Privacy Policy

BIO-key International Privacy Policy

BIO-key understands that you care about how information about you is used. This privacy policy explains how we collect information pertaining to businesses and business people ("Business Information") and all other types of information through our website and online services (the "Site"); how we collect, maintain, and use that information; and how you can manage the way information about you is handled. For individuals residing in the EEA or Switzerland, please scroll down to the "Information for Users in Europe and Elsewhere Outside the U.S." section for more information.

BIO-key Website Privacy Policy

BIO-key MobileAuth App User Data Privacy Policy

BIO-key Accessibility Conformance Report

I. BIO-key Website Privacy Policy

What information does BIO-key gather? For online "form submissions," we collect the following Business Information, if available, for each person:

- Name
- Email address
- Job title and department
- Business phone numbers (general, direct, and fax)
- Company name
- Postal address of company
- Business-related postal address of the person
- Corporate website URLs
- The date the form was sent or received
- Email addresses, names, and job titles of recipients and senders

To ensure the integrity of the database, we take the following steps:

- **Business Information Only** – BIO-key only wants business-related information, such as company name, employee name, job title and department, email address, business phone numbers, company address, etc.

- **Anonymity** – All individuals who visit our Site's personal information will remain anonymous unless they willingly provide us with their information via a "form fill out," submit any inquiry on our site's "Contact Us" page, or make other contribution methods. (The only exceptions are as follows: See "Disclosures to Service Providers," "Disclosures for Legal Reasons," and "Disclosures to a Buyer of the Company" below.)
- **Opt-Out** – Anyone added to the database may request to be removed at any time via email, web, or a toll-free number. We promptly honor such requests.

How else does BIO-key Collect and Use Information? Visitors to our Site may choose to submit their name, email address, and other information to learn more about our services, register to participate in an online demo, attend a webinar, purchase a product, or contact our Support Team. To use certain BIO-key products and services, you may be required to register as a user. From time to time, we may use your email address to send you information and keep you informed of products and services in which you might be interested. You will always be allowed to opt out of receiving such emails. Your contact information may also be used to reach you regarding issues concerning your use of our Site, including changes to this privacy policy. BIO-key may aggregate collected information about our users in a form that does not allow users to be personally identified to understand our customer base and enhance the services we and our strategic partners and customers can provide you. We will use that information solely to fulfill your purchase request. We will store credit card information in an encrypted form and will not sell, share, or use it again without your prior consent. (The only exceptions are described in the sections below on "Disclosures to Service Providers," "Disclosures for Legal Reasons," and "Disclosures to a Buyer of the Company"). BIO-key will use personal information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual to whom the information pertains. BIO-key will take reasonable steps to ensure that personal data is relevant to its intended use, accurate, complete, and current. We also collect information using cookies, as described below.

Cookies: Most websites, including our Site, use a feature of your browser to set a small text file called a "cookie" on your computer. The site placing the cookie on your computer can then recognize the computer when you revisit the website to allow auto log-in and track how you use the site. When you visit our Site, our servers and/or those of our service providers automatically record certain information that your web browser sends, such as your web request, Internet Protocol address, browser type, referring/exit pages and URLs, number of clicks, domain names, landing pages, pages viewed, time and date of use and other information. The information we collect using cookies does not allow you to be personally

identified, but we may link this information to information that you submit while on our Site, which allows you to be personally identified. You are free to decline cookies. You can configure your browser to accept all cookies, reject all cookies, erase cookies, or notify you when a cookie is set. BIO-key may adopt other technologies that serve similar functions as cookies. If we do so, we will disclose it in this privacy policy.

Third-Party Cookies: The use of cookies by our partners, affiliates, tracking utility companies, and service providers is not covered by our privacy policy. We do not have access or control over these cookies. Our partners, affiliates, tracking utility companies and service providers may use session ID cookies to:

- personalize your experience
- analyze which pages our visitors visit
- provide website features such as social sharing widgets
- measure advertising effectiveness
- track which areas of our site you visit to remarket to you after you leave

Google Analytics: We use Google Analytics, a web analytics service provided by Google, Inc., on our Site. Google Analytics uses cookies or other tracking technologies to help us analyze how users interact with and use the Site, compile reports on the Site's activity, and provide other services related to Site activity and usage. The technologies used by Google may collect information such as your IP address, time of visit, whether you are a return visitor, and any referring website. The Site does not use Google Analytics to gather information that personally identifies you. The information generated by Google Analytics will be transmitted to and stored by Google and will be subject to Google's privacy policies. Learn more about Google's partner services and how to opt out of tracking analytics by Google.

Do Not Track Signals: Your browser or device may include 'Do Not Track' functionality. Our information collection and disclosure practices, and the choices that we provide to visitors, will continue to operate as described in this privacy policy, whether a Do Not Track signal is received.

Web Beacons: Our Web pages contain electronic images known as Web beacons (sometimes called single-pixel gifs). These images are used along with cookies to compile aggregated statistics to analyze how our site is used. They may also be used in some of our emails to let us know which emails and links have been opened by recipients. This allows us to gauge the effectiveness of our customer communications and marketing campaigns.

When does BIO-key Share Information? BIO-key may, from time to time, disclose Business Information or other collected information to service providers, solely for providing functions related to our operation of the Site and for no other purpose. For example:

- BIO-key uses service providers to process credit card payments. When you use a credit card to pay for BIO-key's products, information such as your name, billing address, phone number, email address, and credit card Information will be submitted to service providers for verification and to manage any recurring payments.
- BIO-key uses software hosted by a service provider to provide us with information regarding our visitors' activities on our Site. When you visit our Site, that service provider may set cookies on our behalf and may receive information about your browsing activity on our Site.

Disclosures for Legal Reasons: We may disclose collected information, including Business Information, to a third party if we believe in good faith that such disclosure is necessary or desirable: (i) to comply with lawful requests, subpoenas, search warrants or orders by public authorities, including to meet national security or law enforcement requirements, (ii) to address a violation of the law, (iii) to protect the rights, property or safety of BIO-key, its users or the public, or (iv) to allow BIO-key to exercise its legal rights or respond to a legal claim.

Disclosures to a Buyer of the Company: If our company or substantially all of our assets are acquired, or in the event of a merger or bankruptcy, information about you and/or information you provide to BIO-key may be among the transferred assets. You will be notified via email and/or a prominent notice on our Site of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information.

Other Disclosures: If you provide information, including Business Information, in creating or updating your Profile, that information will be included in the database and thus can be viewed by third parties. We post customer testimonials on our Site, which may contain the customer's name. We always¬ get consent from the customer before posting any testimonial. If you wish to update or delete your testimonial, you can contact us at support@bio-key.com with a request marked "Privacy-Urgent." Our Site offers publicly accessible blogs and product reviews. You should be aware that any content you provide in these areas may be read, collected, and used by others who access them. You can request the removal of your personal information from our blog or review section by contacting us at support@bio-key.com with a request marked "Privacy-Urgent." In some cases, we may not

be able to remove your personal information, in which case we will let you know if we cannot do so and why.

Protection of Children: This Site is not intended for users under the age of 13, and we have no intention of collecting personally identifiable information from children (i.e., individuals under the age of 13). Suppose a parent or guardian learns that a child has provided us with personally identifiable information. In that case, the child's parent or guardian should contact us and send a request marked "Privacy-Urgent" to support@bio-key.com if they would like the information submitted by the child deleted from our database. We will use all reasonable efforts to delete such information from our database. BIO-key may have liability to you in case of failure to comply with the law or this policy in handling the onward transfer of your Information to third parties.

How Can You Change or Delete Your Information? To find out if you are in the BIO-key Database, please email support@bio-key.com with a request marked "Privacy-Urgent." If you have a common name, you can help us refine your search by providing information based on geographical location or companies where you have worked. The information provided in such a request will not be stored in our database. Once we have located one or more BIO-key profiles in your name, consider these options for managing your professional profile in BIO-key's database:

Update Your Own Professional Profile Information: Make sure your profile is up to date for our marketing and sales team members who may want to reach you. Verify your profile, and you can request to update your work history, contact information, and even delete web references you do not want to be associated with your professional profile. You can also consolidate multiple profiles in your name to create a comprehensive snapshot of your professional background.

Remove Your BIO-key Profile Completely: If you wish to remove your existing individual profile from the Database completely, please email support@bio-key.com with a request marked "Privacy-Urgent." If you make this choice, your name, employment history, web references, and contact information (including email address) will be removed as soon as possible.

Company Profiles: To find out if your company is in the BIO-key Database, please email support@bio-key.com with a request marked "Privacy-Urgent." Once we have located the profile, consider these options for managing your company profile on BIO-key:

Update Your Company Profile: Verify your BIO-key company profile to update your company description, industry, company location, and more. You can also consolidate multiple patterns to create a comprehensive snapshot of your company. Please email support@bio-key.com with a request marked "Privacy-Urgent" to verify and update your company profile.

Remove Your Company BIO-key Profile Completely: We gather all information about companies from corporate websites, press releases, and SEC documents filed with the US government. The company summaries are created by marketing automation software based on the information we find in those documents. As a company policy, BIO-key does not remove company information from our database. If you feel any company information is incorrect or would like to verify, please email support@bio-key.com with a request marked "Privacy-Urgent."

Data Retention: We will retain your information for as long as your account is active or as needed to provide you with services. We will also keep and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

How Can You Opt Out of Certain Uses of Your Information? BIO-key allows you to "opt out" of having your information used for specific purposes. If you no longer wish to receive our newsletter and promotional communications, you may opt-out of receiving them by following the instructions included in each newsletter or communication or by clicking "unsubscribe" at the bottom of the email transmission. After receiving your request, we will email you to confirm that you have been unsubscribed. BIO-key will not share information about you that you submit when you register for our services with third parties for promotional uses unless you opt into such sharing within your BIO-key account or BIO-key has separately acquired such information from other sources, in which case BIO-key will allow you to opt out via email. If you have registered, submitted a form, or inferred permission for BIO-key to contact you and opted in to share your personal information, you may opt-out by emailing support@bio-key.com with a request marked "Privacy-Urgent." If you have subscribed to BIO-key's email communications, such as newsletters, industry-relevant information, promotional sales material, etc., and opted in to share your business information with BIO-key in exchange for continued email communications, you may opt out of any further sharing of business information, by emailing support@bio-key.com with a request marked "Privacy-Urgent" and BIO-key will no longer collect Business Information from you through this method (however, you will not be able to 'unshare' the Business Information you have previously provided to BIO-key). When BIO-key adds a profile to its

Directory that includes an email address, it sends a message to that email address, offering an opportunity to opt out of inclusion in the Directory.

How Do We Keep Your Information Secure? The security of your information is important to us. We follow generally accepted industry standards to protect the information submitted to us, both during transmission and after receiving it. However, no Internet transmission or electronic storage method is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your information, we cannot guarantee its absolute security. You may also communicate your opt-out request to BIO-key by telephone or postal mail using the contact information at the bottom of this privacy policy.

Links to Other Sites: This Site contains links to other sites not owned or controlled by BIO-key. We are not responsible for the privacy practices of such other sites. We encourage when you leave our Site to be aware and to read the privacy statements of every website that collects personally identifiable information. This privacy policy applies only to information collected by this Site or in the method(s) otherwise discussed herein.

Social Media Widgets: Our Web site includes Social Media Features, such as the Facebook Like button and Widgets, such as the Share this button or interactive mini-programs that run on our website. These Features may collect your IP address, which page you are visiting on our site, and may set a cookie to enable the Feature to function properly. Social Media Features and Widgets are either hosted by a third party or hosted directly on our Site. Your interactions with these Features are governed by the privacy policy of the company providing it.

Information for Users in Europe and Elsewhere Outside the U.S.: If you use our Site outside of the United States, you understand that we may collect, process, and store your personal information in the United States and other countries. The laws in the U.S. regarding personal information may be different from the laws of your state or country. Any such transfers will comply with safeguards as required by relevant law.

Users in the European Union (EEA) and Switzerland*: If you are a resident of the EEA or Switzerland, the following information applies*. Purposes of processing and legal basis for processing: As explained above, we process personal data in various ways depending upon your use of our Sites. We process personal data on the following legal bases: (1) with your consent; (2) as necessary to perform our agreement to provide Services; and (3) as necessary for our legitimate interests in providing the Sites where those interests do not override your fundamental rights and freedom related to data privacy. BIO-key's collection of Business Information and the creation are within BIO-key's legitimate interest to organize

business contact information given the limited impact of this data on an individual's private life. BIO-key has put in place safeguards to protect personal privacy and individual choice, including disclosures of its data processing activities, the use of consent or opt-outs wherever possible.

Right to lodge a complaint: Users that reside in the EEA or Switzerland have the right to lodge a complaint about our data collection and processing actions with the supervisory authority concerned. Contact details for data protection authorities are available here.

Transfers: Personal information we collect may be transferred to, and stored and processed in, the United States or any other country in which we or our affiliates or subcontractors maintain facilities. Upon the start of enforcement of the General Data Protection Regulation (GDPR), we will ensure that transfers of personal information to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR. Please see "Privacy Shield Frameworks" below regarding our compliance with the EU- and Swiss-US Privacy Shields.

Individual Rights: If you are a resident of the EEA or Switzerland, you are entitled to the following rights once the GDPR becomes effective.

Please note: To verify your identity, we may require you to provide us with personal information prior to accessing any records containing information about you.

- The right to access and correction. You have the right to request access to and a copy of your personal data at no charge, as well as certain information about our processing activities with respect to your data. You have the right to request correction or completion of your personal data if it is inaccurate or incomplete. You have the right to restrict our processing if you contest the accuracy of the data we hold about you, for as long as it takes to verify its accuracy.
- The right to request data erasure. You have the right to have your data erased from our Site if the data is no longer necessary for the purpose for which it was collected, you withdraw consent and no other legal basis for processing exists, or you believe your fundamental rights to data privacy and protection outweigh our legitimate interest in continuing the processing.
- The right to object to our processing. You have the right to object to our processing if we are processing your data based on legitimate interests or the performance of a task in the public interest as an exercise of official authority (including profiling); using your data for direct marketing (including profiling); or processing your data for purposes of scientific or historical research and statistics.

Privacy Shield Frameworks: BIO-key complies with the EU-US Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. BIO-key has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, any rights you may have to binding arbitration before a Privacy Shield Panel and to view our certification page, please visit https://www.privacyshield.gov. For information received under the Privacy Shield, BIO-key will require third parties to whom BIO-key discloses personal information to safeguard that personal information consistent with this Policy by contract, obligating those third parties to provide at least the same level of protection as is required by the Privacy Shield Principles. EU citizens may choose to opt-out of such disclosures. In compliance with the EU-US Privacy Shield Principles, BIO-key commits to resolve complaints about your privacy and our collection or use of your personal information. European Union individuals with inquiries or complaints regarding this privacy policy should first contact BIO-key at support@bio-key.com with a request marked "Privacy-Urgent." *The Federal Trade Commission has enforcement authority regarding BIO-key's compliance with the Privacy Shield Principles*.

Your California Privacy Rights: If you are a California resident, California law permits you to request certain information regarding the disclosure of your personal information by us to third parties for the third parties' direct marketing purposes. To make such a request, please send your request, by mail or email marked "Privacy-Urgent", to the address at the end of this policy.

Changes to this Policy: BIO-key reserves the right to modify this privacy policy from time to time, so please review it regularly. If we make material changes to this policy, we will notify you here, by email, and/or by means of a notice on our homepage prior to the changes becoming effective.

Effective Date: This privacy policy was last updated on **October 24th, 2024**.

II. BIO-key MobileAuth App User Data Privacy Policy

BIO-key understands the importance of, and is committed to, protecting and securing the personal data we and our customers process. This User Data Privacy policy sets out how BIO-key protects personal data in relation to the service we provide on our own or on behalf of our customers through the trial and production operation of our MobileAuth app and

server platform (the "**Service**"). With this Service, our customers can provide the following services to you:

- Strong, Passwordless Authentication without a token to carry
- Out-of-Band Authentication to confirm access to systems you use to get things done;
- Biometric Identity-Based Authentication;
- Biometric capture and comparison including liveness checking to protect against fraud and impersonation.

The Service is designed and maintained to improve identity assurance and convenience of authentication through accurate and high-integrity biometric identity confirmation of our customers' end-users. You have a right to a secure identity and authentication that resists phishing and does not impose burdens on you to remember passwords or carry tokens.

How We and Relying Parties Obtain Your Consent to Process Your Data

This MobileAuth app is designed to allow you to biometrically enroll and authenticate yourself with online services (**"Customers"** or "**Relying Parties**") of your choosing who have chosen to use the MobileAuth app to secure your online identity. In most real-world cases, a Relying Party will operate and be responsible for a BIO-key server that implements their own instance of the Service ("**Service Instance**") to perform enrollment and matching of users for their own authentication purposes. In these scenarios, BIO-key neither receives nor retains any data about your use of any Relying Party's Service Instance.

We require Relying Parties to first obtain your informed written consent before collecting your biometric data for enrollment or authentication purposes through the MobileAuth application. Relying Parties will provide and maintain their own privacy policy relating to Service Instances they operate, and any of your data they collect through their use of your installed MobileAuth app. In accordance with applicable privacy laws, they must provide you with information about their planned use of your biometric data, their retention policy, and how to contact them for exercising your rights as a data subject depending on your jurisdiction.

The MobileAuth app is designed to require your consent to the collection and processing of biometric data the first time you connect to any new Relying Party Service Instance not previously authorized by you, and if more than one Relying Party Service has been authorized by you, it will retain in the app on your device a list of Service Instances previously authorized, including copies of the Relying Party's privacy policy and consent terms that you agreed to

for each Relying Party's Service Instance. This information is for your use only, to manage the Relying Party consent agreements you have digitally signed.

Data MobileAuth Collects

The MobileAuth app is only activated by a Service Instance that your Relying Party operates, typically as part of a workflow for user enrollment or authentication on their web site or application, through an instance of BIO-key's software, such as PortalGuard. When enrolling, the Relying Party's web site will display a 2-D bar code, and will instruct you to activate the BIO-key MobileAuth app. When the mobile auth app is activated, it will allow you to press a button to "Register", which activates your device's camera to scan the 2-D bar code from the web site, which uniquely identifies its Service Instance. No camera data except for the decoded contents of the 2-D bar code are obtained from the camera during registration. If the Service Instance is new to your MobileAuth instance, then the Relying Party's informed consent and privacy policy information will be displayed for you to read and agree to before proceeding. If you do not agree, the MobileAuth application will exit, and no data is transmitted from the app about the interaction with the Service Instance, except that you declined consent.

Palm Biometric Capture with Consent

If you give your consent, then your MobileAuth app's unique push notification identifier is sent to the Service Instance, allowing that Service Instance to issue future push notifications for authentication. The app will then allow you to activate the camera on your mobile device, and it will guide you through the capture of an image of your palm, which may be checked for liveness within the MobileAuth app, depending on the requirements of the Service Instance. If determined to be a live capture and not a facsimile, an algorithm within the MobileAuth app will convert the palm image into a set of unique landmarks ("**BIO-key Template**") that distinguish your palm from that of imposters and other users. These landmarks are then securely transported to the consented Service Instance, and there is stored as part of an encrypted enrollment to secure your user identity. No other data is transmitted by the app to the service instance, and no data is retained by BIO-key about the transaction.

Facial Biometric Capture with Consent

If you give your consent, then your MobileAuth app's unique push notification identifier is sent to the Service Instance, allowing that Service Instance to issue future push notifications for authentication. The app will allow you to activate the camera on your mobile device, and

it will guide you through the capture of an image of your face, which may be checked for liveness within the MobileAuth app or by our server, depending on the requirements of the Service Instance. An algorithm within the MobileAuth app will convert the face image into a set of unique landmarks ("**BIO-key Template**") that distinguish your face from that of imposters and other users. These landmarks and the captured image are then securely transported to the consented Service Instance, and there is stored as part of an encrypted enrollment to secure your user identity. No other data is transmitted by the app to the service instance, and no data is retained by BIO-key about the transaction.

BIO-key Will Never Misuse or Sell Your Data

BIO-KEY does not use personal data for any purpose other than the purpose described above, including for marketing or research purposes. BIO-key will never sell any personal data it collects through the Service. To reiterate, BIO-key's direct receipt of data will only be in the context of demonstrations and trials by Customers using BIO-key's servers or as a subcontractor to a Customer using BIO-key's IDaaS service. Otherwise, any Relying Party operating in production will have their own Service Instance and will be responsible for their privacy policy, presented to you for consent before this app will collect and transmit any of your personal information.

BIO-key IDaaS and Its Subcontractor Role to Relying Party

Where a Relying Party utilizes BIO-key's Identity-as-a-Service ("IDaaS"), they will remain responsible for presenting and obtaining consent to their own User Data Privacy Policy, although BIO-key may be hosting their Service Instance for them as a subcontractor data processor. BIO-key will be identified as a data processing subcontractor in their privacy policy, including contact information for data subject rights requests under EU GDPR and US state and federal statutes as applicable.

1. BIO-KEY's Service provides advanced services to identify and validate a user's identity:
    a. Identity Proofing

        At enrollment, a Service Instance may utilize a third-party Identity proofing service to ensure that all the identity claim evidence submitted by you are analyzed and to determine the level of assurance of your identity. The various checks performed include an external system of record (**"SoR"**) to compare the claimed identity with reference identity from a trusted source, such as

your driver's license registry, for identity document verification, and facial recognition match against those verified identity documents.

b. Document capture and Authentication

The document capture and authentication service assess the genuineness of a state (government) identity document such as a Driver's License, Identity card, Resident card, or Passport. The service captures and analyses front and back images and videos of the end user document identity to detect security features and any tampering on portrait or identity information, as well as detects screen captures and photocopies.

c. Biometric capture and comparison, including Liveness
The biometric capture and comparison services ensure that the end user conducting the proofing journey is the same person as claimed on the identity attributes. The service assesses the end user liveness during a capture video session and then compares the acquired (live) portrait with either the portrait on a validated ID document or with a system of record (SoR).

2. In order to provide the Service, BIO-KEY needs to collect personal data related to its Customers' users. This personal data is not collected directly by BIO-KEY, but by BIO-KEY's Customers. The latter shall ensure they have a proper legal basis to collect personal data, such as consent, as appropriate. Customers shall also provide their users with all necessary information with regard to the processing of his / her personal data.
3. Personal data that BIO-KEY may process:
    a. Biometric capture and comparison, including liveness
    End user live portrait of your palm or face, with prior consent. Device information (model, type, OS, browser version), IP address and network routing information, GPS authentication location.
    b. Identity Proofing
    Identity attributes available on the ID document such as names; Date of birth/place of birth; address; nationality; Identity documents Images (Front/Back of submitted IDs) End user live portrait, Device information (model, type, OS, browser version)

    c. Document Capture and Authentication
    Identity documents Images (Front/Back of submitted IDs, all identity information extracted from the document images such as VIZ, MRZ or

barcode) Device information (model, type, OS, browser version) Identity document details (Document Number, Issue date, Expiry date, Issuing country, Jurisdiction) Identity attributes available on the ID document

4. Data retention:

If you have provided consent for ongoing biometric authentication to BIO-key or a Relying Party, a Service Instance may retain your biometric data in encrypted BIO-key Template form until you request it to be deleted, or as required by state or federal law as to deletion of biometric data provided with consent. If you assert that a particular jurisdiction's biometric laws apply to you other than the laws of the State of New Jersey or Minnesota, where BIO-key operates, you must notify BIO-key at the Data Privacy contact below, providing the basis for your residency claim and sufficient information to accurately locate your biometric record, such as the Relying Party identity (if BIO-key is a processing subcontractor). BIO-KEY will delete your submitted Identity Proofing evidence (images, videos, attributes) after the processing is completed, in order to be able to support the Service. All personal data are stored encrypted and can only be accessed by limited and authorized BIO-KEY personnel.

5. Users of the Service:

The users of the Service are employees and customers of BIO-KEY's Customers. Users only interact with and process their own personal data, and the Service will only process data relating to the user being authenticated, in order to authenticate them.

6. Data sharing

BIO-KEY only shares personal data with Affiliates of BIO-KEY as required to perform the service functions, and with their performance subject to the terms of this Privacy Policy. BIO-KEY and BIO-KEY's Affiliates, respectively, may engage third-party sub-processors in connection with the provision of the Service. BIO-KEY's Affiliates and third-party sub-processors may be in countries other than your country. Your personal data, therefore, may be subject to privacy laws that are different from those applicable in your country.

Personal data collected within the European Economic Area (EEA) may thus be transferred to or accessed from a third party located outside the EEA. In such an event, BIO-KEY ensures that the transfer of your personal data is carried out in accordance with applicable privacy law and has put into place appropriate legal instruments such as EU Standard Contractual Clauses.

7. Security measures

BIO-KEY takes the security, integrity, and confidentiality of personal data very seriously. BIO-KEY takes all reasonable steps to protect your personal data using technical, organizational, and security measures to reduce the risks from misuse, interference and loss; and from unauthorized access, modification or disclosure.

8. Your rights

Should you want to get more information on how we handle your personal data, or should you like to have access to your data or have your data rectified or deleted, or withdraw your consent for data we retain, you can contact us at dpo@BIO-key.com or

BIO-key Data Protection Officer (DPO)
101 Crawfords Corner Road, Suite 4116
Holmdel, NJ 07733
USA

If BIO-key does not retain your data, we may notify our Customer of your request, if we have reason to believe they hold your data, and you have sufficiently identified them in your communication.

If you are dissatisfied with how we handle your personal data, you can send us a complaint, and we will make good-faith attempts to resolve the dispute.

9. Privacy Policy updates:

This Privacy Policy may be updated from time to time. Upon update of this Privacy Policy, you will be notified by the MobileAuth app or by email when you next connect to the Service with your account.

BIO-key works with the subcontractors listed below:

For Customers located in the USA:

Name of the subcontractor	**Processing performed by the subcontractor**	**Place of data processing**	**Subcontractor used for the following product**	**Customer Country**
RedRock Biometrics	Palm-based Authentication	USA	MobileAuth Authentication demonstration	USA

AWS Cloud Services	Hosting services for BIO-key IDaaS service	USA	MobileAuth Authentication; Biometric capture	USA

For Customers located in Europe:

Name of the subcontractor	**Processing performed by the subcontractor**	**Place of data processing (Proofing Regions)**	**Subcontractor used for the following product**	**Customer Country**
RedRock Biometrics	Palm-based Authentication	USA	MobileAuth Authentication demonstration	USA
AWS Cloud Services	Hosting services for BIO-key IDaaS service	USA	MobileAuth Authentication; Biometric capture	USA

For Customers located in APAC:

Name of the subcontractor	**Processing performed by the subcontractor**	**Place of data processing (Proofing Regions)**	**Subcontractor used for the following product**	**Customer Country**
RedRock Biometrics	Palm-based Authentication	USA	MobileAuth Authentication demonstration	USA
AWS Cloud Services	Hosting services for BIO-key IDaaS service	USA	MobileAuth Authentication; Biometric capture	USA

Contact Us

If you have questions or concerns regarding this privacy policy, please contact us at:

BIO-key International
101 Crawfords Corner Rd
Suite 4116
Holmdel, NJ 07733
Phone: (866) 846-2594
Fax: (732) 359-1101
Email: support@bio-key.com