UAB BALTIC RED
PRIVACY POLICY

UAB Baltic RED (Data Controller and/or processor) (hereinafter the **Company**), company registration number 300582361, address Islandijos pl. 32, Kaunas, tel. +370 37 239 010, e-mail info@balticred.com, respects your privacy and is committed to safeguarding it in accordance with this Privacy Policy (hereinafter the **Privacy Policy**). The Privacy Policy publicly provides information about the processing of personal data, including the types of personal data processed, processing purposes, legal basis for data processing, data storage periods, and other information required by applicable laws. This Privacy Policy applies to the processing of personal data, both automated and non-automated, involving the systematic collection of personal data. This policy does not apply to the links provided on the website www.balticred.lt to other websites, so we recommend separately reviewing the privacy policies or rules of those websites.

1. Definitions

1.1. **Personal data / Data** means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as name and surname, personal code, location data, and internet identifiers, or based on one or more physical, physiological, genetic, mental, economic, cultural, or social identity traits of that individual.

1.2. **Employee** means a person who has entered into an employment contract, a fixed-term employment contract, or a volunteer activity agreement with the Data Controller.

1.3. **Data processing** means any operation or sequence of operations, such as collecting, recording, sorting, organizing, storing, adapting or modifying, extracting, accessing, using, disclosing, transmitting, distributing, or otherwise changing, by automated or non-automated means of personal data or personal data sets and access to them, as well as matching or interconnection with other data, their restriction, erasure or destruction.

1.4. **Data Controller** is Baltic RED UAB, which, in processing the personal data of natural persons, determines the methods and means of using that data.

1.5. **Data Subjects** are natural persons whose data is processed by UAB Baltic RED.

1.6. **Data Processor** means entities that process personal data controlled by UAB Baltic RED according to the instructions of UAB Baltic RED.

1.7. **Provision of data** – disclosure of personal data by transmission or making them available by any other means (with the exception of publishing them in mass media).

1.8. Other terms used in the Privacy Policy shall be understood as defined in the Republic of Lithuania Law on Legal Protection of Personal Data (LPPD) and/or the General Data Protection Regulation (GDPR).

2. Protection of personal data of natural persons

2.1. The Company treats personal data responsibly. Technical and organisational security measures are used for data protection. Data is stored securely and is accessible to a limited

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

number of individuals. Personal data is processed within the boundaries of the European Union/European Economic Area.

2.2. Without the prior consent of the Data Subject, the Company does not disclose personal data to unrelated third parties. The Company may provide personal data it processes to tax institutions, law enforcement, judicial, or pre-judicial institutions for their investigations or in other cases provided for by law, without the separate consent of the Data Subject.

2.3. Employees responsible for the conclusion or execution of contracts may receive the personal data processed by the Company for their activities. For its operations, the Company also utilizes services provided by third parties, access to personal data may be necessary for the proper provision of such services. In this case, the Company ensures that data processors adhere to confidentiality and ensure proper protection of personal data.

3. Principles and purposes of processing personal data

3.1. Employees, in performing their duties and processing personal data, must:

a) Process personal data lawfully, transparently and fairly;

b) Collect data for specified, clearly defined and for legitimate purposes, and not further process in a way incompatible with those purposes;

c) Adhere to the principles of purposefulness, proportionality, and data minimization when collecting and processing personal data, not demand the submission of unnecessary data, and avoid collecting and processing excessive data;

d) Ensure the accuracy of personal data and, if necessary for the processing of personal data, continuously update them; correct, supplement, destroy inaccurate or incomplete data, or suspend their processing.

e) Personal data shall be kept in a form which permits identification of the Data Subjects for no longer than it is necessary for the purposes for which the data were collected and processed;

f) Personal data must be managed in such a way as to ensure the adequate protection of personal data, including the protection against unauthorized processing or processing of unauthorised data and unintentional loss, destruction or damage by appropriate technical or organisational measures (the principle of integrity and confidentiality).

4. Personal data sources

4.1. **Personal data are provided by the Data Subject himself.** Data Subjects contact the Company, use the services provided by the Company, purchase goods and/or services, leave comments, ask questions, and contact the Company to request information, among other things.

4.2. **Personal data are obtained from other sources.** Data are obtained from other institutions or companies, publicly accessible registers, etc.

5. Personal data processing

5.1. **The Company processes personal data for the following purposes:**

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

5.1.1. **Ensuring the operation and continuity of the Company's activities. For this purpose, the following data are processed:**

- ✓ For the purpose of concluding and executing contracts, personal data of suppliers (natural persons) may be processed: Personal data processed for these purposes may include name(s), surname(s), personal code or date of birth, place of residence (address), phone number, email address, workplace, position, signature, data in the business license (type of activity, group, code, name, periods of activity, issuance date, amount), individual activity certificate number, data related to whether the Data Subject is a VAT payer, bank account and bank, service/goods amount, currency, and other data provided by the individual, as well as data received by the Company in accordance with the law while conducting its activities and/or data that the Company is obliged to process by laws and/or other legal acts.
- ✓ For the purpose of contract formation and execution, the data of supplier representatives are processed, including: name(s), surname(s), telephone number, email address, company name, address, position, authorisation details (number, date, authorised person's date of birth, signature).

- *Contracts, VAT invoices and other related documents shall be stored in accordance with the time limits set out in the General Index of Document Storage approved by Order of the Chief Archivist of Lithuania.*
  - *The legal basis for data processing is the necessity to fulfil a contract, where the client acts as the Data Subject, or to take actions at the client's request before entering into a contract (Article 6(1)(b) of the GDPR), when certain personal data are required by legal regulations (Article 6 (1) (c) of the GDPR).*

5.1.2. **Administration of debtors of a company.** For this purpose, the following data are processed:

- ✓ In administering the Company's debtors and transferring debts for recovery, the personal data of clients (debtors, natural persons) may be processed, including: name(s), surname(s), telephone number, email address, outstanding debt amount, information about services provided and/or goods sold, and other data related to the debt.

- *Contracts, VAT invoices and other related documents shall be stored in accordance with the time limits set out in the General Index of Document Storage approved by Order of the Chief Archivist of Lithuania.*
- *Data relating to the administration of the Company's debtors shall be stored for no longer than necessary for the purposes for which the personal data are processed.*
  - *The legal basis for data processing is the necessity to fulfil a contract, where the client acts as the Data Subject, or to take actions at the client's request before entering into a contract (Article 6(1)(b) of the GDPR), as certain personal data are required to be processed by legal regulations (Article 6(1)(c) of the GDPR), and the necessity to pursue the legitimate interests of the Company to improve its operations and business performance (Article 6(1)(f) of the GDPR).*

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

5.1.3. **Execution of internship contracts: For this purpose, the following data are processed:**

- ✓ For the execution of internship contracts, the following personal data are processed: name(s), surname(s), personal code, or, if not available, date of birth, signature, phone number, email address, address, educational institution, internship duration, and activities.
- *The personal data of trainees contained in the texts of relevant documents (contracts, orders, applications, etc.) (in cyberspace, in electronic or paper format or other media) , are stored in accordance with the General Guidelines for Document Storage approved by the Chief Archivist of Lithuania, specifying the retention periods.*
  - *Legal Basis for Data Processing is the necessity to fulfil a contract, where the trainee acts as the Data Subject, or to take actions at the trainee's request before entering into a contract (Article 6(1)(b)) of the GDPR and when certain personal data are required to be processed by legal regulations (Article 6 (1) (c) of the GDPR).*

5.1.4. **Search for new employees for vacant positions in the Company: For this purpose, the following candidate personal data are processed:**

- ✓ Name, surname, date of birth, address, telephone number, email address, education, and other data specified in the documents submitted by candidates to the Company, including CV.
- *Candidates' personal data are stored until the completion of the selection for the vacant position. If the candidate agrees to a longer retention period, the personal data are stored for the period specified in the consent for personal data processing.*
  - *The legal basis for data processing is consent. Candidates for vacant positions give implicit consent to process their data only until the end of the selection process. After the selection for the vacant position is completed, the data of unsuccessful candidates are deleted, except in cases where candidates provide separate consent for data processing after the selection process (Article 6 (1) (a) of the GDPR).*

5.1.5. **Administering of inquiries, comments and complaints. For this purpose, the following data are processed:**

- ✓ Name(s), surname(s), email address, telephone number, address, subject of the inquiry, comment, or complaint, text of the inquiry, comment, or complaint.
- *Data related to inquiries, comments, and complaints are stored for 1 (one) month from their submission, unless it is necessary to process personal data for a longer period under another legal basis (e.g., settlement of legal disputes). In such cases, personal data are retained for no longer than is necessary for the purposes for which the personal data are processed.*

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

- *The legal basis for data processing is the necessity to process the data to achieve the legitimate interests of the Data Controller or a third party, except where such interests or fundamental rights and freedoms of the Data Subject, which require the protection of personal data, are overridden by the legitimate interests of the controller or of a third party, in particular where the Data Subject is a child (Article 6 (1) (f) GDPR), and the consent of the Data Subject (Article 6 (1) (a) of the GDPR).*

5.1.6. **Purpose of ensuring the safety of the Company employees, other Data Subjects and property (video surveillance). For this purpose, the following data are processed:**

- ✓ Images. Video surveillance systems do not use facial recognition and/or analysis technology, image data captured by these systems are not grouped or profiled by a particular Data Subject (person). The Data Subject is informed about the on-going video surveillance by the information signs with the camera's symbol and the Company's details, which are presented before entering the surveyed area and/or the premises. The video surveillance area may not include the premises where the Data Subject expects absolute personal data protection.
- *The function of recording video footage with video cameras is active 24 hours a day. The surveillance cameras activate based on motion sensors, and the captured personal data (video data) are stored for up to 14 (fourteen) days from the moment of capture. Afterward, they are automatically deleted, except in cases where there is reason to believe that a violation, breach of duties, criminal activity, or other illegal actions have been recorded (until the end of the corresponding investigation and/or case resolution).*
- *Basis for the processing of data processing – the processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular, where the Data Subject is a child (Article 6 (1) (f) of the GDPR).*

5.1.7. **For other purposes** for which the Company has the right to process the personal data of the Data Subject, when the Data Subject has given consent, when data need to be processed for the legitimate interests of the Company, or when processing data is required by applicable laws.

6. Using social networks

6.1. Any information you provide via social media (including messages, use of the Like and Follow fields and other communications) is controlled by the operator of the social network concerned.

6.2. Our Company currently has an account on the social network LinkedIn, whose privacy policy is available at the address https://www.linkedin.com/legal/privacy-policy.

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

6.3. We encourage you to read third-party privacy notices and contact service providers directly if you have any questions about how they use your personal data.

7. Data Protection Officer

7.1. Pursuant to Article 37(1)(b) of the GDPR, the Data Controller and data processor are obliged to appoint a data protection officer when the activities of the Data Controller and data processor meet all of these criteria.

- Main activity – processing of personal data;
- Regular and systematic monitoring of Data Subjects;
- Monitoring of Data Subjects is carried out on a large scale.

7.1. Considering the specific nature of the Company's operations, it can be concluded that the Company's core activity is not the processing of personal data, and the Company does not conduct extensive monitoring of subjects. This means that the first and third criteria are not met, so the appointment of a Data Protection Officer is not necessary.

7.2. Following the recommendations of the data protection working group of Article 29, even when not mandatory under the GDPR, appointing a Data Protection Officer may sometimes be beneficial for companies and is encouraged as a voluntary practice. The Article 29 Data Protection Working Party encourages this voluntary practice.

7.3. Taking this into account, the Company appoints a Data Protection Officer. The Officer can be appointed from among the existing Company employees, a new employee, or a person with whom a service contract would be concluded.

7.4. The Data Protection Officer will assist in ensuring compliance with accountability measures (e.g., conducting impact assessments on data protection and performing or assisting in audits). The Data Protection Officer acts as an intermediary between various stakeholders (e.g., supervisory authorities, Data Subjects, and business units within the organization).

7.5. The Data Protection Officer is not personally responsible for improper data processing. The Data Controller or Data Processor must ensure and be able to prove that data processing complies with the provisions of the General Data Protection Regulation (GDPR). Therefore, the Data Controller or Data Processor is responsible for ensuring the compliance of data processing with the requirements.

7.6. The Data Protection Officer performs the following functions:

- **Informs** the Company and employees involved in data processing about their obligations under the GDPR and other European Union or member state data protection regulations, providing consultation on these matters.
- **Monitors** the compliance of the Company with the GDPR, other European Union or national data protection regulations, and internal company documents in the field of data protection, including issuing directives, increasing awareness and training of employees involved in data processing, and conducting related audits.
- **Provides consultation** on impact assessments and monitors their execution in accordance with Article 35 of the GDPR.
- **Liaisons** with the supervisory authority, namely the State Data Protection Inspectorate.

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

- Acts as a **point of contact** for the supervisory authority when it comes to inquiries related to data processing, including the preliminary consultations specified in Article 36 of the GDPR, and provides consultation on all other matters if necessary.

8. Forms of Disclosure of Personal Data

8.1. The Company undertakes to maintain confidentiality regarding Data Subjects. Personal data may only be disclosed to third parties if it is necessary for the conclusion and drawing up of the contract for the benefit of the Data Subject or for other legitimate reasons.

8.2. The Company may submit personal data to its data processors, who provide services to the Company and process personal data on behalf of the Company. Data processors have the right to process personal data only in accordance with the instructions of the Company and only to the extent necessary for the proper fulfilment of obligations laid down in the Contract. The Company shall use such processors that provide reasonable assurance that appropriate technical and organizational measures will be implemented in such a way that the processing of data complies with the requirements of the GDPR and will ensure the proper protection of the Data Subject's rights.

8.3. The Company may also provide personal data in response to requests from courts or public authorities to the extent necessary to properly enforce existing legislation and instructions from public authorities.

8.4. The Company guarantees that personal data will not be sold or leased to third parties.

9. Storage term of personal data

9.1. The personal data collected by the Company are stored in printed documents and/or in the Company's information systems. Personal data is processed for no longer than necessary for the purpose of data processing or for no longer than required by Data Subjects and/or provided by law.

9.2. Although the Data Subject may terminate the contract and refuse from the Company's services, the Company continues to be obliged to keep the date of the Data Subject for possible future claims or legal claims until the expiration of the data storage periods.

10. Rights of the Data Subject:

10.1. Right to receive information on the processing of data;

10.2. Right to access the data processed;

10.3. Right to request the correction of data;

10.4. Right to request to delete the data (“The right to be forgotten”). This right does not apply if the personal data requested to be deleted are also processed on other legal grounds, such as the processing necessary for the performance of the contract, or when the obligations according to the applicable law.

10.5. Right to restriction of processing;

10.6. Right to disagree with data processing;

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

10.7. **Right to data portability.** The right to data portability may not adversely affect other rights and freedoms. The Data Subject has no rights to the portability of data in relation to personal data processed in a non-automatic weigh ins systematised files, such as paper files;

10.8. **Right to require that only automated data processing, including profiling, is applied;**

10.9. **Right to submit a complaint regarding the processing of personal data to the State Data Protection Inspectorate;**

The Company must ensure the disability for the Data Subject to exercise the rights of the Data Subject specified in the Rules, except in cases established by law, when it is necessary to guarantee state security or defence, public order, prevention, investigation, detection or prosecution of criminal offenses, important economic or financial interests of the state, prevention, investigation and detection of breaches of professional ethics, protection of the rights and freedoms of the Data Subject or other persons.

11. Procedure for the implementation of the Data Subject's rights

11.1. You have the right to apply for the exercise of the rights of the Data Subject orally or in writing by submitting a request (Annex 1) in person, by post or by electronic means using the contacts specified in this Privacy Policy. The request to exercise the rights of the Data Subject must be legible, signed, and must contain the name, surname, address and/or other contact details of the applicant for communication or for which a reply on the exercise of the rights of the Data Subject is requested.

11.2. When a Data Subject contacts the Company regarding the exercise of Data Subject rights, they must verify their identity. Failure to do so will result in the Data Controller being unable to process Data Subject requests, and Data Subject rights will not be implemented. This does not apply if you request information about the processing of personal data in accordance with Articles 13 and 14 of the GDPR.

11.3. If a person decides to address the Data Controller personally regarding the implementation of Data Subject rights, the Data Subject must provide the Data Controller with an identity document. If a person decides to apply to the Data Controller in writing for the exercise of the Data Subject's rights by submitting a request by post, the request shall be accompanied by a copy of the person's identity document certified by a notary public or in accordance with another procedure established by the legislation. In the absence of a copy of an identity document, the Data Subject is requested to come to the Company in person and provide a proof of identity document. If a person decides to submit a request electronically, the request must be signed with a qualified electronic signature.

11.4. If the Company has doubts about the identity of the person submitting the request or the accuracy of the information provided, the Company has the right to request additional information to verify it.

11.5. The Company's answer to the Data Subject must be given not later than within one month from the date of receipt of the Data Subject's request, taking into account the specific circumstances of the processing of personal data. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611
Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com
A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

12. **Responsibilities of the Data Subject**

12.1. The Data Subject must:

12.1.1. To inform the Company about changes in the provided information and data. It is important for the Company to have accurate and valid information about the Data Subject.

12.1.2. To provide the necessary information so that at the request of the Data Subject the Company can identify the Data Subject and a certain that it communicates or co-operates with the specific Data Subject (to provide a personal identity document, or in accordance with the procedure laid down by legal acts or by electronic means of communication that allows the Data Subject to be properly identified). It is necessary for the protection of data of the Data Subject and other persons so that the disclosure of the Data Subject's information is restricted to the Data Subject, without prejudice to the rights of others.

13. Organisational and Technical Measures for Data Protection:

13.1. The Company makes maximum efforts to ensure that the organizational and technical data security measures comply with the requirements of the General Data Protection Regulation (GDPR). The following infrastructural, administrative and telecommunication (electronic) measures are in place to protect personal data against accidental or unlawful destruction, alteration, disclosure or any other unauthorised processing.

14. Final provisions

14.1. By transferring personal data to the Company, the Data Subject agrees with this Privacy Policy, understands its provisions and agrees to comply with it.

14.2. In the course of development and improvement of the Company's operations, the Company reserves the right to unilaterally change this Privacy Policy at any time. The Company has the right to unilaterally, partially, or fully change the Privacy Policy, notifying about it on the website https: //www.balticred.com/.

14.3. Amendments or changes to the Privacy Policy take effect from the day of their publication, i.e., from the day they are posted on the website https: //www.balticred.com/.

15. Contact details

15.1. If you have any questions about the processing of your personal data, or if you have any preferences or comments, please contact us: UAB Baltic RED, company registration number 300582361, address Islandijos pl. 32, Kaunas, tel. +370 37 239 010, e-mail info@balticred.com. Contact details of the Data Protection Officer – duomenuapsauga@balticred.com.

This version was updated on 16 January 2024.

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611

Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com

A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank

Annex 1 to the Privacy Policy of UAB Baltic RED

FORM OF THE REQUEST TO EXERCISE THE DATA SUBJECT'S RIGHT(S)

_____

Full name of the Data Subject (natural person)

_____

(Contact details: place of residence, telephone number, e-mail address (to be specified at the request of the Data Subject) or representative and representation basis, if the request is submitted by the Data Subject's representative)

To the manager of UAB Baltic RED

APPLICATION
ON THE IMPLEMENTATION OF THE DATA SUBJECT RIGHTS (S)

_____20 _____

_____

(place of application)

Please implement the right (s) of the Data Subject*:

*Mark the appropriate box with a cross

- ☐ **Right to receive information on the processing of data.**
- ☐ **Right to access the data processed.**
- ☐ **Right to request the correction of data.**
- ☐ **Rights to request to delete the data ("The right to be forgotten").** This right does not apply if the personal data requested to be deleted are also processed on other legal grounds, such as the processing necessary for the performance of the contract, or when the obligations according to the applicable law.
- ☐ **Right to restrict the data processing.**
- ☐ **Right to object to data processing.**
- ☐ **Right to data portability.** The right to data portability may not adversely affect other rights and freedoms. The Data Subject has no rights to the portability of data in relation to personal data processed in a non-automatic processing of system files, such as paper files.
- ☐ **Right to require that only automated data processing, including profiling, is applied.**

Other information**:

**Indicate what you specifically ask and provide as much information as possible to enable to properly enforce your right (s) (for example, if you want to receive a copy of your personal data, indicate specific data (e.g., dated xxxx xx 2018), a copy of email, video dated xxxx xx 2018 (x h x min. *you want to receive; If you want to correct the data, indicate what of your specific personal data is inaccurate; if you disagree to the processing of your personal data, indicate the arguments on which you base your disagreement, indicate to which particular data processing you disagree with; if you are applying for the right to data portability, indicate in respect of which data you wish to implement this right, or if you would like to transfer it to your device or other Data Controller, and if the latter, then specify him):*

_____

_____

ENCLOSED***:

***If the application is sent by post, a copy of the personal document confirming the identity, certified by a notary public or other legal acts, must be attached to the application. For requests of correction of inaccurate data, copies of the documents confirming the exact data are provided; if they are sent by post, they must be approved by a notary or according to other procedure established by legal acts. If the personal data of the Data Subject, such as his full name, have changed, copies of documents confirming the change of these data must also be presented; if they are sent by post, they must be approved by a notary or according to other procedure established by legal acts.

(signature) *(Full name)*

UAB Baltic RED
Islandijos pl. 32,LT– 47446 Kaunas, Lietuva
Įmonės kodas: **300582361**
VAT code: LT100002612611

Tel.: +370 37 23 90 10
info@balticred.com
www.balticred.com

A/s LT 23 7300 0100 9574 6402
Bank code: 73000
AB Swedbank