Global Data Privacy Policy of SONGWON Industrial Group

1. Purpose and Principles

This Global Privacy Policy contains regulations on the protection of personal data that apply to all full consolidated SONGWON entities (hereinafter individually the "Group Company", collectively the "Group Companies" or the "Group"). It sets out the importance and significance of data protection in terms of respect for the fundamental rights and freedoms of employees, customers and business partners.

This policy provides employees with the most important principles of data protection and enables them to carry out their activities in compliance with data protection law.

The Swiss (FADP) and European (GDPR) data protection laws are serving as basis for this Global Privacy Policy. Both (FADP / GDPR) data protection laws pursue the same two main goals as every other local data protection does:

- to protect natural persons with regards to the processing of their personal data (**fundamental right**) and
- to support the free movement of such data across international borders (**economic aspect**).

The data protection laws FADP and GDPR are applicable in Switzerland and in all EU member states respectively. They apply to the effects of the processing of personal data in Switzerland or in the EU, regardless whether the processing takes place in Switzerland/the EU or elsewhere and regardless whether the personal data concerned relates to persons domiciled in Switzerland/the EU or elsewhere.

2. Subject

The subject of this Global Privacy Policy is the **processing** of **personal data** wholly or partly by automated means. It also relates to the processing of personal data by any other means (on paper, or orally).

For the better understanding of the subject noted above we explain following the key words:

- **What is personal data and what is not?**

Personal data is any information relating to an individual natural person that can be identified. A person can be identified directly or indirectly, by reference to certain information (such as name, ID or social security number, age and date of birth, address, phone number, email address, gender, marital status, photograph, online identifier such as IP address, location, etc.) or to specific physical, physiological, genetic, mental, economic, cultural or social

identity. If the data allows singling out an individual in a group through a combination of different information which alone might not be personal, such data is considered personal data.

In order to consider that the data "relate to" an individual, one of the following three elements, in particular the content one, should be present:

- content (Data about a person)
- purpose (What is the outcome?)
- result (Can the use of data have an impact on a person's rights?)

> ***Example**: The Analysis and Intelligence Unit of the Labour Inspectorate has requested the following information from the Ministry for Social Protection: name and surname, sex, ID number / passport number, date of birth, nationality, address, name and seat of the employer, party for whom the services are provided, location of work, period of posting (number of days), remuneration / basic monthly salary (in EUR), other monthly allowances (in EUR), unemployment benefits received in 2022, victim of an accident at work in 2022.*
>
> *Data such as name and surname, sex, ID number / passport number, date of birth, nationality, address are identifiers based on which an individual can be directly or indirectly identified, hence constitute personal data (**content element**). Information identifying a person as a victim of an accident at work in 2022 is not only personal data but sensitive personal data. Furthermore, even information regarding the period of posting (number of days), remuneration / basic monthly salary (in EUR), other monthly allowances (in EUR), and unemployment benefits received in 2022 are personal data as such data give information about the specific situation of an individual and will likely be used to evaluate, treat in a certain way, or influence a status or behaviour of an individual (**purpose element**). E.g. individuals with longer posting periods and salary below the minimum level might be scrutinised more intensely. Finally, even the name and the address of the employer / a third party and the location of work can be seen as personal data, if such data will be used to have an impact on a certain person's rights and interests (**result element**). E.g. such information might be personal data of the employer and also relate to the individuals working for a certain employer on a specific-construction site as it puts them at a concrete place at a specific time and might lead to further investigations int their employment relationship.*

> ***Note**: Under certain circumstances even the following types of data could be considered as personal data: service history of a person's vehicle, letter sent by an insurance company to an insured person, data collected by an electronic water metre about water use in an apartment, a house evaluation if it can be linked to an individual owning the house or living in it, call log of a telephone, information contained in the minutes of a meeting, which cover certain aspects on an individual).*

- **What is anonymous data?**

Anonymous data is any information relating to a natural person where the person can no longer be identified. Aggregated statistics, ratios, percentages etc. are not personal data as long as the sample group is large enough.

- **What is sensitive personal data?**

Where personal data relate to the health, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, or biometric data of an individual, they are considered a special category of personal data (referred to as "sensitive personal data"). Financial information is not sensitive in this sense. This may even

include data that inadvertently reveal one of these aspects, such as attendance at a particular health clinic or religious event, dietary preferences, etc. These data merit specific protection as they are by their nature particularly sensitive, or their processing could create significant risks to the fundamental rights and freedoms.

> ***Note**: Photographs are covered by the definition of biometric data only when processing through specific technical means allowing the unique identification or authentication of a natural person (e.g. facial recognition).*

- **What is processing?**

Processing includes almost any activity related to personal data such as collection, recording, organization, structuring, access, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, linkage, dissemination or otherwise making available, alignment or combination, restriction, erasure or even destruction.

> ***Example**: All activities of the Analysis and Intelligence Unit of the Labour Inspectorate such as requesting certain data, obtaining data in electronic and physical form (USB key), storing data, extracting information from Excel files and the USB key, analysing data, creating new Excel files, placing Excel files in a cloud, deleting unnecessary data, sending data to the undertakings, receiving additional data, sending data or enabling access to data to the Health and Safety Unit etc. are considered to fall under the definition of processing.*

3. Scope of Application

This Global Privacy Policy applies to all employees of the Group who process personal data.

For all employees, the "Privacy Policy for Employees of the SONGWON Industrial Group" shall apply in addition. (cf. **Annex 1**)

4. Principles for the Processing of Personal Data

If personal data about a certain person shall be processed, such person shall be informed appropriately about each data collection, the identity and contact details of the person responsible for the data processing, the purpose of the processing, the recipient(s) of the data and the country of export in the case of data export. In addition, they observe the following principles when processing personal data:

- **Lawfulness, Processing in Good Faith, Transparency**

Personal data must be processed lawfully, in good faith and in a manner that is comprehensible to the person concerned. "Comprehensibility" requires in particular that the scope and purpose of the acquisition and processing of such data are recognizable or explained to the respective person. Whenever personal data is collected by employees, they must ensure that the person concerned has been informed about and that agreed to the collection of such data.

- **Purpose Limitation (Why are we processing?)**

Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with these purposes. The processing of data for other than the accepted purpose is therefore not permitted.

> ***Example: Hungarian internet and TV provider***
> *In a recent case, the Court of Justice of the European Union needed to decide whether a Hungarian internet and TV provider breached the principle of purpose limitation by moving their customer database into a test database to repair a technical error. The Court ruled that the principle of purpose limitation does not prevent such use of previously collected and stored personal data, since this further processing (fixing a technical problem) is compatible with the specific purposes for which the personal data was initially collected (providing TV and internet services) and customers could expect such further processing.*

- **Data Minimization and proportionality (What exactly do we need for our purpose?)**

Personal data must be adequate and relevant to the purpose and limited to the extent necessary for the purposes of processing. Therefore, no more data may be collected than is reasonably necessary for the processing purpose.

> ***Example: Hotel***
> *The AEPD (Spanish DPA) ruled that a hotel that scanned guests' passports for identification purposes was not compliant with the principle of data minimisation. When guests checked into the hotel, their passport was scanned as part of the registration process. The passport scan included more personal data than what was required for the purpose. Collection of an ID number, for example, would have been sufficient for identification.*

> ***Example: Good practice - Dealing with court requests***
> *The national court requested from the Labour Inspectorate information about 34 persons although the court case only covered one person. The Labour Inspectorate is obliged by national law to cooperate with judicial authorities; however, it seemed that the court's request was excessive in light of the data minimisation principle. Before responding, the Inspectorate should consult its Data Protection Officer (DPO) and not simply transfer all data without further consideration. In order to demonstrate compliance with data protection principles, the Inspectorate could also ask the court for further clarification as to why the data of the remaining 33 persons are also necessary for the processing purpose and document such correspondence. Upon reassurance by the court that the data protection principles had been followed, the Inspectorate could then transfer the files.*

- **Data Protection through Technology Design and through Data Protection-friendly Default Settings ("privacy by design" and "privacy by default")**

The Group Companies shall take appropriate technical and organizational measures to ensure that, by default, personal data is only processed to an extent in which such processing is necessary for the specific purpose in question. Therefore, appropriate measures shall be taken to reasonably limit i) the amount of personal data collected, ii) the scope of its processing, iii) its storage period and iv) its accessibility. E.g. it shall be ensured by means of pre-settings that personal data is made accessible to those person only who need it in the scope of their work.

- **Accuracy (making sure that the data is correct)**

Any employee processing data shall ensure that the information stored about someone is accurate and up-to-date. Employees who become aware of incorrect data shall notify their superior or, if they have the appropriate processing rights themselves and there is no doubt, correct the data independently.

- **Storage Limitation (data retention - how long will we keep the data?)**

Personal data must be stored in a form that permits identification of a specific individual for no longer than is necessary for the purposes for which the data is processed. Data that is no longer required must therefore be deleted or, if necessary, anonymized after consultation with the superior. The question how long data shall be stored cannot be generalized and must be assessed on a case-by-case basis.

- **Data security (integrity and confidentiality) (How can we keep the data safe against the risk of interference?)**

Personal data must be processed in a manner that ensures appropriate security, including protection by appropriate technical and organizational measures. It shall be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. Employees must ensure that only persons, including other employees, can access or process personal data whose authorization has been clearly established.

5. Directory of Processing Activities

The respective Group Company and, if applicable, its representative shall maintain a register of the processing activities (cf. sample in **Annex 2**) under its responsibility. The information required for this purpose can be found in the aforementioned Annex.

6. Rights of Persons affected by the Processing of Privat Data

The following rights and information obligations must be observed when personal data is collected: Thereby, the persons concerned have the right of access to the relevant personal data and they may object to such data processing, or they may request that incorrect information is rectified or deleted.

Unless it is obvious, the names and contact details of the data processors at the time the personal data is collected shall be revealed to the person in question, and in particular he or she shall be informed of the following:

a) the purposes for which the personal data are to be processed,
b) the legal basis or the commercial requirement for the processing;
c) where applicable, the recipients or categories of recipients of the personal data;
d) where applicable, the intention to transfer the personal data to a third country and the appropriate or adequate safeguards.

e) the duration for which the personal data will be stored or, if this is not possible, the criteria for determining this duration;

7. Transfer of Personal Data to Third Parties

Principle

Any transfer of personal data to a third country or an international organization is only permitted if it has been communicated to the person concerned and comparable protection exists for the third country, or for the processor concerned. Third countries are all states other than those in which the data is collected.

In the absence of an adequacy decision by the competent authority, the Group may transfer personal data to a third country or international organization only if it has provided for appropriate safeguards (e.g. the standard data protection clauses of the Group).

Transfers between Group Companies

All Group Companies constitute so-called third parties for data protection purposes. As a basis for a uniform Group-wide procedure, the companies conclude an intercompany agreement (**Annex 3**: Standard Data Processing Agreement), whereby all Group Companies are appointed as both "controller" and "processor". The Agreement regulates the obligations of the contracting parties according to their role as Controller as well as their role as Processor and it shall additionally list the countries to which data may be transferred.

Transfers to other Third Parties

The Group transfers Personal Data to other third parties and grants them access to Personal Data only if it is guaranteed that the data will be lawfully processed and adequately protected by the recipient.

In this case, the respective Group Company shall conclude a corresponding data processing contract with the processor (**Annex 3**) or shall integrate suitable clauses into existing contracts, with which the processor is obliged to comply with the principles of data protection law. In particular, it shall be obligated to protect the data from further disclosure, to process the data only in accordance with the respective instructions of the Group, and to take appropriate technical and organizational measures to protect the personal data and to report personal data breaches.

8. Technical and Organizational Measures

The Group Companies and their IT departments shall take the appropriate technical and organizational measures in compliance with this Global Privacy Policy to ensure the security of personal data in accordance with the applicable data protection regulations.

9. Data Protection-impact Assessment

An assessment of the consequences of intended processing operations is legally required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling. Such activities are not carried out in the SONGWON Industrial Group.

Any Group Company shall seek the advice of the Data Protection Coordinator in advance in case it intends to carry out such systematic evaluation of personal data or profiling.

10. Notification of Personal Data Breaches ("data breach")

In the event of a personal data breach, the respective Group Company shall notify the competent supervisory authority without undue delay in Switzerland if reasonably necessary for the protection of the personal data in question or in the EU. Notification shall take place within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk to the rights and freedoms of natural persons. If the breach is likely to result in a high risk to the personal rights and freedoms of natural persons, the respective Group company shall additionally notify the data subject of the breach without undue delay.

If employees identify or suspect a personal data breach, they can report it via e-mail to: dataprivacy@songwon.com or telephone: +41 52 635 00 00

11. Raising Awareness and Training of Employees

All employees of the Group who have access to personal data have their respective responsibilities in accordance with these data protection instructions, which are pointed out to them during employee induction.

Each Group office shall support its employees in the relevant processes and shall also provide regular data protection training, which shall include, without limitation, the following content:

a) The principles of processing personal data in accordance with these data protection instructions;
b) The responsibility of each employee to ensure that personal data is processed only by authorized persons and for authorized purposes;
c) The necessity and correct application of the forms and processes approved to implement this Global Privacy Policy;
d) The correct application of passwords, security tokens and other access mechanisms;
e) The importance of limiting access to personal information, such as through password-protected screen savers and logouts;

f) Secure storage of physical files and electronic storage media;
g) The need for appropriate authorization and adequate security measures for all transfers of personal data outside the internal network and business premises; and
h) The proper disposal of personal data through the use of secure shredding facilities
i) Specific risks related to personal data in connection with the relevant activities or tasks of a department

12. Compliance/Audit/Reporting

To check whether the requirements of this Global Privacy Policy are being complied with, the Data Protection Coordinator conducts a data protection compliance audit of the respective Group Company in regular intervals and informs the respective management about data protection-relevant risks, identified deficits and measures taken. Based on the results of this report, the relevant management/company defines guidelines for the necessary measures.

As part of the data protection compliance audit, at least the following will be reviewed:

a) Compliance with this Global Privacy Policy;
b) The effectiveness of privacy-related processes, such as those relating to data subjects' rights, transfers of personal data, handling of incidents and complaints related to personal data;
c) The understanding of this Global Privacy Policy and other relevant documents;
d) The accuracy of the personal data stored;
e) The adequacy/suitability of processes to improve compliance and in the event of personal data breaches.

In the event that insufficient compliance is identified, the Data Protection Coordinator - in co-operation with the affected Group Companies - will define an appropriate process and timetable to meet the requirements within a reasonable and specified period of time.

13. Organization

Management of SONGWON
The Executive Board defines the overriding principles for ensuring data protection at the Group. It appoints a person responsible for data protection (the Data Protection Coordinator) who is charged with enforcing the data protection requirements.

Human Resources Department
The HR management and the employees working in the HR department are responsible for the careful processing of personal data for their area of responsibility in compliance with data protection requirements.

Information Technology Department
The Head of IT is responsible for ensuring that data security and data protection measures are implemented in a technically appropriate manner. He is supported in this by the application and system managers in particular. He works closely with the data protection coordinator to check the conformity of the measures. In this way, he assesses risks, incidents and near incidents that could jeopardize data protection.

Supervisors
Supervisors at all levels are responsible for the enforcement of and compliance with data protection regulations in their areas of responsibility. In cooperation with the data protection coordinator, they ensure that their employees are trained and sensitized. They act as role models and promote the motivation of employees to comply with data protection measures.

Data protection coordinator
The Executive committee has appointed a Data Protection Coordinator. The Data Protection Coordinator is the central point of contact for data protection issues and can be contacted via e-mail dataprivacy@songwon.com or telephone +41 52 635 00 47

The Data Protection Coordinator has the following tasks in particular;
a) He/she shall bear the document responsibility for this data protection instruction. Amendments or additions to this directive come into force at the time of publication on the intranet [GIP].
b) He shall support the Group in the enforcement and implementation of data protection.
c) He shall monitor and take into account the development of legal requirements in the area of data protection.

14. Sanctions

Violations of this Global Privacy Policy may result in disciplinary action and/or civil and/or criminal action.

15. Final Provisions

Amendments and Supplements

This Global Privacy Policy may only be amended, supplemented or repealed in writing by a resolution of the Executive Board. Any addition, deletion or modification of individual provisions qualifies as a change or amendment. Excluded from this are corrections of a formal nature.

Supplementary documents

This Global Privacy Policy constitutes the basis for the Group's data protection requirements. Derived from it, further documents may be developed which are necessary in connection with the processing of personal data.