WOMEN EMPOWERMENT FOR RECONCILIATION & DEVELOPMENT (WERD)

DATA PROTECTION POLICY

Rev: June 2020

This Data Protection Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Data Protection Policy, or it has stricter requirements than this Policy.

The content of this Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed

WERD DATA PROTECTION POLICY

1. POLICY STATEMENT

WERD believes that Data and Information should be at the service of every citizen, and that our use of such data shall not violate human identity, human rights, privacy or individual or public liberties. Ensuring data protection is the foundation of trustworthy relationships and WERD's reputation as a credible and responsible organization.

WERD is committed to international compliance with data protection laws. This Data Protection Policy applies to country wide to WERD and is based on globally accepted, basic principles on data protection.

The WERD Data Protection Policy ensures the adequate level of data protection as prescribed by relevant legal frameworks, including in countries that do not yet have adequate data protection laws.

The WERD Data Protection Policy is meant to be a practical and easy to understand document to which all WERD departments, stakeholders and partners can refer to.

2. SCOPE OF POLICY

This Data Protection Policy applies to WERD offices in South Sudan of operation.

This policy applies to all WERD Employees and Related-Personnel.

Related Personnel includes board members, volunteers, interns, visitors and international and local consultants, in addition to individual and corporate contractors/ suppliers, implementing partners and subgrantees. This includes non-WERD entities and their employees and individuals who have entered into partnership, as well as community volunteers and incentive workers. The policy applies both during, and outside, normal work hours.

Actions taken by WERD Employees and Related Personnel outside of working hours that are seen to contradict this policy will be seen as a violation of this policy.

WERD's Data Protection Policy applies to all personal data that WERD holds relating to and identified or identifiable individuals.

3. DEFINITIONS

Personal Data; 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.

Examples or personal data include but are not limited to;

- Names of individuals

- Postal or residential addresses
- Email addresses
- Telephone numbers
- Identity card and passport details
- Date and place of birth
- Identification of relatives
- Fingerprints
- Business reference
- Geo-referencing

Processing of Personal Data; Any operation or set of operations in relation to such data, whatever the mechanism 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.

WERD's Sets of Personal Data: WERD's Data Protection Policy applies to all sets of personal data, currently stored, maintained and handled by WERD, and more specifically to the following identified sets of personal data;

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

4. LEGAL FRAMEWORK AND ASSOCIATED POLICIES

WERD is headquartered in Juba and observes the laws of South Sudan and of the Geneva Canton, including the Federal Act on Data Protection of 19 June 1992 (the Data Protection Act, the "DPA") and the Ordinance to the Federal Act on Data Protection of 14 June 1993 ("ODPA").

This Data Protection Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Data Protection Policy, or it has stricter requirements than this Policy.

The content of this Data Protection Policy must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

WERD has rules and standards that seek to create a consistent approach and which, in some cases, may be stricter than national or local laws. This Policy must, therefore, be followed in addition to the relevant national and local laws on data protection. In the event of conflicts between national legislation and the Data Protection Policy, WERD will work with the relevant institution in the country to find a practical solution that meets the purpose of the Data Protection Policy.

The purpose of the policy is aimed at guiding WERD staff and must be considered together with:

- WERD Code of Conduct and Code of Ethics
- WERD Gender Equality Policy
- WERD Stories and Images Consent Policy
- WERD Protection from Sexual Exploitation, Harassment and Abuse Policy

5. PRINCIPLES FOR COLLECTING PERSONAL DATA

5.1 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 voluntary and informed consent of the data subject concerned.

5.2 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 take decisions with respect to the data subjects.

5.3 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 being collected
- Categories of third parties to whom the data might be transmitted

5.4 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.

5.5 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 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.

5.6 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.

6. PRINCIPLES FOR PROCESSING PERSONAL DATA

6.1 Consent to Data Processing

Processing of personal data can only proceed with the informed consent of the data subject or meet one of the following conditions:

- Compliance with any legal obligation to which WERD is subject
- The protection of the data subject's life
- The performance of a public service mission entrusted to WERD.

6.2 Data Processing Persuant to Legitimate Interest

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.

7. TELECOMMUNICATION AND THE INTERNET

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by WERD primarily for work-related assignments. They are a tool and an organizational resource. They can be used within the applicable legal regulations and internal WERD 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 WERD 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 may 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 WERD. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the WERD regulations.

8. RIGHTS OF THE DATA SUBJECT

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

- To request information on which personal data relating to him/her has been stored, how the data was collected, and for what intended purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected. If personal data is transmitted to third parties, individuals should be informed of such a possibility. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.

- To request his/her data to be deleted if the processing of such data has no legal basis or if the legal basis has ceased to apply; The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

- To object to his/her data being processed and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

9. TRANSMISSION OF PERSONAL DATA

Transmission of personal data to recipients outside or inside WERD is subject to the authorization requirements for processing personal data under Section 6 and requires the consent of the data subject. The data recipient must be required to use the data only for the defined purposes.

In the event that data is transmitted to a recipient outside WERD, this recipient must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation.

The processing of personal data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the individual that merit protection must be taken into consideration.

In certain circumstances, the WERD Data Protection Policy allows personal data to be disclosed, based on a legal obligation, to law enforcement agencies, without the consent of the data subject.

Only the WERD Executive Director can validate any such disclosure in writing, ahead of the disclosure, after ensuring the request is legitimate, motivated by the requester, appropriate, necessary and does not pose a threat or direct risk to WERD.
Before approving such disclosure, WERD's Executive Director will check that the recipient of the data uses the data for the defined purposes only, and that it demonstrates the capacity and will to abide by such an obligation.

Where necessary, WERD's Executive Director will refer to legal advisers for advice, and to WERD's Committee for validation, notably but not only in cases involving direct security threats and implications or global organizational risks including reputation
.

10. PROVIDING INFORMATION

WERD aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the current policy is shared with all WERD staff and available on request by individuals.

A version of this Policy is also available upon request to WERD HQ.

Any subscriber or user of an electronic communication service shall be informed in a clear and comprehensive manner by WERD, except if already previously informed, regarding: the purpose of any action intended to provide access, by means of electronic transmission,

to information previously stored in their electronic connection terminal device, or to record data in this device; the means available to them to object to such action.

11. 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 employees 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, as well as implementation, of roles and responsibilities.

12. PROCESSING SECURITY

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.