PERSONAL DATA PROTECTION POLICY OF THE GROUP

1. PURPOSE AND SCOPE OF APPLICATION

1.1. The aim is to establish uniform principles of personal data protection, which must be followed by AB Ignitis grupė companies of the group in their activities when processing personal data, to define the main personal data protection management measures and responsibilities in the field of data protection management.

2. TERMS

2.1. General terms described in the Glossary: Group/Group of Companies, Personal Data, Enterprise, GDPR, Company.
2.2. **LLPPD** shall mean the Republic of Lithuania Republic of Lithuania Law on Legal Protection of Personal Data.
2.3. **Person** shall mean a natural person (data subject) whose data is processed – customer, potential customer, employee, job candidate, supplier, supplier's representative, contractor, contractor's representative, etc.
2.4. **Data Protection Officer** shall mean an employee assigned to the Compliance and Functional Area of Compliance and Business Risk Management appointed in accordance with the procedure established by the GDPR, performing the functions assigned to him/her by this Policy and the GDPR.
2.5. **Owner of the Personal Data Protection Process** shall mean an employee of the Company of the Group belonging to the Functional Area of Compliance and Business Risk Management, who is assigned to conduct the coordination of the Personal Data Protection Management Process in the Enterprise and cooperation in the Group in accordance with the job description.
2.6. **Data Processing** shall mean any action performed with Personal Data – collection, recording, storage, retention, classification, publication, grouping, modification, aggregation, use, logical and/or arithmetic operations, search, dissemination, destruction, provision, other action or a set of actions.
2.7. **SDPI** shall mean the State Data Protection Inspectorate.

3. GENERAL PROVISIONS

3.1. The Policy has been prepared in accordance with the GDPR and the *Group's Corporate Governance Policy*.

4. PRINCIPLES OF PERSONAL DATA PROTECTION

4.1. Enterprises shall follow the following principles when processing Personal Data in their activities:

4.1.1. **Legality.** Personal Data shall be processed for an established, clearly defined and legitimate purpose and in accordance with the requirements of the GDPR and the LLPPD.

4.1.2. **Proportionality.** Personal Data shall only be processed to the extent necessary for the purposes for which they are processed. Additional Data may be collected or the collected data may be used for purposes other than those collected only in the cases and according to the procedure provided by law or with the express consent of the Person.

4.1.3. **Accuracy.** Enterprises shall take all measures to ensure that the Personal Data they process is accurate and that inaccurate data is corrected or deleted.

4.1.4. **Duration limitation.** Personal Data shall be stored for no longer than required by the purposes of personal data processing or provided by legal acts, if they provide for a longer data retention period.

4.1.5. **Data security.** Enterprises have technical and organisational measures in place to protect Personal Data from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing. These measures must ensure a level of security commensurate with the nature of the Personal Data processed and the risks involved.

4.1.6. **Data transfer.** Personal Data shall be provided to entities established and operating in countries which are not members of the European Union or other countries of the European Economic Area only if they ensure an adequate level of legal protection of personal data through a legally binding and enforceable document between public authorities or bodies, rules binding on companies, standard data protection conditions, an approved code of conduct or an approved certification mechanism as set out in the GDPR.

4.1.7. **Implementation of individual rights.** Enterprises ensure the implementation of individual rights to know about the processing of their Personal Data, to access their Personal Data, to request correction or

deletion of their Personal Data, to restrict data processing, to transfer Personal Data and to object to data processing as provided in the GDPR and LLPPD.

4.2. In order to implement the defined personal data protection principles in the Group and to continuously increase the quality of personal data protection, the Group shall apply advanced technologies and implement quality and efficiency-oriented automation tools in the personal data protection process.

5. PERSONAL DATA PROTECTION MEASURES

5.1. Enterprises aim to ensure the protection of personal data by implementing the following measures:

5.1.1. Monitoring and documentation of data processing activities. Companies of the Group, which are required to keep records of data processing activities in accordance with the requirements of the GDPR, document this process, exercise its control and periodically update the records of activities.

5.1.2. **Impact assessment.** When the processing of personal data may pose a significant risk to the rights of Persons, to the protection of their personal data and/or when such an obligation is established by legal acts, the Enterprises shall carry out a data protection impact assessment.

5.1.3. **Monitoring of security measures.** The personal data protection measures in place are constantly monitored in order to maintain their effectiveness in reducing the risk of personal data breaches.

5.1.4. **Control of data recipients/processors.** Organisational and technical measures are used to control and supervise third parties (recipients/processors) in order to ensure that data is processed lawfully and properly.

5.1.5. **Risk management.** A risk assessment of the processing of personal data is carried out in order to properly manage the risk of personal data breaches and compliance with the GDPR.

5.1.6. **Incident management.** Breaches of personal data protection shall be registered in accordance with the requirements of the GDPR and LLPPD, they shall be reported to SDPI and/or to the Persons whose data were processed during the incident, and measures shall be taken to eliminate these breaches.

5.1.7. **Training and education.** In order to ensure compliance with the requirements of personal data protection and to emphasize the importance of compliance with these requirements in the activities of the Enterprises, the Enterprises' employees shall be educated, both mandatory and optional personal data protection trainings and knowledge tests shall be organised.

5.1.8. **Other measures** that may be effective in ensuring the protection of personal data in Enterprises.

6. PROCESS AND RESPONSIBILITIES OF THE PERSONAL DATA PROTECTION MANAGEMENT IN THE GROUP

6.1. The process of personal data protection management in the Group is part of the Functional Area of Compliance and Business Risk Management.

6.2. The main actors in the personal data protection process are: Head of Functional Area of Compliance and Business Risk Management, Data Protection Officer (Company Personal Data Protection Expert), Owners of Corporate Personal Data Protection Process, Enterprise Managers.

6.3. The Company's Personal Data Protection Expert performs the functions of the Data Protection Officer established by the GDPR in those Enterprises where he/she is required to be appointed in accordance with the requirements.

6.4. In Enterprises where a Data Protection Officer must be appointed, the Owners of the Personal Data Protection Process shall also be appointed. The Owners of this Process shall be employees belonging to/subordinate to the Functional Area of Compliance and Business Risk Management.

6.5. In cases when the owner of the Personal Data Protection Process has not been appointed in the Enterprise, the responsibilities of the Owner of the Process shall be implemented by the Enterprise Manager.

6.6. **The Head of the Functional Area of Compliance and Business Risk Management** shall initiate and coordinate the adoption of the Group's decisions related to the implementation of personal data protection requirements, and the implementation of the necessary measures to ensure compliance with the requirements.

6.7. **The Data Protection Officer shall:**

6.7.1. make suggestions or comments concerning the personal data protection measures applied or intended to be implemented, their compliance or improper compliance;

6.7.2. as required, advise the managers and employees of the Enterprises on issues related to the protection of personal data, advise on the assessment of the impact on data protection, its need, monitor its performance, provide conclusions;

6.7.3. provide the Enterprise Managers or the Owners of the Personal Data Protection Process appointed by them with conclusions on the compliance of the Enterprises' activities and decisions with the personal data protection requirements, possible risks related to non-compliance and possible measures to manage them;

6.7.4. cooperate with the supervisory authority;

6.7.5. act as a contact point for the supervisory authority in matters relating to data processing, including the prior consultation provided for in Article 36 of the GDPR.

6.8. The following conditions must be ensured for the Data Protection Officer:

6.8.1. independence in the performance of functions;

6.8.2. access to all Enterprises' information and documents required for the performance of functions from the Enterprises' employees and divisions, including but not limited to decisions of the Enterprises' management and supervisory bodies, internal legislation, information on investigations conducted in the Enterprises, inquiries from state institutions, received complaints, Enterprises' responses to them related to the protection of personal data;

6.8.3. other conditions under GDPR.

6.9. **Owner of the Personal Data Protection Process shall:**

6.9.1. organise and implement the implementation of measures ensuring personal data protection requirements in the Enterprises, carry out their monitoring;

6.9.2. carry out regular monitoring of the implementation of and compliance with personal data protection requirements in the Enterprise,

6.9.3. provide information to the Head of the Functional Area of Compliance and Business Risk Management, the Head of the Enterprise, and the Data Protection Officer on issues related to the implementation of personal data protection;

6.9.4. provide advice on compliance with personal data protection requirements;

6.9.5. notify the Head of the Functional Area of Compliance and Business Risk Management, the Head of the Enterprise, and the Data Protection Officer about possible non-compliance with the personal data protection requirements.

6.10. **Enterprise Managers shall:**

6.10.1. be responsible for the compliance of personal data protection requirements in the Enterprise with the requirements of legal acts and the Policy;

6.10.2. appoint a Data Protection Officer in cases specified in the GDPR;

6.10.3. ensure the Data Protection Officer and the Owner of the Personal Data Protection Process in the Enterprise with the necessary conditions to perform the functions, if they are appointed;

6.10.4. ensure that the Enterprises' employees are able to make decisions that comply with the requirements of personal data protection legislation and this Policy.

6.11. **Employees of the Enterprises shall:**

6.11.1. ensure that their activities comply with the requirements of personal data protection in accordance with the procedure established by the GDPR, LLPPD, this Policy and other legal acts;

6.11.2. notify the Data Protection Officer of any data security breaches;

6.11.3. be liable for the violation of the legal acts regulating the protection of personal data, the Policy and other internal legal acts regulating the protection of personal data in accordance with the procedure established by the Law and the internal legal acts of the Enterprise;

6.11.4. participate in mandatory data protection training.

7. FINAL PROVISIONS

7.1. The Head of the Functional Area of Compliance and Business Risk Management shall coordinate and oversee the proper implementation and enforcement of the Policy at the Group level and ensure timely updating of the Policy as required.

7.2. In implementing this Policy, the Group's personal data protection guidelines shall be developed and applied at the Group level.

7.3. If necessary, the Enterprises may adopt internal legal acts related to the implementation of the Policy. These documents must in all cases be agreed upon with the Data Protection Officer and not contradict this Policy.

8. RELATED INTERNAL LEGAL ACTS

Group's Corporate Governance Policy

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)

The Republic of Lithuania Law on Legal Protection of Personal Data