Timesheetz Security Document

Introduction

Timesheetz is a product of ETZ Payments Ltd (ETZ). ETZ continually strives to meet and exceed the latest standards of security for Timesheetz customers and users. This document summarises the methods ETZ employs to address the key components of security: confidentiality; availability; integrity; privacy; authentication; authorisation; availability.

Shared Responsibility Model

The shared responsibility model defines the responsibilities of ETZ, the cloud platform provider (Microsoft Azure), and the user:

- Microsoft Azure is responsible for the security 'of' the cloud (infrastructure).
  - ETZ is responsible for security 'in' the cloud:
  - User data.
  - Platform, applications, identity and access management.
  - Operating system, network and firewall configuration.
  - Encryption and data integrity.
- User responsibility: password security.

Infrastructure & Physical Security

Timesheetz is hosted on Microsoft Azure infrastructure and leverages the native security available through Azure.

Database Security

Timesheetz uses Microsoft Azure SQL Database to store and access the database securely on the cloud. Microsoft Azure SQL Database provides encryption for:

- All structured data at rest.
- Unstructured data at rest in blobs, files, tables and queues.
- Transport layer security for data in motion.
- Transparent data encryption for data at rest through.
- Data in use.

Data Centres

Azure data centres are managed by Microsoft with access approval at the facility perimeter, building perimeter, inside the building and on the data centre floor. This approach mitigates the risk of unauthorised physical access to the data and the data centre resources.

Data Location

The Timesheetz database and backups are stored in Northern Europe. Documents are stored in the region where the client's AD Tenant is based (e.g. if ACME recruiting is based in Australia, their docs will be in the APAC region).

Microsoft Azure Compliance

Microsoft Azure is compliant with:

- ISO/IEC 27001:2013 Information Security Management Standards.
- ISO/IEC 27017:2015 Code of Practice for Information Security Controls.
- ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud.

- Cloud Security Alliance STAR (Security, Trust and Assurance Registry) attestation and certification.
- Content Delivery and Security Association CPS (Content Protection and Security) Standard.
- EU Data Protection Directive 95/46/EC (transfer of EU customer personal data to countries outside the European Economic Area).
- Cyber Essentials Plus (UK), cyber security risk mitigation.

Availability

Microsoft Azure provides numerous levels of redundancy to ensure maximum availability of Timesheetz. Azure SQL Database guarantees the Timesheetz database is running 99.99% of the time.

Administrative and Personnel Controls

ETZ employees are serious about confidentiality. Employees undergo training and are subject to confidentiality agreements to ensure that personal data is:

- Processed fairly and lawfully
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

Data Disposal

Physical documents are shredded, and digital storage devices such as hard drives and USB drives are physically destroyed when they are no longer needed.

Employee Access

The principle of least privilege is applied to employee access. This means that employees are given the minimum set of access privileges required to achieve their duties. When the duties of an employee change, the access privileges are updated accordingly. When an individual's employment ceases, all access privileges are rescinded, and confidentiality agreements persist.

Application Security

Access Control

Timesheetz permits clients to configure access both by user and by role. This means that clients can control which roles or individuals have access to which sets of information.

Authentication and Authorisation

Goowid identity server powers user authentication and authorisation for Timesheetz. Goowid uses Transport Layer Security cryptography to encrypt communications between Timesheetz servers and web browsers and provides secure delegated access by issuing security tokens. Security tokens control user access to Timesheetz. Goowid was last pen tested in April 2019.

IP Range Based Authentication

Timesheetz can control access by IP address. This allows IP addresses within a range that is suspected of belonging to malicious users to be blocked.

Development

Timesheetz is developed and maintained with security in mind. Our developers use best practice development methods including Open Web Application Security Project (OWASP) tools and documentation to ensure that Timesheetz is built and maintained to industry accepted security standards.

Logging and Auditing

ETZ uses a variety of logging and auditing tools to monitor systems and information for any suspicious activity, security-related events, or triggered security detection systems. This can assist in the identification and investigation of any potential security incidents. Retention for sensitive data logs is a maximum of 14 days.

Service Level Security

Timesheetz provides security between users and the service using HTTPS/TLS. This authenticates the Timesheetz website to the user and protects the privacy and integrity of data exchanged between user and Timesheetz with encryption.

Security and Penetration Tests

ETZ audits Goowid (Identity server used by Timesheetz) with independent penetration testers on a regular basis and with every major release to identify any potential vulnerabilities. Any identified weaknesses are resolved prior to release by our in-house development team.

Data Breach Response

Background

ETZ has a designated Data Protection Officer who is responsible for ensuring that ETZ adheres fully with current data protection legislation and closely follows the Data Protection Regulator's suggested best practices. This includes ensuring that a methodology is in place to address any data breaches that although are unlikely to occur, may nevertheless occur.

Data Protection Legislation is concerned only with personal data (general personal data and sensitive personal data). Personal data is any data capable of identifying an individual. There's the EU's General Data Protection Legislation 2018 and the UK Data Protection Act 2018 (which transposes the GDPR into national legislation). The legislation applies to any company providing goods and/or services to EU residents and is considered to be the global standard for data protection.

The Regulator's primary concern is that of data containment in the event of a data breach. The Regulator also requires any data breach to be notified to it within 72 hours and to those affected as soon as is practicable. As per the guidelines, in the event of a breach, ETZ will assess the likelihood and severity of the resulting risk to individuals' rights and freedoms. High risk situations affecting individuals' rights and freedoms require notification, whereas low risk situations not affecting individuals' rights and freedoms do not require notification, but nevertheless records will be kept by ETZ in line with best practice.

Why is This Important?

As explained in Recital 85 of the GDPR:

> "A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights,

discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Response Steps

Phase 1: Fact-Finding

- Assess the nature of the breach, how, when, what time, why, who was affected, who reported it.

Phase 2: Crisis Response

- Containment of the data.
- Analysis of the content of the data.
- Assessment regarding reporting duties – considering whether the breach poses a risk to individuals' rights and freedoms.
- Notification to customer, and if relevant to the Data Protection Regulator.

Phase 3: Reports

- Control gap analysis and make good the gaps by implementing solutions to ensure there are no repeats. This could include further targeted training, implementation of further controls or abolition of faulty controls.
- Investigation Report. ETZ will always notify customers of any data breaches, whether big or small, and will produce a full investigation report to provide to customers.

Disaster Recovery

Certain incidents such as natural disasters can be difficult to anticipate and plan for but have the potential to disrupt business operations. Microsoft Azure provides numerous levels of redundancy to ensure that Timesheetz is resilient against unexpected major incidents. Additionally, ETZ makes use of Azure's disaster recovery solution and geo-redundant storage.

> "Geo-redundant storage (GRS) is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year by replicating your data to a secondary region that is hundreds of miles away from the primary region. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable." (www.microsoft.com, April 2019)

Website Infrastructure

The web application runs in a server cluster for scalability, availability and reliability. The server cluster provides redundancy in case of any hardware failure across any of the web servers.

Data Backup

Timesheetz database runs in Azure SQL Server and is automatically backed up with point intime restore. Backups are retained for 35 days.

Document Backup

All documents are stored within Azure Storage V2, with Geo-Replication in place.

Additional Resources

An introduction to Microsoft Azure security:

https://docs.microsoft.com/en-us/azure/security/azure-security