CBSYS Biometric Data Privacy Statement

This privacy statement applies to the ZK Technology Corp Clocking device and Microsoft Azure facial recognition services. It governs the privacy practices of both ZK Technology, Microsoft and CBSYS Ltd with respect to the Privacy Commissioner New Zealand.

Facial / fingerprint image

When accounts are created in the system, facial templates / fingerprints can be linked to the account by presenting / scanning of user's face / fingerprint on the device scanner or camera.
The facial image is displayed on the screen as a verification to the end user when they are using the device for the time attendance or door access.
It is also unfeasible to reconstruct a fingerprint/ facial image with the information from users biometric data as only the sampled points are recorded, not the entire fingerprint or face.

Customer Biometric Data

Customer biometrics data will be used only to provide customer the services including purposes compatible with providing those services. For example, we may use biometric data to identifying user, providing them ability to log their time and job. We will not use biometric data or derive information from it for any purposes other than identification and verification within the services.
CBSYS product and system will control all access to biometric data other than access initiated by you or your end users, neither ZK or Microsoft will have access to biometric data except when such access is granted by CBSYS Ltd for the purpose of ZK, Microsoft resolving a customer support incident or problem or where such access is required for them to perform maintenance or improvements.
Again biometric data is not an image, they are sample points measurement data.

Software

CBSYS services requires, or maybe enhanced by, the installation of local software, web based software or smartphone/ tablet apps. These software may transmit biometric identification data and time data from a device/app to or from CBSYS only, in a case where facial recognition is required over smartphone / tablet, data will be sent to Microsoft to complete the facial recognition task.

Security

We are committed to helping protect the security of your information that includes any biometrics data. We have implemented data encryption and will maintain appropriate technical and organisational measures intended to protect your information / data against accident loss, destruction, or alteration; unauthorised disclosure or access.

Data Location

Data will be stored solely within our server in Sydney, Australia, CBSYS services do not control or limit the regions from which you or your end users may access data