Privacy Policy

KIBSTrust

Last modified: 30.06.2022 (see the archived versions)

Content

1. Introduction

KIBS AD Skopje (KIBS) promotes and implements a large part of its operations through its websites which are the basic tool for communication with the stakeholders regarding our products and services. Different KIBS business lines, each with its own specifics, can be addressed differently in respect to the privacy of your personal data. This Privacy Policy (Policy) does not apply to services related to KIBS as a payment system operator, services related to information resulted from or based on information for or from the payment system, as well as services offered through our partners or resellers.

This Policy is a result of our endeavor to bring our customers closer to the processing of personal data related to the activities of the Trusted Service Provider (TSP) and Identification Provider (IDP) which is organizationally part of KIBS but recognized under the brand name KIBSTrust. The Trusted Service Provider and the Electronic Identity Provider provide services for which KIBS holds a public authorization.

In full compliance with the legal obligations KIBSTrust takes care of your right to privacy. We stores only the personal data that is necessary to exercise business, legal and other powers related to its business activity.

This Policy is prepared to inform you about the practice of how we implement our obligations in internal operations and work with our users of products and services. KIBSTrust products and services are hereinafter referred to as: Services.

This Policy applies where you, as our service user, have a direct relationship with KIBSTrust, in other words, you are one of our customers, contacts, suppliers, contractors (including former employees or former contractors). In such circumstances KIBSTrust will act as a data controller and will make decisions related to observing the personal data we hold about you.

This Policy does not apply to products or services owned and offered by our partners, agents, other third parties and their services or websites which you may access while browsing our websites. In reference to the foregoing, we encourage you to read the Privacy Policy of those third parties.

Below we will inform you what data we collect about you, how we use the collected data, where the data is processed, your rights related to the data we store about you, how you can withdraw the permission to use your data, the security provisions of your data storage, and how to update or delete your data.

2. Consent

By entering your data on our websites or mobile applications, you expressly agree to this Policy, that is, you accept the terms set forth in it. If you do not agree to any part or all this Policy, do not continue your activity on our websites or our mobile applications.

3. What type of information do we collect?

KIBSTrust collects your data when you place an order for any digital certificate or time stamp, you want to create your electronic identity, apply for access / subscription to the Services, subscribe to one of our newsletters, you use our online chat service, download information documents about our Services, register for a webinar or organize online meeting, respond to a survey or fill in an assist form before or after a sale of services, or when you make a support request.

Without limitations to the preceding paragraph, we may request information from you that may be personal whenever you interact with us and to receive service, support, or information from us.

You may be asked to enter your first and last name or other data contained in your personal identification documents, e-mail address, postal address, numbers of personal identification documents, personal identification number, mobile phone number, parameters that can help us improve marketing, download technical data for your mobile device, download your biometric data including photo and / or video material that confirms your liveliness, details of the organization you work for and other personal data.

If, based on your wish, you choose to pay for our services by using our virtual e-shop, you will be asked for data related to your payment card by the card processor through which the payment is provided. Please ask for and read the Card Payment Provider Privacy Policy on its website.

KIBSTrust treats personal identification data as confidential, except for data that is part of the issued digital certificate. This data can be verified using external commercial applications and as such is considered to be public and allows verification of your electronic identity.

Depending on the business activities and needs, we can collect additional information about you by using data sources - third party databases (public and private) and / or databases made available to us by state institutions in order to improve our services.

KIBSTrust does not store your sensitive financial transaction data (payment card number, financial information, etc.).

You will be always asked to provide consent to the public disclosure of your data.

4. What do we use your data for?

The personal data that will be requested from you and the reasons for its request will be clearly stated at the time of the request. Regardless whether your personal data is publicly available or private, it will not be sold, exchanged, or put on disposal to any other company. We use your personal data to carry out our business activities, legal obligations, and requirements. We collect personal data when:

4.1. Creating your account

Creating an account is a mandatory element for receiving a Service from KIBSTrust. The account can be created within the website or mobile application. You manage the account. Closing the account does not mean deleting your personal data from KIBSTrust systems.

4.2. Service order processing

Your data, public or private, will not be sold, exchanged, given, or delivered to another company for a reason that is not in accordance with the defined working process of service delivery without your consent.

4.3. Improving customer service

Your data helps us respond more effectively to your requirements before and after the sale and the requirements of the technical support.

4.4. Sending recovery notifications

The e-mail address you provide for processing the order as contact and / or user ID for opening account can be used to send you notifications for issuance, revocation, renewal of digital certificates, expiration of deadlines and information on the performance of other services in accordance with publicly announced rules and procedures for their issuance, depending on the service or product.

4.5. Sending messages via e-mail

KIBSTrust can send you message for:

- periodic bulletins for the activity, issuance of a new version of service, to inform you about security updates, information related to the services, surveys, as well as notifications on the status of the implemented system maintenance or availability of the services;
- information about the verification of your identity either face-to-face with our authorized employees or remotely and assessment whether you will become a user of our services or products and services of third parties, in accordance with the publicly announced rules and procedures for conducting these activities (CP/ CPS).

5. Obligation to report data change

As our client, you are obliged to inform us upon every change of data that you have previously voluntarily entrusted us with.

6. Lawful basis for processing personal data

We will process your personal data for the purpose of performance of our contract with you or the legitimate interest of KIBSTrust, which are our usual business activities adjusted to Law for electronic documents, electronic identification and trusted services (MK-eIDAS) and its bylaws and EU Regulation 910/2014 known as eIDAS.

In other cases, we will request your consent for the processing of the personal data you may submit.

Your refusal to provide personal data to us for certain Services may hinder us from fulfilling your order for those Services. Also, if you deny or withdraw your consent to use personal data or opt out of receiving information about KIBSTrust's Services this may result in you not being made aware of renewal notices, periodic company newsletters, new service updates, security updates, related product or service information, and status updates on maintenance windows or service availability.

See section 13 below for how to withdraw your consent

7. Sharing personal data

To ensure quality of work, better technical performance, for statistical purposes and marketing while creating services, we create partnerships with other companies (third parties). In such strictly controlled conditions, we can share your personal data and your personal data can be processed based on our legitimate reason for providing products and services to all our users.

Below is a review of the companies' profile and the reason for establishing a partnership. This is not a final review and can be changed according to our needs for constant improvement. We work with analytics indicator providers, financial institutions and we may obtain information about you from them. We may cooperate with Twitter, Google, Facebook, LinkedIn and others to enable you to register for the Services using the credentials you hold with those companies. Below is a non-exhaustive list of third parties we work with. The cooperation can be continuously expanded, or we can stop working.

Third party	**Why we work with them**
EU Trusted Service Provider	For the provision of specific technical and technological services for which KIBSTrust does not invest funds in its infrastructure.
Company for providing personal identity and identification documents verification	A specific service for which KIBSTrust does not invest in its infrastructure.
Various financial companies (banks, funds, insurance companies, etc.)	Placement of our products and services, including enabling us to collect, process and store identity data.
International companies that provide Internet browsing and search services and social networking platforms	Monitoring the performance of our online offer, for statistical processing of data related to the activity of our websites, marketing.

Additionally, we may disclose your personal data to third parties:

- if we are obliged to disclose or share your personal data in order to comply with any legal or regulatory obligation or requirement;
- enforce or apply the terms of use of our services and other agreements or investigate potential breaches; or
- to protect the rights, property or security of our systems or our other users.

8. Keeping data

In order to meet the audit requirements of the TSP and IDP KIBSTrust, the personal data that is filled in or collected during the application will be kept for a minimum of ten (10) years depending on the product or service class and may be retained in hardcopy or electronic form. For all details, please read the rules and procedures published for each KIBSTrust Service, published in the public document repository:

https://www.kibstrust.com

9. Cancelation of e-mail notifications

If you wish to cancel receiving e-mails at any time, you can do so through the cancelation instructions published on the trusted provider's websites and / or included at the end of each e-mail.

10. How do we protect your data?

KIBSTrust undertakes all prescribed technical and organizational measures for the protection of personal data, prevention of unauthorized access and their abuse, seeking to apply the latest achievements in this field.

Our protection procedures are subject to regular controls carried out in accordance with the European standards and requirements of the domestic legislation and are a result of the latest technological achievements.

11. Use of web cookies and web beacons to perform Services

Web cookies are small text files that are stored on your computer to track and / or enhance user's perception of the websites they visit.

In addition, like most online businesses, KIBSTrust uses cookies and web beacons on our websites and through marketing related emails to gather and analyze some personal data such as the visitor's IP address, browser type, ISP, referring page, operating system, date/time and basic geographical information.

We use cookies and web beacons to compile aggregate data about site traffic and site interaction so that we can gauge the effectiveness of our communications and offer better site experiences and tools in the future. We may contract with third-party service providers to assist us in better understanding our site visitors. These service providers are not permitted to use the information collected on our behalf except to help us conduct and improve our business.

First time visitors may choose to not have any activity monitoring cookies set in their browser. We use an opt-out identification cookie to tag these users as having made this decision. Those cookies that pertain to site performance, experience improvement and marketing are programmed not to execute when an opt-out cookie is present in a visitor's browser. Opt-out cookies persist until a visitor clears their browser cookies, or until their expiration one year after the set date. A visitor is required to opt out again after one year to disable any activity monitoring cookies.

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

For more information on using cookies, visit our website:

https://www.kibstrust.com

in a document related to our Cookies Policy. On our websites, as a user, you can give or refuse to give consent to the usage of the type of cookies used.

12. Using records for diagnostic or collecting statistical information

Our servers automatically record information (create records - logs), created by your use of our services. The data in these records may contain information such as your IP address, type of browser, operating system, referent web pages, visited pages, location, your mobile operator, device and application identifiers, browsing terms, and cookies information. We use this information for diagnostics and improvement of our services. We will either delete the data from the records or remove any account identifiers, such as username, full IP address or e-mail address, ten (10) years after your last activity.

13. Opting out and withdrawing consent

If at any time you would like to unsubscribe from receiving future emails, we include unsubscribe instructions at the bottom of each email.

Renewal notices may be cancelled on a per digital certificate basis by logging into your certificate management system account and disabling renewal notices.

Email preferences for CIT related/collected information can be updated and changed within CIT.

If KIBSTrust is processing your personal data based on your consent, you may withdraw your consent at any time via sending message to address soglasnost@kibstrust.com or by contacting us at one of the addresses shown in section 17 below. Your request will be processed in next tree (3) working days.

14. Do we disclose information to third parties?

We do not sell, trade, or otherwise transfer your personal information to third parties. This does not include trusted third parties who assist us in the operation of our website, the completion of applications for digital certificate or any other services that help us optimize or add value to the services we offer, such as offering integrated products or services of third parties. In circumstances where data is shared with such third parties, they are required to comply with the terms of confidentiality. This prevents such third parties from selling, trading, marketing or otherwise distributing information about KIBS users.

We may also make your information available to third parties when we believe that this is in compliance with the law or to protect our rights, property or security.

Our Policy is to inform you that there is a requirement for transfer of your personal data on the basis of law, unless that transfer is prohibited by another law or court order.

15. Registration

Proper registration has been made with a competent body in accordance with the legal obligation regarding the collection, processing and archiving of personal data. For more information about our registration or filling a complaint against us, you can contact:

Personal Data Protection Agency
bul. Goce Delchev no. 18
PO Box 417, 1000 Skopje
https://www.dzlp.mk/mk/kontakt

16. Collecting personal data and your rights

In accordance with the legal regulations in the Republic of North Macedonia, you have established rights and obligations for protection of privacy that KIBSTrust fully respects. In addition, we strive to respect the European Union rules for protection of privacy.

Manner of collecting personal data:

- We always ask for your explicit consent for all personal data you need to submit.
- We do not collect your personal data unless you initiate activity on our websites that requires data collection for the purpose of providing services.
- We use the data you have submitted to identify you, verify data you have submitted, provide you with information in hardcopy or electronic form in order to make our services available to you.

Your rights and obligations

- You are responsible for providing KIBSTrust with true, accurate, current and complete personal information. Also, you are responsible to maintain and promptly update the information to keep it true, accurate, current and complete.
- You can exercise your rights by contacting us in writing. We will require you to provide identification in order to verify the authenticity as the data subject. We will make reasonable efforts to respond to and process your request as required by law.
- To the extent of applicable law, you may have the right to request erasure of your personal information, restriction of processing as it applies to you, object to processing and the right to data portability. You also have the right to lodge a complaint with a supervisory authority.
- If you provide any information that is untrue, inaccurate, not current or incomplete, or if we have reasonable grounds to suspect that such information is untrue, inaccurate, not current or incomplete, we have the right to suspend or terminate your account and refuse any and all current or future Services.

- Right of access and correction - you are entitled to request information what personal data of yours we store and make correction to data that you consider incomplete or inaccurate. You are also entitled to request the data that you consider incomplete or inaccurate be supplemented or updated.
- Right to restrict processing – you are entitled, under certain conditions, to request that we restrict the processing of your data.
- Right to object to processing - you are entitled, under certain conditions, to object to the processing of your personal data and right to submit a complaint to supervisory authority.
- Right to transfer data - you are entitled, under certain conditions, to ask us to transfer the data we have collected about you to another organization or to deliver it to you.
- Right not to be subject to a decision based solely on automatic processing - this right extends to the right not to be profiled on the basis of which legal conclusions related to you can be made unless there is a legal ground for that with adequate provision of your rights, freedoms and personal interests.

17. How we protect your personal data

To prevent unauthorized access to personal information and to prevent and recover from loss of confidentiality, integrity or availability of personal data, we have established internal policies and procedures for safety measures. In order to achieve the above objectives, we have implemented the following measures

1. Establish a policy for the appropriate handling of personal information and personal data in accordance with laws, regulations, and guidelines.
2. Establishment of policies that stipulate rules around acquisition, use, storage, provision, deletion, and disposal of Personal Data, as well as the responsible persons and their roles
3. Organisational security control measures, such as the establishment of a responsible person, clarification of the employees who process personal data and the scope of personal data processing, implementation of a reporting and communication system to the responsible person in the event that a fact or indication of a violation of the law and/or policies are detected, and periodic inspections regarding the Personal Data processing status is in line with policies and procedures.
4. Personal security measures, such as stating matters concerning confidentiality of personal data in employee handbook, and conducting periodic training on personal data processing related rules and policies
5. Physical security measures, such as physical access control for employees, restrictions on equipment brought into the office, and restrictions and controls on the removal of equipment and electronic media and documents that process or contains Personal Data to prevent them from being stolen or lost, etc.
6. Technical security control measures, such as the introduction of systems to protect information systems that handle personal data from unauthorized external access or unauthorized software
7. Implementation of security control measures based on an understanding of the systems for the protection of personal information in the countries where personal data is processed
8. Appointment of a Data Protection Officer who oversees all data handling processes and activities

18. Protecting the privacy of minors

KIBSTrust Services are not designed for, not marketed to, minors. We do not knowingly collect or solicit personal data from minors, and we do not knowingly allow such persons to use the Services.
If you are a minor, please do not attempt to use the Services or send any information about yourself to us. In the event that we learn that we have collected personal data from a minor we will delete that information as quickly as possible.
If you believe we have any information from or about a minor, please contact us using the contact information in part 19 below.

19. Amendments to the Privacy Policy

If amendments are made to this Policy, users of our services will be notified by publication on our websites and/or by sending an e-mail notifying of a new version availability.

With the publication of the new version of this document, its previous version ceases to be valid. The previous version will remain available for your reminder at https://www.kibstrust.com/mk-MK/Home/Dokumenti.

20. Statement

KIBSTrust is committed to ensuring an effective, scalable, and reliable personal data protection system that is capable to rendering efficient and decisive actions in the event of a breach or compromise but also to deliver a strong and robust privacy framework.

KIBSTrust fully fulfills its responsibilities as a controller of the personal data of its users and interested third parties. It manages the collection, transmission and storage of such information not only in a lawful and ethical manner, but also in a way that is expected of someone registered by the regulator in the Register of Trusted services providers and for electronic identification schemes.

KIBSTrust is also committed to adhere to legislative, regulatory, and contractual requirements and managing the associated risk present in this Services.

The policy is dynamic in nature and includes a commitment to continual improvement through a process of incident reporting, risk assessment and regular audits. This policy is reviewed at least annually or if any major changes occur.

21. Contact and other information

If you want to contact us, complain, or get information of what we store for you, we offer you the following options:

- Send us a letter to the address: Blvd. Kuzman Josifovski Pitu 1, 1000 Skopje.
- Call the phone number: +389 2 3297 401
- Send an e-mail to: ozlp@kibstrust.com.

We will respond to any request related to the protection of personal data within a legal deadline.

These Policy is prepared in Macedonian and English version. In case of any discrepancies between these versions, the Macedonian version shall prevail.

END OF DOCUMENT