Press release Box-ID: 1074407

iCOGNIZE GmbH
Justus-von-Liebig-Straße 9
63128 Dietzenbach, Germany
http://www.icognize.de

Contact
Mr Roberto Creutziger
060743103613
roberto.creutziger@icognize.de

09/01/2021

iCOGNIZE files patent on GDPR-compliant method for securing biometric data

The Hessian company has applied for a patent on its new split-template method for securing biometric data

Logo_Split_Template

(PresseBox) (Dietzenbach, 09/01/2021) The Hessian company iCOGNIZE has applied

(PresseBox) (Dietzenbach, 09/01/2021) The Hessian company iCOGNIZE has applied for a patent on its new split-template method for securing biometric data. In this new process, biometric data is split directly after gathering, rendering it unrecognizable.

Since biometric data contains mathematical descriptions of certain characteristics of body features such as fingerprints, iris or facial details, and vein patterns, it is considered highly critical and must be protected in a particular manner - not only to avert data breaches but especially to prevent cybercriminals from stealing entire sets of biometric data.

The process can be used wherever sensitive data needs to be protected more strongly – also outside of biometric systems. For example, with the split-template method, tokens can be protected even better against unauthorized access.

To clarify the process and the advantages of the split-template method, we need to take a detailed look at previous methods:

Potential security gaps in biometric access controls

In high-security biometric access controls, biometric characteristics such as fingerprints, veins, or iris features are recorded by a corresponding sensor system and compared to biometric features already stored in the system. If these results show sufficient similarities, a so-called "match" is found. Biometric data used for comparison belongs to the person who presented the corresponding biometric feature. Since the system recognizes the person, who previously generated the biometric data set used for comparison, the person is thereby identified.

Cybercriminals can steal or manipulate this biometric data. For example, if fingerprint data is published online, any person with the appropriate knowledge can create a mock-up for a so-called "presentation attack" and thus defraud biometric security systems.

For the person, whose fingerprint was exposed, this means that their it can never again be used in the biometric system. Since the biometric feature is now known in its pure form, a replica can be generated at any time. In addition, digital fingerprints are sensitive, personal data that must be specially protected according to the EU-GDPR. They may be exempt from permanent storage altogether. For this reason, data protection law prohibits the central storage of sensitive biometric data. This in turn may mean that bio-

metric systems are not allowed to be used in various applications.

Difficulties of previous solutions

To circumvent these issues, there currently is one procedure in place: for later comparison, biometric data is stored on servers that belong to a highly secure and non-vulnerable IT infrastructure.

This works quite well in practice. However, due to increasingly complex IT procedures, it is becoming more and more difficult and cost-intensive to maintain this level of highly secure infrastructure.

In addition, and as mentioned above, centralized storage of personal data, such as biometric data, is a fundamental data protection issue.

Is mobile data storage a GDPR-friendly alternative?

To comply with the GDPR, biometric data must be stored exclusively on mobile media such as RFID cards or mobile devices. This way, users can access their personal data at any time and also delete it if in doubt.

By holding the card or mobile device up to a corresponding reader, the data is recorded. The system then compares the data and immediately deletes the used data. This way, biometric data is only in the system at the time of use and is not persistently stored there. In order for this method to comply with the EU-GDPR, additional prerequisites need to be met.

EU-GDPR (Article 9)

- **Consent:** the data subject has given explicit consent to the processing of biometric data for one or more specified purposes, except where Union or Member State law provides that the prohibition may not be lifted by the data subject's consent.
- **Processing is necessary** for the controller or the data subject to carry out the obligations and exercising specific rights in the field of employment, social security, and social protection law. This is to be authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

However, the disadvantage is that in this environment, personal biometric data is much

However, the disadvantage is that in this environment, personal biometric data is much less protected: for example, cards often get lost and mobile devices could have shady apps installed that can read the data.

This environment meets data protection requirements - but in terms of IT security, the data is not secured or monitored. Consequently, both methods can only be used to a limited extent for highly secure data storage of critical data records.

Why is the split-template process better?

The split-template method uses the best of the methods described, taking it to the next level to make biometric data unrecognizable:

- First, critical data blocks are split into two or more data portions.
- The individual portions are then stored on different media and/or in different locations.
- Storage locations can be data carriers such as the RFID card AND the server within the IT infrastructure.

As a result of the split process, the biometric data collected is no longer considered personal data according to the GDPR. The split data can no longer be used for its actual purpose, as no conclusions can be drawn about the actual data record. Furthermore, when a storage location is compromised, cybercriminals do not gain possession of the entire biometric data. This effectively prevents them from creating a mock-up with the stolen data.

iCOGNIZE GmbH

iCOGNIZE ist auf biometrische Sicherheitslösungen spezialisiert. Seit 2007 entwickelt und produziert das Unternehmen biometrische Handvenenscanner zur Identifikation bzw. Authentifizierung die sich über unterschiedlichste Schnittstellen in andere Systeme der Sicherheitstechnik integrieren lassen. Technologien wie RFID und Bluetooth sind integraler Bestandteil des Produktportfolios.

Der Unternehmensstandort ist Dietzenbach - nahe Frankfurt am Main. Hier besitzt der Biometrie-System-Entwickler außerdem eine eigene Forschungsabteilung und kooperiert eng mit Hochschulen und anderen Forschungsinstituten, um Innovationen im Bereich biometrischer Sicherheitstechnik voranzutreiben.