Data and Security Statement

This Data and Security Statement applies to the products, services, websites and apps (**the Services**) offered by Virtech Pty Ltd which are branded as EzyCheckin. This Data and Security Statement also forms part of the terms and conditions of the End User Licence Agreement for EzyCheckin customers.

Your Privacy and Data Protection Laws

**Personal data** is data subject to protection under privacy legislation. In Australia, privacy legislation means all applicable privacy legislation, including the *Privacy Act 1988 (Cth)*, regulations as amended and any similar applicable laws. We take our responsibility under the privacy legislation to protect and secure your personal data seriously and strive for complete transparency around our security practices. Our Privacy Policy further details the ways in which we handle your personal data.

Security Policies

We maintain and regularly review and update our information security policies. This includes full end-to-end encryption using Google Firebase Authentication and Firestore as the database. Personal data is encrypted when you enter it, and is then encrypted in transit.

All personal data is stored in encrypted form at our data centre hosted in Sydney, Australia in accordance with security controls including ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2 and SOC 3.

Process for release of contact tracing data

Each venue in EzyCheckin is assigned a private password. This password can only be released by the venue to a public health officer in the event that the public health officer requires the data for contact tracing purposes or contact tracing compliance purposes. No Venue will have access to any personal data. This data will only be provided to authorised public health officers.

Public health officers will contact a business if a person diagnosed with COVID-19 states that they attended the business during a time that they may have been infectious. This can be in person or via telephone. Public health officers will then request the details of each guest and staff member for a specific date and time period.

The venue owner will provide their password to the public health official and contact details for EzyCheckin Support. The public health official will then contact EzyCheckin with id verification details which EzyCheckin support will verify..

EzyCheckin support will then provide the data specific to that venue to the public health official for contact tracing purposes. This activity will be logged (that is, date and time, whether the request was made for a compliance check or for contact tracing), the public health official who made the request and their relevant ID.

We will delete all personal data held by us on a rolling 56 day cycle, or as required by law.

For further information about data privacy and security practices, please contact us at ezycheckin.com.au

This statement was last updated 8 October 2020.