BIEASES Privacy Policy

For the United Kingdom and European Economic Area
Last Updated: December 23rd, 2023

1. Overview

BIEASES Ltd. is incorporated in the United Kingdom (UK) under reference number 14323423 with a registered address of 288 Chase Road, London, United Kingdom, N14 6HF. BIEASES Ltd. also has the trading name of "BIEASES".

BIEASES Wallet is a payment platform which serves both Private and Merchant customers by offering the functions of Recharge, Withdrawal, P2P transfer, P2B Transfer, International remittance as well as the online Payment. BIEASES Wallet provides a broad network of international transfers, and it brings our customers fast, secure, and simple payment solutions.

As a registered data controller under ICO reference number ZB532383. BIEASES is committed to protecting Personal Data.

This document outlines BIEASES's approach to privacy notice in regarding to all the personal data BIEASES processed in accordance with the General Data Protection Regulation (GDPR). In this Privacy Policy, we provide customers with explanation on what kind of personal data we collect when customers use our services (Services).
This document shall be subject to periodic reviews in accordance with changes in:

- Local and international legislation.
- Industry best-practice.

When writing 'you', we mean you as – a potential, existing or former client, our client's employee or other parties, such as beneficial owners, authorised representatives, business partners, other associated parties or a person contacting us by e–mail or using other communication means.

Internal changes in the business that impact the products available and relevant revenue streams.

Senior Management must approve all changes before they are put into effect. Minor changes shall be reflected by incrementing the version number as 1.1, 1.2, 1.3, etc.
Where significant changes to the document are made, these shall be reflected in a new version number as 1.0, 2.0, 3.0, etc.

2. Principles relating to processing of personal data

We are responsible for ensuring security of your personal data made available to us, in particular to prevent unauthorized access to your data. We are also responsible for ensuring all users with the opportunity to benefit their rights regarding their own personal data.

When processing personal data, we follow the principles of:

- legality, fairness and transparency
- purpose limitation.
- data reduction.
- accuracy.
- limitation of the length of the storage;
- integrity and confidentiality.

3. Our Data Protection Officer

As a registered data controller determining the purposes and means of processing personal data, BIEASES takes the confidentiality and integrity of its customer data very seriously. As stewards of customer information, BIEASES strive to assure all data is protected from unauthorized access whilst also ensuring that relevant data is available when needed.

BIEASES are also committed to ensuring that all personal data is handled in accordance with the Data Protection Laws, its principles, and any additional regulations and/or guidance laid out by the UK government or the FCA.

As part of its business operations, BIEASES ensures the safe, secure, ethical, and fair use of all personal data and always upholds the highest standards of data handling. BIEASES ensures that all employees understand, have access to, and can easily interpret this Data Protection Policy and its procedures.

The General Data Protection Regulation (GDPR) regulates the processing of personal data, which includes organisation, altering, adapting, retrieving, consulting on, storing, using, disclosing, transmitting, disseminating, or destroying any such data. As such BIEASES have put into place robust measures, policies, procedures, and controls concerning all aspects of personal data handling.

Data Protection Officer (DPO) responsible for ensuring customer information is processed and protected correctly.

3.1 Data Protection Officer Responsibilities

BIEASES has applied all relevant due diligence and screening procedures, to ensure that the DPO is suitably qualified and competent to carry out all obligations imposed upon the DPO by BIEASES.

BIEASES's Senior Management are responsible for ensuring that the DPO has sufficient autonomy, support, and resources to effectively carry out their responsibilities. The DPO is reassessed annually to ensure that they are aware and fully understand the responsibilities of their function and are sufficiently competent to meet such responsibilities.

The DPO reports directly to BIEASES's Senior Management during monthly meetings, the DPO seeks guidance and approval from Senior Management during such meetings.
The DPO carries out an annual risk assessment to assess all risks related to data protection within BIEASES.

The DPO operates alongside the Money Laundering Reporting Officer (MLRO), the Chief Technology Officer (CTO), and any other relevant member of BIEASES's Senior Management. This is to ensure that all processes, systems, and employees comply with the requirements of the relevant data protection legislation, financial

regulations, the prevention of financial crime, and industry best practice.
In the performance of their duties the DPO has the following responsibilities:

- To inform and advise BIEASES's Senior Management and any employees responsible for the carrying out and processing of customer information.
- To monitor compliance with GDPR, associated data protection provisions within BIEASES's policies, including the procedures outlined in this document.
- To oversee the assignment of responsibilities, awareness-raising and training of all employees involved in information processing and safeguarding.
- To carry out and review audits of the above-mentioned policies, procedures, employee duties and training programs.
- To act as the point of contact for all BIEASES employees for any information related concerns or doubts.
- Responsibility for due diligence, privacy impact assessments, risk analysis, and data transfers where personal data is involved.
- The maintenance of adequate and effective records and management reports.
- To be aware of, and understand, all risks associated with the collection, processing, and storage of information, this includes staying up to date with all legislation, regulations, and industry best practice.

3.2 The Information Commissioners Office

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to UK Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes:

- The Data Protection Act 2018.
- General Data Protection Regulation.
- The Privacy and Electronic Communication (EU Directive) Regulations 2003.
- Freedom of Information Act 2000.
- The Environmental Information Regulations 2004.

The ICO acts to:

- Uphold information rights for the purposes of the public interest.
- Promote openness from public bodies relating to information and the public's privacy.
- Issue enforcement notices and fines for breaches in any of Regulations, Acts and/or Laws regulated by the ICO.

The ICO acts as the UK's data protection authority and has oversight and enforcement rights in relation to the collection, handling, and storing of personal information, this includes responding to any related complaints.

As a registered Data Controller with the ICO, BIEASES are required to follow ICO legislation.

4. What information we collect

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

Type of information	Personal data
a) Basic personal data	First, last, middle, maiden names, job title, etc.
b) Identification information and other background verification data	Name, surname, personal identity code, date of birth, any other unique sequence of symbols granted to you, intended for personal identification, country of birth, address, nationality (in the case of a stateless person – the state which issued the identity document), citizenship, gender, copy of passport or ID card and its details (e.g., type, number, place and date of issuance, expiry date, MRZ code, signature), evidence of beneficial ownership or the source of funds (funds for account opening or transactions, occupation/employment information), source of wealth (information on how wealth was obtained), tax information (tax residence, tax identification number), number of shares held, voting rights or part of share capital, title, 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.
c) Transaction Data	Such as currency, amount, location, date, time, IP address, payer's and payee's name and registration information, messages and documents sent or received with the payment.
d) Details of your activities in your website account or mobile application	History of the actions performed in your website account, mobile application, technical information, including the internet protocol (IP) address used to connect your computer to the internet, your log-in information (e.g., login time), browser type and version, time-zone setting, operating system and platform, type of device you use, unique device identifier.
e) Details of your activities in our website	History of the actions performed in our website, technical information, including the internet protocol (IP) address used to connect your computer to the internet, browser type and version, time zone setting, operating system and platform, type of device you use.
f) Details of your existing bank account/-s	Financial institution account number, IBAN number, payment card number.
g) Information related to legal requirements	Data that enables us to perform anti-money laundering requirements and ensure the compliance with international sanctions, including the purpose of the business relationship and whether you are a politically exposed person / an immediate family member of a politically exposed person / a known associate of a politically exposed person, if at any time in the preceding year you have been entrusted with a prominent public function / are an immediate family member of a person who has been entrusted with a prominent public function / are a known associate of a person who has been entrusted with a prominent public function, and other data that is required to be processed by us in order

Type of information	Personal data
	to comply with the legal obligation to "know your client" (collected data will differ depending on the client's risk score). (KYC)
h) Information obtained and/or created to fulfil the requirements of applicable legislation	Data that the Company is required to provide to public authorities, such as tax administrators, courts, including data on income, payments and other information held by the Company.
i) Contact details	Phone number, e-mail, residential address.
j) Communication details	Content of email correspondence or any other form of communication with us (i.e., live chat, blogs, posts).
k) Information about your behavior	Social media account details, interests, product or service preferences, other information about your behavior and your activity on our website, mobile application.
l) Special category data	Biometric data.

5. How we use your personal data

We will only use your personal data for the purpose for which we collected it which include the following:

- To register you as a new customer
- To process and deliver your card
- To manage your relationship with us
- To enable you to load your card, make payments and make withdrawals
- To enable you to participate in a membership scheme, prize draw, competition or complete a survey
- To improve our website, products/services, marketing, or customer relationships
- To fight financial crime; and
- To recommend products or services which may be of interest to you.

6. Where we collect your personal data

We collect information you provide directly to us when you:

- fill out any forms on our website and/or mobile application.
- open an account or use any other Services.
- contact us by using other means of communication (e.g., via our social network accounts).

We may also receive your personal data from third parties. In particular:

- we may receive personal data from banks or other financial institutions including card schemes, credit reference agencies, fraud prevention agencies, government and law enforcement agencies on whose behalf or for whose benefit we provide financial services.
- we may receive personal data from third parties such as public or private 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.
- 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.
- we may receive personal data from a third party which is connected to you or is dealing with us, for example, business partners, sub–contractors, service providers, merchants etc.
- we may receive personal data from other entities which we collaborate with.

7. Why we process your personal data

There are several purposes of processing our customers' personal data.

Purpose	Legal basis	Categories of personal data
a) To register an account	Data subject's consent.	• Basic personal data; • Contact details; • Other personal data needed.
b) To conclude the contract with you, or to take steps at your request prior to entering into a contract	Taking necessary steps before conclusion of the contract and/or conclusion of the contract; Legal obligations.	• Basic personal data; • Identification and other background verification data; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing services).
c) To perform the contract concluded with you, including (but not limited to) provision of the Services	Performance of the contract; Legal obligations.	• Basic personal data; • Identification and other background verification data; • Monetary operation details; • Details of your activities in your website account or mobile application; • Details of your existing bank account/-s; • Information related to legal requirements; • Contact details; • Communication details; • Other personal data needed

Purpose	Legal basis	Categories of personal data
		(in order to evaluate the possibility of providing services).
d) To carry out ongoing Client Due Diligence (CDD) and manage ML/TF risk, identify, investigate and report suspicious activities and potential market abuse	Legal obligations.	• Basic personal data; • Identification and other background verification data; • Monetary operation details; • Details of your existing bank account/-s; • Information related to legal requirements; • Contact details. • (the scope of processed personal data depends on the client's risk category, specific situation and may include all of the above categories of personal data or a part of this personal data)
e) To enable us to comply with anti-money laundering and anti-terrorist financing requirements and to enforce compliance with the requirements relating to sanctions (including Know Your Customer ("KYC") obligations, such as to determine the purpose of the business relationship and whether you are a politically exposed person, as well as the source of funds)	Legal obligations.	• Basic personal data; • Identification and other background verification data; • Monetary operation details; • Details of your existing bank account/-s; • Information related to legal requirements; • Contact details; • Other personal data needed.
f) To comply with other legal requirements under applicable legislation in areas such as the provision of payment services, financial markets and financial services, market abuse, personal data protection, accounting and taxation	Legal obligations.	• Basic personal data; • Identification and other background verification data; • Information obtained and/or created in order to fulfil the requirements of applicable legislation; • Contact details; • Other personal data needed.
g) To identify you remotely	Your consent.	• Special category data.
h) To prevent, limit and investigate any misuse or unlawful use or disturbance of the	Performance of the contract;	• Basic personal data; • Identification and other background verification data;

Purpose	Legal basis	Categories of personal data
Services or to establish, exercising and defend legal claims	Legitimate interest; Legal obligations.	• Monetary operation details; • Details of your activities in your website account or mobile application; • Details of your activities in our website; • Details of your existing bank account/-s; • Information related to legal requirements; • Contact details; • Communication details; • Other personal data needed (in order to evaluate the possibility of providing services).
i) To ensure adequate provisions of the Services, the safety of information within the Services, as well as to improve, develop and maintain applications, technical systems and IT-infrastructure	Legitimate interest.	• Basic personal data; • Contact details; • Details of your activities in our website; • Communication details; • Other personal data needed (in order to evaluate the possibility of providing services).
j) To assess the quality of our Services and improve and deliver a more personalized experience	Legitimate interest.	• Information about your behavior; • Communication details; • Details of your activities in your website account or mobile application; • Details of your activities in our website; • Contact details.
k) To provide an answer when you contact us via our website or other communication means	Your consent.	• Basic personal data; • Contact details; • Communication details; • Other personal data needed (in order to evaluate the possibility of providing services).

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 payments details).

If you provide us personal data about other people (such as your spouse or family) or you ask us to share their personal data with third parties, you confirm that you have brought this Privacy Policy to their attention beforehand.

8. Our identification tools

In order to perform your identity verification, we use the services provided by our partner "AuthID and Sumsub" (hereinafter – "verification partners"). The Service Provider takes the photo images or video recordings of your face and your ID document that you provide through a mobile application or a dedicated website using the camera. For more information on our verification partners, please read their Privacy Policy.

Our verification partners' solutions are used for comparing live photographic data or video record of you 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.

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.

We ensure that your face similarity check is a process of comparing data acquired at the time of verification, i.e., this is a one-time user authorization by comparing person's photos to each other. Your facial template is not created, recorded or stored. It is not possible to regenerate the raw data from retained information.

Using our verification partners' services, personal data is used for your identification, since they verify the identity 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. If you do not feel comfortable with this identification method, you may contact us by e-mail at bieases@bieases.com for an alternative way to identify you.

9. How we share your personal data

The following is a list of key recipients, to whom your personal data might be disclosed to:

- public authorities, institutions, organisations, courts and other third parties, but only upon request and only when required by applicable laws, or in cases and under procedures provided for by applicable laws; e.g. HM Revenue & Customs, regulators, including the FCA, and other authorities;
- third parties providing services to the Company including providers of legal, financial, fraud prevention agencies, credit reference agencies, auditing, tax, business management, personnel administration, accounting, advertising (including online advertising), direct marketing, customer service, communications, data centres, 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; e.g. Comply Advantage, Sumsub, AuthID, Intercom, AWS, Google, Facebook, etc.

- third parties for the purpose of performance of the contract concluded with you;
- Third parties helping us provide your product or service; e.g. FCA-regulated companies that help us provide the product / services, our issuer Moorwand and various third-parties to support our additional products (e.g. Plaid, Thunes, Tell Money, etc.), Our payments processor (Thredd).
- our affiliate companies – i.e., companies belonging to the same group;
- third parties, when we intend to enter into a business sale transaction and/or to perform legal and/or financial due diligence of us prior to such transaction;
- other persons with your consent.
- Police and law enforcement – i.e., Police, NCA, Information Commissioner's Office.

10. How we protect your personal data

Please note that, although no system of technology is completely secure, we have to implement appropriate security measures in order to minimize the risks of unauthorized access to or improper use of your personal information.

We and our third-party service providers that may be engaged in the processing of personal data on our behalf (for the purposes indicated above) are contractually obligated to respect the confidentiality of the personal data.

A variety of logical and physical security measures are used to keep your personal data safe and prevent unauthorized access, usage, or disclosure of it (the list indicated below is not exhaustive): we use antivirus software, information security policies, access restriction, we regularly review our information collection, storage, and processing practices to prevent unauthorized access to our systems, we use mandatory data encryption and password protection, carry out regular penetration tests and backup of data, etc.

11. How long we keep your personal data

We will keep your personal data for as long as it is needed for the purposes for which your data was collected and processed, including for the purposes to comply with any legal, regulatory, tax, accounting or reporting obligations. This means that we store your data for as long as it is necessary for provision of the Services and as required by the retention requirements in laws and regulations. It shall be determined by us, taking into account the legitimate purpose of the data retention, the legal basis and the principles of lawful processing of personal data.

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:

- as long as your consent remains in force, if there are no other legal requirements which shall be fulfilled with regard to the personal data processing;
- in case of the conclusion and execution of contracts – until the contract concluded between you and us remains in force and up to 5 years after the relationship between you and us has ended;
- the personal data collected for the implementation of the obligations under the Law on the Prevention of Money Laundering and Terrorist Financing shall be stored up to 8 (eight) years as provided in the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania. The retention

period may be extended for a period not exceeding 2 (two) years, provided there is a reasoned request from a competent authority;

- the personal data submitted by you through our website or via e-mail is kept for an extent necessary for the fulfilment of your request and to maintain further cooperation, but no longer than 6 months after the last day of the communication, if there are no legal requirements to keep them longer;
- in case your application is rejected, your personal data shall be stored for a period of 3 months, except when such data was collected for the implementation of the obligations under the Law on the Prevention of Money Laundering and Terrorist Financing were submitted reports to the Financial Crime Investigation Service.

In the cases when the terms of data keeping are indicated in the legislative regulations, the legislative regulations are applied.

We may retain your personal data for a longer period when:

- it is necessary in order for us to defend ourselves against existing or threatened claims, or to exercise our rights, or for the proper resolution of dispute, complaint or claim;
- there is a reasonable suspicion of illegal activity;
- it is required by applicable laws;

Upon expiration of the retention period, we will delete and/or reliably and irrevocably depersonalize your data as soon as possible, within a reasonable time required to perform such action.

12. Direct marketing: Email, SMS and Push Notification

In case you are existing clients (i.e., you already use our Services), we may use your e-mail address for direct marketing purposes, but only with regard to products and/or services that are similar or related to the Services, and only if you do not object to such use of your e-mail address. You are also granted with a clear, free of charge and easily enforceable possibility to object or withdraw from such use of your contact details.

In other cases, we may use your personal data for the purpose of direct marketing, only if you give us your prior consent regarding such use of the data.

We are entitled to offer the services provided by our business partners or other third parties to you or find out your opinion on different matters in relation to our business partners or other third parties taking account of the legal basis for this, i.e., your prior consent.

In case you do not agree to receive these marketing messages offered by us, our business partners or third parties, this will not have any impact on the provision of Services to you as the client.
We provide a clear, free-of-charge and easily enforceable possibility not to give your consent or, at any time, to withdraw your consent to receive our marketing messages. We shall state in each notification sent by e-mail that you are entitled to object to the processing of the personal data, and to refuse receiving messages from us. You shall be able to refuse to receiving our marketing messages by clicking on the respective link in each marketing e-mail received from us.

13. Automated decision making

In some cases, we may use automated decision-making which refers to a decision taken solely on the basis of automated processing of your personal data.

Automated decision-making refers to the processing using, for example, a software code or an algorithm, which does not require human intervention.

We may use forms of automated decision making on processing your personal data for some services and products. You can request a manual review of the accuracy of an automated decision in case you are not satisfied with it.

For more information about your rights please see the section Your legal rights.

14. International transfer of personal data

The data we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or one of our suppliers. Such staff may be engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting your personal data, you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy. This can be done in a number of different ways, for example:

- 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.
- the recipient has signed or contains in its terms of service (service agreement) standard contractual clauses adopted by the European Commission.
- special permission has been obtained from a supervisory authority.

We may transfer personal data to a third country by taking other measures if it ensures appropriate safeguards as indicated in the GDPR or on the basis of derogations.

15. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data including the right to receive a copy of the personal data we hold about you, the right to rectification if we hold incorrect data about you and the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues (www.ico.org.uk).

Email: casework@ico.org.uk

Tel: 0303 123 1113

Website: https://ico.org.uk/global/contact-us/

- Your rights to be informed. You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data.

- Your rights to access. You have the right to request from us the copies of your personal data. Where your requests are excessive, in particular if they are being sent with a repetitive character, we may refuse to act on the request, or charge a reasonable fee taking into account the administrative costs for providing the information. The assessment of the excessiveness of the request will be made by us.
- Your rights to rectification. You have the right to request us to correct or update your personal data at any time, in particular if your personal data is incomplete or incorrect.
- Your rights to data portability. The personal data provided by you is portable. You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.
- Your rights to be forgotten. When there is no good reason for us to process your personal data anymore, you can ask us to delete your data. 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.
- Your rights 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).
- Your rights 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 in order to provide our Services, we may need to close your payment account as we will not be able to provide the Services.
- Your rights to file a complaint with a supervisory authority. You have the right to file a complaint directly the State Data Protection Inspectorate of Lithuania if you believe that the 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 and which may be found by this link: https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas.
- Rights related to automated decision-making. You have the right not to be subject to a decision which is based solely on automated processing and which produces legal or other significant effects. In particular, 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.
- Right to withdraw your permission. If you have given us consent, we need to use your personal data, you can withdraw your consent at any time. It will have been lawful for us to use the personal data up to the point you withdrew your permission
- If you would like to exercise any of these legal rights, please contact us via e-mail: bieases@bieases.com. For security reasons, we will not be able to process your request if we are not sure of your identity, so we may ask for your ID as proof.
- Your requests will be fulfilled, or fulfilment of your requests will be refused by specifying the reasons for such refusal, within 30 (thirty) calendar days from the date of submission of the request that complies with our internal rules and the GDPR. The afore-mentioned time frame may be extended by 60 (sixty) calendar days taking into account the complexity and number of the requests. The Company will inform

you of any such extension within 30 (thirty) calendar days of receipt of the request, together with the reasons for the delay.

- We may refuse to satisfy your request if the exception and/or limitation to the exercise of data subjects' right set out in the GDPR apply, and/or if your request is found to be manifestly unfounded or disproportionate. If we refuse to satisfy your request, we will give you our reason for such refusal in writing.

16. Cookie policy

If you access our information or Services through our website, you should be aware that we use cookies.

For more information on how to control your cookie settings and browser settings or how to delete cookies from your device, please read the Cookie Policy available on our website www.bieases.com .

17. Links to other websites

Our website may contain links to other websites which are not operated by the Company. When you decide to click on these links and be led to such websites, we recommend familiarising yourself with their privacy policies or notices, cookie policies and/or other documents. The Company assumes no responsibility for the content, policies or practices of such third-party websites or services.

18. Contact us

You may contact us by writing an e-mail to bieases@bieases.com