StoneLock and General Data Protection Regulation Compliance

Last Updated August 2020

The General Data Protection Regulation (GDPR) went into effect in the European Union on May 25, 2018 and governs the security and privacy of personal data of anyone living in the EU. 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 bulletin provides an overview of how StoneLock's solution set facilitates compliance with this important personal data standard.

StoneLock is an opt-in biometric identity management system specifically designed for physical access control. Once user consent is attained[1] by the organization's controller, enrollment in a StoneLock system is easily achieved with the cooperation of the user. StoneLock's biometric data is a proprietary data format that retains less than 5% of facial data scanned by the reader and is therefore not recognizable as PII. StoneLock maintains all biometric data and personal data within the system and does not expose this information to any applications connected to a StoneLock system.

A StoneLock solution has two components that hold either biometric data or other personal data: the Reader (edge device) and the Gateway. Biometric data is held in volatile memory in the Reader and in non-volatile memory in the Gateway. The Reader is provided with a tamper switch that immediately shuts off power from the device when opening the control box. The loss of power wipes the biometric data, thereby protecting from any violations of personal data that might arise from theft of a faceplate.

The StoneLock Gateway stores the biometric data on its hard drive in a database. High availability functions within the Gateway allow for the restoration of data and permissions within the solution once compromised hardware is restored. The biometric data is transferred between the Reader and the Gateway and between Gateways using TLS v1.2 handshaking and encryption. Files consumed from external data sources are held in the Gateway along with the Biometric Data Sets, using the same encryption and high availability structure. All data transfer and event profiling are traceable within the solution. An array of Gateways allows for complete control of the transfer of information as for the geographic isolation of data as required by local law or enterprise customer.

In normal operations no recognizable photos, videos or likenesses of the user are captured by the StoneLock GO.

In troubleshooting mode, a near-infrared capture of the face occurs as a byproduct of the troubleshooting mode and is completely separate from any biometric data that is captured. The near-infrared image is transferred to the Gateway to be used for diagnostic purposes. The images can be downloaded for review and disposed of by the end user. The images are never stored on the Reader.

StoneLock is dedicated to maintaining compliance with the European Union's General Data Protection Regulation and other evolving privacy standards. Contact StoneLock (www.stonelock.com) with further questions regarding EU GDPR compliance.

[1] Under 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 (Article 5) and presumes specific, informed and unambiguous consent given freely by the data subject (Articles 1 & 7). 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. 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.