StoneLock Privacy Policy

Last Updated: February 17, 2020

The privacy rights of the users of StoneLock's biometric facial recognition identity management products are central to StoneLock's mission of providing the most secure and safe and business solutions possible for purposes of secure access control. It is StoneLock's policy to adhere to the highest standards for biometric information and biometric identifiers. StoneLock therefore strives to adhere to the standards set forth by the Illinois Biometric Information Privacy Act (BIPA) as well as biometric information under the EU's General Data Privacy Regulation (GDPR) with respect to users registered and authenticated by StoneLock products. Consideration is also given to emerging privacy standards, such as California Consumer Privacy Act (CCPA) enacted in 2018.

The Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. (BIPA), enacted in 2008 and currently adopted in Illinois, Washington and Texas, sets forth a comprehensive set of rules for companies collecting biometric data of citizens living within those states in the areas of informed consent prior to collection, limited right to disclosure, protection obligations and retention guidelines, the profiteering from biometric data and the private rights of individuals harmed by BIPA violations. Because StoneLock does not scan or otherwise calculate face geometry, StoneLock data does not fall under BIPA as biometric information.

The European Union's General Data Protection Regulation (GDPR), effective May 25, 2018, governs the security and privacy of personal data of anyone living in the European Union. GDPR lays down rules relating to the protection of fundamental rights and freedoms of European citizens and their personal data, the processing and free movement of such personal data, and ensures that the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the processing of personal data.

The California Consumer Privacy Act (CCPA), enacted in 2018, establishes consumer rights in the State of California relating to the access to, deletion of and sharing of personal information that is collected by businesses. The scope of the CCPA is primarily focused on regulating businesses that collect and profit from personal information. StoneLock is an opt-in enterprise biometric that does not leave the StoneLock system in normal use, so much of the CCPA does not apply to StoneLock data when used correctly, aside from general consent, scope of use, non-profiteering, and deletion policies which apply to all personal information.

This Privacy Policy was developed to provide important information regarding StoneLock's general adherence to the standards for biometric data set forth by these standards[1].

About the StoneLock Solution

The StoneLock solution maintains all biometric data and personal data within the solution. StoneLock has the ability to add authorized persons, assign privileges, and delete profiles. Unless otherwise requested by the customer, StoneLock does not expose any information collected for these purposes to any applications incompatible with the specific activity for which it

[1] Under both BIPA and GDPR law personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject, collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes (BIPA 740 ILCS 14/15 Sec. 15; GDPR Article 5) and presumes specific, informed and unambiguous consent given freely by the data subject (BIPA 740 ILCS 14/15 Sec. 15; GDPR Articles 1 & 7). BIPA 740 ILCS 14/15 Sec. 15 and GDPR Article 9 prohibits the processing of personal data revealing biometric data unless specifically carrying out the obligations and exercising specific rights in the field of employment. GDPR Article 88 further provides for specific rules to ensure the protection of right and freedoms in respect of the processing of employees' personal data in the employment context.

is intended. StoneLock's biometric data consists of a dataset of facial features in a proprietary, unrecognizable data format, and is not identifiable as PII. StoneLock data is updated solution-wide with every verification, maintaining the "most current" biometric profile with each use.

The StoneLock Pro solution has two devices that hold biometric data and personal data: the Reader (edge device) and the Gateway. The Reader stores the biometric data in the Control Box on the secure side of the door. The reader can be set up to store the biometrics in volatile memory. With this setup removal of power immediately destroys the biometric data, thus protecting against the violation of personal data. High availability functions within the Gateway allow for the restoration of data and permissions within the solution once compromised hardware is restored.

The Gateway stores the biometric data on its hard drive in a proprietary NOSQL database storage 256 encryption cipher. The biometric data is transferred between the Reader and the Gateway and between Gateways using TLS v1.2 handshaking and encryption. Configuration of clusters of Gateways allow for complete control of the global transfer of data as well as the geographic isolation of data as required by local law or enterprise custom.

The personal data within the solution is a color image (JPEG compressed file) captured at the time of enrollment and verification. On the StoneLock Pro, at the discretion of the customer, these images are displayed in the Client Event Viewer as a secondary form of verification of the individual. The storage of these images is configurable by the customer and can be completely disabled. This feature is only available on the StoneLock Pro and is ***not*** available with the StoneLock GO.

The StoneLock GO solution has two devices that hold biometric data and personal data: the Reader (edge device) and the Gateway. The Reader is provided with a tamper switch that immediately removes the biometrics from the Reader when activated. The Biometrics are restored to the Reader upon reconnection to the Gateway the Reader is authorized to communicate with.

Only user biometrics and credential information (needed to send to the Access Control System to unlock the door) are sent to the Reader. All data is secured using AES 256 and is transferred between the Reader and the Gateway TLS v1.2 handshaking and encryption.

The Gateway and Reader both use a SQL based database. Multiple Gateways communicate to the single Database using TLS v1.2. Configuration of Gateways allow for complete control of the global transfer of data as well as the geographic isolation of data as required by local law or enterprise custom.

When the GO reader is paired with a StoneLock REM (Reader Expansion Module), the REM keeps the network drop at the GO secure. The REM uses an iptables firewall to allow the GO to communicate only to the Gateway over TLS v1.2.

Data that is obtained when a user registers with StoneLock Products:

All users of StoneLock products will need to register and be enrolled prior to authentication by StoneLock Products.

Under BIPA (740 ILCS Sec. 15 (B)(3)), it is advised that such registration process include an explicit consent from the employee or authorized person for the use the biometric data collected

by StoneLock Products. Additionally, under BIPA (740 ILCS 14/15) biometric identifiers may only be retained for 3 years after the subjects last employment.

CCPA is currently a fluid standard; Generally, employment-related data is considered personal information under the standard. CCPA amendment AB 25 in July of 2019 specifically excludes information collected by a business in the natural course of employment from CCPA, but that amendment becomes inoperative at the end of 2020. Customers falling under CCPA should keep current with obligations to this standard.

In all use cases, StoneLock recommends the implementation of proper consent, scope of use, non-profiteering, and deletion policies when collecting employee biometric data. When used correctly and with proper internal controls, StoneLock is designed with features that support privacy compliance.

Purposes and Legal Grounds

(a) StoneLock correlates a unique user ID with the biometric data obtained by the StoneLock product to allow access to the specific authorized users. The legal ground for correlating the unique user ID with the biometric data is based on the legitimate interest in providing the highest possible security in a work or business environment for the protection of persons and property.

(b) Such use is also necessary for carrying out obligations of the controller or data subject in the field of employment law, necessary for reasons of public interest in public health, and is vital for legal claims in protecting authorized persons in work/business settings from premises liability due to theft, violence or other inappropriate behavior.

Data obtained when authorized users are authenticated with StoneLock products.

StoneLock products are not biometric surveillance tools for the identification of unknown persons in a public environment. StoneLock products use near-infrared light to obtain metadata to create biometric data generated by StoneLock's proprietary algorithms. Authentication with a StoneLock product is performed by referencing the biometric data using proprietary systems with the live subject using the specific StoneLock device.

The StoneLock Pro will collect a JPEG photograph triggered by any attempted use, including the successful and failed authentication of any registered or unregistered person attempting to use a StoneLock product. There is no biometric data derived from this photograph by any StoneLock products. The StoneLock Pro is the only StoneLock product with this capability. The StoneLock GO ***does not*** have the capability to capture a jpeg or stream video.

Individual biometric signature data is not exportable or accessible. StoneLock may, ***with proper approvals***, access genericized data ***that does not constitute personal information of any individual*** for the purpose of improving StoneLock's proprietary algorithms and systems.

Purposes and Legal Grounds

a) The legal ground for obtaining the biometric data is based on the legitimate interest in providing the highest possible security in a work or business environment for the protection of persons and property.

b) As such, the StoneLock Product(s) and services are necessary for carrying out obligations of the controller or data subject in the field of employment law and is vital for legal claims in protecting work or premises liability from theft, violence or inappropriate behavior.

c) The use of genericized data is for the legitimate purpose of providing the highest possible security in a work or business environment by analyzing genericized data to better improve StoneLock's products, proactively averting the controverting StoneLock systems, and better protecting the integrity of StoneLock systems, qualifying as "specified, explicit and legitimate purposes" in keeping with both the data minimization principal and requirements for data protection for enterprise security.

In the Event of a Data Breach

In the unlikely event of a data breach, genericized data would not constitute biometric identifiers under BIPA or data subject to GDPR. StoneLock will nevertheless provide notice of such data breach within 72 hours by posting a notice on our website (*www.stonelock.com*).