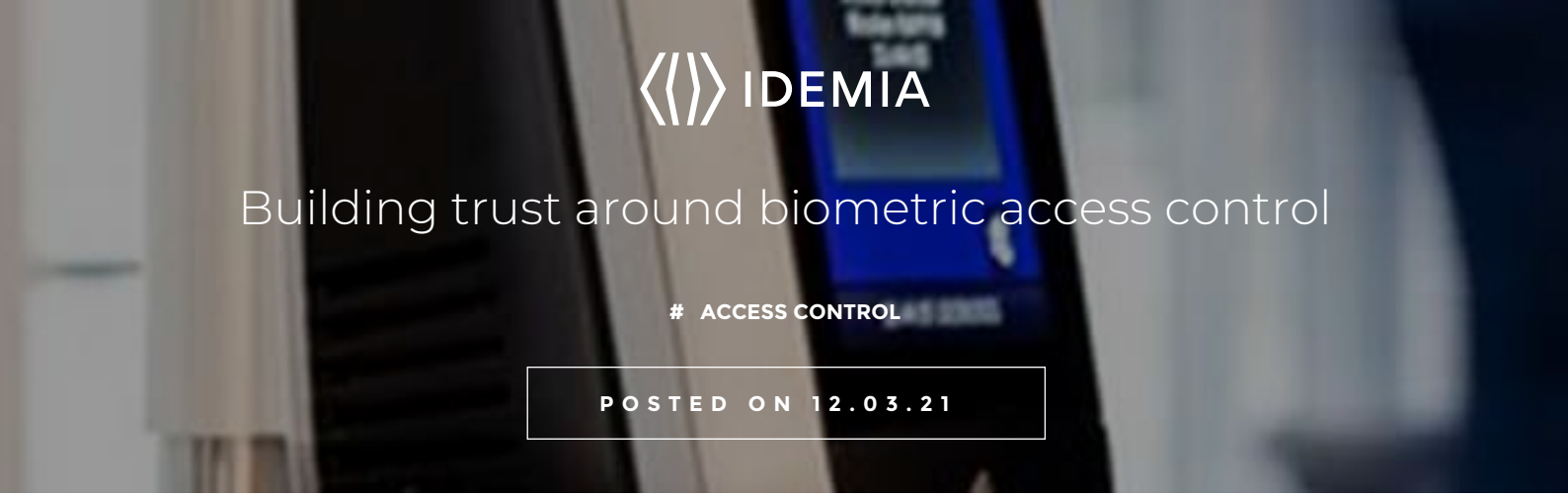


Building trust around biometric access control

ACCESS CONTROL

POSTED ON 12.03.21

As companies increasingly turn to biometrics to secure and streamline access control, they often encounter one common hurdle: easing the concerns of those who may be weary of the "futuristic" technology. While they may not be familiar with the specifics of biometrics data privacy and regulatory aspects, very rigorous processes are in place to protect the personal data of employees and visiting clients and guests.

Common misconceptions about biometric data

First off, it is important to understand that biometric devices and systems only use biometric *templates*—**they don't store entire fingerprint or face images** as many might assume. Each template consists of a selection of random points of a fingerprint or facial scan. These points are encrypted and stored anonymously.

All of this means that in the off chance that someone unauthorized manages into a company's system, the stolen data is useless. The employee **data points cannot be reconstituted** to create an entire fingerprint or facial scan. Also, companies cannot cross reference employees' biometric templates with national registries or any other external databases. In short, the secured template serves one sole purpose: to identify the employee onsite and grant access. Period.

Protecting biometric data privacy and guiding company practices

Employees can rest assured that their data is also protected by **several national and international regulations**. One of the most recent, and perhaps farthest reaching, is the General Data Protection Regulation (GDPR). Companies need to comply with these legal guidelines, put in place to give European citizens control over their personal data. One of the key GDPR rules is that **employees must provide explicit consent** for the use of their biometric data—and can withdraw consent at any given moment.

GDPR requires that companies **prove the need for biometric access control** on their premises, through a Data Protection Impact Assessment (DPIA). Through this self-audit process, they will have to explain in particular, why they need biometrics for identity management, what devices they will use and how these devices will be deployed, **how they will collect and protect data**, and provide a detailed list of people who will be able to access to the data.

These efforts combined, not only help to put employees' minds at ease, but also ensure that companies use and store data properly and according to the highest regional and international standards.