Document Reference: TC013
Version Number: 1.2

Data Security

Prepared by: Zoë Mouter
On: 2nd May 2024
Last updated on: 1st July 2024

Table of Contents

1. Data Processors and Sub Processors

1.1. Egress Systems Ltd, company number 04872869, work with two partners to provide our hosted Focus Net Time & Attendance solutions: HR Industries Ltd, company number 05487860 and Dolphin ICT Ltd, company number 06206916.

1.2. HR Industries Ltd own the copyright to the Focus Net Time & Attendance software provided under the Hosting Services agreement and host the Focus Net web application. They provide development support to Egress Systems in the form of bug fixes and product enhancements. HR Industries have no unattended access to the data servers hosting customer data.

1.3. Dolphin ICT provide Egress Systems with a range of IT services to enable Egress Systems to provide the Hosting Services. These include provision of high availability virtual server hosting, software subscriptions services, licencing management, back-up services, server monitoring and management and managed anti-virus. Egress Systems have a service level agreement with Dolphin ICT to ensure optimal availability of the Hosting Service. Dolphin ICT have access to Customer data servers and process the data in terms of providing backup services.

2. Data Server Security

2.1. For our fully cloud based service the customer's data is stored on Microsoft Azure UK based data servers on an SQL Express database.

2.2. The customer's data is stored in a discrete SQL Express instance and is not visible to other customers. No database sharing between customers is possible or permitted.

2.3. Customers can optionally choose to have their data stored on their own servers and implement their own security infrastructure. In this hybrid architecture, no customer data is stored on Egress Systems' servers.

2.4. The customer's data never leaves the cloud service apart from backup purposes (see below), unless agreed with the customer. Typical instances where this may be agreed with the customer are when sharing data with a third-party HRIS application via the Focus API or third-party API.

2.5. Access to the Egress Systems' Azure servers is limited to a small pool of support personnel and our designated IT service providers, Dolphin ICT Ltd.

2.6. Access to the Azure servers is via IP Secured Remote Desktop Access secured via an SSL certificate, so data in-transit is encrypted. Two factor authentication is in operation.

2.7. From time to time, HR Industries development staff may be granted temporary access to the customer data servers when aiding Egress Systems in resolving problems. This access is only granted through a secure, encrypted, permission-based service initiated by Egress Systems and is actively monitored by Egress Systems staff throughout the duration of the access. Access is terminated at the end of the support session.

2.8. All access to the customer server is enabled, logged and auditable using Azure controls.

2.9. Data is never transferred outside of the EU for EU based customers.

3. Data Backup Security

3.1. Our cloud servers are backed up using Cove Data Protection and physically held in N-Able's UK based Data Centres which are ISO 27001, ISO 9001, PCI DSS, SOC 1 Type II and SOC 2 Type II compliant.

3.2. Cove Data Protection uses AES 256-bit encryption, in transit and at rest.

3.3. Backups are encrypted on-site, then transferred over one-way TLS 1.2 connections and stored encrypted in the cloud. Backup data is only decrypted during a recovery process.

3.4. Full image incremental backups are taken at a minimum daily up to hourly, depending on the server.

3.5. In addition to the full server image each individual customer's database has a separate SQL backup taken daily enabling discrete customer database recovery without affecting other customers in the event of accidental data loss.

3.6. Full server image and SQL backups are kept for for 90 days for each customer so if personal data is removed from your own Focus system it will automatically disappear from all active backups after 90 days.

3.7. Data recoveries are tested by Dolphin ICT biweekly.

4. Web Application Security

4.1. Focus Net web servers are hosted on Amazon Web Services (AWS) at AWS data centres located in Dublin and Ireland, managed by the Focus Net application developers HR Industries Ltd.

4.2. HR Industries have a virtual private network setup meaning only they can access the servers, and they can only do so from their single fixed office IP address. Egress Systems and Dolphin ICT personnel have no access to the AWS servers at any time.

4.3. Internal AWS tools are used for general monitoring of the AWS web server servers. HR Industries also have a custom program called Focus Cloud Control that monitors each customer's website instance for outages, timeouts, errors or other information. Loss of service is actioned within five minutes.

4.4. A multiple server architecture is in place ensuring server redundancy for all servers and a spare server is always available to act as a replacement in the event of catastrophic failure for existing servers.

4.5. No customer data is held on any AWS server and therefore HR Industries can replicate the licensing database on each new server.

4.6. HR Industries have referred to the CIS Benchmarks during their system design, specifically for:

CIS Microsoft IIS 10 Benchmark

CIS Microsoft Windows Server 2019 Benchmark

CIS Microsoft SQL Server 2019 Benchmark

CIS AWS Compute Services Benchmark

4.7. HR Industries carries out regular penetration tests using a platform called Detectify (https://detectify.com/) on their own test servers. They do not intrude upon individual customer installations.

4.8. Users are given complex password management tools, including the ability to set requirements of length, numbers, special characters, along with expiry periods and 'previously used' limits. Users may also use two factor authentication to access the Focus software.

5. Proxy Service Security

5.1. The Focus Net Cloud Proxy Service provides access to the designated database server from the Focus Net website. This is a Windows service which is installed with SQL server. It connects to the Focus Net website on SSL and exposes specific APIs to the website on the SSL connection (not HTTP). These APIs are a WCF Duplex callback contract. This means it they are only available when a connection is made to the website.

5.2. Each customer has their own discrete proxy service installation on the database server securely registered with a unique serial number that links it to the singular customer database.

5.3. The Focus.net login page is secured with a company key unique to each customer. Without the unique company key users will be unable to access the login screen.

6. Biometric Data Security

6.1. Egress Systems processes biometric data when biometric terminals (fingerprint or facial recognition) are purchased alongside the Focus Net application. The vast majority of terminals offered by Egress Systems are manufactured by Suprema inc. Specific GDPR and data encryption information from Suprema can be provided on request.

6.2. Suprema terminals also offer alternative methods of clocking by RFID card, or via ID + PIN which enables customers to give their personnel the opportunity to opt out of biometric data collection and still be able to use the clocking terminals.

6.3. Biometric template protection is offered through the four principles outlined in ICO guidance of irreversibility, unlinkability, revocability and renewability.

6.3.1. Irreversibility and security: the biometric template is stored in the form of an encrypted binary string, not as an image. As such the data subject's face or fingerprint cannot be reconstructed from the biometric template as insufficient information is present.

6.3.2. Unlinkability: the template formats are proprietary to the manufacturer so it would not be possible to share the biometric data between biometric recognition systems of different manufacturers.

6.3.3. Revocability and renewability: biometric templates can easily be revoked or cancelled either on the devices directly or via the Focus software. The templates could be replaced if held within the Focus database without the need to take a new biometric sample.