

PRIVACY POLICY

TABLE OF CONTENT

1. INTRODUCTION	2
2. TERMS USED IN THE RULES	2
3. PERSONAL DATA CONTROLLER AND PERSONAL DATA PROCESSING PRINCIPLES	2
4. OUR CONTACT INFORMATION.....	3
5. YOUR PERSONAL DATA THAT WE COLLECT, ITS PURPOSES AND LEGAL BASIS	3
6. SOURCES OF PERSONAL DATA	9
7. PROFILING AND AUTOMATED DECISION-MAKING	9
8. DIRECT MARKETING.....	10
9. OUR IDENTIFICATION TOOLS.....	10
10. RECIPIENTS OF YOUR PERSONAL DATA	11
11. International transfer of personal data	11
12. TERMS OF STORAGE OF PERSONAL DATA	12
13. SECURITY MEASURES IN PLACE.....	12
14. YOUR RIGHTS AND THEIR IMPLEMENTATION	13
15. COOKIE POLICY	14
16. VALIDITY AND AMENDMENT OF THE RULES	14

1. INTRODUCTION

1.1. BEBAWA (also referred to as "we", "us", "BEBAWA" or "Company"), company code 305483424, having its registered office at Mėsiniu str. 5, Vilnius Republic of Lithuania, provides services based on the electronic money license No. 70 issued by the Bank of Lithuania on 09 06 2020.

BEBAWA cares about the privacy of your personal data protection and therefore seeks to ensure a fair and transparent processing of personal data and comprehensively inform you about the processing of their personal data. This privacy policy (hereinafter the Privacy Policy) determines the key aspects relating to terms under which the Company collects, uses, discloses and protects your personal data and, accordingly, defines your privacy rights.

1.2. Please read the Privacy Policy carefully. Should you have any questions regarding the processing of your personal data, please contact us using the contact information provided in this Privacy Policy.

2. TERMS USED IN THE RULES

2.1. Personal data shall mean any information about you, which you provide to us or which we obtain from other sources and which enables us to identify you (for instance, personal data may include your given name and surname, date of birth, personal ID No., contact information, information about your creditworthiness and other information that is required for the appropriate provision of our Services, video data recorded by our video cameras, information about the agreements concluded with us, information about the use of our services, etc.).

2.2. When writing 'you', we mean you as – a potential, existing or former Client, duly authorised representative of our Client, any natural person who uses, has used, has expressed an intention to use the Services (either electronically, for instance, by using our internet websites www.bebawa.com, logging into the e-services system of BEBAWA, etc., or personally) or is otherwise connected with the Services or users of these Services (end-users or clients of our business clients (merchants, banking correspondents, other entities, including obliged entities, etc.)), other parties, such as beneficial owners, authorised representatives, business partners, other associated parties or person contacting us using e-mail or other communication measures, through which we can be accessed.

2.3. Client refers to either an individual or a business client who maintains an Account with the Company.

2.4. Account means an electronic record inside the Company's system which allows to identify the Client, execute transactions and contain information on the transactions performed by the Client.

2.5. Services shall mean the services provided by BEBAWA that are described in BEBAWA's website at <https://www.bebawa.com/>.

3. PERSONAL DATA CONTROLLER AND PERSONAL DATA PROCESSING PRINCIPLES

3.1. BEBAWA shall act as a data controller in respect of your Personal data that it processes. In the process of processing of your Personal data, BEBAWA shall adhere to the following:

3.1.1. The General Data Protection Regulation (EU) 2016/679 (hereinafter the GDPR);
3.1.2. The Law on Legal Protection of Personal Data of the Republic of Lithuania;
3.1.3. The Law on Electronic Communications of the Republic of Lithuania;
3.1.4. Other legal acts regulating the protection of personal data;
3.1.5. Instructions and recommendations of the State Data Protection Inspectorate and other competent authorities;
3.1.6. Good data protection practice around the EU.

3.2. BEBAWA shall be responsible and shall ensure that the following principles be adhered to in the process of processing of your Personal data:

- 3.2.1. legality, fairness, and transparency which means that the personal data with respect to you is processed in a lawful, honest, and transparent way;
- 3.2.2. purpose limitation which means that the personal data is collected for specified, clearly defined, and legitimate purposes and shall not be further processed in a way that is incompatible with those purposes;
- 3.2.3. data reduction which means that the personal data must be adequate, appropriate and is only necessary for the purposes for which it is processed;
- 3.2.4. accuracy which means that the personal data must be accurate and, if necessary, updated. All reasonable steps must be taken to ensure that personal data that is not accurate in relation to the purposes for which it is processed shall be immediately erased or corrected;
- 3.2.5. limitation of the length of the storage which means that the personal data shall be kept in such a way that your identity can be determined for no longer than is necessary for the purposes for which the personal data is processed;
- 3.2.6. integrity and confidentiality which means that personal data shall be managed by applying appropriate technical or organizational measures to ensure the proper security of the personal data, including the protection from unauthorized processing or processing of unauthorized data against accidental loss, destruction, or damage.
- 3.2.7. the accountability principle: we hold ourselves responsible for the compliance with data protection principles and rules and can demonstrate compliance with them at any time.

3.3. Your personal data is considered confidential information and may only be disclosed to third parties following the rules and procedures provided in this Privacy Policy and the applicable legal acts.

4. OUR CONTACT INFORMATION

4.1. Should you have any questions regarding the protection of your Personal data, please e-mail our DPO at dataprotection@BEBAWA.com or send us a letter to Bebawa UAB, Mėsinių str. 5 Vilnius, Lithuania.

5. YOUR PERSONAL DATA THAT WE COLLECT, ITS PURPOSES AND LEGAL BASIS

5.1. Categories of personal data being processed:

The personal data we collect can be grouped into the following categories:

Type of information	Personal data
Basic personal data:	first, last, middle names.
Identification information and other background verification data	In terms of natural persons, including duly authorised representatives of the legal entity: first, last, middle names of the representative of the client, personal identity number or date of birth (for foreigners), registration address, residence address, nationality, copy of identification document (passport, ID card, driving licence or residence permit) and its details (e.g., photograph, type, personal number (date of birth for foreigners), document number, issuance place and date, expiry date, MRZ code, signature, nationality, etc.), number and validity period of the residence permit in the Republic of Lithuania, place and date of its issue (applies to foreigners). Information/confirmation about you, your immediate family members, and close associates of being or not being Politically Exposed Persons (PEP status), tax information (country of tax residency, taxpayer identification number), information and/or evidence on your source of wealth/funds, other financial information (various payment documents, outstanding financial obligations and their fulfilment, owned assets, types and value of owned assets, credit history and creditworthiness, expenditure and income,

	<p>origin of assets and/or property such as information about the parties to the transactions that you concluded, conditions of such transactions etc.), information on education/occupation/employment status (information about the acquired qualifications, financial knowledge, current and former employers, professional experience, economic and commercial activities performed (for instance, farming, engagement in an individual activity, etc.), visually scanned or photographed image of your face or image that you provide through a mobile or desktop camera while using our identification application, video and audio recordings for identification.</p> <p>In terms of legal persons: evidence of organizational structure and ultimate beneficial ownership (UBO), legal person's registration document (extract from the official registry, articles of association, act of incorporation and similar), evidence on the right of representation, information and/or evidence on the source of wealth/funds, other financial information (various payment documents, outstanding financial obligations and their fulfilment, owned assets, types and value of owned assets, credit history and creditworthiness, expenditure and income, origin of assets and/or property such as information about the parties to the transactions that you concluded, conditions of such transactions etc.), information on the CEO (name, surname, personal identification number (for a foreigner - date of birth), nationality (if a person is stateless, - the country that issued the personal identification document), the director's personal utility bill, the shareholder's, personal utility bill, information on the activity of the legal person (including, but not limited information on the partners, geography of activities and similar).</p> <p>UBO's or controller's of the Company personal information: name, surname, personal identification number (for a foreigner - date of birth), number, validity period, place and date of issue of the residence permit in the Republic of Lithuania, nationality (if a person is stateless, - the state that issued the personal identity document), address, tax information (country for tax residency, taxpayer identification number), number of shares held, voting rights or share capital part, job title, information on the source of wealth/funds, other financial information (various payment documents, outstanding financial obligations and their fulfilment, owned assets, types and value of owned assets, credit history and creditworthiness, expenditure and income, origin of assets and/or property such as information about the parties to the transactions that you concluded, conditions of such transactions, etc.).</p> <p>Other data that enables us to perform anti-money laundering requirements and ensure compliance with international sanctions, including the purpose and intended nature of the business relationship and other data that is required to be processed by us to comply with the legal obligation to "know your client" (collected data will differ depending on the client's profile).</p>
Transaction data	Transaction details (IBAN number, beneficiary details, date, time, amount of transaction, and currency which was used, purpose of payment, name, surname, IP address of sender and receiver, address), actions performed using payment instruments, cash contributions and withdrawals, deposits, account number and/or credit card number, location, the unique number of your payment account in our system, messages and documents confirming monetary operation or transaction or other documents having legal force related to the performance of the monetary operations or conclusion of the transactions (e.g. invoices and/or contractual documentation (original documents)), any other data incoming or outgoing together with the transaction.
Details of your activities	Information about the computer or mobile device you use to access our Services, including device identifiers, mobile network information, type of

	operating system, system version, and the type of browser used, information about the use of our Services, including access times, pages viewed, IP address, the page visited before and after navigating to our website, your login data used to log in to our electronic services system, login information (for instance, login session time and duration, requests, etc.), browsing information, including details of when and from what location the login to the BEBAWA electronic services system or internet website was affected, etc.
Contact details	Phone number, email, correspondence address, residence address.
Information relating to customer reliability and compliance with legal requirements	AML framework documentation in case where the Client is a financial institution
Special category data:	Biometric data (for remote identification purposes, whereby a person's unique characteristics, e.g. face images are confirmed).
Criminal records	Data about criminal records and / or absence of criminal records
Audio-visual information	Recording of part of the remote client identification session
Merchant's customer's data	Merchant's customer's data Basic personal data, Transaction data, Contact details
Other Business client's customer's data	Business client's customer's Basic personal data, Transaction data, Contact details, source of funds, source of wealth

5.2. Purposes and legal basis for personal data processing

Purpose	Legal basis	Categories of personal data
For the conclusion of the contract or the performance of measures at your request prior to the conclusion of the contract.	<ul style="list-style-type: none"> Contract performance Legal obligations 	<ul style="list-style-type: none"> Basic personal data Identification and other background verification data Audio-visual information Information relating to customer reliability and compliance with legal requirements Criminal records Contact details Other personal data needed to conduct the client's risk assessment, perform customer due diligence (CDD), enhanced due diligence (EDD), screening against sanctions, PEP, other lists, and perform other AML and sanction compliance-related processes
Client identification	<ul style="list-style-type: none"> Legal obligations Public Interest Substantial public interest (to verify 	<ul style="list-style-type: none"> Basic personal data Audio-visual information Identification and other background verification data

	your identity using biometric data)	<ul style="list-style-type: none"> Special category data (biometric data)
Fulfilment of the contract concluded with you, including but not limited to the provision of the Services.	<ul style="list-style-type: none"> Contract performance Legal obligations 	<ul style="list-style-type: none"> Basic personal data Transaction data Contact details Merchant's customer's data, when needed to provide Services. Other Business client's customer's data Other personal data needed to provide Services.
Compliance with the obligations under the Law of the Republic of Lithuania on the Prevention of Money Laundering and Terrorist Financing	<ul style="list-style-type: none"> Legal obligation Public interest 	<ul style="list-style-type: none"> Basic personal data Identification and other background verification data Transaction data Merchant's customer data Other Business client's customer data (in cases when the situation demands processing such personal data category) Details of your activities Audio-visual information Information relating to customer reliability and compliance with legal requirements Criminal records Contact details Other personal data needed to conduct the client's risk assessment, perform ODD, EDD, screening against sanctions, PEP, other lists, and perform other AML and sanction compliance-related processes.
Ensuring compliance with international sanctions	<ul style="list-style-type: none"> Legal obligation Public interest 	<ul style="list-style-type: none"> Basic personal data Identification and other background verification data Transaction information

		<ul style="list-style-type: none"> Information relating to customer reliability and compliance with legal requirements Contact details Other Business client's customer's data Merchant's customer data Other personal data needed
Prevention, discovery, investigation, and reporting of potential money laundering, terrorism financing, breach of international sanctions, and other related violations, including potentially suspicious transactions and the Services abuse	<ul style="list-style-type: none"> Legal obligations Public Interest 	<ul style="list-style-type: none"> Basic personal data; Identification and other background verification data; Transaction data; Merchants' customer data; Other Business client's customer data Contact details; Details of your activities; Other personal data is needed (the scope of processed personal data depends on the Client's profile and specific situation).
Handling complaints, requests, enquiries, email correspondence	<ul style="list-style-type: none"> Contract performance Legal obligations Legitimate interest (to be efficient about how we meet our obligations and keep to regulations that apply to us, how we can improve the Services) 	<ul style="list-style-type: none"> Basic personal data Contact details Communication details Transaction data / Identification and other background verification data / Merchant's customer data – in cases when analysis and resolution of the complaint/request demands processing such personal data category
Exercising and defending legal claims	<ul style="list-style-type: none"> Legitimate interest (to protect BEBAWA during the legal dispute) 	<ul style="list-style-type: none"> Basic personal data; Identification and other background verification data; Transaction data; Audio-visual information Information relating to customer reliability and

		<p>compliance with legal requirements</p> <ul style="list-style-type: none"> • Criminal records • Contact details; • Communication details; • Details of your activities; • Other personal data needed to evaluate the legitimacy of the provision of Services or other actions performed by the Company and / or client - where it is required in the particular situation or /and when it is required by the essence of the legal claim.
Ensure adequate provision of the Services, the safety of information within the Services	<ul style="list-style-type: none"> • Legitimate interest (enabling us to improve and deliver a better Service , to meet our obligations and keep to regulations that apply to us, to conduct research and analysis, including to produce statistical research and reports) 	<ul style="list-style-type: none"> • Basic personal data • Communication details • Contact details • Details of your activities
To provide an answer when you contact us through our website or other communication measures (customer support)	<ul style="list-style-type: none"> • Legitimate interest (to develop our products and services and to be efficient in meeting our obligations) 	<ul style="list-style-type: none"> • Basic personal data • Contact details • Communication details (content and history).
Direct marketing	<ul style="list-style-type: none"> • Legitimate interest (for existing clients - to develop and market our products and keep to regulations that apply to us) • Your consent 	<ul style="list-style-type: none"> • Contact details

5.3. We do not process special category data related to your health, ethnicity, or religious or political beliefs unless required by law or in specific circumstances where, for example, you reveal such data while using the Services (e.g., in payment details).

- 5.4. If you provide us personal data about other people (such as business client's customer data, business client's representative data, etc.), you confirm that you have brought this Privacy Policy to their attention beforehand.
- 5.5. The definitions used above are understood as follows:
 - 5.5.1. Legitimate interest: interest of the Company or of a third party, provided that your interests or the fundamental rights and freedoms are not overriding, and such use of your personal data is balanced against your human rights and freedoms.
 - 5.5.2. Contract performance: processing your personal data where it is necessary for the performance of a contract to which you are a party or to take pre-contractual measures before entering such a contract.
 - 5.5.3. Legal Obligations: Processing your personal data where it is necessary for compliance with a legal or regulatory obligations that we are subject to.
 - 5.5.4. Consent: Your consent shall mean any freely given, specific, informed, and unambiguous indication of your wishes by which you, by a statement or by a clear affirmative action, signify your agreement to the processing of personal data relating to you. We can request your consent for processing when we do not have another legal basis for processing your data.

6. SOURCES OF PERSONAL DATA

- 6.1. BEBAWA collects Personal data obtained directly from you when you:
 - 6.1.1. fill out applications or other forms in order to order our Services,
 - 6.1.2. correspond with us by e-mail, present specific documents to us, submit requests or claims,
 - 6.1.3. call us or contact us in another manner, use our internet websites or electronic services system, participate in our customer surveys or promotional campaigns.
- 6.2. BEBAWA may also obtain your personal data from other legitimate sources:
 - 6.2.1. Other financial institutions (for instance, other banks operating in Lithuania) in case the personal data is received while executing payment operations;
 - 6.2.2. we may receive your personal data from our business clients, obliged entities;
 - 6.2.3. Third parties, such as various State institutions, private or public and registers and databases. This includes information to help us check your identity, if applicable, information about your spouse and family, and information relating to your transactions;
 - 6.2.4. Persons administering joint debtor data files (for instance, UAB Creditinfo Lietuva);
 - 6.2.5. Legal entities, where you are related to such legal entities in any manner (for instance, you are a representative, employee, contractor, founder, shareholder, participant, etc. of such legal entities);
 - 6.2.6. Other natural persons (for instance, when they provide data of their spouses, children, other persons who are their relatives or are affiliated to them, as well as co-debtors, guarantors, providers of collaterals and other persons);
 - 6.2.7. Other natural persons or legal entities in the process of fulfilling contractual or legal requirements and documents provided to us (for instance, information in property valuation reports, certificates, etc.);
 - 6.2.8. Our partners or other legal entities, which use BEBAWA to provide services to you.
In the process of engaging in our operations, we may combine the available information about you that is obtained from different sources.
 - 6.2.9. occasionally, we will use publicly available information about you from publicly available sources (e.g., media, online registers, and directories) and websites for enhanced due diligence checks, security searches, and other purposes related to Client due diligence processes;
 - 6.2.10. other entities with which we collaborate.

7. PROFILING AND AUTOMATED DECISION-MAKING

- 7.1. Profiling is a method of automated processing of your personal data that BEBAWA employs. Profiling is used in order to automate the processing of customer personal data and be able to evaluate certain

personal traits of customers and in this manner analyse and forecast a variety of aspects such as a person's financial situation, remote customer identification, personal preferences and interests.

7.2. Profiling may be used to process the available customer data and take decisions (with human intervention) regarding your creditworthiness and financial risks as well as to provide you with appropriate advice or offer you specific services customised to your needs and ensure a more effective monitoring of transactions and operations for the purposes of identifying and preventing money laundering and/or terrorist financing and/or fraud. This enables us to ensure the smoothness, promptness and objectivity of the aforementioned processes. Normally, such profiling is based on the fulfilment of the legitimate interests of BEBAWA, but it may also be exercised on the basis of an applicable legal obligation, implementation of the respective agreement or customer consent.

8. DIRECT MARKETING

8.1. BEBAWA may also process personal data in order to improve the quality of its services and develop new proposals with consideration of customer needs. Where a customer does not express its disagreement to the processing of its data for direct marketing purposes, we may process the customer's personal data in order to select and present general and customised offers of similar BEBAWA services (depending on the manner and the types of our services the customer uses). This profiling for marketing purposes shall be based on our legitimate interest. If you disagree that your personal data be processed for direct marketing purposes, please notify us of this immediately.

8.2. In other cases, we may use your personal data for the purpose of direct marketing, if you give us your prior consent regarding such use of the data. In case you do not agree to receive these marketing, messages or calls offered by us, this will not have any impact on the provision of Services to you as the Client.

8.3. We provide a clear, free-of-charge and easily realisable possibility for you at any time not to give your consent or to withdraw your given consent for sending proposals put forward by us. We shall state in each notification sent by e-mail that you are entitled to object to the processing of the personal data or refuse to receive notifications from us. You shall be entitled to refuse to receive notifications from us by clicking on the respective link in each email notification.

9. OUR IDENTIFICATION TOOLS

9.1. In order to perform your identity verification, we use the services provided by our partner Veriff OÜ, Niine 11, 10414 Tallinn, Estonia (hereinafter – Veriff) who acts as BEBAWA's data processor. The Processor takes the photo images and video recordings of your face and your ID document that you provide using the camera. For more information on Veriff please read their [Privacy notice](#).

9.2. Veriff solution is used for comparing live photographic data and your ID document, to comply with legal obligations (e.g., implementation of the obligations under the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other fraud and crime prevention purposes) and risk management obligations.

9.3. The result of the face similarity (match or mismatch) will be retained for as long as it is necessary to carry out verification and for the period required by anti-money laundering laws.

9.4. When using Veriff services, the personal data is used for your identification, since Veriff compare the image of the person in the identity document and the person captured in the photo. This process shall allow us to verify your identity more precisely and make the process quicker and easier to execute.

10. RECIPIENTS OF YOUR PERSONAL DATA

- 10.1. In its operations, BEBAWA may involve different processors of your personal data (i.e. certain service providers). Such data processors chosen by us shall only process your personal data according to our instructions. For instance, data processors may include companies providing data storage services, companies developing and supporting software, companies providing communications services, companies performing analysis of online activity, companies providing marketing services and other service providers. Your personal data may only be disclosed by BEBAWA to these data processors to the extent necessary for providing the respective services.
- 10.2. We shall ensure that the chosen data processors adhere to the requirements of the GDPR, laws and other applicable legal acts and recommendations issued by competent authorities. The relationship of BEBAWA and a specific data processor (except in cases where such relationship is regulated by laws or other legal acts) shall be regulated by the respective written agreement or written conditions.
- 10.3. BEBAWA may also provide your personal data to the recipients of the following categories:
 - 10.3.1. public authorities, institutions, organisations, courts and other third parties, when required by applicable laws, or in cases and under procedures provided for by applicable laws;
 - 10.3.2. third parties providing services to the Company including providers of legal, financial, auditing, tax, business management, personnel administration, accounting, advertising (including online advertising), direct marketing, communications, data centers, hosting, cloud and/or other services. In each case, we provide such third parties with only as much data as necessary to provide their services. Service providers engaged by us may process your personal data only in accordance with our instructions and may not use them for other purposes;
 - 10.3.3. third parties for the purpose of performance of the contract concluded with you, such as, banking correspondents, commercial banks, other financial institutions, beneficiaries of transaction funds receiving the information in payment statements together with the funds of the transaction, etc.;
 - 10.3.4. third parties, when the Company intends to enter into a business sale transaction and/or to perform legal and/or financial due diligence of the Company prior to such transaction;
 - 10.3.5. other persons with your consent.

11. INTERNATIONAL TRANSFER OF PERSONAL DATA

- 11.1. In case your personal data is transferred outside the EEA or EU, we will take the necessary steps to ensure that your data is treated securely and following this Privacy Policy. We will ensure that it is protected and transferred in a manner consistent with the legal requirements applicable to the personal data. This can be done in several different ways, for example:
 - 11.1.1. the country to which we send the personal data, a territory or one or more specified sectors within that third country or the international organization is approved by the European Commission as having an adequate level of protection;
 - 11.1.2. the recipient has signed or contains in its terms of the service (service agreement) standard contractual clauses approved by the European Commission;
 - 11.1.3. special permission has been obtained from a supervisory authority.
- 11.2. In addition, we may transfer your Persoal data to third country i fit is necessary for the performance of a contract between you and us, i. e. for provision of the Services (for example, if you make international payment).
- 11.3. We may transfer personal data to a third country by taking other measures if it ensures appropriate safeguards as indicated in the GDPR. It should be noted that the providers of payment and other services that are involved in the implementation of your agreements concluded with us may be also established or operate in a State outside of the EU/EEA. Such a State may lack an adequate level of data protection (for instance, it may be a State that the European Commission has not included on the list of States with an adequate level of data protection). In any case, we will take all reasonable legal and technical steps on our side to ensure that your personal data is used securely.

12. TERMS OF STORAGE OF PERSONAL DATA

- 12.1. We will keep your personal data for as long as it is needed for the purposes for which your data was collected and processed and as required by the retention requirements in laws and regulations. If the legislation of the Republic of Lithuania does not provide any applicable data retention period, we shall determine it, considering the legitimate purpose of the data retention, the legal basis, and the principles of lawful processing of personal data.
- 12.2. The terms of data retention of the personal data for the purposes of the processing of the personal data as specified in this Privacy Policy are as follows:
 - 12.2.1. if your consent remains in force and there are no other legal requirements that shall be fulfilled concerning the personal data processing. We reserve the right to retain records of any consent given and withdrawn for a period of time necessary to protect our rights;
 - 12.2.2. the personal data collected for the implementation of the obligations under the Law on Prevention of Money Laundering and Terrorist Financing shall be stored for up to 8 (eight) years. The retention period may be extended for a period not exceeding 2 (two) years, provided there is a reasoned request from a competent authority;
 - 12.2.3. the personal data you submit through our website or via email as customer support inquiries, the data to the extent necessary to resolve the complaint is kept for 1 year after the decision is taken / request has been resolved;
 - 12.2.4. in case of your complaints, materials related to their examination, a document indicating the specific result of the examination of complaints, and the response provided to you for at least 3 years from the date of submission of the final response to you. In case decision is challenged, the retention period is 3 years after final decision.
- 12.3. When the terms of data keeping are indicated in the legislative regulations, the legislative regulations are applied.
- 12.4. Your personal data may also be stored for a longer term, where it is necessary to defend the rights and legitimate interests of BEBAWA, provide a response to an inquiry, settle a complaint or dispute and in other cases envisaged by legal acts.
- 12.5. On expiry of the term of processing of personal data, your personal data shall be destroyed or irreversibly anonymised.

13. SECURITY MEASURES IN PLACE

- 13.1. BEBAWA shall implement a variety of organisational and technical security measures that help to protect your personal data against accidental or unauthorised destruction, alteration, disclosure, access and/or any other unauthorised processing. BEBAWA requires that the data processors, which are involved by BEBAWA to process your personal data or which have access to your personal data in the process of providing services to BEBAWA, implement the appropriate organisational and technical measures to ensure the security and integrity of your personal data.
- 13.2. Some of the technical and organizational measures we use are:
 - 13.2.1. We periodically test the systems;
 - 13.2.2. We use secure passwords and 2FA to limit access to data;
 - 13.2.3. We regularly update our software;
 - 13.2.4. We implement reasonable security practices and procedures to help protect the confidentiality and security of your information, including any non-public personal information. We protect your information using reasonable physical, technical, and administrative security measures, including by limiting access to your information to employees with a need to know such information.

13.3. Nevertheless, it should be borne in mind that in certain cases the transmission of information by electronic means of communication (e-mail, mobile phone, etc.) may be less secure for reasons not depending on the technical or organisational measures implemented by BEBAWA. To ensure the security of your confidential data, we recommend that you do not provide us with any information via less secure electronic systems or via any electronic systems not used by BEBAWA.

14. YOUR RIGHTS AND THEIR IMPLEMENTATION

14.1. You have the following rights in respect of your personal data as envisaged in legal acts:

14.1.1. **The right to be informed.** You have the right to be provided with clear, transparent and easily understandable information about how we process your personal data.

14.1.2. **The right to access.** You have the right to request a copy of your personal data from us. Where your requests are excessive if they are repetitive, we may refuse to act on them or charge a reasonable fee, considering the administrative costs of providing the information. We will assess the excessiveness of the request.

14.1.3. **The right to rectification.** You have the right to request us to correct or update your personal data at any time if your personal data is incomplete or incorrect.

14.1.4. **The right to data portability.** When a legal basis for data processing is consent or contract, you have the right to request that we transfer your data that we have collected to another organisation, or directly to you, under certain conditions.

14.1.5. **The right to be forgotten.** When there is no good reason for us to process your personal data anymore, you can ask us to delete it. We will take reasonable steps to respond to your request. If your personal data is no longer needed and we are not required by law to retain it, we will delete, destroy, or permanently de-identify it.

14.1.6. **The right to restrict processing.** You have the right to restrict the processing of your personal data in certain situations (e. g., you want us to investigate whether it is accurate; we no longer need your personal data, but you want us to continue holding it for you in connection with a legal claim).

14.1.7. **The right to object processing.** Under certain circumstances, you have the right to object to certain types of processing (e. g., receiving notification emails). However, if you object to us using personal data which we need to provide our Services, we may need to close your payment account as we will not be able to provide the Services.

14.1.8. **The right to file a complaint with a supervisory authority.** You have the right to lodge a complaint with a competent supervisory authority, if you believe that your personal data is processed in a way that violates your rights and legitimate interests stipulated by applicable legislation. You may apply in accordance with the procedures for handling complaints that are established by the State Data Protection Inspectorate of the Republic of Lithuania and which may be found by this link: <https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas> or <https://vdai.lrv.lt/en/>.

14.1.9. **Rights related to automated decision-making.** You have the right not to be subject to a decision that is based solely on automated processing, and which produces legal or other significant effects. You have the right to obtain human intervention; to express point of view; to obtain an explanation of the decision reached after an assessment; and to challenge such a decision.

14.1.10. **Right to withdraw your consent.** If personal data is processed based on your consent, you can withdraw it at any time. Withdrawal will not affect the lawfulness of processing of your data before the withdrawal.

14.2. In order to exercise your above rights, you must present a written application to us by e-mail to dataprotection@bebawa.com or by sending your application to Mėsinių str. 5 Vilnius, Lithuania. The information contained in your written application must be sufficient to identify you (for instance, you must specify your full name, date of birth, residence address and other contact information); you must also provide information on which of the above rights and to what extent you wish implemented. Upon receipt of your written application, we may request that you additionally confirm your identity and/or refine the scope of implementation of the specific data subject right that you wish implemented.

14.3. A received written application shall be examined, and a response shall be provided to you within 30 calendar days from the date the appropriate written application is received. In exceptional cases, which require additional time, we, subject to prior notice given to you, may extend the original term of 30

BEBAWA

calendar days for considering the claims contained in your application by up to 60 additional calendar days.

15. COOKIE POLICY

- 15.1. If you access our information or Services through our website, you should be aware that we use Cookies.
- 15.2. The cookie policy of BEBAWA, which shall constitute an integral part of the Privacy Policy, shall be published on our internet website www.bebawa.com/cookie-policy/.

16. VALIDITY AND AMENDMENT OF THE RULES

- 16.1. You may familiarise yourself with these rules at any time by visiting the websites of BEBAWA (www.bebawa.com).
- 16.2. We shall be entitled to amend Privacy Policy unilaterally at any time. In this case, we will notify you about the respective amendments to the Privacy Policy and publish the new wording of the Privacy Policy in our website as well as email you about it in case the changes are significant.