



Privacy Policy



Table of Contents

- 1. INTRODUCTION 4
 - 1.1. Our Role in Your Biometric Data Privacy 4
 - 1.2. Welcome and Overview 4
 - 1.2.1. Who Manages Your Data? 4
 - 1.2.2. Our Role 4
 - 1.2.3. Understanding Your Data 4
- 2. DEFINITIONS 4
 - 2.1. Key Terms and Their Meanings 4
- 3. MAIN PRIVACY PRINCIPLES 6
 - 3.1. Data Security Measures 6
 - 3.2. Privacy-First Design 7
 - 3.3. Lawful and Clear Data Processing 7
 - 3.4. Data Ownership and Transparency 7
 - 3.5. Data Retention Policies 7
 - 3.6. Data Accuracy and Necessity 8
- 4. DATA COLLECTION AND PROCESSING 8
 - 4.1. Enrollment Process 8
 - 4.2. Facial Authentication Technology 8
 - 4.3. Step-by-Step Data Collection Process 8
 - 4.3.1. Image Capture: 8
 - 4.3.2. Facial Feature Extraction: 8
 - 4.3.3. Biometric Matching: 9
 - 4.3.4. Identity Verification: 9
 - 4.4. Technologies Used in Facial Authentication 9
 - 4.4.1. High-Resolution Cameras 9
 - 4.4.2. Facial Recognition Algorithms 10
 - 4.4.3. Secure Databases 10
 - 4.4.4. AI Tools: Computer Vision and Machine Learning: 10
- 5. TYPES OF DATA WE COLLECT 10
 - 5.1. Biometric Data 10
 - 5.2. Identity Verification Data 10
 - 5.3. Technical and Machine-Readable Data 10
- 6. HOW AND WHY WE USE YOUR DATA 11
 - 6.1. Purpose of Data Processing 11
 - 6.2. Legal Basis for Processing 11
- 7. DATA ACCESS AND SHARING 12
 - 7.1. Access by System Owners 12
 - 7.2. Sharing with Third Parties 12
 - 7.3. Disclosure to Authorities 12
 - 7.3.1. Disclosure to Data Controllers, Data Processors, and Authorized Recipients: 12
 - 7.3.2. Legal Basis for Sharing 12
 - 7.4. Data Transfer Outside the EEA 12
- 8. RIGHTS TO BIOMETRIC DATA 13
 - 8.1. Rights Depending on Location 13
 - 8.1.1. The Right to Know 13
 - 8.1.2. The Right to Access & Portability 14



8.1.3. The Right to Correction	14
8.1.4. The Right to Deletion	14
8.1.5. The Right to Non-discrimination.	15
8.1.6. The Right to Withdraw the Consent	15
8.1.7. The Right to Object	15
8.1.8. The Right to Restriction of Processing	15
8.1.9. The Right to Submit a Complaint and Make Appeals	15
8.1.10. Authorized Agents	15
8.2. Exercising Your Rights	16
8.3. Contacting Us	16
9. DATA SECURITY MEASURES	16
9.1. Physical, Technical, and Organizational Measures	16
9.2. Reporting Data Breaches.	16
10. DATA RETENTION POLICIES	16
10.1. Retention Period Determined by System Owners.	16
10.2. Extended Storage and Permanent Erasure.	17
11. TECHNOLOGICAL ASPECTS OF OUR SERVICE PROVISION.	17
11.1. Use of Algorithm and Machine Learning:	17
11.2. Automated Authentication	17
11.3. Ethical Machine Learning Practices:.	17
12. CHILDREN'S BIOMETRIC DATA	18
12.1. Handling of Children's Data	18
12.2. Guardian Consent	18
13. LEGAL GROUNDS FOR PROCESSING FOR A NEW PURPOSE	18
13.1. Conditions under GDPR.	18
13.2. New Purposes for Data Processing	18
13.2.1. Context of Data Collection:	18
13.2.2. Nature of the Biometric Data:	18
13.2.3. Consequences for You:	18
13.2.4. Protection Measures:	18
14. JURISDICTION-SPECIFIC NOTICES	19
14.1. California.	19
14.1.1. Notice of Collection and Additional Information for Residents of California	19
14.1.2. Additional Disclosures	19
14.1.3. Purposes for Collection	19
14.1.4. Use of Sensitive Personal Information.	19
14.1.5. Your Privacy Rights:	19
14.1.6. More Information.	19
14.2. Colorado, Illinois, Washington, and Texas	20
14.2.1. Illinois and Texas Regulations.	20
14.2.2. Colorado Regulations.	20
14.2.3. Washington Regulations	20
14.2.4. General Provisions	20
15. CONTINUOUS PRIVACY IMPROVEMENT	20
15.1. Commitment to Ongoing Privacy Enhancements	20
16. CONTACT DETAILS AND INFORMATION	20
16.1. Contacting Alcatraz AI's Data Protection Officer	20
16.2. Availability of and Changes to the System Privacy Notice	21

At Alcatraz AI Inc., we specialize in advanced biometric authentication systems, ensuring robust security and protecting your biometric privacy.

1. INTRODUCTION

1.1. Our Role in Your Biometric Data Privacy

Welcome! This Privacy Policy explains how we protect and respect your Biometric Data privacy. If you’re reading this, it’s likely because your employer, school, bank, airport, or another organization is using Alcatraz AI’s system (we call them System Owners).

1.2. Welcome and Overview

1.2.1. Who Manages Your Data?

Your System Owner manages the data entered into our system, including Biometric Data (like facial features) and Personally Identifiable Information (PII) such as email addresses or badge numbers.

1.2.2. Our Role

We are the Data Processors. This means we handle, process, and protect your data on behalf of the System Owners. We make sure your data is kept secure and complies with all relevant privacy laws and standards.

1.2.3. Understanding Your Data

To fully understand how your data is collected, processed, and protected, please read this Privacy Policy along with your System Owner’s privacy notice (for example, your employer’s privacy notice).

If you have any questions or need more details, please contact your System Owner or us directly at privacy@alcatraz.ai. Your privacy and security are important to us, and we are committed to safeguarding your data. Thank you for trusting Alcatraz.

If you’re looking for a job at Alcatraz or visiting our website, please review the privacy policy on our home page. This isn’t the privacy policy you are looking for. If you’re looking for our Data Protection Officer, you can contact her at privacy@alcatraz.ai.

2. DEFINITIONS

2.1. Key Terms and Their Meanings

Term	Meaning
Alcatraz, Alcatraz AI, our, us, we	Alcatraz AI, Inc., a Delaware corporation headquartered in Cupertino, California.
Alcatraz AI Rock System	Our all-in-one device that combines facial biometrics, AI, and Machine Learning for greater security, less friction, and improved compliance with Data Laws that is hosted either On-Prem or in the Cloud.

Access Control System (ACS)	A security system that controls who can enter certain areas in a building, data center, rooms, or campus using methods like keycards, Biometric Data, or PIN codes.
Access Point	A specific location, like a door or turnstile, where users undergo facial authentication to enter a secure area. These points use our Rock hardware and Alcatraz Admin Portal software for identity verification.
Authentication	The process of confirming a person's identity. This can be done using something you know (like a PIN code), something you have (like a key fob or badge), and something you are (like a biometric feature such as facial recognition).
Biometric Data	Unique physical characteristics, such as facial features, that are used by our system to verify your identity.
Cloud	The Alcatraz AI system architecture when it is hosted and managed in the cloud by Alcatraz AI through a subscription-based service.
Customer Agreement	The contract between Alcatraz or our Channel Partners and the System Owners (our customers).
Data Controller	The System Owner (like your employer) who decides how and why your personal and Biometric Data is processed. They ensure compliance with data protection laws and instruct Alcatraz on how to handle the data.
Data Laws	Rules and regulations about data privacy and security that apply worldwide, including laws like GDPR in Europe, BIPA in Illinois, and others in the US and Canada.
Data Processor	This is Alcatraz AI. We process Biometric Data on behalf of the Data Controller (your employer or organization).
EEA	European Economic Area, which includes the EU countries plus Norway, Iceland, and Liechtenstein.
GDPR	General Data Protection Regulation, a key privacy law in the European Union that protects personal data.

On-Premise (a.k.a. On-Prem)	The Alcatraz AI Rock System architecture when it is installed and run within the physical infrastructure of the System Owner's facilities instead of being hosted by Alcatraz AI in the Cloud.
Personally Identifiable Information (PII)	Information that can identify you, such as your name, email address, badge number, or phone number. This includes Biometric Data.
Processing	The various actions performed on data, such as collecting, recording, storing, using, and deleting PII and Biometric Data.
Rock	Collectively, the Alcatraz AI hardware, software, SDK, and any associated documentation and enhancements.
System End User	This is you, the individual whose PII or Biometric Data is being processed.
System Owner	The organization that licenses Alcatraz AI Rock System and controls the data. They are also the Data Controller.
System Owner Administrator	A person working for or representing the System Owner who acts as an Administrator for the Alcatraz Solution.
You or your	The individual whose Biometric Data is processed by Alcatraz AI.

Understanding these terms will help you better grasp how your data is handled and protected. If you have any questions, please refer to your organization's privacy notice or contact them directly.

3. MAIN PRIVACY PRINCIPLES

Your Biometric Data is collected during the enrollment process with the Alcatraz solution. This can be done using a mobile device, webcam, or directly through the Rock device. Each time you approach a Rock, it authenticates your identity using your Biometric Data.

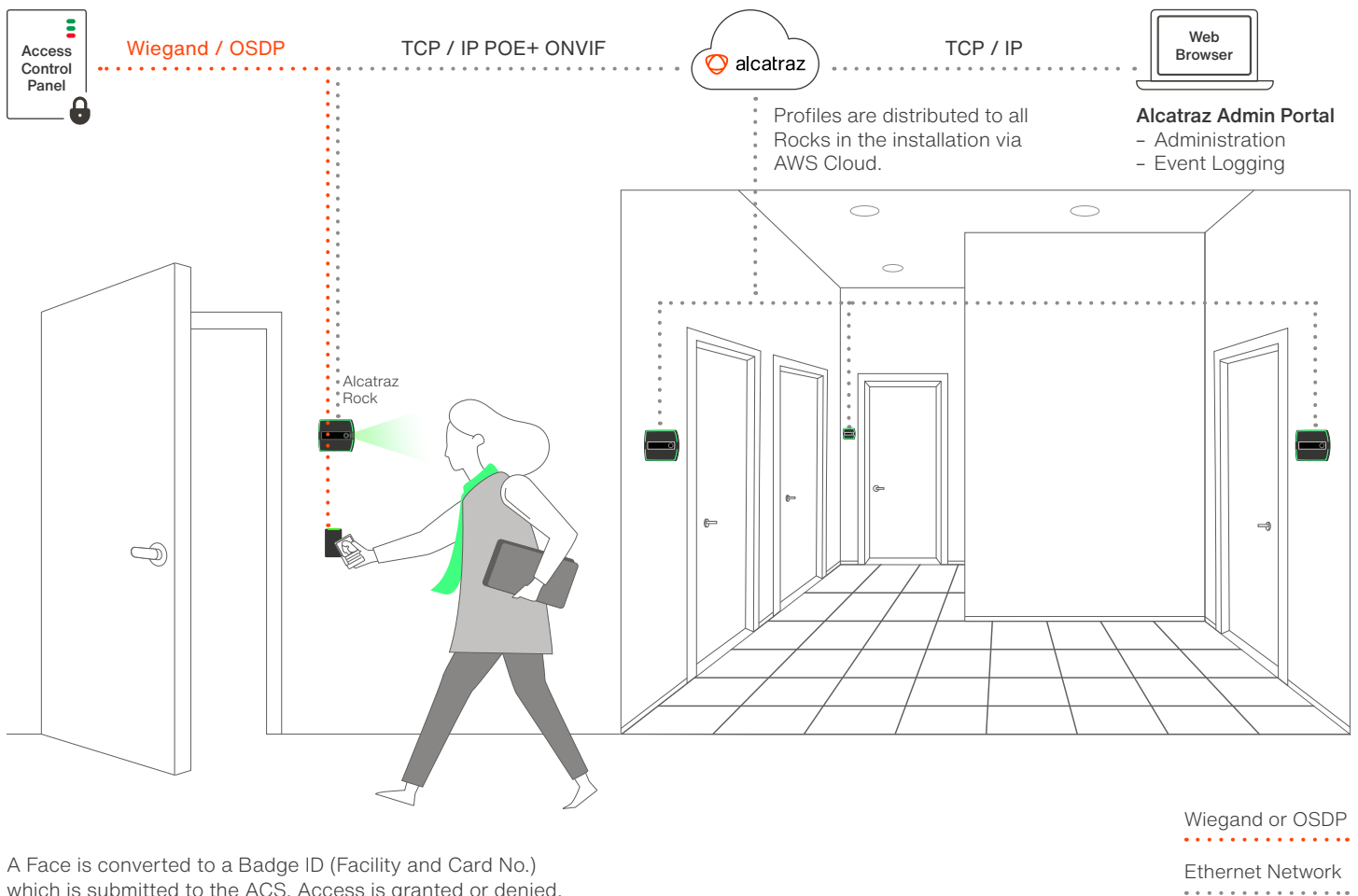
3.1. Data Security Measures

Facial authentication is a biometric technology that verifies your identity based on your unique facial features. Here's how it works:

- **Image Capture:** Advanced cameras and AI-driven algorithms capture and analyze your facial data, creating a digital biometric template, which we call the Digital Profile.
- **Real-Time Matching:** This process ensures proper authentication by matching your facial features against the stored template in real-time.
- **Enhanced Security:** Facial authentication offers better security than traditional access control credentials like PINs or access cards because it is harder to replicate and doesn't require physical tokens or memorized PINs.

For more details about facial authentication, visit our blog at [Alcatraz AI Blog](#) on [Facial Authentication](#).

3.2. Privacy-First Design



3.3. Lawful and Clear Data Processing

We protect your Biometric Data by encrypting it both when it is stored and when it is being transmitted. Our Alcatraz AI solution is designed with privacy in mind:

- When scanned, your profile is immediately turned into an encrypted “data b.l.o.b. (binary large object)” that cannot be converted back to an image.
- You are identified only by your Badge ID or Facility Code without exposing your images, names, genders, roles, emails, or phone numbers.
- If you do not use the system for a set time (like 90 days, for example), your biometric profile is deleted. The retention period is controlled by your System Owner.
- If you opt-out, your Badge ID is added to a list to prevent your face from being enrolled as a credential.

3.4. Data Ownership and Transparency

We build our solution with privacy as a priority. Our employees are trained to follow our privacy rules, ensuring that data protection is a part of everything we do.

3.5. Data Retention Policies

We only process Biometric Data for specific purposes. For example, while we may provide a video feed, it won't directly identify you without another system's help.

Who owns the data?

The System Owner (your employer or organization) owns the data. Alcatraz just processes it on their behalf.

3.6. Data Accuracy and Necessity

We handle your data securely and legally to prevent misuse. We work to eliminate discrimination or bias in our Services. Independent organizations test the Alcatraz AI's algorithms to ensure they are fair and accurate. We do not use your data to train the Alcatraz's AI algorithms. We do not share your data with other Alcatraz customers and only process your data based on the instructions given by your System Owner.

We keep your Biometric Data only as long as needed by law, contract, or to provide our Services. After this period, we permanently delete your data. We strive to keep your data accurate and only process what is necessary for authentication. Your Biometric Data is handled with the utmost care and respect for your privacy.

4. DATA COLLECTION AND PROCESSING

4.1. Enrollment Process

We collect and process unique facial data using 2D and 3D imaging technologies to create a secure binary representation of your facial features (Digital Profile), which is used for identity verification.

4.2. Facial Authentication Technology

Facial authentication is a biometric technology that verifies your identity based on your unique facial features. Here's how it works:

- **Image Capture:** Advanced cameras and AI-driven algorithms capture and analyze your facial data, creating a digital biometric template, which we call the Digital Profile.
- **Real-Time Matching:** This process ensures proper authentication by matching your facial features against the stored template in real-time.
- **Enhanced Security:** Facial authentication offers better security than traditional access control credentials like PINs or access cards because it is harder to replicate and doesn't require physical tokens or memorized PINs.

For more details about facial authentication, visit our blog at [Alcatraz AI Blog on Facial Authentication](#).

4.3. Step-by-Step Data Collection Process

Facial authentication typically follows these steps to verify your identity:

4.3.1. Image Capture:

- The process starts by capturing images of your face using a camera. The Alcatraz Rock uses an integrated camera for this task.

4.3.2. Facial Feature Extraction:

- Key features of your face, such as the position of your eyes, the shape of your nose, and the contours of your face, are extracted from the captured images.

- These features are then converted into a unique biometric template, which digitally represents your identity. Alcatraz captures more detailed data than most facial biometric solutions, creating a more accurate Digital Profile template.

4.3.3. Biometric Matching:

- The Digital Profile generated from the captured image is compared against a stored database of enrolled users' Digital Profiles.
- This comparison uses advanced algorithms to measure the similarity between the captured and stored biometric templates.

How do the algorithm and Biometric Data relate to each other?

A one-way encrypted algorithm converts the Biometric Data and badge ID into a binary string. This data set is encrypted when it is at rest and stored on the Alcatraz Rock and when the data is in transit on the network.

4.3.4. Identity Verification:

- If the similarity between the captured and stored biometric templates exceeds a certain threshold, your identity is verified, and access is granted.
- If the similarity is below the threshold, access is denied.

Do you gather PII other than Biometric Data?

Yes, but limited. The Alcatraz AI solution collects the badge ID from your current Access Control System (ACS) but does not capture your name, gender, job title, or other PII. We take pictures at 30 frames per second, continuously analyzing those pictures when you're standing in front of the Rock device. This analysis turns the image into a binary data set in real-time. During enrollment, this data set, called an embedding, becomes part of your Digital Profile.

By following these steps, Alcatraz AI ensures secure and efficient facial authentication, providing enhanced security for access control without compromising your privacy.

4.4. Technologies Used in Facial Authentication

Facial authentication systems rely on a combination of hardware and software technologies to work effectively. These include:

4.4.1. High-Resolution Cameras

These cameras capture clear and detailed images of your face, which helps in accurate facial recognition.

4.4.2. Facial Recognition Algorithms

Advanced algorithms extract key features from the captured images and compare them against stored Biometric Data to identify you.

4.4.3. Secure Databases

Your Biometric Data is stored in secure databases, protecting it from unauthorized access or tampering.

4.4.4. AI Tools: Computer Vision and Machine Learning:

These technologies enhance the accuracy and reliability of facial authentication systems. They help the system adapt and improve over time, ensuring it performs well in various real-world situations.

These technologies work together to ensure that facial authentication is both secure and efficient, providing a reliable method for identity verification.

5. TYPES OF DATA WE COLLECT

5.1. Biometric Data

We collect and process unique facial data using 2D and 3D imaging technologies to create a secure binary representation of your facial features (Digital Profile), which is used for identity verification. We may collect and process, among other data, the following Biometric Data collected either directly from you or the System Owner:

Biometric Data of the System End User includes biometric identifiers (such as your facial geometry) and the data from the System End User's prior interactions with the Rock. Enrollment data, may include images of your face. These images can be deleted if set to do so by the System Owner after the enrollment process is complete. Biometric Data captured from enrollment images is converted to an encrypted number which is compared against a number generated when you approach a Rock to assess whether a match exists.

Technical data (Device Signature), including but not limited to information about the date, time, and your activity in the Services. Machine-readable data, metadata, and device and network information to ensure that the system works properly or troubleshoot issues that arise. Your System Owner decides which of the above applies to you.

In what form and how is my facial data stored?

The biometric profiles are stored in an encrypted format. They can be stored indefinitely or automatically deleted after a predefined period if they are not accessed for a defined period of time.

5.2. Identity Verification Data

This includes images of you captured during the entire session if enabled by the System Owner. The Biometric Data from these images is converted into an encrypted number. This encrypted number is compared with a new number generated each time you approach a Rock to verify your identity. This does not include your name or other identifiable information.

5.3. Technical and Machine-Readable Data

Technical Data includes information about the date, time, and your activities within the Services provided. Machine-Readable Data include metadata and device and network information to ensure the system functions correctly and to troubleshoot any issues.

6. HOW AND WHY WE USE YOUR DATA

6.1. Purpose of Data Processing

We collect and process unique facial data using 3D and 2D imaging technologies to create a secure digital representation of your facial features, known as a Digital Profile. This profile is used for identity verification.

We may collect and process the Biometric Data directly from you or through the System Owner. This includes biometric identifiers such as your facial geometry and data from your previous interactions with the Rock.

Your Biometric Data is used strictly to authenticate your identity and ensure secure access to specific areas controlled by the System Owner (such as buildings, rooms, or facilities).

6.2. Legal Basis for Processing

Processing of Biometric Data is allowed only under certain conditions as outlined in Article 6 of the GDPR, which include:

- Your consent.
- Performance of a contract.
- Legal obligations.
- Protection of vital interests.
- Public interest.
- Legitimate interests.

Your System Owner decides which of these conditions applies to you. We provide biometric authentication Services to System Owners. This means we authenticate that you are the same person that enrolled in the Alcatraz Rock System when you enter an Access Point.

Scenario:

You work for SmartCo, Inc., a System Owner using our Alcatraz AI solution for secure building access. With your permission, you enroll your facial data for a faster and more convenient and more secure way to enter SmartCo. When you attempt to gain access after enrolling, the Alcatraz AI solution securely compares your facial features to the data captured during enrollment, granting you access immediately upon successful authentication.

We use the collected data, including photos for ongoing authentication services. This data is used only to provide the service and related business purposes and not to infer any other characteristics.

We collect your data through the enrollment process within our service. The System Owner then stores this data either On-Premises or in the Cloud. System Owners are responsible for gaining your consent and providing you with a privacy notice regarding the collection and use of your Biometric Data.

Typically, we collect: (a) Personal Information - Information received from the System Owner, such as badge data (no names or other personal data). (b) Evidence and Records - Legal basis for processing data, such as consents or written releases.

7. DATA ACCESS AND SHARING

7.1. Access by System Owners

System Owners may access your Biometric Data whether the Alcatraz AI service is hosted in the Cloud or on-premises.

7.2. Sharing with Third Parties

Providing your Biometric Data for access through an Access Point is voluntary. We believe it is best practice for the System Owner to obtain your written consent prior to enrolling with the Alcatraz AI System. If you do not consent or withdraw your consent, your face will not be enrolled and you will be unable to use our service to authenticate your identity. The System Owner will offer alternative access methods.

Your Biometric Data must be used responsibly and securely to provide you with a safe, private and reliable method for identity verification. If you have any questions, please contact your System Owner.

7.3. Disclosure to Authorities

Due to legal requirements, we may have to disclose or grant access to your Personally Identifiable Information (PII) and Biometric Data to authorities and supervisory authorities (e.g., a court or a government agency).

Only if enrollment images are stored would this be useful information. If not, our biometric profile would not be compatible with any back-end system a government agency uses. Since the Alcatraz AI Rock platform does not use or store names, the only way to determine which profile belongs to you is by cross-referencing your badge number from within the Access Control System software which contains names and other identifiable information for each badge holder.

7.3.1. Disclosure to Data Controllers, Data Processors, and Authorized Recipients:

Unless stated otherwise in this Privacy Notice or noted otherwise to you separately, we may disclose your Biometric Data to Data Controllers for whom we are Data Processors (e.g., System Owners), to our authorized Data Processors (sub-processors), and authorized third-party sites (e.g., external registries), as well as to persons who legally have the right to receive your Biometric Data.

For example, a System Owner Administrator's PII can be used as contact information for ongoing notices and updates about the Alcatraz AI Rock solution, companies carrying out satisfaction surveys, authorities and organizations intermediating or providing (electronic) mail, compliance or payment services, and similar entities; Office Visitors' Biometric Data can be shared with IT and security partners, provided that:

- The respective purpose and the processing are lawful.
- We have carefully assessed that the authorized Data Processors or sub-processors will comply with data protection requirements.
- The Biometric Data processing is carried out following our guidelines and based on a valid agreement.

If you have questions about our authorized Data Processors or sub-processors, please contact us at privacy@alcatraz.ai.

7.3.2. Legal Basis for Sharing

System End User's Biometric Data can only be shared with Alcatraz and persons who legally have the right to receive your Biometric Data if there is a valid legal basis.

7.4. Data Transfer Outside the EEA

We process your Biometric Data within the EEA. If we need to transfer your Biometric Data outside the EEA (e.g., for using sub-processor services and technical infrastructure), the transfer will follow the requirements, principles, and safeguards as stated in applicable data protection laws, such as relying on adequacy decisions issued by the European Commission or standard contractual clauses adopted by the European Commission (or other relevant authority), or complying with applicable data transfer accountability requirements.

While such Biometric Data is outside of your country or province of residence, it may be subject to the laws of the country, province, or state in which it is held. It may be subject to disclosure to governments, courts, law enforcement, or regulatory agencies of such other country, province, or state under the laws of that territory.

Where Alcatraz acts as the Data Controller, we provide further information on the safeguards applied (if relevant), including a copy of them and/or the extent of transferring Biometric Data upon request.

These guidelines ensure that your Biometric Data is shared responsibly and securely, in compliance with legal standards. If you have any questions or concerns about how your data is shared, please contact us at privacy@alcatraz.com.

8. RIGHTS TO BIOMETRIC DATA

8.1. Rights Depending on Location

Depending on where you live, you may have the right to:

- Request to know more about and access your Personal Information.
- Ask for the deletion of your Personal Information.
- Ask for correction of inaccurate Personal Information.
- Object to certain processing of your data.
- Withdraw your consent where we process your information on that basis.
- Ask us to restrict certain processing of your data.

Depending on where you live, you as a System End User may have the following rights concerning your Biometric Data:

8.1.1. The Right to Know

The right to obtain confirmation whether we are processing Biometric Data about you and to obtain specific details about the Biometric Data we have collected, including:

- The categories of Biometric Data collected.
- The categories of sources of the Biometric Data.
- The purposes for which the Biometric Data was collected.
- The categories of Biometric Data disclosed to third parties (if any), and the categories of recipients to whom the Biometric Data was disclosed, especially recipients in other countries or international organizations.
- Information about the existence of automated decision-making (if any), including profiling, as referred to in Article 22(1) and (4) of the GDPR. This includes meaningful information about the logic involved and the significance and envisaged consequences of such processing for you.
- Where possible, the expected period for which the personal data will be stored or, if not possible, the criteria used to determine that period.
- The categories of Biometric Data sold (if any), and the categories of third parties to whom the Biometric Data were sold.

These rights ensure that you have control over your Biometric Data and understand how it is being used. If you have any questions or need to exercise your rights, please contact your System Owner.

Alcatraz will NEVER sell your data nor share it for cross-context behavioral advertising purposes.

8.1.2. The Right to Access & Portability

The right to obtain access to the Biometric Data we have collected about you.

Digital Profile's are proprietary and are not interoperable with other systems. System Operators can provide detail on the Biometric Data that has been collected about you only by your badge ID number.

8.1.3. The Right to Correction

You have the right to correct inaccuracies in your Biometric Data, considering the nature of the Biometric Data and the purposes of its processing.

There is no way to “correct” your Biometric Data in the Alcatraz AI solution. You can remove your Biometric Data and reenroll by contacting the System Owner directly. The Data Processor is not authorized to handle consent withdrawal requests because it operates under the instructions of the Data Controller and does not have the authority or access to make decisions regarding the collection, use, or deletion of your data. Contacting the System Owner ensures that your request is addressed by the entity responsible for managing and protecting your Personal Information.

8.1.4. The Right to Deletion

The right to have us delete the Biometric Data we maintain about you unless the applicable law prohibits us from doing so.

Please contact the System Owner directly if you wish to delete your Biometric Data. Alcatraz, as the Data Processor, is not authorized to handle deletion requests because we operate under the instructions of the Data Controller (your employer or organization) and do not have the authority to make decisions regarding the collection, use, or deletion of your data. Contacting the System Owner ensures that your request is addressed by the entity responsible for managing and protecting your personal information.

Alcatraz does not have access to your consent form or your biometric profile, as the System Owner can only access these. While we value every individual and prioritize your protection, to Alcatraz, you are represented only as encrypted data (1s and 0s). We cannot identify or find you without the System Owner's information.

8.1.5. The Right to Non-discrimination

The right to not receive retaliatory or discriminatory treatment in connection with a request to exercise the above rights.

8.1.6. The Right to Withdraw the Consent

The right to take back the consent you gave us for the processing of Biometric Data. Withdrawal of your consent will not affect the legality of the processing based on consent before the withdrawal.

If you wish to withdraw your consent for a System Owner (Data Controller) to use your Personally Identifiable Information (PII), please contact the System Owner directly. Alcatraz, as the Data Processor, is not authorized to handle consent withdrawal requests because we operate under the instructions of the Data Controller and do not have the authority to make decisions regarding the collection, use, or deletion of your data. Contacting the System Owner ensures that your request is addressed by the entity responsible for managing and protecting your personal information.

8.1.7. The Right to Object

You have a right to file an objection on grounds relating to your particular situation if your Biometric Data processing is not collected for a legitimate interest or public interest. Through cooperation with the System Owner, we will no longer process your PII unless we show compelling legitimate grounds for the processing that override your interests, rights, and freedoms or for establishing, exercising, or defense of legal claims.

8.1.8. The Right to Restriction of Processing

The right which, in some instances, allows you to direct us to limit the processing of your Biometric Data for a certain period (e.g., if you have filed an objection to Biometric Data processing).

8.1.9. The Right to Submit a Complaint and Make Appeals

If you find that applicable data protection laws have not been complied with, we would appreciate it if you contact us at privacy@alcatraz.ai (including for any appeals of our decisions). However, you also have the right to complain directly to a data protection authority about our collection, use, or other processing of your Biometric Data. For more information, please contact your local data protection authority in the EEA or in the United Kingdom. The contact details for each EU data protection authority are here: https://edpb.europa.eu/about-edpb/about-edpb/members_en. The contact details for the UK data protection authority, the Information Commissioner's Office, are available here: <https://ico.org.uk/make-a-complaint/>. If you are in the United States and have concerns about the results of an appeal, you may contact the attorney general in the state where you reside.

8.1.10. Authorized Agents

You may have the right to submit a rights request via an authorized agent. If you are submitting a rights request as an authorized agent, you must provide proof of your authorization to make the request. This could be a valid power of attorney or proof of signed permission from the individual who is the subject of the request. Please do not provide any sensitive personal information, such as a driver's license or other government-issued ID, with this request.

Sometimes, we may need to contact the individual who is the subject of the request to verify their identity or confirm that you have permission to submit the request. If you are an authorized agent seeking to make a request, please contact us at privacy@alcatraz.ai.

8.2. Exercising Your Rights

If you wish to exercise any of your rights regarding Biometric Data, you must first contact the System Owner. Only the System Owner has access to and control over your Biometric Data.

8.3. Contacting Us

If you have any questions about this Privacy Notice, please send a request to us at privacy@alcatraz.com. We will respond to your request by email within one month or sooner if required by applicable law. If needed, this period may be extended by two further months, considering the complexity and number of requests. We will inform you of any such extension within one month of receiving your request and explain the reasons for the delay.

9. DATA SECURITY MEASURES

9.1. Physical, Technical, and Organizational Measures

We use various commercially reasonable measures (physical, technical, organizational) to protect your Biometric Data from unauthorized or arbitrary modifications, disclosure, acquisition, destruction, loss, theft, misuse, alteration, or unauthorized access. These measures include data encryption and compliance with up-to-date ISO Standards.

However, electronic transmission or storage of information is not always 100% secure. Despite the security measures we have implemented, such as data encryption and compliance with ISO Standards, we cannot guarantee that data loss, misuse, or alteration will never occur.

9.2. Reporting Data Breaches

If you have any information about an actual or suspected data breach, please inform us immediately at privacy@alcatraz.ai. We will promptly address the issue and inform our lead data protection supervisory authority if applicable.

10. DATA RETENTION POLICIES

Learn about the duration for which we store your Biometric Data. This section explains our policy on data retention.

10.1. Retention Period Determined by System Owners

System Owners, not Alcatraz, determine the appropriate retention period for Personally Identifiable Information (PII). System Owners must consider the amount, nature, and sensitivity of PII, as well as the purposes for which it is processed. They also need to consider the periods required to retain Biometric Data to meet legal obligations, address complaints or queries, and protect legal rights if claims are made.

The Rock captures my facial data during enrollment and at Access Points if there is a Security Event. How does the Alcatraz AI solution handle data retention?

The Alcatraz AI solution provides System Owners with options for retaining and managing Security Event data. System Owners can choose whether to retain enrollment and event images and for how long. Most System Owners delete enrollment images and optimize storage by setting short retention periods.

We store your data for the period outlined in the Agreement with the System Owner or as long as necessary for the establishment, exercise, or defense of legal claims, or for anti-fraud purposes. For more information about the data retention period, refer to the privacy notice provided to you by the System Owners.

10.2. Extended Storage and Permanent Erasure

We may store your Biometric Data for a longer period than the Agreement duration if we have a lawful basis to do so. After the Biometric Data storage period ends, we permanently erase your Biometric Data. Alcatraz processes, maintains, and uses aggregated or de-identified information only in a de-identified fashion and will not attempt to re-identify this information except as permitted by law.

What is your retention period?

The System Owner controls the retention period for all PII, with limits for multi-tenant System Owners.

11. TECHNOLOGICAL ASPECTS OF OUR SERVICE PROVISION

Our approach to identity authentication focuses on ensuring security and reliability. By harnessing automatic algorithms, such as Computer Vision and Machine Learning, we maximize efficiency and security to authenticate individuals reliably. We only authenticate an individual against their enrolled data – nothing else.

11.1. Use of Algorithm and Machine Learning:

Alcatraz does not use your data to train the algorithms. The algorithms we deploy are fully trained using mathematical models developed from data provided by individuals who consented specifically for this purpose.

11.2. Automated Authentication

Our authentication engine, trained with Machine Learning, automates the process of verifying your identity without human involvement. When we use this fully automated process, the System Owner will inform you and may ask for your explicit consent. In some cases, where there are other legal grounds for this processing, such as legal obligations, consent might not be needed. You have the right to ask for information and an explanation about the logic behind the authentication decision. You also have the right to request human intervention or to object to the decision based on your particular situation.

By integrating these advanced technologies, we ensure that your identity is authenticated securely and reliably while respecting your privacy and rights. If you have any questions or concerns, please contact your System Owner.

11.3. Ethical Machine Learning Practices:

At Alcatraz, we are committed to conducting Machine Learning ethically and with the utmost respect for human rights and freedoms. Machine Learning helps us provide better, more secure, and faster services and helps prevent and detect security issues. The data sets used for developing, testing, and training are kept in separate, tracked, and highly secure data research environments.

12. CHILDREN'S BIOMETRIC DATA

This section explains how we handle Biometric Data for children.

12.1. Handling of Children's Data

We may process Biometric Data for children (under 16 years of age, depending on jurisdiction). The Data Controller (your employer or organization) will ensure there is a legal basis for this processing, such as obtaining consent from the child's guardian.

You have rights regarding the use of your Biometric Data, including the rights to:

- Access your data.
- Correct any inaccuracies in your data.
- Request deletion of your data.
- Object to or restrict certain uses of your data.

These rights help ensure that your Biometric Data is used appropriately and that you control how it is handled. If you have any questions or need to exercise your rights, please contact your System Owner.

12.2. Guardian Consent

If we find out that we have collected a child's Biometric Data without the guardian's consent, we will delete the information as soon as possible.

13. LEGAL GROUNDS FOR PROCESSING FOR A NEW PURPOSE

13.1. Conditions under GDPR

If we need to process your Biometric Data for a new purpose that is different from the one it was originally collected for, or if it is not based on your consent, we will carefully evaluate whether this new processing is allowed. We will also provide you with all the necessary information before proceeding, in accordance with applicable laws. By considering these factors, we aim to make sure that any new processing of your Biometric Data is justified, transparent, and compliant with legal requirements. If you have any questions or concerns about how your data might be used for new purposes, please contact your System Owner.

13.2. New Purposes for Data Processing

We assess whether there is a connection between the original purpose for collecting your Biometric Data and the new purpose.

13.2.1. Context of Data Collection:

We consider the circumstances under which your Biometric Data was collected, especially the relationship between you and use.

13.2.2. Nature of the Biometric Data:

We evaluate the type of Biometric Data being processed, particularly if it involves sensitive Biometric Data.

13.2.3. Consequences for You:

We look at the potential impact of the new processing on you.

13.2.4. Protection Measures:

We ensure proper protection measures, such as encryption, are in place to safeguard your data.

14. JURISDICTION-SPECIFIC NOTICES

14.1. California

You may have different rights depending on where you reside. These terms prevail should there be any ambiguity between this section and any other part of this document.

14.1.1. Notice of Collection and Additional Information for Residents of California

California law requires us to disclose additional information about our collection, use, and disclosure of personal information. If you live in California, this section applies to you.

14.1.2. Additional Disclosures

Categories of Personal Information Collected: In the preceding 12 months, we have collected the following categories of Personal Information: identifiers, biometric information, demographic information, commercial information, internet or other electronic activity information, geolocation data, audio, electronic, or similar information, professional or employment-related information, inferences, and sensitive personal information. For more details, please see section 4 of Alcatraz's Privacy Notice.

14.1.3. Purposes for Collection

We collect personal information for the business and commercial purposes described in section 5 of our Privacy Notice. In the preceding 12 months, we have disclosed personal information for these purposes to the following categories of recipients:

- **System End User Data:** Identifiers, demographic information, commercial information, internet or other electronic activity information, geolocation data, audio, electronic, or similar information, inferences, and sensitive Biometric Data have been disclosed to Data Controllers (e.g., System Owners), authorized Data Processors (sub-processors), third-party sites (e.g., external registries), and, on a case-by-case basis, to supervisory authorities, courts, and government agencies.
- **System Owner Administrator Data:** Identifiers, commercial information, internet or other electronic activity information, audio, electronic, or similar information have been disclosed to authorized Data Processors, authorities, organizations providing (electronic) mail, compliance or payment services, and, on a case-by-case basis, to supervisory authorities, courts, government agencies, debt collection agencies, and credit registers.
- **Advertising and Marketing:** Identifiers, commercial information, electronic, or similar information have been disclosed to advertising and marketing partners, and companies conducting satisfaction surveys.

14.1.4. Use of Sensitive Personal Information

We do not use sensitive personal information for any purpose other than to perform the Services or to improve, upgrade, or enhance the Services.

14.1.5. Your Privacy Rights:

- **Access, Correction, or Deletion:** To ask for access, correction, or deletion of your personal information, contact our Data Protection Officer (DPO) via email at privacy@alcatraz.ai.
- **Authorized Agents:** You have the right to submit a rights request via an authorized agent.
- **California Notice of Financial Incentives:** We may offer financial incentives, such as coupons or other benefits, to System Owners who participate in feedback or research surveys. Detailed information will be provided at the time of collection. You can opt into a financial incentive by following the sign-up or participation instructions and opt-out at any time by following unsubscribe instructions or contacting us at privacy@alcatraz.ai.

14.1.6. More Information

For more details about the privacy rights, you have as a California resident, how to exercise your rights, and how we verify your requests, please see section 7 above.

For more information about the data points, we collect and the categories of sources of such collection, see section 4 of Alcatraz's Privacy Notice. See section 10 for information about how long we keep the data points we collect.

14.2. Colorado, Illinois, Washington, and Texas

14.2.1. Illinois and Texas Regulations

- **Illinois:** The Illinois Biometric Information Privacy Act (BIPA) regulates the collection, storage, use, and retention of “biometric identifiers” and “biometric information.” Biometric identifiers include retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry.
- **Texas:** The Business and Commerce Code of Texas on the Capture or Use of Biometric Identifiers regulates similar aspects of Biometric Data.
- **Data Collection:** Alcatraz collects face scan information during identity authorization. We use this information to verify identity, prevent fraud, and provide authentication services to our System Owners.
- **Data Destruction:** For Illinois residents, we will destroy Biometric Data when the initial purpose has been satisfied or within 3 years of the last interaction with our System Owners. For Texas residents, data will be destroyed the later of one year after the purpose expires or one year after any recordkeeping obligations end.

14.2.2. Colorado Regulations

- **Data Collection and Consent:** Personal and Biometric Data will be collected lawfully and fairly, only with your consent. The Colorado Privacy Act grants new rights to access, delete, and correct personal data, and to opt-out of data sale, targeted advertising, and profiling.
- **Data Destruction:** Data will be destroyed the later of one year after the purpose expires or one year after any recordkeeping obligations end.

14.2.3. Washington Regulations

- **Data Access and Deletion:** You have the right to access and request deletion of your data. Affiliates, processors, contractors, and third parties must also delete the data if requested. There may be delays in deletion due to legal obligations, ongoing transactions, or security risks.
- **Data Destruction:** Data will be destroyed the later of one year after the purpose expires or one year after any recordkeeping obligations end.

14.2.4. General Provisions

Unless prohibited by law, your Biometric Data is accessible only to us and our service providers. We do not share Biometric Data with third parties, except with System Owners for authentication purposes.

By proceeding with verification or authentication, you agree that you have read the relevant disclosures and voluntarily consent to Alcatraz’s collection, storage, retention, use, and disclosure of your Biometric Data.

Alcatraz uses reasonable industry standards to store, transmit, and protect your Biometric Data. We do not sell, lease, trade, or profit from your Biometric Data.

15. CONTINUOUS PRIVACY IMPROVEMENT

15.1. Commitment to Ongoing Privacy Enhancements

We are committed to continuously improving our privacy practices. This policy is reviewed regularly and updated as needed to ensure it meets the highest standards for data protection and clarity.

16. CONTACT DETAILS AND INFORMATION

16.1. Contacting Alcatraz AI’s Data Protection Officer

Please review this Privacy Notice carefully and contact our Data Protection Officer (DPO) at privacy@alcatraz.ai if you have any comments, questions, or concerns.

16.2. Availability of and Changes to the System Privacy Notice

This Privacy Notice is available through your System Owner or by request to privacy@alcatraz.ai. Please note that we may occasionally update this Privacy Notice. If we do, we will let you know by revising the date of the Privacy Notice. If we make material changes, we will provide the System Owner with additional notice, such as by adding a statement to the Services or sending you a notification.

These practices ensure that you are always informed about how we handle your Biometric Data and any changes to our privacy practices. If you have any questions or need further information, please contact your System Owner or reach out to us at privacy@alcatraz.ai.



Contact Us

10061 Bubba Rd Cupertino, CA 95014

legal@alcatraz.ai

(650) 600-0197

Connect with Us



www.alcatraz.ai



[linkedin.com/company/alcatraz](https://www.linkedin.com/company/alcatraz)



twitter.com/alcatrazai