Chronologic Ltd
Biometric Terminals - GDPR Considerations

Introduction

Biometric terminals have become increasingly popular as they are able to keep more accurate track of employees' time and attendance. Unlike RFID clocking terminals you don't need to issue swipe cards or fobs, (or replace them when they inevitably get lost).

Also with a biometric clocking system there is virtually no risk of buddy clocking as biometric characteristics are unique.

The purpose of this document is to clarify how biometric terminals in the workplace work and how GDPR relates to the use of biometric data for clocking in employees.

How biometric terminals work

Different types of biometric clocking terminal use a person's physical characteristics, such as fingerprints, face or hand. The way the codes are created are unique to each type of terminal.

When an employee is first registered on a biometric terminal, a range of sample points are scanned which are then put through an algorithm and a unique code or template is created, i.e. a string of encrypted data. The template is stored on the clocking system as a baseline against which the terminal subsequently looks for a match.

Once registered, when the employee places their finger for example, on a biometric fingerprint scanner, the system attempts to match a stored template with the reading of the live scanning sample points to verify the individual and record their clocking activity.

Facial recognition works in exactly the same way. We do not use terminals that capture images of a face. The face is again sampled and an encrypted code created.

Biometric terminals only collect a small amount of biometric data and it is a one-way process. The stored code doesn't contain enough data to recreate in any way the complex physical characteristics of a fingerprint, face or hand.

Impact of the General Data Protection Regulations ("GDPR")

GDPR is Regulation (EU) 2016/679 of the European Parliament of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. GDPR came into force on 25 May 2018.

Article 5(1)(f) of the GDPR states that personal data shall be:

'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'. The GDPR has further considerations in Article 32, 'security of processing' and allows for: 'pseudonymisation and encryption of personal data'

The biometric terminals supplied by Chronologic satisfy the GDPR requirements of Article 5(1)(f). As the biometric data is securely encrypted and irreversible to its original image, it does not need to be separated from an employee record and separately deleted.

Data Housekeeping and terminals

As a practical 'housekeeping' measure it is useful to remove a leaving employee's template from clocking terminals of all types and the system databases to ensure your organisation isn't storing obsolete clocking data.

Applicability

This document is applicable to all types of biometric terminals used by the Chronologic WFM systems, uAttend and Citadel.

Disclaimer

Chronologic Ltd is a technology-based business and does not provide legal advice to its customers. This document is provided in good faith as our understanding of the technical operation of the biometric terminals that we supply and our general knowledge of GDPR. If you need detailed legal advice on GDPR and its implications you should seek advice from a member of the Law Society or equivalent legal background.