INTERNAL POLICY ON PERSONAL DATA PROCESSING

I. GENERAL PROVISIONS

1. The Internal Policy on Personal Data Processing (hereinafter referred to as the **Policy**) establishes the rules of personal data processing in UAB MT Group (hereinafter referred to as **MT**) by regulating the principles of data processing, categories of processed data, purposes, retention periods; procedures for exercising the rights of the data subjects; the rules of access to personal data; the basic technical - organisational measures; the procedure for assessing the impact on data protection; the rules of dealing with personal data security breaches and informing about them; etc.
2. Definitions used in the Policy:
   - 2.1. **Personal Data Breach Log** - a log that records personal data breaches.
   - 2.2. **GDPR** - General Data Protection Regulation (EU) 2016/679 of April 27th 2016.
   - 2.3. **Data Subject** - MT employees, as well as the third parties who have contracted with MT for the provision of services or the acceptance of services, candidates for vacant positions in the company, and other persons who communicate their personal data for the purpose of smooth cooperation.

II. PRINCIPLES OF DATA PROCESSING, PURPOSES OF DATA PROCESSING, CATEGORIES OF THE DATA AND RETENTION PERIODS

3. MT employees are required to comply with the following principles for the processing and protection of personal data in the performance of their duties:
   - 3.1. Personal data shall be collected for defined and legitimate purposes established by law and shall be processed in a manner consistent with those purposes;
   - 3.2. Collection and processing of personal data shall respect the principles of purpose, necessity and proportionality, shall not require data subjects to provide data that are not necessary, and shall not accumulate or process redundant data;
   - 3.3. Processing of personal data is accurate, fair and lawful;
   - 3.4. Personal data shall be accurate and, where necessary for the processing of personal data, kept up-to-date: accuracy, up-to date and completeness shall be of paramount importance and shall be assessed in relation to the purposes for which the data are processed. The updating of personal data shall be the responsibility of a specially designated employee or, in the absence of such a person, the employee to whom the updated information was first provided;
   - 3.5. Personal data shall be kept in a form which permits identification of data subjects when necessary for the purposes for which the data were collected and processed.

3.6. Personal data shall be retained for as long as the documents containing the personal data are required to be retained by law or regulation.

3.7. Personal data shall be processed in such a way that applying appropriate technical or organisational measures would ensure adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4. MT's personal data is processed for the following purposes:

4.1. For the purpose of certification of MT employees;

4.2. For the purpose of further training of MT employees;

4.3. For the purpose of dealing with complaints and requests;

4.4. For the purpose of signing and performing contracts;

4.5. For the purpose of maintaining the list of MT staff;

4.6. For the purpose of organising training;

4.7. For the internal administration of current and former staff;

4.8. For the internal administration of persons applying for vacancies offered by the MT;

4.9. For the purpose of participation in the activities of the MT.

5. The purposes of the processing of MT personal data are determined in accordance with the GDPR, the Law on Legal Protection of Personal Data of the Republic of Lithuania, the Labour Code of the Republic of Lithuania and other legal acts.

6. For the purposes set out in point 4. of the Policy, the following personal data are processed:

6.1. For the purpose referred to in point 4.1, the certified employee's name, surname, former surname (in case of change, a document proving the change shall be enclosed at the same time, showing the name of the spouse), personal identification number, address, identity card (passport) number, date and place of issue, telephone number, e-mail address, certificate number and date of issue, qualifications awarded, name and position of the workplace where the employee is (or was) employed, number of the minutes of the certification commission, data, data of the documents supporting the education;

6.2. for the purpose referred to in point 4.2 of the Policy, the name of the certified employee, former name (if changed, a document proving the change, e.g. showing the name of the spouse, shall be attached at the same time), address, telephone number, e-mail address, certificate number and date of issue, qualification awarded, and the number of the minutes of certification commission;

6.3. for the purpose referred to in point 4.3 of the Policy, name, surname, place of work, position, email address, date of birth;

6.4. for the purpose referred to in point 4.4 of the Policy, the name of the employee, date of birth.

6.5. For the purpose referred to in point 4.5 of the Policy, the employee's name, surname, place of work, job title, email address, date of birth, telephone number;

6.6. for the purpose referred to in point 4.6 of the Policy, the employee's name, surname, place of work, position, email address, date of birth, telephone number;

6.7. for the purpose referred to in point 4.7 of the Policy, the employee's name, surname, telephone number, e-mail address, personal identification number, residential address, bank account number;

6.8. for the purpose referred to in point 4.8 of the Policy, the employee's name, surname, place of work, job title, email address, date of birth, telephone number, qualifications awarded, documents proving qualifications;

6.9. for the purpose set out in paragraph 4.9 of the Policy, the employee's name, place of work, position, email address, date of birth, telephone number.

7. Personal data is collected in the following ways:

7.1 Directly from the data subjects or representatives of the data subjects;

7.2 From registers and information systems.

8. Personal data shall not be stored for longer than the purposes for which the personal data are processed and the time limits laid down by law require.

9. Only personal data shall be processed by the Company and only for the purpose and on the legal basis specified in the records of the processing activities.

10. Records of data processing activities shall be kept in writing, including in electronic form.

III. IMPLEMENTATION OF RIGHTS OF DATA SUBJECTS

11. Data subjects have the following rights:

11.1. Right to know (be informed) about the processing of their data;

11.2. Right to have access to the processing of their personal data;

11.3. Right to have their data rectified;

11.4. Right to have the data erased (right to be forgotten);

11.5. Right to restrict processing;

11.6. Right to data portability;

11.7. Right to object to the processing of personal data.

12. The data subject shall have the right to submit a free-form request to MT for the exercise of their rights. The request must be written in the official language and must include the name and contact details of the person making the request. The request must be submitted in a form that allows the identify of the applicant to be established (signed by e-signature, hand-delivered to the company, etc.).

13. MT shall provide the data subject with information on the action taken following the request without undue delay, but in any event within one month of receipt of the request referred to in point 12. That period may be extended by a further two months, if necessary, depending on the complexity of the request. The company shall inform the data subject of such extension within one month of receipt of the request, together with the reasons for the delay. When the data subject submits the request by electronic means, the information shall also be provided to the data subject by electronic means where possible, unless the data subject requests otherwise.

IV. ACCESS TO PERSONAL DATA

14. The right of access to process personal data shall be granted to employees of the MT who need the data for the performance of their functions. Employees may only carry out acts on the data which they are authorised to perform and which are necessary for the performance of their job functions.
15. The MT may grant access rights to process personal data to Data Processors on the basis of contracts concluded within the scope of the contract.
16. Access to personal data shall be terminated upon termination of the employment relationship, termination of the contract with the Data Processors and in other cases where the granting of such access would infringe the rights of the data subjects.
17. Holders of access to personal data shall respect the principle of confidentiality.

V. TECHNICAL, ORGANISATIONAL MEASURES TO ENSURE DATA PROTECTION

18. MT applies the following measures to ensure the security of personal data:
    18.1. Compliance with the Clean Desk Policy;
    18.2. Computer workstation is left unattended with the screen locked;
    18.3. Use of legal software;
19. MT employees with access rights to personal data shall immediately inform their direct manager, if they become aware of a personal data breach or a threat of a personal data breach (omissions or actions by individuals that may cause or threaten the security of personal data).
20. After assessing the nature of the breach and the consequences likely to result, the responsible official shall decide on the measures necessary to remedy the personal data breach and its consequences.
21. In the event of a personal data breach, the MT shall notify the State Data Protection Inspectorate without undue delay and, if possible, within 72 hours of becoming aware of the personal data breach.
22. The MT shall document all personal data breaches, including the facts relating to the personal data breach, the impact of the personal data breach and the corrective actions taken. The breaches shall be documented in the Personal Data Breach Log.
23. Where a personal data breach is likely to result in a serious risk to the rights and freedoms of natural persons, the MT shall, without undue delay, notify the personal data breach to the data subject.

VI. FINAL PROVISIONS

24. Personal data is not transferred to the third countries and international organisations.
25. Employees shall be held liable for non-compliance with the Policy in accordance with the procedure laid down by law.