timeware®
Workforce Management Systems

ON PREMISE SOFTWARE

timeware® Biometrics and Data Security

suprema
SECURITY & BIOMETRICS

Suprema's biometric solutions, including face authentication and fingerprint technology, do not store photographic images. Instead, they create encrypted mathematical templates derived from key features. These templates are securely stored on the device and cannot be reversed into a face or fingerprint. Compliant with ISO standards, such as ISO 27001 for information security, ISO 27701 for privacy management, and ISO 30107-3 for anti-spoofing, they ensure data protection. This approach, used for both facial and fingerprint biometrics, offers customers peace of mind, knowing that their staff's biometric data remains private, secure, and aligned with international standards.

Why Face Authentication?

To ensure the highest standards of data protection, Suprema's software and hardware devices are meticulously designed and developed in compliance with ISO/IEC 27001, ISO/IEC 27701, and GDPR (General Data Protection Regulation). At every stage of product design and development, Suprema strictly adheres to GDPR, the world's most stringent privacy and data protection law.

To showcase Suprema's commitment to data privacy and security, Suprema announced the terminology change to 'Facial Authentication' instead of 'Facial Recognition'. Because 'Facial Recognition' identifies faces through detection and surveillance. However, 'Facial Authentication' emphasizes user consent. Suprema's security ensures authentication only with explicit user agreement, setting us apart from passive recognition methods.

Adding to this, Suprema's exclusive authentication method 'Template on Mobile (ToM)' securely stores facial templates on users' smartphones, eliminates the need for reliance on company servers for biometric data storage. This mitigates the need to entrust companies with the protection of their sensitive biometric data and significantly aids organizations in achieving GDPR compliance by eliminating the necessity of storing users' biometric data on central servers, thus decentralizing data management.

(See Suprema 'Biometrics GDPR document')

Data Protection Impact Assessment

Before introducing biometric attendance technology, organisations should complete a Data Protection Impact Assessment (DPIA), consult with employees or staff representatives, and provide clear documentation explaining how biometric data will be processed, protected, and retained. As biometric information is classified as special category data under UK GDPR, organisations should also consider their lawful basis for processing and whether an alternative non-biometric attendance method should be made available.

CYBER ESSENTIALS PLUS

Citation ISO Certification
Management System Standards
ISO 9001: 2015
ISO 14001: 2015
ISO 27001: 2022
REGISTERED
Certificate No: IMS-491342025, 509932026

Company Name: timeware (UK) Ltd.
Registered Office: 3 Fieldhouse Road, Rochdale, Greater Manchester, OL12 0AD.
Company Reg. No: 05886806.
Registered in: England.

t2-0674. Copyright NMD³ Ltd

www.timeware.co.uk
support@timeware.co.uk
+44 (0) 1706 658222