Time & Attendance and Biometric Data

Owner: Legal
Classification: **PUBLIC**

How does Fourth's Time & Attendance solution use biometric data?

Biometric authentication measures the unique, invariable biological characteristics of an individual. One of the most common uses of biometric data is fingertip information to authenticate an individual's identity, for example as part of Fourth's Time & Attendance solution.

Fourth sources the clocks for its Time & Attendance solution from a third party manufacturer (Synel). .

The clocks allow an individual to "swipe in" and "swipe out" in order to register attendance. The biometric (fingertip) information is initially captured during the enrolment of the individual and immediately translated into a ***template*** (akin to a barcode, using an algorithm). This template cannot be used to reconstitute the fingerprint itself, rather the template is a form of one-way encryption. The algorithm cannot be reverse engineered to obtain an image of the fingerprint.

Neither the fingerprint, nor an image of it, is stored, either on the clock or elsewhere.

What personal data is stored?

The template created from the fingerprint information is linked to the employee's name, number and badge number; therefore, personal data is stored on the clock (or on the hosted server – see "Where is the personal data stored?" below), but **not** biometric/sensitive personal data.

During each subsequent authentication of an individual, the biometric information is again captured, immediately translated into a template, and compared against the stored template. If the individual is a valid user, the two algorithms will match, and authentication is achieved. To put it another way, each time an individual scans their finger to register attendance, the clock recreates a template from the scanned fingerprint information using the algorithm and the two templates are compared to determine the identity of the individual.

Where is the personal data stored?

The Customer's use of the clocks determines where the personal data is stored.

1. **Where the clocks operate at Customer Sites independently (i.e. where staff only work at one site)** – the personal data will be stored in the database on the hardware (clock) for subsequent authentications.

2. **Where the Customer has multiple clocks which work together (i.e. where staff are able to authenticate their fingerprints between multiple Customer Sites)** - the personal data will be stored on the hosted server. For USA Customers this will be located in the USA. For all other Customers, this will be located in the EEA.

If you have further questions about how fingerprint data is used by Fourth solutions, please contact your Customer Success Manager for more information.

29 January 2018