StoneLock® Privacy Policy

Last Updated: May 23, 2018

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 data. 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.

The Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. (BIPA), enacted in 2008 and currently adopted in Illinois, and in substantially similar form in Washington and Texas, sets forth a comprehensive set of rules for companies collecting biometric data[1] 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.

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.

This Privacy Policy was developed to provide important information regarding StoneLock's general adherence to the standards for biometric data set forth in these regulations[2].

About the StoneLock Solution

StoneLock is an opt-in biometric identity management system for physical access control. Subject to human resources oversight and policies, authorized users of StoneLock products will need to register and be enrolled prior to authentication by StoneLock products. Once user consent is attained by the organization's controller, enrollment in a StoneLock solution is easily achieved with the willing cooperation of the user.

StoneLock products maintain all biometric metadata and personal data within the StoneLock 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 is intended. StoneLock's biometric data consists of a dataset of facial features that

[1] Because StoneLock does not scan or in any way base it's biometric comparisons on face geometry, StoneLock metadata does not fall under BIPA's definition of biometric information generated by biometric identifiers.

[2] 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.

are pseudonymized into a proprietary metadata format that is not considered PII[3]. StoneLock's metadata is updated solution-wide with every verification, maintaining the "most current" biometric profile with each use.

The StoneLock solution has two devices that hold biometric metadata and personal data: the Reader (edge device) and the Gateway. Biometric metadata is held in volatile memory in the Reader and in non-volatile memory in the structure. Biometric metadata is stored in the database fully encrypted using a SHA 512 key and an AES Gateway. The Reader is provided with a tamper switch that immediately removes power from the device on the opening of the control box. The removal of power immediately destroys the biometric metadata, 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 metadata on its hard drive in a proprietary NOSQL database storage 256 encryption cipher. The biometric metadata is transferred between the Reader and the Gateway and between Gateways using TLS v1.2 handshaking and encryption. All data transfer and event profiling is traceable within the solution. 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. 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 and transfer of these images is configurable by the customer and can be completely disabled. The images are not stored on the Reader. When stored on the Gateway, the storage life is configurable, and a Garbage Collection routine permanently destroys the image.

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 of the biometric metadata collected by StoneLock Products. Additionally, under BIPA (740 ILCS 14/15) biometric data defined by the statute as a biometric identifier may only be retained for 3 years after the subjects last employment.

Purposes and Legal Grounds

(a) StoneLock correlates a unique user ID with the biometric metadata 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 metadata 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.

[3] StoneLock metadata is typically generated from less than 5% of available face data and is not recognizable as the user.

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 data to create biometric metadata generated by StoneLock's proprietary algorithms. Authentication with a StoneLock device is performed by referencing the biometric metadata using proprietary systems while the live subject appears before the specific StoneLock device.

As described above, the StoneLock Solution may also collect personal data in the form of 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. This JPEG file resides in a log under the control of the system administrator, who may purge the log as required by policy or disable the collection of the JPEG altogether with no adverse effect to the operation of the system. There is no biometric data derived from this photograph by a StoneLock product.

Individual biometric metadata 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 metadata 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*).