StoneLock and General Data Protection Regulation Compliance

A StoneLock White Paper

The General Data Protection Regulation (GDPR) is a new law governing 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. GDPR comes into effect May 25, 2018. This bulletin provides an overview of how StoneLock provides a solution set designed to facilitate compliance with this new personal data standard.

StoneLock is an opt-in biometric identity management system for physical access control. Once user consent is attained[1] by the organization's controller, enrollment in a StoneLock solution is easily achieved with the willing cooperation of the user. The StoneLock solution maintains all biometric data and personal data within the solution. StoneLock does not expose this information to any applications connected to the solution. StoneLock's biometric data consists of a dataset of facial features that are pseudonymised into a proprietary data format that is not considered PII.

The StoneLock solution has two devices that hold biometric data and 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 removes power from the device on the opening of the control box. The removal of power immediately destroys the biometric data, thus protecting against the violation of personal data.

The StoneLock Gateway stores the biometric data on its hard drive in a proprietary NOSQL database fully encrypted using a SHA 512 key and an AES 256 encryption cipher. 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 is traceable within the solution. Configuration of the Gateway cluster allows 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.

A color image (JPEG compressed file) of the face of enrollee is captured at the time of enrollment and verification. This JPEG is a byproduct of this process and is completely separate from the Biometric data that is captured. The JPEG image is also transferred to the Gateway and permanently stored in the file system. 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.

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.