PERSONAL DATA PROTECTION POLICY

WHEREAS:

i. on 25 May 2018, 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), hereinafter referred to as "**GDPR**", and the Act of 12 May 2018 on the protection of personal data (Journal of Laws of 2018, item 1000);

ii. the Regulation imposes an obligation on economic operators to adapt their personal data processing standards to the provisions of the Regulation;

The Management Board of SHARE HOME SILESIA sp. z o.o., by resolution of 25.05.2018, decided to adopt this Personal Data Security Policy, which together with its appendices:

i. describes the principles and procedures for the processing of personal data and for protecting them against unauthorised access;

iii. ensures that the Company's processing of personal data complies with the provisions of the GDPR; and

iv. constitutes a personal data protection policy within the meaning of the said Regulation.

ARTICLE 1
DEFINITIONS

1. Whenever the following terms are used in this document, they shall have the meanings given below:

1.1. **"Controller" or "Company" –** means SHARE HOME SILESIA spółka z ograniczoną odpowiedzialnością with its registered office in Katowice, ul. Konduktorska 33, 40-155 Katowice, entered in the register of entrepreneurs of the National Court Register under the number KRS 0000658555, REGON: 366336021, NIP: 6342884703 with a share capital of PLN 13,815,000.00.

1.2. **"Information System Administrator" "ASI" –** means a person or department within the Administrator's structure or an external entity acting on behalf of the Controller and dealing with the management of the IT system, i.e., inter alia, supervising the operation of servers, managing user accounts, installing software, ensuring the security of the system and the collected data, as well as supervising, detecting and removing irregularities in the operation of the Controller's IT system and performing installations, configurations and repairs of hardware.

1.3. **"Policy"** – means this Personal Data Protection Policy and its appendices.

1.4. **"GDPR" –** means 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) of 27 April 2016 (OJ . EU.L No 119, p.1).

1.5. **"Personal Data**" – means information about an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by name, by an identification number, by location data, by an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

1.6. **"Processing of Personal Data" –** means an operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means,

such as collection, recording, organisation, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.7. **"Processor**" – means a natural or legal person, public authority, entity or other body that processes personal data on behalf of the Controller.

1.8. **"Information System**" – means a set of functionally related and cooperating devices, programs, information processing procedures and tools used for the purpose of Processing Personal Data.

1.9. **"User"** – means a person who has access to the resources of the IT system and who is authorised by the Controller to process Personal Data.

1.10. "**Dataset**" – means a structured set of personal data accessible according to specific criteria, regardless of whether the set is centralised, decentralised or functionally or geographically dispersed; accessible according to specific criteria, regardless of whether the set is dispersed or functionally divided.

1.11. **"Consent" –** means a freely given, specific, informed and unambiguous indication of the will by which the data subject, by means of a statement or a clear affirmative action, gives his or her consent to the processing of personal data concerning him or her.

1.12. **"Recipient of data" –** means a natural or legal person, public authority, entity or other body to whom personal data is disclosed, whether or not a third party. However, public authorities which may receive personal data in the context of a particular proceeding in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities must comply with the data protection rules applicable pursuant to the purposes of the processing.

ARTICLE 2
OBJECTIVES OF INTRODUCING THE POLICY

1. This Policy governs the Company's principles of processing Personal Data.
2. The purpose of introducing the Policy is to establish standards and rules of conduct allowing the implementation of the Controller's obligations with regard to the protection of Personal Data, in particular by establishing rules aimed at:

2.1. processing Personal Data within the Company in accordance with the law;

2.2. preventing access to Personal Data by unauthorised persons;

2.3. securing Personal Data against unauthorised disclosure, theft, destruction, damage or other unlawful acquisition and use.

ARTICLE 3
SCOPE OF THE POLICY

1. This Policy applies to all Personal Data Sets processed by the Controller, in particular:

1.1. Personal Data Files maintained both in electronic and traditional (paper, written) form, including data stored in all the Controller's existing IT systems and possible IT systems to be implemented in the future, regardless of the manner in which the Personal Data is recorded and the type of media on which it is recorded;

1.2. Personal Data processed by the Controller on its own behalf, as well as data processed by the Controller on the basis of agreements on entrusting the processing of personal data;

1.3. Personal Data processed in all buildings and premises of the Controller.

2. The scope of application of the Policy covers all persons, regardless of their position and the nature of the legal relationship, including employment or service provision (including trainees, apprentices, apprentices, persons undertaking activities on the basis of an appointment, and persons performing work under a contract of mandate or a contract for specific work) and regardless of the place of performance, who have access to the Personal Data collected, processed and stored by the Controller in connection with its activities.
3. Persons with access to Personal Data are required to comply with the measures set out in this Policy and in common law. These measures shall continue to be binding even after the termination of the basic relationship to which access to the Personal Data related.

ARTICLE 4
DATA PROCESSING PRINCIPLES

1. The Controller's system for processing Personal Data is based on the following principles:
   1.1. the lawfulness, fairness and transparency of the Processing of Personal Data;
   1.2. purpose limitation – i.e. the Processing of Personal Data for specified, explicit and legitimate purposes;
   1.3. data minimization – i.e. processing only of those Personal Data which are necessary for the indicated purpose of the Processing;
   1.4. correctness – i.e. taking all reasonable steps to ensure that Personal Data which is inaccurate in relation to the purposes of its Processing is erased or rectified without delay;
   1.5. storage limitation – i.e. to keep the Personal Data for no longer than it is required for the purposes of the Processing;
   1.6. integrity and confidentiality – Processing of Personal Data in a manner that ensures adequate security against unauthorised or unlawful Processing and against accidental loss, destruction or damage and by means of appropriate technical and organisational measures.
2. The Controller processes Personal Data only in cases specified by law.
3. Only persons who have been authorised by the Controller (i.e. Users), in accordance with the template attached as **Appendix No. 3** to the Policy, may be authorised to process Personal Data.
4. Termination of the employment relationship or any other legal relationship pursuant to which the User was granted access to Personal Data, or a change in the scope of responsibilities (such that the User's access to all or some of the Personal Data is no longer necessary), shall result in the loss of access to Personal Data or a change in the scope of access, and shall be recorded in the register of persons authorised to process Personal Data, a specimen of which is enclosed as **Appendix No. 4** to the Policy.
5. The Controller shall familiarise persons authorised to process Personal Data with data protection regulations, in particular the provisions of the GDPR and this Policy.
6. Where the processing is to be carried out on behalf of the Controller, the Controller shall only use the services of such processors that provide sufficient guarantees to implement appropriate technical and organisational measures to ensure that the processing meets the requirements prescribed by law and the requirements set out in the Policy and to protect the rights of the Personal Data Subjects. Processing by a processor is carried out on the basis of an agreement according to the template attached as **Appendix No. 9** to the Policy. The Controller shall keep records of contracts concluded for the processing of Personal Data in accordance with the template attached as **Appendix No. 6** to the Policy.

ARTICLE 5
OBLIGATIONS OF THE CONTOLLER

1. The tasks of the Personal Data Controller include, in particular:
   1.1. the organisation of the protection of Personal Data in the Company, including the division of tasks and responsibilities for the protection of Personal Data;
   1.2. deciding on the purposes and means of processing and on the techniques to be used to secure Personal Data;
   1.3. taking appropriate action in the event of a breach or suspected breach of security of Personal Data;
   1.4. issuing, changing and withdrawing authorisations to process Personal Data for all persons having access to Personal Data processed in the Company;
   1.5. regular risk assessment and impact assessment of the processing of Personal Data;
   1.6. concluding agreements with entities processing Personal Data on behalf of the Controller and keeping a record of agreements concluded with processors in accordance with the model constituting **Appendix No. 6** to the Policy;
   1.7. keeping a register of security incidents involving the processing of Personal Data in accordance with the template attached as **Appendix No. 5** to this Policy;
   1.8. identifying Personal Data resources, the relationship between resources, to identify uses of the data, in particular the processing of sensitive data, the processing of de-identified data, the processing of children's data, profiling;
   1.9. verifying whether there is any co-management of Personal Data;
2. The Controller shall keep a register of persons authorised to process Personal Data, the specimen of which is attached as **Appendix No. 4** to this Policy. These records shall record:
   2.1. the name and surname of the person authorised to process the Personal Data;
   2.2. the position and designation of the organisational unit;
   2.3. the date of granting, modifying the scope of and withdrawing the authorisation to process Personal Data;
   2.4. identification of the Data Set to which the User has access.
3. The Controller shall keep a Register of Personal Data Processing Activities, in which each Personal Data Processing Activity shall be recorded, indicating at least:
   3.1. the name and contact details of the Controller and any joint controllers and, where applicable, the Controller's representative;
   3.2. the name of the processing activity;
   3.3. purposes of processing;
   3.4. description of categories of data subjects and categories of Personal Data;
   3.5. the categories of recipients to whom the Personal Data has been or will be disclosed;
   3.6. transfer of Personal Data to a third country or international organisation, together with the name of the latter (if applicable);
   3.7. planned time limits for deletion of specific categories of Personal Data (where possible);
   3.8. a general description of the technical and organisational security measures;
   3.9. basis for the Processing of Personal Data.

4. The Controller inventories consents to the processing of Personal Data and inventories and prepares a justification of cases where, in accordance with the RODO, Processing of Personal Data occurs on a basis other than consent.
5. The Controller shall provide the persons whose Personal Data it processes with all information required by law both at the time the Personal Data is collected and after its collection, insofar as the law imposes additional information obligations on the Controller, and shall document the fulfilment of the information obligations.
6. The Controller shall ensure that the requests of the Personal Data subjects are fulfilled within the time limits indicated in the RODO.

ARTICLE 6

TASKS OF THE INFORMATION SYSTEM ADMINISTRATOR AND AUTHORISED PERSONS

1. The tasks of the Information System Administrator include:
   1.1. preventing access by unauthorised persons to the IT System where Personal Data is processed, in particular through the correct configuration of systems and devices;
   1.2. assigning an ID and a password to each User and granting, modifying and restricting User rights in accordance with the Controller's decision;
   1.3. ensuring reliable operation of servers, local area network, computers and other devices affecting security of data processing and ensuring secure data exchange within the internal network and secure teletransmission;
   1.4. supervising the operation of mechanisms for User authentication and access control to systems used for the Processing of Personal Data.
2. The duties of all persons authorised to Process Personal Data include:
   2.1. processing Personal Data only to the extent and for the purposes arising from their duties and the authorisation given to Process Personal Data;
   2.2. maintaining the confidentiality of information which has come to their knowledge in the course of their duties, including log-in credentials (e.g. passwords, logins);
   2.3. ensuring the security of storage media and devices used for Personal Data Processing both on and off the Company's premises;
   2.4. notification of all suspected or actual irregularities in the processing of Personal Data to the Administrator;
   2.5. acting in accordance with internal regulations concerning the Processing of Personal Data, in particular those concerning the protection of Personal Data and Personal Data carriers, described in the IT System Management Instruction, a specimen of which is attached as **Appendix 8** to the Policy.

ARTICLE 7
INFORMATION OBLIGATIONS

1. Where Personal Data is collected from the Data Subject, the Controller shall inform the Data Subject, in accordance with the template attached as **Appendix No. 1** to the Policy, of the following:
   1.1. your identity and contact details;
   1.2. the contact details of the Data Protection Officer, if any;
   1.3. the purpose of the Processing of Personal Data and the legal basis for the Processing;
   1.4. Recipients of the data or their categories, if any;

1.5. the intention to transfer Personal Data to a third country or international organisation and the European Commission's determination or lack of determination.

2. Processing of Personal Data by the Controller of the person to whom the Personal Data relates additionally requires that the person gives his/her written consent in accordance with the template attached as **Appendix No. 2** to the Policy.

ARTICLE 8
DATA PROTECTION INCIDENTS

1. The controller shall have procedures in place in the event of a breach of the protection of Personal Data, allowing for the identification and verification of the breach and, where necessary, shall also immediately inform the competent supervisory authority and notify the person to whom the Personal Data relate.
2. In the event of a breach of Personal Data or threat of a breach, the Controller shall take appropriate remedial measures.

ARTICLE 9

ORGANISATIONAL MEASURES USED

1. The Controller shall apply security measures for premises, offices, places and data carriers, regardless of their form, which protect the processed Personal Data against access by unauthorised persons.
2. Only authorised persons have access to the premises where Personal Data is processed. Unauthorised persons may enter the processing area only with the Controller's consent or in the presence of a person authorised to process Personal Data.
3. The Controller shall acquaint each User with the rules of protection of Personal Data applicable in the Company, as proof of which the User submits a declaration, a specimen of which is **Appendix No. 3a** to the Policy. The Controller shall keep records of persons who have familiarised themselves with the Company's Personal Data protection rules, in accordance with the template attached as **Appendix No. 7** to the Policy.
4. The IT System Management Manual, which includes a description of technical measures for securing the IT System, is attached as **Appendix No. 8** to the Policy.

ARTICLE 10
FINAL PROVISIONS

1. The policy is available at the Controller's premises.
2. The policy comes into force on 25 May 2018.
3. The appendices to the Policy form an integral part of it and are:

3.1. Appendix No. 1 – Template of information on the processing of personal data

3.2. Appendix No. 2 – Template of the declaration of consent to the processing of Personal Data

3.3. Appendix No. 3 – Template of the authorisation to process Personal Data

3.4. Appendix No. 3a – Declaration of the person authorised to process Personal Data

3.5. Appendix No. 4 – Register of persons authorised to process Personal Data

3.6. Appendix No. 5 – Record of incidents concerning the processing of Personal Data

3.7. Appendix No. 6 – Register of contracts for the processing of Personal Data

3.8. Appendix No. 7 – Records of persons who have read the documentation on the protection of Personal Data.

3.9. Appendix No. 8 – Information System Management Instruction

3.10. Appendix No. 9 – Model agreement on entrusting the processing of Personal Data