Approved by Order No. TVĮ-02 of the CEO of UAB Urban Inventors
25 May 2018

UAB URBAN INVENTORS
RULES FOR THE PROCESSING OF PERSONAL DATA

1. General Provisions

1.1. UAB Urban Inventors rules for the processing of personal data (hereinafter – **Rules**) establish the organisational and technical measures implemented by the controller of personal data – UAB Urban Inventors (hereinafter – **Company**), which are intended to protect personal data (hereinafter – **Personal Data**) against accidental or unlawful destruction, alteration, disclosure, and against any other unlawful processing.

1.2. Organisational and technical data security measures implemented by the Company ensure a level of security that corresponds to the nature of the data managed by the Company and the risk posed by the processing of such data.

1.3. These Rules have been prepared in accordance with the following legal acts and standards:

1.3.1. General Data Protection Regulation of the European Union which entered into force on 25 May 2018 (hereinafter – **GDPR**);

1.3.2. Republic of Lithuania Law on Legal Protection of Personal Data (hereinafter – **LLPPD**);

1.3.3. Republic of Lithuania Law on Electronic Communications (hereinafter – **LEC**);

1.3.4. Other legal acts governing data protection and processing.

1.4. Terms and definitions:

1.4.1. **LLPPD** – Republic of Lithuania Law on Legal Protection of Personal Data;

1.4.2. **Personal Data** – any information relating to a natural person who has been identified or who can be identified; a natural person who can be identified is a person who can be directly or indirectly identified in particular by reference to an identifier such as name and surname, personal identification number, location data and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.4.3. **Personal Data Breach** – a security breach that causes unintentional or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to transferred, stored or otherwise processed Personal Data;

1.4.4. **GDPR** – General Data Protection Regulation (EU) 2016/679;

1.4.5. **Company** – UAB Urban Inventors, code 302675889, address Laisvės Ave. 3, Vilnius:

1.4.6. **LEC** – Republic of Lithuania Law on Electronic Communications;

1.4.7. **Inspectorate** – State Data Protection Inspectorate, address A. Juozapavičiaus str. 6, LT-09310 Vilnius;

1.4.8. **Rules** – UAB Urban Inventors rules for the processing of personal data;

1.4.9. **Direct Marketing** – an activity intended for offering goods or services to individuals by mail, telephone or any other direct means and/or for obtaining their opinion about the offered goods or services.

1.4.10. Other terms used in these Rules shall have the same meaning as in the GDPR, LLPPD or other applicable legislation.

2. Data Processing Principles

2.1. Personal Data is processed in the Company in accordance with the GDPR, LLPPD, LEC and other legal acts and standards regulating the protection, processing and information security of personal data.

2.2. Personal data in the Company:

2.2.1. Data is collected and processed for defined and legitimate purposes established prior to data collection, and not further processed in a way incompatible with those purposes (purpose limitation principle);

2.2.2. Data is processed with the consent of the data subject or other basis for lawful data processing;

2.2.3. Data is processed accurately, fairly and lawfully;

2.2.4. Processed data must be accurate and, if necessary for the processing of personal data, up to date. Inaccurate or uncomprehensive data must be rectified, supplemented, deleted or its processing must be suspended (principle of accuracy);

2.2.5. Data is processed in an identical and relevant manner, and only to the extent necessary to achieve the purposes for which it is processed (principle of data reduction);

2.2.6. Data is retained so as to permit the identification of data subjects for no longer than is necessary for the purposes for which the data is collected and processed;

2.2.7. Data is processed in such a way as to ensure the adequate protection of personal data, including the protection against unauthorised processing or processing of unauthorised data and unintentional loss, destruction or damage by applying appropriate technical or organisational measures (principle of integrity and confidentiality).

2.3. Categories of personal data processed by the Company, the purposes of processing such data, data scope, retention periods, etc. are specified in Annex 1 to the Rules.

2.4. Authorised employees of the Company who process Personal Data must maintain the confidentiality of Personal Data, unless the data is intended for public disclosure. This obligation shall continue to apply after transfer to another position within the Company or upon termination of the employment or contractual relationship with the Company.

3. Data Processors

3.1. The Company can authorise data processors to process its controlled data, i.e. providers of information technology and electronic communications services, advisers, auditors, consultants, and other persons who process data controlled by the Company according to its purposes and instructions.

3.2. If the Company authorises a data processor to process Personal Data, the selected data processor shall guarantee the necessary technical and organisational data protection measures and ensure that such measures are complied with.

3.3. The Company concludes written agreements with the data processors specifying that the data processors must process data strictly according to the instructions of the Company. These agreements shall also include the obligations of the controller provided for in Article 28 of the GDPR.

3.4. The list of data processors authorised by the Company and their functions is provided in Annex 1 to the Rules.

4. Provision of Data

4.1. Personal data managed by the Company shall be provided to third parties only with the consent of the data subject or under another legal basis for the provision of data.

4.2. Data managed by the Company is provided in accordance with the data provision agreement concluded between the Company and the data recipient (in case of multiple data provision) or at the request of the data recipient (in case of one-time data provision).

4.3. The data provision agreement must specify the purpose of the use of the data, legal basis for the provision and receipt of such data, as well as the conditions, procedures and scope of the data to be provided. The data subject's request for data must specify the purpose of the use of the data, legal basis for the provision and receipt of such data, as well as the scope of the requested data.

4.4. Priority shall be given to the automatic provision of data, however, when providing Personal Data at the request of the data recipient, priority shall be given to the provision of data by electronic means.

4.5. Personal Data managed by the Company shall be provided to data recipients outside the European Economic Area only after ensuring an adequate level of data protection and obtaining the permission of the Inspectorate if such is necessary and the Company cannot rely on 'appropriate safeguards' provided for in Article 46(2) of the GDPR.

4.6. The list of data recipients managed by the Company is provided in Annex 1 to the Rules.

5. Data Subject Rights

5.1. Data subject whose Personal Data is processed in the Company shall have the following rights:

5.1.1. Right to know (be informed) about the processing of his or her personal data;

5.1.2. Right to access his or her Personal Data and familiarise with the procedures for processing such data;

5.1.3. Right to require rectification or deletion of his or her Personal Data, or suspension of the processing of such data (excluding retention) when Personal Data is processed in violation of the regulatory requirements and these Rules;

5.1.4. Right to object to the processing of his or her Personal Data;

5.1.5. Right to receive personal data related to him or her, which he or she has provided to the Company in a systematised, commonly used and computer-readable format (right to data portability);

5.1.6. If Personal Data is processed on the basis of consent, the right to withdraw his or her consent at any time, without prejudice to the lawfulness of the consent-based data processing carried out before the withdrawal;

5.1.7. Right to lodge a complaint with the Inspectorate regarding the processing of Personal Data.

5.2. In exercising the right provided for in Clause 5.1.2 of the Rules, the data subject may apply to and receive confirmation from the Company on whether personal data related to him or her is being processed. If the said data is being processed, the data subject shall have the right to access his or her personal data and the following information:

5.2.1. Data processing purposes;

5.2.2. Categories of appropriate personal data;

5.2.3. Data recipients or categories of data recipients to whom personal data has been or will be disclosed, in particular data recipients in third countries or international organisations;

5.2.4. If possible, the period for which personal data will be retained or, if not possible, the criteria for determining this period;

5.2.5. The right to request the controller to rectify or delete personal data or to restrict or object to the processing of personal data relating to the data subject;

5.2.6. The right to lodge a complaint with the Inspectorate;

5.2.7. All available information on the sources of personal data, if such data is collected from other sources and not from the data subject;

5.2.8. Information on automated decision-making, including profiling which has legal consequences for the data subject or which has a significant effect on him or her in a similar way;

5.2.9. Information on the transfer of data to a third country or international organisation.

5.3. Information specified in Clause 5.2 shall be provided to the data subject when employees of the Company establish the identity of the data subject. Upon receipt of a request from the data subject regarding the processing of his or her data, the Company must respond whether it processed any data related to the data subject and provide the requested data to the data subject no later than within one month from the date of the data subject's request. If necessary, the specified period may be extended for two more months depending on the complexity and number of requests. The Company shall inform the data subject of such extension within one month after receipt of the request, as well as provide the reasons for such delay. At the request of the data subject, such Personal Data must be provided in writing. Personal Data shall be provided to the data subject free of charge.

5.4. If, after accessing his or her Personal Data, the data subject finds that his or her Personal Data is incorrect, incomplete or inaccurate, the data subject may inform the Company thereof which shall then immediately check the Personal Data and rectify any incorrect, incomplete or inaccurate data and/or suspend the processing of such data, with the exception of retention.

5.5. If, after accessing his or her Personal Data, the data subject finds that his or her Personal Data is processed unlawfully or unfairly, the data subject must inform the Company thereof which shall then immediately check the lawfulness and fairness of the processing of Personal Data free of charge, and destroy any unlawfully or unfairly collected data at the request of the data subject or suspend the processing of such data, with the exception of retention.

5.6. If data processing is suspended, the data concerned shall be retained until it is rectified or destroyed (at the request of the data subject or at the end of the data retention period). Other processing operations with such data may only be carried out in the following cases:

5.6.1. For the purpose of proving circumstances which led to the suspension of data processing;

5.6.2. If the data subject consents to further processing of his or her data;

5.6.3. If it is necessary to protect the rights or legitimate interests of third parties;

5.6.4. To make, enforce or defend legal claims;

5.6.5. For overriding reasons relating to the public interest of the European Union or a Member State.

5.7. The Company shall immediately notify the data subject of the rectification or destruction of data, or suspension of data processing, whether or not carried out at the request of the data subject.

5.8. Personal Data shall be rectified and deleted or their processing shall be suspended on the basis of the identity of the data subject and the documents confirming his or her data upon the request of the data subject.

5.9. If the Company's employees doubt the accuracy of the data provided by the data subject, they must suspend the processing of such data, check the data and rectify it if necessary. Such data may only be used to verify its accuracy.

6. Authorisations to Process Personal Data

6.1. Access rights and authorisations to process Personal Data are granted only to those employees of the Company who require the Personal Data to be able to properly carry out their job functions.

6.2. Authorised employees of the Company may only carry out those actions for which they have been granted rights.

6.3. Access rights and authorisations to process Personal Data are granted to employees, deleted and changed by the person responsible for the implementation of the Rules.

6.4. The list of persons to whom the Company has granted the right to process data and their functions is provided in Annex 1 to the Rules.

6.5. The Company's employees who are granted the right to process data shall be informed and their training shall be organised by the person responsible for the implementation of the Rules, by taking into account the legal requirements, as well as the Company's actual needs and financial capabilities.

7. Data of Candidates

7.1. Candidates for job positions in the Company shall be informed in advance about the processing of their data and their rights. This is done by including a link to the Company's privacy policy in job postings.

7.2. Candidates' personal data may be stored only during the period the candidates are being selected for a specific position in the Company. At the end of the selection process (when a new employee is hired), the CVs, cover letters, contact details and other data sent by other candidates are deleted immediately.

7.3. The data of candidates who have not been selected may be retained for a longer period (of up to one year) after the end of the selection process only if the candidate provides his or her consent to the retention of his or her personal data.

7.4. Upon recruitment of a candidate, the data of the candidate which is not necessary for the conclusion of the employment contract shall also be deleted.

7.5. The Company does not process the personal data of candidates for purposes that are not related to the candidate's qualifications, professional experience and professional qualities.

7.6. Procedures for processing personal data of candidates performed by the Company are described in Annex 1 to the Rules.

7.7. The Company shall not process the personal data of candidates relating to their convictions and criminal offences, unless such personal data is necessary to verify that the person complies with the requirements for the performance of duties and job functions established by laws and implementing legislation.

8. Direct Marketing

8.1. Personal data may be processed for direct marketing purposes only with the consent of the data subject.

8.2. The Company may send direct marketing offers without obtaining a separate consent when all of the following conditions are met:

8.2.1. Contact details are obtained when selling goods or providing services to the Company's customers;

8.2.2. Advertising messages are intended for the marketing of similar goods or services of the Company;

8.2.3. Advertising messages provide a clear, free and easily accessible opportunity to object to or refuse such use of data;

8.2.4. The customer does not initially object to such use of data during the provision of each offer.

8.3. Data may be processed for direct marketing purposes, provided that the collection of personal data is subject to a retention period.

8.4. The Company must provide a clear, free and easily accessible opportunity for the data subject to express his or her consent or objection to the processing of his or her Personal Data for direct marketing purposes in each advertising message (e.g., by providing the option to 'Unsubscribe').

8.5. The collection and use of a personal identity numbers for direct marketing purposes is prohibited.

8.6. It is prohibited to send an email or call a person asking if he or she agrees to receive direct marketing offers without the person's prior consent.

9. Procedures for the Use of Information and Communication Technologies and Employee Monitoring and Control in the Workplace

9.1. The Company's telephone, computer equipment, Internet and e-mail are provided to employees for work purposes only.

9.2. Employees shall not have the right to install computer programs on the Company's computers. This can only be done by persons authorised by the Company.

9.3. Communication shall be monitored to protect the Company's confidential information from being transmitted to competitors and to protect the Company's legitimate interests. In case of suspicion of a breach of duty or fraudulent activity against the interests of the Company, or if there are any signs of a criminal offence, the responsible representatives of the Company may be obliged to check an employee's documents stored at his or her workplace, his or her work computer or electronic storage media in order to investigate the circumstances of the offence.

9.4. Data about employee browsing history and communication is not monitored continuously. The monitoring and review of such data is carried out only when there is a reasonable suspicion of violation of legal acts or job duties, and only the data that is related to such possible violation is reviewed. Retained data may be transferred to third parties if the Company considers that such data transfer is necessary to ensure the interests of the Company and if such data transfer will not violate the legitimate interests and rights of employees.

9.5. The Company shall not ensure the confidentiality of personal information of its employees if they use the work tools provided by the Company (computer, mobile phone, Internet access and other information technology and telecommunications equipment) for personal purposes.

9.6. The present Rules shall be used to inform employees in advance that the Company may check the content of communication programs (e.g., Skype) installed in the work tools assigned to them (computers, mobile phones and other information technology and telecommunications equipment) or other electronic correspondence to the extent necessary to achieve the purposes set out in these Rules.

9.7. The Company reserves the right to restrict access to separate websites or software without providing the employee with a separate notification. If the aforesaid measures are insufficient, the Company may check employee compliance with the e-mail and internet resource usage requirements for the purposes specified in these Rules, and, when examining incidents, transfer the equipment used by employees to be examined by third parties who have the right to receive such data according to the procedures established in legal acts.

10. Other Personal Data Security Measures

10.1. Personal data security breaches in the Company are continuously handled by the person responsible for the implementation of the Rules. Once the Company identifies specific data protection risks, it shall immediately inform the responsible persons and take all possible technical and organisational measures to eliminate them.

10.2. Assessment of risks posed by data processing shall be performed regularly in the Company. Necessary data security measures are implemented taking into account the results of the risk assessment. Results of the assessment or audit are formalised if it is determined that data protection is insufficient in the Company.

10.3. In case of data breaches or accidental loss of data, data in the Company shall be restored from copies by the decision of the person responsible for the implementation of these Rules and with the assistance of competent employees of the Company.

10.4. In order to protect personal data processed by the Company from loss or unauthorised alteration, it shall be regularly archived, copied and/or stored on special media. Archiving, copying and retention of personal data in the Company is controlled by the person responsible for the implementation of these Rules with the assistance of competent employees of the Company.

10.5. By considering the technical feasibility development level, implementation costs and Personal Data processing nature, scope, context and purposes, as well as the risks of various probability and severity posed by Personal Data processing to the rights and freedoms of natural persons, the Company shall implement appropriate technical and organisational measures in order to ensure a security level that would match the posed risk, including, *inter alia*, if necessary:

10.5.1. Pseudonymisation and encryption of Personal Data;

10.5.2. Ability to ensure continuous confidentiality, integrity, availability and resilience of Personal Data processing systems and services;

10.5.3. Ability to recreate, in time, the conditions and possibilities to use Personal Data in the event of a physical or technical incident;

10.5.4. Regular process of assessment of the inspection, evaluation and effectiveness of technical and organisational measures which ensure data processing security.

10.6. The Company shall take measures to ensure that Personal Data is not processed by any natural person subordinate to the Company who has access to the said data, excluding cases when the Company gives instructions to process data, or when the person is obliged to do so in accordance with the applicable regulatory requirements.

10.7. Personal Data in the Company shall be destroyed by the decision of the person responsible for the implementation of these Rules upon the expiry of the data retention periods or on other grounds provided for in legal acts or these Rules.

10.8. Connection to the Company's computers, computer network and database is protected by a confidential password. The password consists of at least 8 characters that can be a combination of Latin letters and numbers without using any personal information. Passwords in the Company are changed every 60 days, as well as during the first login. Company's employees must maintain the confidentiality of passwords.

10.9. Only licensed software may be used on the Company's computers.

10.10. The Company's internal computer network is protected by an effective firewall.

11. Final Provisions

11.1. These Rules shall become effective after they are coordinated with the employees' representatives (if any) and approved by the Head of the Company.

11.2. These Rules may be amended or supplemented by coordinating such changes with the employees' representatives (if any). Amendments are approved by order of the Head of the Company, by adding new text of the Rules thereto.

11.3. The following annexes are an integral part of these Rules:

11.3.1. Annex 1 – Records of data processing activities of the Company;

11.3.2. Annex 2 – List of employees who have read the Rules.

11.4. Every employee of the Company shall be responsible for compliance with these Rules.

11.5. The Company's employees are familiarised with the Rules by signature.

11.6. These Rules are reviewed once a year and updated as necessary.