous indication of a data subject's wishes by which they signify agreement to the processing of their personal data.
Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or otherwise processed.
Data Protection Officer (DPO)	The designated person responsible for overseeing RRP+ compliance with data protection law, providing guidance on data processing activities, and serving as a point of contact for data subjects and supervisory authorities.
Anonymization	The process by which personal data is irreversibly altered in such a way that the data subject can no longer be identified directly or indirectly.
Pseudonymization	The processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, which is kept separately and securely.
Cross-Border Transfer	Any transfer of personal data to a country or territory outside Rwanda, subject to adequacy, contractual safeguards, or other lawful mechanisms under applicable data protection law.
Automated Decision-Making	Any decision concerning a data subject that is made solely on the basis of automated processing, including profiling, which produces legal effects or similarly significantly affects the individual.
Profiling	Any form of automated processing of personal data intended to evaluate certain personal aspects relating to a data subject, including their health, preferences, or behavior.

3. Scope

This policy applies to all personal and sensitive data collected, processed, stored, or shared by RRP+ in the course of its operations. It establishes the framework for lawful, fair, and transparent handling of such data and ensures compliance with **Law No. 058/2021 on the Protection of Personal Data and Privacy**.

3.1 Who the Policy Applies To

This policy applies to:

- **RRP+ Staff**: All permanent, temporary, and contract employees.
- **Volunteers**: Individuals providing unpaid services to RRP+.
- **Peer Educators**: Individuals engaged in community outreach, education, or HIV-related programs.
- **Contractors and Consultants**: Third-party service providers who process personal data on behalf of RRP+.
- **Partner Organizations**: Entities collaborating with RRP+ that access, share, or process personal data for programmatic purposes.

All individuals and entities under this scope are expected to comply with this policy and adhere to applicable data protection principles.

3.2 Types of Personal and Sensitive Data Covered

This policy covers, but is not limited to:

- **Personal Identification Information**: Names, addresses, phone numbers, email addresses, national ID numbers.
- **Health and HIV-Related Data**: HIV status, treatment information, medical history, and any other health-related information.
- **Sensitive Demographic Data**: Age, gender, marital status, and other data that may reveal personal or social characteristics.
- **Professional Data**: Employment records, educational background, performance records.
- **Other Personal Data**: Any other information that can identify an individual, whether collected electronically, on paper, or verbally.

3.3 Application of the Policy

- **Internal Use**: Applies to all internal data collection, processing, storage, and sharing within RRP+.
- **External Use**: Governs data sharing with donors, partners, governmental authorities, or other third parties.
- **Cross-Border Considerations**: Covers transfers of personal data outside Rwanda, ensuring compliance with legal requirements for international data transfers.

This scope ensures that all personal and sensitive information handled by RRP+ is protected throughout its lifecycle, safeguarding the rights of data subjects and maintaining the organization's accountability.

4. Policy Principles/ Policy Statement

RRP+ is committed to ensuring the protection, confidentiality, and lawful processing of all personal and sensitive data it collects, stores, or shares. This commitment applies to all staff, volunteers, peer educators, contractors, and partner organizations.

The organization aligns its practices with **Law No. 058/2021 on the Protection of Personal Data and Privacy** and international best practices, especially concerning the handling of sensitive health and HIV-related information.

4.1 Core Data Protection Principles

RRP+ adheres to the following principles when processing personal data:

1. **Lawfulness, Fairness, and Transparency**
   - Personal data shall be processed lawfully, fairly, and in a transparent manner.
   - Data subjects will be informed about how their data is collected, used, and shared.
2. **Purpose Limitation**
   - Data shall be collected only for specified, explicit, and legitimate purposes.
   - It will not be further processed in a manner incompatible with those purposes.
3. **Data Minimization**
   - Only data that is adequate, relevant, and necessary for the intended purpose shall be collected.
4. **Accuracy**
   - Personal data shall be accurate, complete, and kept up to date.
   - Reasonable steps shall be taken to correct or delete inaccurate data without delay.

5. **Storage Limitation**
    - Personal data shall be kept only as long as necessary for the purpose of processing.
    - Data no longer required shall be securely deleted or anonymized.
6. **Integrity and Confidentiality**
    - Appropriate technical and organizational measures shall be implemented to protect personal data against unauthorized access, loss, or damage.
7. **Accountability**
    - RRP+ is responsible for demonstrating compliance with all data protection principles.
    - All staff, peer educators, and partners are accountable for adhering to this policy.

4.2 Policy Statement

RRP+ shall:

- Treat all personal and sensitive data, especially HIV-related information, with the highest level of confidentiality.
- Ensure that data subjects' rights are respected, including rights to access, correction, deletion, and objection.
- Require all staff, volunteers, peer educators, contractors, and partners to follow strict data protection practices.
- Conduct regular risk assessments, audits, and training to maintain compliance with this policy.
- Immediately address any data breaches according to the procedures outlined in this policy.
- Only share data with third parties where legally permissible and with appropriate safeguards.

4.3 Simplified Commitments for Staff and Peer Educators

As an RRP+ staff member, volunteer, or peer educator, you are expected to:

1. **Respect Privacy:** Never share someone's personal or health information without proper authorization.
2. **Collect Responsibly:** Only gather data needed for your work or project.
3. **Keep Data Safe:** Use secure passwords, lock physical files, and follow cybersecurity guidelines.
4. **Be Accurate:** Ensure the information you collect is correct and update it if necessary.
5. **Follow the Rules:** Adhere to RRP+ policies and legal requirements at all times.
6. **Report Issues:** Immediately notify your supervisor or the Data Protection Officer if there is a data breach or misuse.

5. Roles/ Responsibilities

RRP+ assigns clear roles and responsibilities to ensure compliance with **Law No. 058/2021** and to maintain the confidentiality, integrity, and security of personal and sensitive data.

5.1 RRP+ as Data Controller

- Determines the purposes and means of processing personal data.
- Ensures all processing activities comply with the law and this policy.
- Implements data protection measures, including technical and organizational safeguards.
- Conducts regular risk assessments, audits, and reviews of data practices.
- Maintains accountability for any data shared with third parties.

5.2 Data Protection Officer (DPO)

- Oversees RRP+ compliance with data protection laws and policies.
- Provides guidance on personal data processing and risk management.
- Acts as the main contact point for data subjects and the supervisory authority (NCSA).
- Monitors and reports on data breaches and recommends corrective actions.

5.3 Data Processors (Contractors, Consultants, Partners)

- Process personal data only on behalf of RRP+ and under documented instructions.
- Maintain confidentiality and implement appropriate security measures.
- Report any breaches or misuse immediately to RRP+.

5.4 Staff Responsibilities

- Collect and process data lawfully, fairly, and transparently.
- Limit data collection to what is necessary for the task.
- Keep personal and sensitive information accurate and up to date.
- Safeguard all physical and electronic data.
- Report breaches or data misuse immediately to the DPO or supervisor.

5.5 Peer Educators and Volunteers

- Respect confidentiality of beneficiaries' information at all times.
- Only collect, record, or share data required for program activities.
- Follow guidance and instructions from RRP+ staff regarding data handling.
- Immediately report any suspected data breach or unauthorized access.

5.6 Supervisors and Managers

- Ensure their teams understand and comply with this policy.
- Monitor data processing activities within their units.
- Provide training and support to staff and volunteers on data protection.
- Take corrective action in case of non-compliance.

5.7 Simplified Commitments for Staff, Peer Educators, and Volunteers

1. **Protect Data:** Keep all personal and sensitive information safe.
2. **Collect Only What's Needed:** Avoid collecting unnecessary information.
3. **Be Honest and Accurate:** Ensure data is correct and up to date.
4. **Follow Instructions:** Use data only as authorized by RRP+.
5. **Report Problems:** Immediately tell your supervisor or the DPO if there is a breach, loss, or misuse of data.
6. **Respect Privacy:** Never share beneficiary data outside RRP+ without proper authorization.

6. Operational Guidance / Data Collection and Processing Rules

This section provides practical guidance on how RRP+ staff, volunteers, and peer educators should collect, process, and manage personal and sensitive data in compliance with **Law No. 058/2021** and organizational standards.

6.1 General Principles for Data Collection and Processing

- **Lawful and Fair Processing:** Collect and use personal data only for legitimate purposes and with the knowledge or consent of the data subject.
- **Transparency:** Inform data subjects why their data is being collected, how it will be used, and with whom it may be shared.
- **Minimization:** Collect only the information necessary to achieve the intended purpose.
- **Accuracy:** Ensure all data collected is correct, complete, and up to date.
- **Security:** Implement appropriate physical, technical, and organizational measures to protect data.

6.2 Rules for Data Collection

1. **Obtain Consent Where Required**
    - Ensure that consent is freely given, specific, informed, and unambiguous.
    - Document consent appropriately, particularly for sensitive data such as HIV-related information.
2. **Inform Data Subjects**
    - Clearly explain the purpose of data collection.
    - Provide information about data subjects' rights, including access, correction, and deletion.
3. **Limit Collection**
    - Collect only the information necessary for program activities.
    - Avoid requesting sensitive information unless absolutely required for the service or project.
4. **Use Secure Collection Methods**
    - Use password-protected digital forms, secure databases, or locked physical forms.
    - Avoid collecting personal data through insecure or public channels.

6.3 Rules for Data Processing

- **Purpose Restriction:** Use collected data only for the purpose communicated to the data subject.
- **Access Control:** Only authorized personnel should access personal or sensitive data.
- **Anonymization and Pseudonymization:** Where possible, anonymize or pseudonymize data to reduce risks.
- **Regular Review:** Periodically check data for accuracy and relevance.

6.4 Data Storage and Retention

- Store data securely in locked cabinets, encrypted devices, or secure cloud systems.
- Retain data only for as long as necessary for the stated purpose or as required by law.
- Safely destroy or anonymize data when no longer needed.

6.5 Data Sharing Guidelines

- Share data internally only with staff or units that require it for their roles.
- Share externally only when legally permitted, with agreements and safeguards in place.
- Avoid sharing sensitive HIV-related data unless absolutely necessary and authorized.

6.6 Breach Prevention and Reporting

- Immediately report any accidental loss, unauthorized access, or misuse of data to the supervisor or Data Protection Officer (DPO).
- Follow RRP+ breach management procedures to contain and mitigate risks.

6.7 Simplified Instructions for Staff, Peer Educators, and Volunteers

1. **Ask Permission:** Always get consent before collecting personal information.
2. **Explain Clearly:** Tell people why you need their data and how it will be used.
3. **Collect Only What You Need:** Don't gather unnecessary information.
4. **Keep It Safe:** Store data securely—use passwords, encryption, or locked cabinets.
5. **Share Carefully:** Only share data with authorized people.
6. **Fix Errors:** Correct wrong information immediately.
7. **Report Problems:** Tell your supervisor or DPO if data is lost, stolen, or misused.

7. Lawful Bases for Processing Personal Data

RRP+ processes personal and sensitive data only when there is a legal or legitimate basis to do so, in accordance with **Law No. 058/2021 on the Protection of Personal Data and Privacy**. This ensures all data collection, storage, and sharing is lawful, fair, and respects the rights of data subjects.

7.1 Lawful Bases for Processing

RRP+ relies on the following lawful bases for processing personal data:

Consent

- Data subjects voluntarily provide informed consent for their data to be collected and used.
- Consent must be freely given, specific, informed, and unambiguous.
- For sensitive data, such as HIV-related information, explicit consent is required.
- Data subjects have the right to withdraw consent at any time.

Legal Obligation

- Processing is necessary to comply with Rwandan laws, regulations, or directives from authorities.
- Examples include reporting to the Rwanda Biomedical Center (RBC) or health authorities.

Contractual Necessity

- Processing is necessary to fulfill obligations under a contract or agreement with a data subject.
- Examples include agreements with staff, volunteers, or program beneficiaries.

Legitimate Interests

- Processing is necessary for RRP+'s legitimate interests, provided it does not override the rights and freedoms of data subjects.
- Example: Data analysis for program improvement or service delivery, ensuring no harm to the individuals concerned.

Vital Interests

- Processing is necessary to protect the life or safety of a data subject.
- Example: Emergency medical response for beneficiaries.

7.2 Special Considerations for Sensitive Data

- HIV-related and other sensitive health data require **explicit consent** before collection, storage, or sharing.
- Extra safeguards must be implemented, such as limited access, encryption, anonymization, and secure storage.

7.3 Documentation and Accountability

- All lawful bases for processing must be **documented and justified.**
- Staff, peer educators, and volunteers must follow RRP+ procedures for consent collection and record-keeping.
- The DPO will periodically review processing activities to ensure compliance.

7.4 Simplified Guidance for Staff, Peer Educators, and Volunteers

1. **Ask for Consent:** Always explain why you are collecting data and get explicit permission.
2. **Respect Withdrawals:** If someone withdraws consent, stop processing their data immediately.
3. **Follow Legal Rules:** Only process data if you have a legal or programmatic reason.
4. **Handle Sensitive Data Carefully:** Limit access, secure storage, and use anonymization where possible.
5. **Keep Records:** Document consent and the purpose of data collection for accountability.

8. Rights of Data Subjects and Procedures for Exercising Them

RRP+ is committed to protecting the rights of all data subjects as established under **Law No. 058/2021 on the Protection of Personal Data and Privacy**. This section outlines the rights of individuals whose personal or sensitive data is collected, processed, or stored by RRP+, and the procedures for exercising those rights.

8.1 Rights of Data Subjects

Data subjects have the following rights:

Right of Access

- Individuals have the right to request access to their personal data held by RRP+.
- RRP+ must provide a copy of the data in a structured, commonly used format.

Right to Rectification

- Data subjects can request correction of inaccurate, incomplete, or outdated personal data.

Right to Erasure ("Right to be Forgotten")

- Data subjects can request the deletion of their personal data when it is no longer necessary, consent is withdrawn, or processing is unlawful.

Right to Restriction of Processing

- Individuals can request the temporary limitation of their personal data processing under certain circumstances, e.g., while a dispute over accuracy is resolved.

Right to Object

- Data subjects can object to processing based on legitimate interests or for direct marketing purposes.

Right to Data Portability

- Individuals can request a copy of their personal data in a structured, machine-readable format for transfer to another controller.

Rights Related to Automated Decision-Making and Profiling

- Data subjects can request not to be subjected to decisions based solely on automated processing, including profiling, that significantly affect them.

8.2 Procedures for Exercising Rights

Submitting Requests

- Data subjects can submit requests in writing, verbally, or through electronic channels to the Data Protection Officer (DPO) or designated RRP+ staff.
- Requests should include the data subject's identity and the specific right they wish to exercise.

Verification

- RRP+ may verify the identity of the requester to prevent unauthorized access or disclosure.

Response Time

- RRP+ will respond to requests without undue delay, and at the latest **within 30 days** of receipt.

Fulfillment of Requests

- Data will be provided, corrected, deleted, or restricted according to the request, subject to legal obligations and exemptions.
- If a request cannot be fully granted, the data subject will be informed with reasons.

Record-Keeping

- All requests and actions taken will be documented to demonstrate compliance.

8.3 Simplified Guidance for Staff, Peer Educators, and Volunteers

1. **Listen and Inform:** If a beneficiary asks about their data, explain that they have the right to access, correct, delete, or restrict their data.
2. **Refer Requests:** Direct the request to the DPO or designated staff.
3. **Do Not Share Without Approval:** Never provide personal data to the requester yourself unless authorized.
4. **Support the Process:** Help beneficiaries understand the forms or procedures if needed.
5. **Report Issues:** Notify your supervisor or DPO if a request cannot be handled or if there is a concern.

9. Data Sharing and Third-Party Processors

RRP+ recognizes that data sharing is sometimes necessary to achieve organizational objectives but commits to doing so in a lawful, secure, and accountable manner. This section outlines rules for sharing personal and sensitive data internally and externally, as well as managing third-party processors.

9.1 Internal Data Sharing

- **Need-to-Know Principle:** Data should only be shared internally with staff or teams who require it for legitimate programmatic or operational purposes.
- **Access Controls:** Internal sharing must be done through secure channels, with access limited to authorized personnel.
- **Documentation:** All internal data sharing must be logged, including purpose, date, and persons involved.

9.2 External Data Sharing

- **Legal and Contractual Compliance:** Personal data may only be shared with donors, partners, or governmental agencies if there is a legal obligation, contractual requirement, or explicit consent from the data subject.
- **Data Sharing Agreements:** All external sharing must be governed by formal agreements specifying the purpose, security measures, and responsibilities of the receiving party.

- **Sensitive Data Restrictions:** HIV-related and other sensitive personal data must only be shared when strictly necessary and with appropriate safeguards.

9.3 Controller-to-Controller Transfers

- When sharing data with another organization that also determines the purpose and means of processing, RRP+ ensures:
  - Both parties understand and agree to their respective responsibilities.
  - Data subjects' rights and legal obligations are respected.
  - Written agreements clearly define the limits and purpose of processing.

9.4 Cross-Border Transfers

- Transfers of personal data outside Rwanda are only permitted under the following conditions:
  1. **Adequate Safeguards:** RRP+ must provide evidence that appropriate technical, organizational, and contractual safeguards are in place to protect personal data.
  2. **Supervisory Authority Authorization:** Prior authorization must be obtained from the National Commission for the Control of Personal Data Protection (NCSA) before any transfer.
  3. **Limited Purpose:** Transfers should only occur when necessary for legitimate purposes such as program delivery, reporting to partners, or legal obligations.
- Special care must be taken when transferring sensitive personal data, such as HIV-related information, to ensure confidentiality and security.

9.5 Third-Party Processors

- **Definition:** A data processor is any external party that processes personal data on behalf of RRP+.
- **Due Diligence:** RRP+ conducts due diligence to ensure processors comply with data protection standards.
- **Processing Agreements:** All processors must sign formal agreements outlining their obligations, including confidentiality, security, and breach reporting.
- **Monitoring:** RRP+ monitors processors' compliance through audits, reports, or periodic reviews.

9.6 Simplified Guidance for Staff, Peer Educators, and Volunteers

1. **Share Only When Necessary:** Only share data internally or externally if required for your work.
2. **Get Permission:** Do not share sensitive data without approval from your supervisor or the DPO.
3. **Use Secure Channels:** Always use encrypted emails, secure platforms, or locked physical files for sharing.
4. **Respect Agreements:** Follow the terms of any contracts or agreements when working with partners or donors.
5. **Cross-Border Transfers:** Do not transfer personal data outside Rwanda without authorization from the supervisory authority and evidence of adequate safeguards.
6. **Report Concerns:** Notify your supervisor or DPO if you suspect improper data sharing or breaches.

10. Data Security and Breach Management

RRP+ is committed to ensuring the confidentiality, integrity, and availability of personal and sensitive data, particularly HIV-related information. This section outlines the security measures, breach prevention, and response procedures in accordance with **Law No. 058/2021**.

10.1 Data Security Measures

RRP+ implements a combination of physical, technical, and organizational safeguards to protect personal data:

1. Physical Security

- Store paper records in locked cabinets or restricted-access rooms.
- Maintain visitor logs and restrict access to authorized personnel only.
- Secure portable devices such as laptops and USB drives.

2. Technical Security

- Use strong passwords, multi-factor authentication, and regularly updated software.
- Encrypt sensitive personal and HIV-related data during storage and transmission.
- Implement access controls based on roles and responsibilities.
- Regularly back up electronic data in secure locations.

3. Cybersecurity Safeguards

- Install and maintain antivirus and firewall protections.
- Monitor for suspicious activities, malware, and unauthorized access attempts.
- Ensure secure Wi-Fi and network connections for all devices processing data.

10.2 Data Protection by Design and Default

- Embed privacy and security measures into all systems, processes, and projects involving personal data.
- Limit access to personal data by default and ensure data minimization principles are applied.
- Conduct risk assessments before implementing new data processing activities.

10.3 Risk Assessments and Data Protection Impact Assessments (DPIA)

- Conduct regular risk assessments to identify vulnerabilities in data handling.
- Perform DPIAs for high-risk processing activities, such as processing HIV-related data or large-scale beneficiary data.
- Implement mitigation measures for any identified risks.

10.4 Personal Data Breach Management

1. Reporting Breaches

- Staff, peer educators, and volunteers must immediately report any suspected or confirmed data breach to their supervisor or the DPO.

- Reports should include the nature, scope, and potential impact of the breach.

2. Internal Response

- The DPO will coordinate investigation and containment measures.
- Take immediate steps to prevent further unauthorized access or data loss.

3. Notification to Supervisory Authority

- If a breach is likely to result in risk to the rights of data subjects, RRP+ will notify the National Commission for the Control of Personal Data Protection (NCSA) without undue delay.
- Provide evidence of measures taken to protect personal data and mitigate risks.

4. Notification to Affected Data Subjects

- When a breach may adversely affect individuals, RRP+ will inform data subjects promptly, explaining the nature of the breach and measures taken to protect their data.

5. Corrective Measures

- Identify and implement improvements to prevent recurrence.
- Review and update policies, procedures, and technical measures as necessary.

10.5 Simplified Guidance for Staff, Peer Educators, and Volunteers

1. **Keep Data Safe:** Lock physical files, secure devices, and use passwords.
2. **Follow Rules:** Use only authorized platforms and methods for storing or sharing data.
3. **Be Alert:** Watch for suspicious activity or unauthorized access.
4. **Report Immediately:** Tell your supervisor or DPO if data is lost, stolen, or exposed.
5. **Support Containment:** Help implement corrective actions to prevent further risks.

11. Training and Awareness, Monitoring, and Compliance

RRP+ recognizes that effective data protection relies on informed and vigilant staff, volunteers, peer educators, and partners. This section outlines the organization's approach to training, monitoring compliance, and enforcing accountability.

11.1 Training and Awareness

- **Mandatory Training:** All staff, volunteers, peer educators, and relevant contractors must complete regular training on personal data protection, including HIV-related data.
- **Content of Training:** Training covers:
  - RRP+ data protection policies and procedures
  - Data subject rights and lawful bases for processing
  - Secure handling, storage, and sharing of personal data
  - Reporting and responding to data breaches
  - Data protection by design and default principles
- **Awareness Campaigns:** Periodic reminders, workshops, and updates are provided to maintain awareness of best practices and legal obligations.

- **New Joiners:** Data protection training is mandatory for all new staff and volunteers as part of onboarding.

11.2 Monitoring and Audit

- **Regular Audits:** RRP+ conducts periodic audits of data processing activities, storage systems, and access controls to ensure compliance.
- **Internal Monitoring:** Supervisors and the DPO regularly monitor adherence to the policy and provide guidance where gaps are identified.
- **Documentation:** Records of audits, monitoring activities, and corrective actions are maintained for accountability.

11.3 Compliance Mechanisms

- **Policy Adherence:** All individuals under the scope of this policy are required to comply with its provisions.
- **Reporting Non-Compliance:** Any suspected violation of this policy must be reported to the supervisor or DPO immediately.
- **Sanctions for Non-Compliance:**
    - Non-compliance may result in disciplinary action, including verbal/written warnings, suspension, or termination of employment or engagement.
    - Contractors or partners found in violation may face contract termination or legal consequences.
- **Continuous Improvement:** Feedback from audits, breaches, and staff observations informs updates to policies, procedures, and training programs.

11.4 Simplified Guidance for Staff, Peer Educators, and Volunteers

1. **Participate in Training:** Attend all mandatory data protection and privacy sessions.
2. **Follow Procedures:** Always follow RRP+ data protection policies and instructions.
3. **Be Vigilant:** Monitor your own practices and the practices of your team for compliance.
4. **Report Problems:** Tell your supervisor or DPO if you see someone violating data protection rules.
5. **Learn and Improve:** Apply lessons from training, audits, and feedback to your daily work.

12. Annexes

RRP+ recognizes that effective personal data protection requires integration with other organizational policies and access to practical tools.

Annex 1: Mapping of RRP+ Practices to Data-Protection Principles

Data-Protection Principle	RRP+ Practical Application	Responsible Person
Lawfulness, Fairness & Transparency	Collect data only with lawful basis (consent, legal obligation, etc.); provide privacy notices in Kinyarwanda/English	DPO / Field Officers
Purpose Limitation	Collect data solely for HIV program, membership, and service delivery purposes	Program Managers
Data Minimization	Collect minimum required variables (no unnecessary personal details)	Data Collectors
Accuracy	Verify forms monthly; update contact and treatment info regularly	M&E Officer
Storage Limitation	Retain only for project duration + 3 yrs, then anonymize/destroy	DPO / IT Officer
Integrity & Confidentiality	Encrypt digital files, lock paper records, limit access	IT Officer / Program Managers
Accountability	Maintain records of processing, conduct quarterly audits	Executive Secretary, DAF and DPO

Annex 2: Data-Subject Rights – Quick Reference Procedure

Purpose:

To ensure that all individuals whose personal data is processed by RRP+, including People Living with HIV (PLHIV), staff, volunteers, and partners, can exercise their rights under **Law No. 058/2021 on the Protection of Personal Data and Privacy** in a consistent, transparent, and timely manner.

Rights of Data Subjects

Right	Description	Example in RRP+ Context	Required Action
Right of Access	Request confirmation that RRP+ holds their personal data and obtain a copy.	A beneficiary asks for a copy of their registration form.	Verify identity → Provide copy within 30 days → Log action.
Right to Rectification	Correct inaccurate or incomplete data.	Participant changes phone number or clinic.	Update database → Confirm correction to requester.
Right to Erasure ("Right to be Forgotten")	Request deletion of their data if no longer needed, or if consent withdrawn.	Former peer educator asks RRP+ to delete her records.	Assess legal need → If no retention obligation, delete securely.
Right to Restrict Processing	Pause use of data while dispute is resolved.	Beneficiary contests accuracy of viral-load record.	Freeze record (read-only) until resolved.
Right to Object	Refuse data use for specific purposes (e.g., communications).	Member objects to use of image in advocacy materials.	Stop processing for that purpose → Note objection.
Right to Data Portability	Receive data in a machine-readable format for transfer.	Staff requests Human Resource (HR) record for transfer to another employer.	Export CSV/PDF and transmit securely.
Rights re: Automated Decisions & Profiling	Refuse decisions made solely by systems without human input.	Automated eligibility system denies support.	Ensure human review before final decision.

Procedure for Handling Requests

Step 1 – Receive and Log Request

- Accept via letter, email, form, or verbal statement.
- Record immediately in the *Data-Rights Request Register* (see table below).
- Forward to **Data Protection Officer (DPO)** within 24 hours.

Step 2 – Verify Identity

- Confirm requester's identity (National ID, membership card, or known contact).
- For minors or dependent PLHIV, verify guardian consent.
- Document verification method.

Step 3 – Acknowledge Receipt

- Within **5 working days**, send written or electronic acknowledgment using the template below.
- Include expected response timeframe (≤ 30 days).

Step 4 – Assess Request

- DPO and responsible manager determine:
  - Which right is invoked;
  - Whether legal exemptions apply (e.g., data required by donor, etc);
  - Actions and responsible persons.

Step 5 – Implement Decision

- **Grant:** Fulfill request, update systems, issue confirmation.
- **Refuse (partially or fully):** Provide written justification citing legal grounds.
- **Extend:** If complex, one-time 30-day extension allowed with notice.

Step 6 – Communicate Outcome

- Provide clear written response in Kinyarwanda or English.
- Deliver securely (sealed envelope or encrypted email).
- Include appeal information (to RRP+ DPO or NCSA).

Step 7 – Archive and Report

- File all documentation (request, ID proof, correspondence, outcome).
- Log completion in *Data-Rights Request Register*.
- DPO compiles quarterly report to Senior Management Team and Board.

Templates for Communication

A. Acknowledgment of Request

Subject: Acknowledgment of Your Data-Protection Request

Dear [Name],

RRP+ has received your request dated [Date] concerning [type of right].

We will process it in accordance with Law No. 058/2021 and respond within **30 days**.

For questions, contact the Data Protection Officer at jbtugirimana@rrpplus.org.

Sincerely,

[Name] – Data Protection Officer, RRP+

B. Fulfillment Confirmation

Subject: Confirmation of Action on Your Data Request

Dear [Name],

Your request for [e.g., correction of contact details] has been completed on [Date].

Updated information: [summary].

Thank you for helping us keep your information accurate.

Best regards,

[Name] – Data Protection Officer, RRP+

C. Refusal or Partial Refusal Notice

Subject: Response to Your Data-Protection Request

Dear [Name],

After review, RRP+ cannot fully grant your request to [type of request] because [reason, e.g., data required by legal reporting].

You may appeal to the RRP+ Executive Secretary or file a complaint with the National Cyber Security Authority (NCSA).

Sincerely,

[Name] – Data Protection Officer, RRP+

Data-Rights Request Register (Tracking Log)

No	Date Received	Name / ID	Right Invoked	Verified (Y/N)	Action Taken	Response Date	Outcome (Granted / Denied)	Staff Handling	Notes
1	15-Nov-25	A.B.	Access	Y	Copy of file provided	30-Nov-25	Granted	JBT / Field Officer	—
2	20-Nov-25	C.D.	Erasure	Y	Deleted non-essential records	05-Dec-25	Partial	DPO	Retained legal reports only

Special Guidance for HIV-Related or Sensitive Requests

- Confirm that the request comes **directly from the data subject** or authorized guardian—never share via intermediaries.
- All HIV-status data must be transmitted in **sealed or encrypted form** only.
- If deletion or transfer could endanger continuity of care, consult the Program Manager and DPO before proceeding.
- Maintain absolute confidentiality: no verbal disclosure of HIV-related data to non-authorized persons.

Escalation and Appeals

If the requester is not satisfied:

1. They may appeal in writing to the **RRP+ Executive Secretary** within 15 days.
2. If unresolved, they may lodge a complaint with the **National Cyber Security Authority (NCSA)**, which oversees Law No. 058/2021 enforcement.
3. The DPO must cooperate fully with NCSA investigations.

Responsibilities Summary

Role	Key Duties
Data Protection Officer (DPO)	Receives, logs, verifies, coordinates response, communicates results, reports quarterly.
Program Managers	Ensure data updates and corrections in systems; provide requested copies.
Field Officers / Peer Educators	Support beneficiaries to complete forms and understand their rights.
IT Officer	Implement data corrections, deletions, and security during transfers.
Executive Secretary	Approves complex or sensitive disclosures; handles appeals.

Annex 3: Data-Security Standards Checklist

Category	Standard	Status (Yes/No/N.A.)	Responsible
Physical Security	Paper files locked after use		
	Visitors signed in/out		
Technical Security	Password-protected computers		
	Antivirus + firewall installed		
Access Control	Role-based access list updated quarterly		
Encryption	HIV-related data encrypted at rest & transit		
Backup	Weekly encrypted backup maintained off-site		
Incident Logging	All breaches recorded in Breach Log		
Training	Annual data-protection refresher done		

Annex 4: Personal Data Breach Handling Procedure

Step	Action	Responsible	Timeline
1	**Detect & Report** – Any staff/volunteer reports suspected breach to DPO via email/phone	All staff	Immediately
2	**Contain** – Secure systems/files, revoke access, isolate affected device	IT Officer	Within 2 hrs
3	**Assess Impact** – Determine categories/volume of data, risk to subjects	DPO + Program Manager	Within 24 hrs
4	**Notify NCSA** (if risk likely)	DPO / Executive Secretary	≤ 72 hrs
5	**Notify Affected Individuals** (if high risk)	DPO	≤ 5 days
6	**Remediate & Document** – Apply corrective actions, record in Breach Register	DPO + IT Officer	Ongoing
7	**Review & Learn** – Update controls, training	Senior Management Team (SMT) and DPO	Within 30 days

Annex 5: Data-Sharing and Third-Party Agreement Template

Between: Rwanda Network of People Living with HIV (Acronym RRP+)

And: _____ ("Processor/Partner")

1. Purpose

To define obligations on protection of personal and sensitive data processed on behalf of RRP+.

2. Roles

- RRP+ = Data Controller
- Partner = Data Processor

3. Obligations of Processor

- Process only on documented instructions from RRP+.
- Maintain confidentiality; restrict access to authorized staff.
- Implement appropriate technical & organizational measures (encryption, passwords, backups).
- Report any data breach to RRP+ within 24 hours.
- Permit audits by RRP+ or NCSA.

4. Termination

Upon contract end, return or securely destroy all RRP+ data and confirm in writing.

5. Governing Law

Law No. 058/2021 of 13/10/2021 on the Protection of Personal Data and Privacy, Republic of Rwanda.

Signatures

_____ Partner Date _____
_____ RRP+ Executive Secretary Date _____

Annex 6: Standard Consent Forms

A. Beneficiary Consent Form (for PLHIV Program Participants)

Purpose of Data Collection: To provide HIV support services and monitor outcomes.

Data Collected: Name, contact, HIV status, treatment adherence, and service records.

Storage & Protection: Encrypted digital database / locked cabinet.

Rights: You may access, correct, or withdraw consent at any time by contacting RRP+ DPO (ibtugirimana@rrpplus.org).

Signature of Participant: _____ Date _____

Witness / Peer Educator: _____ Date _____

B. Staff and Volunteer Confidentiality Agreement

I understand that all personal and HIV-related information obtained through RRP+ activities is confidential. I will:

- Use data only for authorized RRP+ purposes.
- Keep files and devices secure.
- Report any suspected breach immediately.

Name: _____

Position: _____

Signature: _____

Date: _____

Annex 7: Acknowledgment of Understanding and Compliance

For RRP+ Staff, Volunteer, and Peer Educator Acknowledgment Form

I, the undersigned, acknowledge that I have received, read, and understood the **RRP+ Personal Data Protection Policy** (Version 1.1, October 2025).

I agree to comply fully with its provisions and with Rwanda's **Law No. 058/2021 on the Protection of Personal Data and Privacy**.

I understand that:

- I am personally responsible for safeguarding the confidentiality of personal and sensitive data obtained in the course of my duties;
- I must report any suspected or actual data breach immediately to my supervisor or the Data Protection Officer; and
- Any breach of this policy may result in disciplinary or legal action.

Full Name	Position / Role	Signature	Date