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 who, according to the nature of work, has the right to carry out certain functions related to Data Processing.

1.3. **Candidate** - an individual who has provided his/her Personal Data in connection with a recruiting 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. **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.

1.7. **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 related to scientific 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. **Policy** - this Personal Data Protection Policy.

1.11. **Processing** - any operation or set of operations, which 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.

1.12. **Processor** - a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

1.13. **Data Recipient** - a natural or legal person, public authority, agency or another body, to which the Personal Data is disclosed, whether a third party or not.

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 for the Employees by the Controller on matters regarding Personal Data protection.

1.16. Oher terms and definitions used in the 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 – **AEC**).

2. GENERAL PROVISIONS

2.1. The purpose of this Policy is to define the regulation of Personal Data processing procedures, the implementation of the rights of Data Subjects, and the technical and organisational measures intended for the protection of Personal Data according to the GDPR, ALPPD, AEC and other legislation that establishes the protection of Personal Data.

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

2.2.1. Personal Data related to the 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 archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial 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 that Personal Data that are inaccurate in regard to the purposes for which they are processed are erased or rectified without delay ('accuracy');

2.2.5. Personal Data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is 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) 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 abovementioned principles ('accountability').

2.3. Personal Data shall be retained only for the duration laid out in this Policy for each type of Personal Data. Retention and erasure shall be carried out in accordance with Sections 12 and 13 of this Policy, respectively.

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 they are no longer required for said purposes.

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

2.6. Data access rights of the 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 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 which may pose a threat to the security of the 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 a director of the Controller adopts a decision to revoke the appointment of the Authorised Employee to process Personal Data, and informs the Authorised Employee about it.

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. The procedure for managing all processing carried out by data Processors is laid down in Section 19 of this Policy.

2.11. Transfer of Personal Data to Processors shall be allowed only when appropriate contracts are concluded between Processors and the data Controller. The contents of said contracts shall adhere to the requirements for data processing contracts described in Section 14 of this Policy.

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

2.13. 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. DATA QUALITY

3.1. The Controller ensures that the Data Subject`s Personal Data shall be:

3.1.1. Processed fairly and lawfully;

3.1.2. Processed with the Data Subject`s consent or according to another criterion for the lawful processing of Personal Data;

3.1.3. Adequate, up to date and not excessive in accordance with the devised purposes;

3.1.4. Accurate.

3.2. The Controller shall maintain a record of processing operations. The Controller shall assign a person responsible with the task of maintaining the said record, under the responsibility of the Controller.

4. PROCESSING PERSONAL DATA OF EXPERTS

4.1. The Controller carries out research projects. In accordance with this, and for the purposes of the conclusion and performance of contracts (the provision of an offer to a contracting authority; execution of a project), the provision of offers for cooperation, and the recommendation of an Expert to third parties and for research purposes, the Controller processes the following categories of Experts` Personal Data:

4.1.1. First name;

4.1.2. Last name;

4.1.3. Telephone number;

4.1.4. Address;

4.1.5. Personal ID number;

4.1.6. Social security number (or equivalent);

4.1.7. Email address;

4.1.8. Bank account number;

4.1.9. Rate/ pricing;

4.1.10. Date of birth;

4.1.11. Workplace;

4.1.12. Professional experience;

4.1.13. Skype name;

4.1.14. Correspondence;

4.1.15. Publications;

4.1.16. Opinion of the expert on certain issues relating to the research.

4.2. The Controller shall not transfer the above-mentioned Personal Data to Data Recipients unless otherwise required by law.

4.3. The Controller has the right to transfer the Expert's Personal Data to subcontractors and/or freelance experts acting as data Processors.

5. PROCESSING OF PERSONAL DATA FOR THE ESTABLISHMENT AND MAINTENANCE OF A DATABASE OF EXPERTS

5.1. The Controller maintains a database of Experts for the purposes of potential future cooperation. In accordance with this, and for purposes of the establishment and maintenance of the said database of Experts, the Controller processes the following categories of Experts` Personal Data:

5.1.1. First name;

5.1.2. Last name;

5.1.3. Telephone number;

5.1.4. Address;

5.1.5. Email address;

5.1.6. Workplace;

5.1.7. Skype name;

5.1.8. Correspondence;

5.1.9. Pricing;

5.1.10. Curriculum vitae;

5.1.11. Other relevant information and documents provided by the Experts.

5.2. The Controller shall not transfer the above-mentioned Personal Data to Data Recipients unless otherwise required by law.

5.3. The above-mentioned Personal Data shall be processed by Insightly, Inc., 680 Folsom St., San Francisco, California 94107, United States of America, acting as a Processor that provides cloud-based database

management solutions.

5.4. The above-mentioned Personal Data is kept for no longer than 5 years after the last contact by PPMI, its Employees or agents with an Expert.

6. PROCESSING PERSONAL DATA OF RESPONDENTS

6.1. The Controller carries out research projects.

6.2. In accordance with this, for research purposes, the Controller processes the following categories of Respondents' Personal Data:

6.2.1. First name;

6.2.2. Last name;

6.2.3. Gender;

6.2.4. Career stage;

6.2.5. Telephone number;

6.2.6. Email address;

6.2.7. Nationality and citizenship;

6.2.8. Employer;

6.2.9. Additional information depending on the aims of a project.

6.3. The Controller may transfer the above-mentioned Personal Data of the Respondents to these Data Recipients: external experts hired to carry out particular tasks in a project, subcontractors or partners that carry out specific tasks under a contractual agreement.

6.4. The Controller has the right to transfer the Respondent's Personal Data to survey tools, subcontractors and/or freelance experts acting as data Processors.

6.5. The Respondents` Personal Data shall be kept no longer than is necessary for the execution of the particular scientific research project for which the said Personal Data has been collected. Personal Data shall be rendered anonymous in such manner that the Respondents are no longer identifiable as soon as their identities are not required for the implementation of a particular project.

7. PROCESSING PERSONAL DATA OF CANDIDATES

7.1. The Controller carries out recruitment and staff selection.

7.2. In accordance with this, for the purposes of recruitment and staff selection, the Controller processes the following categories of Candidates' Personal Data:

7.2.1. First name;

7.2.2. Last name;

7.2.3. Telephone number;

7.2.4. Email address;

7.2.5. Address;

7.2.6. Nationality;

7.2.7. Curriculum vitae;

7.2.8. Tasks;

7.2.9. Samples of writing.

7.3. The Controller shall not transfer the above-mentioned Candidate data to Data Recipients unless otherwise required by law.

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

8.1. The Controller processes the Personal Data of its Employees for the purposes of internal administration. In accordance with this, for the purpose of internal administration, Controller processes the following categories of Employees` Personal Data:

8.1.1. First name;

8.1.2. Last name;

8.1.3. Telephone number;

8.1.4. Address;

8.1.5. Personal ID number;

8.1.6. Social security number;

8.1.7. Passport/personal ID card No.;

8.1.8. Email address;

8.1.9. Bank account No.;

8.1.10. Date of birth;

8.1.11. Skype name;

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

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

8.1.14. Salary;

8.1.15. Time spent working;

8.1.16. Accrued and used vacation;

8.1.17. Family status;

8.1.18. Citizenship;

8.1.19. Pictures.

8.2. The Controller shall not transfer the above-mentioned data to Data Recipients unless otherwise required by law.

9. RIGHTS OF DATA SUBJECTS

9.1. A Data Subject shall exercise the following rights in accordance with the procedures established in the GDPR and the ALPPD:

9.1.1. The right to be informed;

9.1.2. The right to access;

9.1.3. The right to erasure;

9.1.4. The right to rectification;

9.1.5. The right to restrict processing;

9.1.6. The right to data portability;

9.1.7. The right to object;

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

9.2. 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.

9.3. Rights laid down in paragraphs 9.1.2 - 9.1.8 of this Policy are carried out in accordance to the Data Subject Request Processing Procedure, and within the timescales stated in the GDPR.

9.4. The above-mentioned timescales laid down in the GDPR are as follows:

Table 1 –Timescales for processing requests by the Data Subjects

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 of 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

9.5. The standardised method for Data Subjects to receive access is initiated through the submission of a Subject Access request form by the Data Subject which can be received by email: personaldata@ppmi.lt.

9.6. The standardised method of withdrawing consent by Data Subjects shall be carried out through the submission of a Subject Consent Withdrawal Request Form which can be received by email: personaldata@ppmi.lt.

9.7. The Controller cannot formally base its decision to deny the request of a Data Subject or delay its processing on the grounds of departing from the above-mentioned forms.

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

9.9. The Controller has the right to give 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.

10. CONSENT

10.1. 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.

10.2. 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.

10.3. 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.

10.4. The Controller shall be able to demonstrate that the Data Subject has consented to the processing of his or her Personal Data for one or more specific purposes.

10.5. The Data Subject`s declaration of consent pre-formulated by the Controller shall be provided in an intelligible and easily accessible form, using clear and plain language.

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

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

11. TECHNICAL AND ORGANISATIONAL MEASURES RELATING TO PERSONAL DATA SECURITY

11.1. The organisational and technical data security measures implemented by the Controller and described below shall guarantee a level of security to match the nature of the Personal Data processed by the Controller, and the risks entailed in processing it.

11.2. The measures are in accordance with the General Requirements for Organisational and Technical Data Security Measures approved by the director of the Supervisory Authority.

11.3. 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.

11.4. **Organisational data security measures:**

11.4.1. The Controller has internal documents in force that regulate Personal Data security.

11.4.2. Monitoring and control shall be carried out to ensure their compliance with the applicable legal acts.

11.4.3. The person responsible for data protection does not carry out functions as an information system administrator.

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

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

11.5.2. Access to Personal Data shall only be granted to Authorised Employees who need the data to perform their functions.

11.5.3. Authorised Employees shall only be able to perform actions using Personal Data that are granted by the Data Controller.

11.5.4. Passwords for access to Personal Data are required to be: confidential, unique, consisting of no less than 8 symbols; do not include any personal information; changed no less than once every 2 months and on first sign-in.

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

11.6. **Personal Data access control:**

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

11.6.2. A limited number of failed log in attempts shall be specified.

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

11.6.4. In a Personal Data search request, the purpose of Personal Data usage shall be laid down.

11.6.5. Records of access to Personal Data shall be preserved for 1 year.

11.7. **Physical data security measures:**

11.7.1. The Controller shall ensure the security of the premises in which the Personal Data are kept and ensure that only authorised Employees have access to said premises.

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

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

(1) Data security control shall be ensured;

(2) Personal Data shall be deleted after use;

(3) Personal Data shall be encrypted.

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

11.9. **Deletion of Personal Data:**

11.9.1. The Controller shall ensure the Deletion of Personal Data after the end of a set Personal Data retention period.

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

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

11.10.2. Actions of Personal Data copying and, in an event of an accidental loss of information, actions performed to restore Personal Data, shall be registered (in particular, who and when carried out said actions).

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

11.11. If non-conformities are found in Personal Data management systems, they will be corrected according to the Corrective Action Procedure.

12. DATA RETENTION PERIODS

12.1. The Controller applies different Personal Data retention periods according to the categories of Personal Data processed.

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

CATEGORY OF THE DATA SUBJECTS	RETENTION PERIOD
Experts	No longer than 5 years after the last contact with the Expert
Respondents	No longer than necessary for the performance of a particular scientific research project for which the said Personal Data has been collected
Candidates	3 years after the provision of the Personal Data
Employees	Up to 50 years after termination of an employment contract, in accordance with the requirements set out in the General Terms for Document Retention Index

12.3. Exceptions to the above-mentioned retention periods may be made as long as such deviations do not violate the rights of the Data Subjects, are in line with the legal requirements, and are documented.

12.4. Documents for which the Legal Department has issued a litigation holding order shall be retained and destroyed as specified by the Legal Department.

13. DESTRUCTION OF DATA

13.1. Destruction is defined as physical or technical action sufficient to render the data contained in the document irretrievable by ordinary commercially available means.

13.2. Project managers/ authorised persons shall maintain and enforce a detailed list of approved destruction methods appropriate for each type of data stored, whether in physical storage media or in database records or backup files.

13.3. Paper documents containing Personal Data shall be shredded, and the remnants disposed of in a secure manner.

14. REQUIREMENTS FOR DATA PROCESSING CONTRACTS

14.1. In a contract with a data Processor, the Controller shall include provisions that cover the following information:

14.1.1. Subject-matter of the processing;

14.1.2. Duration of the processing;

14.1.3. Nature of the processing;

14.1.4. Purposes of the processing;

14.1.5. Types of Personal Data;

14.1.6. Categories of Data Subjects;

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

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

14.1.9. Security measures relating to the processing;

14.1.10. Outsourcing by using other Processors;

14.1.11. Aid in implementing the rights of the Data Subjects;

14.1.12. Aid in providing notices on data breaches;

14.1.13. Aid in carrying out a data protection impact assessment;

14.1.14. Aid in consulting with the supervisory authority;

14.1.15. Data deletion and return policies;

14.1.16. Way(s) of proving compliance;

14.1.17. Right to audit.

14.2. The above-mentioned provisions shall be included either in the main contract or in an additional agreement on the security of transferred Personal Data.

15. PERSONAL DATA PROTECTION BY DESIGN

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

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

15.3. 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.

15.4. Privacy by design means that each new program or system that makes use of Personal Data must take the protection of such data into consideration. Privacy must be taken into account during the whole life cycle of the program or system development.

15.5. Examples of measures intended to fulfil the requirement of data protection by design are:

15.5.1. Limitation of the amount of data collected;

15.5.2. Ability to control;

15.5.3. Transparency;

15.5.4. User-friendly systems;

15.5.5. Data confidentiality;

15.5.6. Data quality;

15.5.7. Pseudonymisation;

15.5.8. Rapid data anonymisation;

15.5.9. Provision of the ability of Data Subjects to oversee data processing;

15.5.10. Provision of the ability of the data Controller to create and improve security measures;

15.5.11. Proper training of Employees;

15.5.12. Audit and policy reviews in the context of data protection;

15.6. Data protection by default requires the application of the strictest privacy settings to a particular program or system at the outset of when that program or system is made available.

15.7. Examples of measures intended to fulfil the requirement of data protection by default are:

15.7.1. Only data that are necessary for the exact purpose of processing shall be processed by default;

15.7.2. Technology must be designed so as to avoid unnecessary data processing;

15.7.3. Data protection-friendly default settings;

15.7.4. Features that aren't necessary shall be configurable.

15.8. These measures are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of Data Subjects.

15.9. The Controller shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of Personal Data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that, by default, Personal Data is not made accessible to an indefinite number of natural persons without the individual's intervention.

15.10. An approved certification mechanism may be used by the Controller as an element to demonstrate compliance with the requirements set out in the paragraphs above.

15.11. The Controller shall consider if a data protection impact assessment is necessary at the beginning of the development lifecycle of a new or updated program or system, according to the procedures set out in

the Data Protection Impact Assessment Procedure.

16. DATA PROTECTION OFFICER

16.1. 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 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.

16.2. Based on these criteria, the Controller does not require a Data Protection Officer to be appointed.

17. PROCEDURES FOR THE MANAGEMENT OF PERSONAL DATA BREACHES AND RESPONSE TO SUCH BREACHES

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

17.2. 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 on appropriate measures to eliminate the Data security violation and its effects.

18. DATA ACCESS CONTROL

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

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

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

19.1. Responsibilities:

19.1.1. Research Directors and Research Managers are responsible for approving the selection of all Processors of Personal Data, in line with the requirements of this Procedure.

19.1.2. A subcontracted IT company is responsible for ensuring that adequate technical and other resources are made available that may be required to support monitoring.

19.1.3. The Coordinator is responsible for carrying out regular monitoring and audits of third-party compliance.

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

19.3. Processing by a Processor shall be governed by a contract or other legal act under European Union or Member State law, that is binding on the Processor with regard to the Controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the types of Personal Data and categories of Data Subjects and the obligations and rights of the Controller.

19.4. All Data processing contracts shall allow the Controller to conduct regular audits of the Processor's security arrangements during the period in which the Processor has access to the Personal Data.

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

19.6. All Personal Data processing contracts shall require each Processor and, where applicable, the Processor's representative, to maintain a record of all categories of processing activities carried out on behalf of the Controller, containing:

19.6.1. The name and contact details of the Processor or Processors and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative;

19.6.2. Where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, the documentation of suitable safeguards;

19.6.3. Where possible, a general description of the technical and organisational security measures.

19.7. If a Processor infringes the GDPR by determining the purposes and means of processing, the Processor shall be considered to be a Controller in respect of that processing.

20. TRAINING

20.1. The Controller shall provide appropriate Training to Employees having permanent or regular access to Personal Data.

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

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

21. LIABILITY

21.1. Employees who violate the GDPR, ALPPD, AEC and other legal acts that establish the protection of Personal Data or the provisions laid out in the Policy shall be held liable according to the laws of the Republic of Lithuania.

22. FINAL PROVISIONS

22.1. This Policy may be revised once per calendar year on the initiative of the Controller and/or when laws on the protection of Personal Data change.

22.2. The Policy and its amendments shall take effect from the date of their approval. Employees will be introduced to the Policy and its amendments by signature.

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