Approved by
BIA Senate
On 23 October, 2019 protocol No 140

Baltic International Academy
Privacy Policy

Issued in accordance with the
General Data Protection Regulation
and the Law on the Processing of Personal Data

1. General provisions

1.1. This BIA Privacy Policy (hereinafter - the Policy) regulates the main principles and rules regarding the collection, processing and storage of personal data and the operating rules of the Data Controller's website www.bsa.edu.lv (hereinafter - the website) of SIA "Baltijas Starptautiskā akadēmija", registration number: 40003101808, legal address: Lomonosova street 4, Riga, LV-1003, contact information for personal data protection issues: Lomonosova street 4, Riga, LV-1003, it@bsa.edu.lv (hereinafter - the Data Controller).

1.2. For the purposes of this Policy, a Data Subject is any natural person whose personal data will be recorded on the website.

1.3. The Data Controller shall comply with the following principles of data processing:

1.3.1. Personal data shall be processed lawfully, fairly and transparently in relation to the Data Subject;

1.3.2. Personal data are collected for an accurate, explicit and legitimate purpose and not further processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the original purposes;

1.3.3. Personal data are adequate, relevant and include only what is necessary for the purposes of their processing;

1.3.4. Personal data are accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay;

1.3.5. Personal data shall be stored in a form which permits identification of Data Subjects for no longer than is necessary; personal data may be stored longer in so far as personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures necessary to safeguard the rights and freedoms of Data Subjects;

1.3.6. Personal data shall be processed in such a way as to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

1.3.7. The Data Controller is responsible for the above principles and is able to demonstrate compliance with them.

1.3.8. The use of third party services may be subject to third party terms and conditions. Therefore, when using these third party services, it is recommended to read the applicable terms and conditions.

1.3.9. This Policy has been prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 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 - GDPR), and the applicable laws and regulations of the Republic of Latvia.

2. Collection, processing and storage of personal data

2.1. The Data Subject consents to and does not object to the management and processing of his or her personal data by the Data Controller in accordance with the procedures set out in the Privacy Policy and the law.

2.2. By entering their personal data, the Data Subject grants the Data Controller the right to collect, organise, use and manage their personal data provided directly or indirectly by visiting the website for any of the purposes set out in this Privacy Policy.

2.3. The Data Subject is responsible for ensuring that the data provided are accurate, correct and complete. Intentionally entering incorrect data is considered a violation of the Privacy Policy. If the data provided changes, the Data Subject must correct it immediately and, if this is not possible, inform the Data Controller. The Data Controller and Processor shall not be liable for any damage caused to the Data Subject and/or third parties if the Data Subject has provided incorrect and/or incomplete personal data or has failed to request the addition and/or amendment of data after they have been changed.

3. Personal data processing

3.1. The Data Controller - IT Education Foundation provides two types of content:

3.1.1. Computer science content for Academy staff and students;

3.1.2. *Moodle* courses, knowledge tests on the courses taken and proof of knowledge for all interested parties.

3.2. When registering as a *student* in the "BSA e-Learning Environment" you will be required to provide information about yourself: Name, surname, e-mail.

3.3. When registering as an *academic staff* in the "BSA e-Learning Environment" you will be required to provide information about yourself: Name, surname, e-mail.

3.4. By logging in with "BSA e-Learning Environment" you are subject to the Privacy Policy.

3.5. The legal basis for processing personal data is Article 6(1)(a) GDPR (processing with the Candidate's consent), (b) (processing for the performance of a contract or for an action taken at the Candidate's initiative prior to entering into a contract).

4. Procedures and time limits for the storage of personal data, data repositories and transfer sites

4.1. When processing and storing personal data of Data Subjects, the data processor shall implement organisational and technical measures to ensure the protection of personal data against accidental or unlawful destruction, alteration, disclosure and any other unlawful means of processing.

4.2. The Data Processor collects your personal data for as long as you use our services and in accordance with the applicable rules. The Data Processor does not undertake in any way to store all your data for an indefinite period of time. You may have access to some data (Name, Surname, Email, Phone number, Date of birth) while you have an active account with us. The data may be deleted at any time during your active use of the account in accordance with the terms set out above.

4.3. The servers owned by the Data Processor and the third party servers (data centre) where the Data Processor processes and stores data shall be located only within the territory of the European Union (Latvia). The Data Processor undertakes not to transfer any data outside the European Economic Area.

5. Rights of the Data Subjects

5.1. Data Subjects have the rights of the Data Subject guaranteed by the GDPR and these rights are not limited or diminished by this Policy. Data Subjects shall have the right, at any time and upon request, to inspect and receive information about the personal data processed by the Data Controller, to exercise their right to rectify their outdated, incomplete or incorrect personal data, to request the suspension of personal data processing activities if the data processing is not in accordance with the law and the requirements of this Policy.

5.2. To the extent that processing of personal data is based on consent, the Data Subject shall have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent given prior to the withdrawal.

5.3. Data Subjects may exercise their existing rights by submitting a written application by e-mail to it@bsa.edu.lv or by post to Lomonosova street 4, Riga, LV-1003 or by directly visiting the Data Controller's office during business hours. The Data Controller may request additional identifying or supporting information if it is deemed necessary and proportionate in a particular case.

5.4. If the Data Subject is dissatisfied with the activities of the Data Controller and considers that the Data Controller has processed the personal data of the Data Subject in a way that does not comply with the legal requirements, the Data Subject may lodge a complaint with the Data Inspectorate.

6. Information on the use of cookies

6.1. The website of the Data Controller uses cookies. Cookies are small text files that are stored in the visitor's browser or device (personal computer, mobile phone or tablet).

6.2. By using cookies, we aim to provide a more enjoyable experience for people who browse the site and to improve the site.

6.3. Cookies used on the website can be grouped in the following ways:

6.3.1. Functional cookies (startit_session, start_it_courses_session) are designed to enable the website to perform its main functions. These cookies allow you to browse the website and use the functions you want.

6.3.2. Performance (analytical) cookies (_utma, _utmz, _utmc, _utmb, _utmt / Google Analytics) collect anonymous information about how visitors use the website. By providing information about the pages visited, the time spent on the website and possible problems such as error messages, these cookies help the Data Controller to understand how visitors behave on the web. This information helps us to improve the website's performance.

6.4. The Data Subject may delete or block cookies by selecting the appropriate settings in the browser that allow all or some cookies to be blocked. It is known that using browser settings that block all cookies (including necessary cookies) may cause problems when using all or part of the functions of the website. For further information on cookies and how to manage or delete them, please visit www.aboutcookies.org.

7. Risk management

7.1. The risk management provisions of the Security Policy are designed to mitigate the level of threats and to ensure the confidentiality, integrity and availability of information, as well as to mitigate potential losses.

7.2. Risk management is based on the classification of information resources. In planning risk management activities, the IT Systems Security Manager, in cooperation with resource holders, shall carry out an IS risk analysis.

7.3. The purpose of the risk analysis is to assess:

7.3.1. the likelihood of an IS threat occurring, where an IS threat is an intentional or negligent act or omission or a potential event that could result in the deletion, suppression, alteration, corruption of information resources or technical resources or the release of information to unauthorised persons;

7.3.2. the potential damage to the information resource holder or the BIA if IS security is inadequate.

7.4. A risk analysis shall be carried out on a regular basis (at least annually) for all IS, as well as for each new IS-related project and IS that have undergone changes that may affect the security of the IS. The risk analysis shall take into account the state of play with regard to IS security measures.

7.5. A risk management plan for the implementation of security measures is prepared in accordance with the results of the risk analysis, and a business continuity and disaster recovery plan is developed.

7.6. The risk analysis shall be carried out using the risk analysis methodology set out in the BIA's Information Systems Security Risk Management Policy.

8. Final provisions

8.3. Legal relations related to this Policy are governed by the GDPR and applicable laws and regulations of the Republic of Latvia.

8.4. The Data Controller shall not be liable for any damages, including damages resulting from any interruption in the use of the Website, corruption or loss of data,

arising out of the acts or omissions of the Data Subject or third parties acting on behalf of the Data Subject, including incorrect input of data, other errors, deliberate misuse and other unlawful use of the Website. The Data Controller shall also not be liable for any disruption to the access/use and/or damage of the website resulting from acts or omissions of third parties unrelated to the Data Subject, including problems with electricity, internet access, etc..

8.5. The Data Controller shall have the right to change this Policy in whole or in part at any time.

8.6. Changes or additions to the Policy shall take effect on the date they are published on the Data Controller's Website.

8.7. If the Data Subject continues to use the website and the Data Controller's services after the Policy has been updated or amended, the Data Subject shall be deemed to have consented to such updates and/or amendments.

Date and version of the document: valid from 26.10.2019.