PPMI GROUP, UAB

PERSONAL DATA PROTECTION POLICY

1. MAIN DEFINITIONS USED IN THE POLICY

1.1. **ALLPD** – the Act on the Legal Protection of Personal Data of the Republic of Lithuania.

1.2. **Authorised Employee** – an Employee of the Controller, appointed by the order of the Managing Director and who, according to the nature of work, has the right to carry out certain functions relating to Data Processing.

1.3. **Candidate** – an individual who has provided his/her Personal Data in connection with a recruitment process carried out by the Controller.

1.4. **Controller** – PPMI Group, UAB, legal entity code 300654654, and Public Policy and Management Institute (VšI „Viešosios politikos ir vadybos institutas"), legal entity code 135021457, registration address Gedimino pr. 50, LT-01110 Vilnius, Lithuania, acting as joint controllers.

1.5. **Data Subject** – an Employee, Expert, Respondent, Candidate or any other natural person whose Personal Data is processed by the Controller.

1.6. **Data Recipient** – a natural or legal person, public authority, agency or other body to which Personal Data is disclosed, whether a third party or not.

1.7. **Employee** – an individual who has concluded an employment contract or a similar contract with the Controller.

1.8. **Expert** – an individual who acts under a contract with the Controller and provides expert knowledge on matters relating to research conducted by the Controller.

1.9. **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.10. **Personal Data** – any information relating to an identified or identifiable natural person ('Data Subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.11. **Policy** – this Personal Data Protection Policy.

1.12. **Processing** – any operation or set of operations that are performed by automatic and non-automatic means upon Personal Data, such as collection, recording, accumulation, storage, classification, grouping, combination, alteration (supplementing or rectifying), disclosure, making available, use, logical and/or arithmetic operations, retrieval, dissemination, destruction.

1.13. **Processor** – a natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Controller.

1.14. **Respondent** – an individual who participates in research activities (surveys, interviews, focus groups and workshops) conducted by the Controller.

1.15. **Training** – training organised by the Controller for its Employees, on matters relating to the protection of Personal Data.

1.16. Other terms and definitions used in this Policy are in line with the terms used in the GDPR, the ALLPD and the Act on Electronic Communications of the Republic of Lithuania (hereinafter referred to as the **AEC**).

2. GENERAL PROVISIONS

2.1. The purpose of this Policy is to regulate the processing of Personal Data by the Controller, and to define the technical and organisational measures undertaken by the Controller and intended for the protection of Personal Data in accordance with the GDPR, ALPPD, AEC and other legislation that establishes protections for Personal Data.

2.2. The Controller shall ensure that it complies with the following fundamental principles of data protection:

2.2.1. Personal Data relating to a Data Subject shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

2.2.2. Personal Data shall be collected for specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with those purposes. Further processing for the purposes of archiving in the public interest, for scientific or historical research purposes, or for statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the original purposes ('purpose limitation');

2.2.3. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

2.2.4. Personal Data shall be accurate and, where necessary, kept up to date. Every reasonable step shall be taken to ensure Personal Data that are inaccurate with regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

2.2.5. Personal Data shall not be kept in a form that permits the identification of Data Subjects for any longer than is necessary for the purposes for which the Personal Data is processed. Personal Data may be stored for longer periods insofar as it will be processed solely for the purposes of archiving in the public interest, for scientific or historical research purposes, or for statistical purposes in accordance with Article 89(1) of the GDPR, subject to the 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');

2.2.6. Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');

2.2.7. The Controller shall be responsible for, and be able to demonstrate compliance with, the aforementioned principles ('accountability').

2.3. An exhaustive list of Personal Data processed by the Controller shall be provided in the Controller's records of processing activities. These shall contain continually updated information about the purposes for which Personal Data is processed; Personal Data processing procedures, scopes and terms; as well as other information indicated in Article 30 of the GDPR.

2.4. When Personal Data is used as evidence in civil, administrative or criminal proceedings or other cases determined by law, Personal Data shall be kept for as long as is necessary for the said processing purposes, and shall be destroyed immediately when it is no longer required for said purposes.

2.5. Personal Data accrued shall be stored (processed) on a server controlled by the Controller. Access to Personal Data shall only be granted to Authorised Employees and Data Processors.

2.6. The data access rights of a data Processor shall be repealed upon termination of the Personal Data processing contract concluded with the Controller, or upon the expiry of the said contract.

2.7. Authorised Employees are required to:

2.7.1. Process Personal Data in accordance with the legislation of the European Union and the Republic of Lithuania, as well as with this Policy;

2.7.2. Not disclose, transfer or create any other means of accessing Personal Data to persons that are not authorised to process Personal Data;

2.7.3. Immediately inform the Controller about any suspicious circumstances that may pose a threat to the security of Personal Data.

2.8. An Authorised Employee shall lose the right to process Personal Data when his/her employment contract expires, as well as when the director of the Controller adopts a decision to revoke the appointment of the Authorised Employee to process Personal Data, and informs the Authorised Employee of this.

2.9. Personal Data shall be transferred to data Processors and Data Recipients when the basis for such a right and/or duty is provided by legislation.

2.10. Transfer of Personal Data to data Processors shall be allowed only when appropriate contracts have been concluded between the Processors and the data Controller. The contents of said contracts shall adhere to the requirements for data processing contracts described in Section 12 of this Policy.

2.11. Transfers of Personal Data to third countries or international organisations may be permitted where the relevant conditions for transfer to third countries or international organisations, specified in Chapter V of the GDPR, are met.

2.12. Personal Data may be provided by the Controller to an investigating body, prosecutor or court as evidence in administrative, civil or criminal cases, or in other cases prescribed by law.

3. PROCESSING PERSONAL DATA OF EXTERNAL EXPERTS

3.1. The Controller carries out research and technical assistance projects. In accordance with this, and for the purposes of the conclusion and implementation of contracts (the provision of an offer to a contracting authority; execution of a project), the provision of offers for tenders, and for research purposes, the Controller may process the following categories of Experts' Personal Data:

3.1.1. First name;

3.1.2. Last name;

3.1.3. Workplace;

3.1.4. Date of birth;

3.1.5. Telephone number;

3.1.6. Skype name or name of any other social media account that the expert uses for work-related communication;

3.1.7. Address/email address;

3.1.8. Personal ID number;

3.1.9. Bank account number;

3.1.10. Rate/pricing;

3.1.11. Correspondence;

3.1.12. Opinion of the expert on certain issues of research;

3.1.13. Professional experience;

3.1.14. Publications.

4. PROCESSING PERSONAL DATA OF RESPONDENTS

4.1. The Controller carries out research and technical assistance projects. In order to implement such projects, the Controller may process Respondents' Personal Data.

5. PROCESSING PERSONAL DATA OF CANDIDATES

5.1. For the purposes of recruitment and staff selection, the Controller may process Candidates' Personal Data.

6. PROCESSING OF EMPLOYEE DATA FOR THE PURPOSES OF INTERNAL ADMINISTRATION

6.1. The Controller processes the Personal Data of its Employees for the purposes of:

6.1.1. Conclusion and execution of the employment contract;

6.1.2. Generating salary slips;

6.1.3. Compilation of time sheets;

6.1.4. Compilation of work schedules;

6.1.5. Calculation and payment of salary;

6.1.6. Evaluation and calculation of taxes, application of tax benefits;

6.1.7. Dismissal of an employee from current duties;

6.1.8. Calculation of annual leave;

6.1.9. Verification of suitability for the position;

6.1.10. Internal administration (transfers within the group of companies).

6.2. The Controller may process the following categories of Personal Data of its Employees:

6.2.1. First name;

6.2.2. Last name;

6.2.3. Telephone number;

6.2.4. Address;

6.2.5. Personal ID number;

6.2.6. Social security number;

6.2.7. Passport/personal ID card No.;

6.2.8. Email address;

6.2.9. Bank account No.;

6.2.10. Date of birth;

6.2.11. Other contact details if provided by employee;

6.2.12. Opinion of the employee on certain issues relating to research;

6.2.13. Curriculum vitae including information on education, personal experience, qualifications, position, recruitment, redeployment;

6.2.14. Salary;

6.2.15. Time spent working;

6.2.16. Accrued and used annual leave vacation;

6.2.17. Family status, citizenship, photographs.

6.3. In most cases, where there are other legal bases for the processing of Personal Data, consent cannot be the legal basis for the processing of Employees' Personal Data. If prior consent is given by the Employee, the Controller shall also have the right to process other Personal Data of the Employee. In cases where consent is the only legal basis for the processing of Employees' Personal Data, Employees shall have the right to withdraw their consent at any time pursuant to the procedure established in these Rules and/or the exercise of other rights of Data Subjects provided in these Rules.

7. RIGHTS OF DATA SUBJECTS

7.1. Any Data Subject may exercise the following rights in accordance with the procedures established in the GDPR and the ALPPD:

7.1.1. The right to be informed;

7.1.2. The right to access;

7.1.3. The right to erasure;

7.1.4. The right to rectification;

7.1.5. The right to restrict processing;

7.1.6. The right to data portability;

7.1.7. The right to object;

7.1.8. Rights in relation to automated decision-making and profiling.

7.2. The right to be informed shall be implemented, *inter alia*, by informing Employees in writing and providing necessary information to Experts and Respondents upon their consent.

7.3. The rights laid down in paragraphs 8.1.2 - 8.1.8 of this Policy shall be carried out in accordance with the procedure for processing Data Subject requests, and within the timescales stated in the GDPR.

7.4. The timescales for processing Data Subject requests are as follows:

DATA SUBJECT REQUEST	TIMESCALE
The right to be informed	When Personal Data is collected (if supplied by the Data Subject) or within one month (if not supplied by the Data Subject)
The right to access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision-making and profiling	Not specified

7.5. Data Subjects may obtain access to their data by submitting a subject access request form. This request should be sent to: personaldata@ppmi.lt.

7.6. Data Subjects may withdraw consent by submitting a consent withdrawal request form. This form should be sent to personaldata@ppmi.lt.

7.7. The Controller cannot formally base its decision to deny the request of a Data Subject or delay its processing on the grounds that the Data Subject has failed to use, or has improperly used, the aforementioned forms.

7.8. The Controller shall inform Data Subjects about their rights in a concise, transparent, intelligible, and easily accessible way, using clear and plain language.

7.9. The Controller has the right to provide a reasoned refusal to grant the request of a Data Subject to exercise their rights in the situation referred to in subparagraph (b) of paragraph 5 of Article 12 of the GDPR, namely that the Data Subject's request is manifestly unfounded or excessive.

8. CONSENT

8.1. Unless there are other grounds for processing laid out in the GDPR or the ALPPD, explicit consent must be obtained from the Data Subject in order to collect and process his/her Personal Data.

8.2. The Controller shall be able to demonstrate that a Data Subject has given unambiguous consent to the processing of his or her Personal Data. Depending on the context in which the data is collected, a prominent notice, together with a clear affirmative action, may suffice to obtain implied consent without the need for an opt-in box.

8.3. The Controller shall be able to demonstrate that the Data Subject's consent is based on his or her genuine and free choice. This means that the performance of a contract, including the provision of a service, shall not be made conditional on consent to the processing of data that is not necessary for the performance of this contract.

8.4. The Data Subject's declaration of consent shall be provided in an intelligible and easily accessible form, using clear and plain language.

8.5. The Controller shall be able to demonstrate that the processing of data is limited to conditions bound by the explicit consent given by the Data Subject.

8.6. When the Controller cannot ensure that a Data Subject's consent would comply with the requirements laid out above and/or in the GDPR, an alternative lawful basis for data processing shall be chosen.

9. TECHNICAL AND ORGANISATIONAL MEASURES RELATING TO PERSONAL DATA SECURITY

9.1. The organisational and technical data security measures implemented by the Controller and described below shall guarantee a level of security that matches the nature of the Personal Data processed by the Controller, and the risks related to its processing.

9.2. The measures shall be in accordance with the General Requirements for Organisational and Technical Data Security Measures approved by the director of the Supervisory Authority (State Data Protection Inspectorate).

9.3. These measures shall be updated and improved by taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons.

9.4. **Organisational data security measures:**

9.4.1. The Controller shall have internal documents in place that regulate the security of Personal Data.

9.4.2. Monitoring and control shall be carried out to ensure the compliance of such documents with the applicable legal acts.

9.5. **Managerial and supervisory responsibilities regarding access to Personal Data:**

9.5.1. Security, management and supervision of access to Personal Data shall be ensured.

9.5.2. Access to Personal Data shall only be granted to Authorised Employees who require the data in order to perform their functions.

9.5.3. Authorised Employees shall only be able to perform such actions using Personal Data as are granted by the Data Controller.

9.5.4. Passwords that allow access to Personal Data are required to be confidential, unique, and to consist of no fewer than eight symbols. They shall not include any personal information, and shall be changed no less than twice per year and on first sign-in.

9.5.5. If the Personal Data is processed within an internal network, protection from unlawful connection via electronic networks shall be ensured.

9.6. **Personal Data access control:**

9.6.1. Registration and requests to access Personal Data shall be recorded and controlled.

9.6.2. Records shall be generated of access to Personal Data, including: connection ID, date, time, connection result (successful, unsuccessful).

9.6.3. Records of access to Personal Data shall be preserved for six months.

9.7. **Physical data security measures:**

9.7.1. The Controller shall ensure the security of the premises in which Personal Data is kept, and ensure that only Authorised Employees have access to the said premises.

9.8. **Personal Data receipt (provision) security measures:**

9.8.1. When Personal Data is received/provided using an external data storage device or by email:

(i) Data security control shall be ensured;

(ii) The Personal Data shall be deleted after use;

(iii) The Personal Data shall be encrypted.

9.8.2. When Personal Data is received/provided via external data transfer networks, the use of safe protocols and passwords shall be ensured.

9.9. **Deletion of Personal Data:**

9.9.1. The Controller shall ensure the Deletion of Personal Data after the end of the Personal Data retention period.

9.10. **Operation and maintenance of hardware and software:**

9.10.1. Protection of computer equipment from malicious software shall be ensured.

9.10.2. It shall be ensured that information systems will not be tested by using real Personal Data.

9.11. If non-conformities are found in the Personal Data management system, they shall be corrected in accordance with the Corrective Action Procedure.

10. DATA RETENTION PERIODS

10.1. The Controller shall process Personal Data in compliance with the data storage terms established in the Index of the Timeframe of Storage of General Documents (approved by Order No V 100 of the Chief Archivist of Lithuania of 9 March 2011) and the terms established in the records of processing activities, in consideration of the purposes of personal data processing. Where any discrepancies exist between the indicated regulation and the records of processing activities, the records of processing activities shall prevail. The Controller shall apply the relevant Personal Data retention periods according to the categories of Data Subjects whose Personal Data is being processed.

10.2. The Controller shall apply the following Personal Data retention periods:

CATEGORY OF DATA SUBJECT	RETENTION PERIOD
Experts	Up to 5 years after the last contact with the expert
Respondents	As indicated in the project-specific privacy statement
Candidates	3 years after receiving CV and/ or other personal data
Employees	Up to 50 years after termination of an employment contract, in accordance with the applicable national regulation

10.3. By decision of the Controller, Personal Data may be stored for a longer term pursuant to the procedures and terms and conditions established by legal acts (for example, where there are grounds to believe that the Personal Data may be required for the investigation of a criminal offence or other incident conducted in the premises of the Controller or the building where the premises are situated). In such cases, the Personal Data shall be stored until the respective decision of law enforcement or judicial authorities with regard to the criminal offence or other decision or conclusion of persons investigating/analysing the incident (for example, insurers in the case of a natural disaster), or other persons investigating/analysing an event that has caused damage to the Controller.

11. DESTRUCTION OF PERSONAL DATA

11.1. After the expiry of the established term for the processing of Personal Data, the Personal Data shall be destroyed.

11.2. Destruction of Personal Data is defined as a physical or technical action sufficient to render the data contained in the document irretrievable by ordinary commercially available means.

11.3. During the destruction process, paper documents containing the Personal Data shall be shredded, and the remnants disposed of in a secure manner.

12. REQUIREMENTS FOR DATA PROCESSING CONTRACTS

12.1. In a contract with a data Processor, the Controller shall include provisions pertaining to the specific contract. These might include the following information:

12.1.1. Subject-matter of the processing;

12.1.2. Duration of the processing;

12.1.3. Nature of the processing;

12.1.4. Purposes of the processing;

12.1.5. Types of Personal Data;

12.1.6. Categories of Data Subjects;

12.1.7. Rights and responsibilities of the parties stemming from Personal Data regulation;

12.1.8. Obligation of confidentiality on the part of the Processor's employees;

12.1.9. Security measures relating to the processing;

12.1.10. Outsourcing by using other Processors;

12.1.11. Assistance in implementing the rights of the Data Subjects;

12.1.12. Assistance in providing notices on data breaches;

12.1.13. Data deletion and return policies.

12.2. The aforementioned provisions shall be included either in the main contract, annex to the contract or in an additional agreement on the security of the Personal Data transferred.

13. PERSONAL DATA PROTECTION BY DESIGN

13.1. The Controller shall adopt internal policies and implement measures that meet, in particular, the principles of data protection by design and data protection by default.

13.2. The Controller shall, both at the time of the determination of the means used for processing and at the time of the processing itself, implement appropriate technical and organisational measures.

13.3. The Controller shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity posed by the processing to the rights and freedoms of natural persons.

13.4. Privacy by design means that each new programme or system that makes use of Personal Data must take into consideration the protection of such data. Privacy must be taken into account throughout the entire life cycle of the programme or system development.

13.6. The Controller shall implement appropriate technical and organisational measures to ensure that, by default, only such Personal Data is processed as is necessary for each specific purpose for which the processing is intended. That obligation applies to the amount of Personal Data collected, the extent of its processing, the period of storage and its accessibility.

13.7. The Controller shall consider if a data protection impact assessment is necessary at the beginning of the development lifecycle of a new or updated programme or system, according to the procedures set out in the Data Protection Impact Assessment Procedure.

14. DATA PROTECTION OFFICER

14.1. Under the GDPR, a Data Protection Officer is required if a Controller performs large-scale monitoring or if its core activities consist of processing operations that require the regular and

systematic monitoring of Data Subjects on a large scale, or where the core activities of the Controller or Processor consist of the processing on a large scale of special categories of Personal Data.

14.2. Based on these criteria, the Controller does not require a Data Protection Officer to be appointed, however the Controller has set up a team to work on GDPR-related matters.

15. PROCEDURES FOR THE MANAGEMENT OF PERSONAL DATA BREACHES AND RESPONSES TO SUCH BREACHES

15.1. Employees of the Controller must inform an Authorised Employee and (or) their immediate superior if they notice violations of data security (inaction or actions of persons that may cause or are causing a threat to the security of data).

15.2. After conducting an evaluation of the risks posed by the data security violation, the impact of the violation, and the damage and consequences, in accordance with the Personal Data Breach Response Procedure, the Controller shall make decisions regarding appropriate measures to eliminate the data security violation and its effects.

16. DATA ACCESS CONTROL

16.1. Access to Personal Data and the right to perform data processing operations shall be limited to Authorised Employees.

16.2. Access to Personal Data shall only be available using devices attributed to Authorised Employees, using personal passwords, and employing other security measures as required.

17. PROCEDURE FOR MANAGING PERSONAL DATA PROCESSING CARRIED OUT BY EXTERNAL PROCESSORS

17.1. The Controller works with only those third parties (experts, partners, subcontractors) that can provide the necessary technical, physical and organisational security measures to meet the requirements set by the Controller for the processing of Personal Data on its behalf.

17.2. The Controller works with third parties on the basis of a contract that includes provisions on Personal Data protection, obliging the parties to the contract to act in compliance with the GDPR.

17.3. Such contracts shall forbid Processors from using further providers (subcontractors) for the processing of Personal Data without the written authorisation of the Controller.

17.4. The Controller provides guidelines and advice to Processors on how to deal with Personal Data in a GDPR-compliant way throughout the implementation of the contract.

18. TRAINING

18.1. The Controller shall provide appropriate and regular Training to Employees who have a permanent or regular access to Personal Data.

18.2. The contents of this Training must assist Employees in the performance of their duties in compliance with the requirements laid out in the GDPR and other legislation on Personal Data protection.

18.3. Training sessions shall be documented, including, in particular, their dates, topics, Employees who have taken part in them, and the results of any follow-up that is carried out.

19. LIABILITY

19.1. In accordance with the laws of Lithuania, Employees may be personally liable in the case of significant violation of this Policy due to negligence or wilful misconduct.

20. FINAL PROVISIONS

20.1. This Policy may be revised regularly on the initiative of the Controller and/or when changes are made to the laws governing the protection of Personal Data.

20.2. The Policy and its amendments shall take effect from the date of their approval.

20.3. Enquiries about this Policy or the use of your personal information by PPMI may be sent to: personaldata@ppmi.lt.