Data Protection Policy

1 Purpose

WELDO is committed to document its business activities with records that are complete, authentic, reliable, secure and accessible and comply with data protection requirements of EU GDPR throughout their lifecycle, from planning and creation to ultimate disposal. It also ensures to comply with all data protection principles.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

2 Scope

This policy applies to all staff of WELDO (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with WELDO). Adherence to this policy is mandatory and non- compliance could lead to disciplinary action.

3 Policy Overview

Our Data Retention Policy and processes comply fully with the GDPR's Article 5 principle:

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

4 Roles and Responsibilities under GDPR

4.1 Top Management

All those in senior managerial role at WELDO are responsible for sponsoring & approving funds required for GDPR implementation, Approving data protection/privacy policy and its objectives, Ensuring that compliance with data protection legislation under the DPA, EU GDPR, any other data protection legislation and good practice can be demonstrated

4.2 Data Protection Officer

Data Protection Officer/GDPR owner is responsible for single point of contact for GDPR related activities, ensuring implementation of the data protection policy, training and ongoing awareness as required by the data protection policy. Ms. Sijal Aziz (email: dpo@weldo.org) has been appointed as Data Protection Officer/GDPR owner and is responsible for compliance under GDPR.

4.3 Employees

Employees are responsible for ensuring that they comply with data protection/privacy policy and its objectives, adhere to data protection/privacy policy directions such as consent management, document retention, detection of data breach and breach notification.

4.4 General Responsibilities

4.4.1 The Data Protection Officer/GDPR owner is responsible for ensuring that WELDO does not collect information that is not required for the purpose for which it is obtained.

4.4.2 All data collection forms (electronic or paper-based), including data collection requirements include a Data Protection Policy or link to Data Protection Policy are approved by the Data Protection Officer.

4.4.3 Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by internal audit or external experts to ensure that collected data continues to be adequate, relevant and not excessive.

4.4.4 Data Protection Officer is responsible to ensure that Personal data is accurate and kept up to date with every effort to erase or rectify without delay.

4.4.5 WELDO ensures that no data should be kept unless it is reasonable to assume that it is accurate.

4.4.6 WELDO ensures that all employees are trained in the importance of collecting accurate data and maintaining it.

4.4.7 It is also the responsibility of the data subject to ensure that data held by WELDO is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.8 Employees/Clients/Vendors should be required to notify WELDO of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of WELDO to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.9 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.10 Data Protection Officer will review the retention dates of all the personal data processed by WELDO, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose as defined in 'Data Retention & Erasure Policy'. This data will be securely deleted/destroyed in line with the Secure Disposal as defined in 'Data Retention & Erasure Policy'.

4.4.11 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests.

5 Data Protection Principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

5.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

5.2 Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

5.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimization).

5.4 Accurate and where necessary kept up to date (Accuracy).

5.5 Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

5.6 Processed in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

5.7 Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

5.8 Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

6 Lawful, Fairness, Transparency

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

6.1.1 Lawful – identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing”, for example consent.

6.1.2 Fairly – in order for processing to be fair, the data processor has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

6.1.3 Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject using clear and plain language.

7 Purpose Limitation

7.1 Collected only for specified, explicit and legitimate purposes

7.2 Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of GDPR register of processing.

7.3 WELDO shall not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have provided Consent where necessary.

8 Data Minimization

8.1 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimization).

8.2 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

8.3 WELDO may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

8.4 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9 Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

9.1 WELDO maintains a records retention and disposal schedule to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. Refer to “Data Retention & Erasure Policy”.

9.2 WELDO will take all reasonable steps to destroy or erase all Personal Data that we no longer require in accordance with WELDO’s Data Retention & Erasure Policy. This includes requiring third parties to delete such data where applicable.

9.3 Data Subjects must be informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10 Security Integrity and Confidentiality

10.1 Protecting Personal Data

10.1.1 Personal Data must be secured by appropriate technical and organizational measures against unauthorized or unlawful Processing, and against accidental loss, destruction or damage.

10.1.2 WELDO regards the lawful and correct handling of personal data as essential to its successful operation. To this end WELDO maintains an Information Security Management System certified to the international security standard ISO 27001 to protect the confidentiality, integrity and availability of corporate information, including personal data entrusted to us by our customers, employees and stakeholders.

10.1.3 The WELDO Information Security Management System maintains data security by protecting the confidentiality, integrity and availability of Personal Data, defined as follows:

10.1.4 **Confidentiality** means that only people who have a need to know and are authorized to use the Personal Data can access it.

10.1.5 **Integrity** means that Personal Data is accurate and suitable for the purpose for which it is processed.

10.1.6 **Availability** means that authorized users are able to access the Personal Data when they need it for authorized purposes (including Data Subjects when exercising their Rights under GDPR).

10.1.7 WELDO employees are responsible for protecting the Personal Data that it holds. WELDO employees must comply with and not attempt to circumvent the administrative procedures, physical and technical safeguards that are implemented and maintained in accordance with the GDPR and the ISO27001 standard to protect Personal Data. These are set out within the WELDO Information Security Policies.

10.2 Reporting a Personal Data Breach

10.2.1 The GDPR requires Controllers to notify certain Personal Data Breaches to the Information Commissioner’s Office and, in certain instances, the Data Subject.

10.2.2 The Data Breach Management Policy sets out the procedures in place to deal with any suspected Personal Data Breach.

10.2.3 If a WELDO employee knows or suspects that a Personal Data Breach has occurred, they should follow the Data Breach Management Policy. Immediately

advise their line manager and contact the DPO. They should preserve all evidence relating to the potential Personal Data Breach.

11 The rights of the data subjects

11.1 Data Subjects have rights when it comes to how WELDO handles their Personal Data. These include rights to:

11.1.1 receive certain information about the Data Controller's Processing activities (the Privacy Notice);

11.1.2 request access to their Personal Data that we hold (commonly known as a. subject access request);

11.1.3 ask WELDO to rectify inaccurate data or to complete incomplete data;

11.1.4 ask WELDO to erase Personal Data if we have no lawful basis to process it;

11.1.5 restrict Processing in specific circumstances;

11.1.6 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format

11.1.7 challenge Processing which has been justified on the basis of WELDO's legitimate interests or in the exercise of WELDO's official authority; and

11.1.8 object to direct marketing and decisions based solely on Automated Processing, including profiling (ADM);

11.2 Where applicable WELDO employees must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

11.3 WELDO employees must immediately forward any Data Subject rights request received to the Data Proceesing Officer via dpo@weldo.org.

12 Retention and Disposal of Data

12.1 WELDO will not keep personal data in a form that permits identification of data subjects and for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

12.2 The retention period for personal data is defined in 'Data Retention and Erasure Policy' along with the statutory obligations WELDO has to retain the data.

12.3 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the 'Data Retention and Erasure Policy'.

13 Privacy by Design and Data Protection Impact Assessment (DPIA)

13.1 WELDO is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

13.2 WELDO employees must complete a DPIA screening questionnaire to establish whether one will needed to be completed for any Processing we plan to undertake as part of a new project or procurement.

13.3 WELDO should conduct a DPIA when implementing major system or business change programs involving the Processing of Personal Data including:

13.3.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

13.3.2 Automated Processing including profiling and ADM;

13.3.3 large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

13.3.4 large scale, systematic monitoring of a publicly accessible area.

13.4 A DPIA must include:

13.4.1 a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

13.4.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

13.4.3 an assessment of the risk to individuals; and

13.4.4 the risk mitigation measures in place and demonstration of compliance.

14 Audits, monitoring and training

14.1 Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. Regular audits of our data protection processes and information security management system will be carried out in accordance with our ISO 9001 & 27001 accreditations.

14.2 Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. WELDO will keep this policy under review and amend or change it as required. Notification should be given to the DPO of any breaches of this policy. Compliance with this policy will be in full and at all times.

14.3 Training

All employees of WELDO will receive adequate training on provisions of data protection law specific for their role. Further training will be given as requested or if there is a move in role or responsibilities.

15 Reporting Data Breaches

15.1 Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as we have become aware of a breach. WELDO has a legal obligation to report any data breaches to its relevant partners within 72 hours.

15.2 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

15.2.1 Investigate the failure and take remedial steps if necessary

15.2.2 Maintain a register of compliance failures

15.2.3 Notify the DPO of any compliance failures that are material either in their own right or as part of a pattern of failures

15.3 Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.