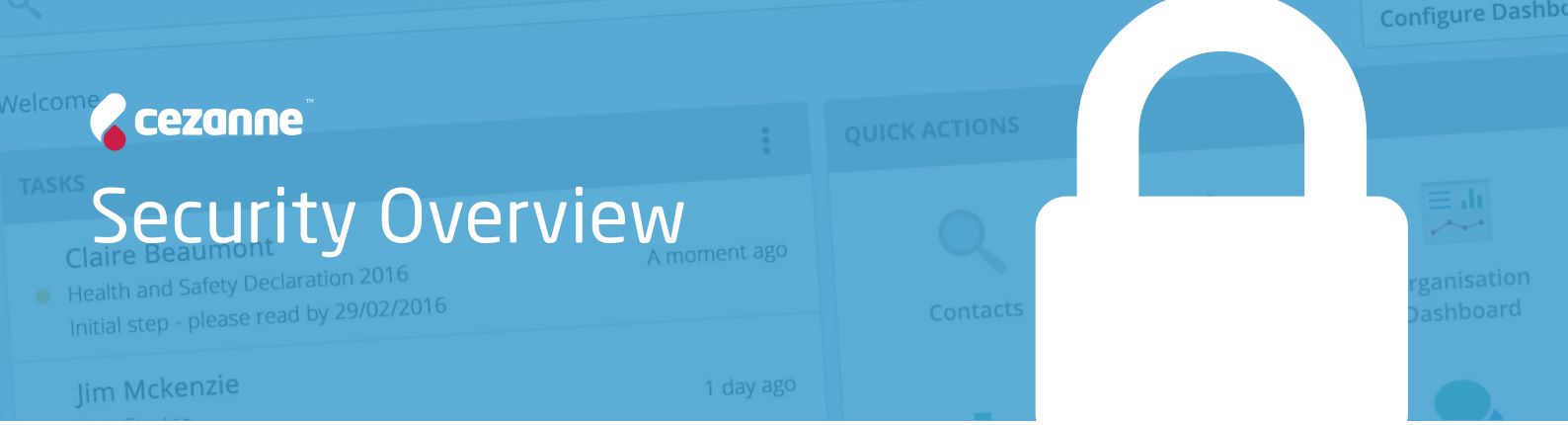

Security Overview

As a team, we have a long history of developing and delivering HR software solutions to customers worldwide, including many of the world's most-demanding organisations.

We know the value of your HR data – and the importance of keeping it safe – and we constantly review our service in the light of evolving best-practice.

End to end security

Security is at the heart of what we deliver, from the architecture of the Cezanne HR application to on-going third-party penetration testing to hosting with the world's leading specialist Cloud infrastructure provider, Amazon Web Services (AWS) from their European data centre in Ireland.

This paper provides an overview of the approach we take to providing you with a robust, secure HR software service.

Secure by design

N-tier application architecture

Cezanne HR is designed around a multi-tiered architecture that is recommended for web-based applications. The architecture partitions application functionality into independent layers: the presentation layer (or browser client), the business logic (application server) and the data layer (database).

The presentation layer never communicates directly with the database layer. All communication is performed via the business logic, which provides its own security checks before permitting access to the data. This prevents requests from a web browser going directly to the database. The application also verifies the user role at every request.

Data encryption

The service makes use of strong encryption to protect customer data (which is stored on an encrypted file system) and communications, including SSL Certification from Network Solutions. SSL (Secure Sockets Layer) is the standard security technology for creating an encrypted link between a web server and a browser. You will know you have created an SSL link when the URL is in green, begins with "https://" and there is a padlock symbol either at the beginning or end of the URL.

User authentication

Secure mechanisms are used to verify the identity of users attempting to access the system. Customers have the option to enhance the standard combination of username (e-mail address) and password by enabling dual authentication (2FA) via email and/or an authentication app on a mobile device, or by integration with an approved Single Sign-On (SSO) provider.

Cezanne HR supports a number of Single Sign-On options which customers can enable. These range from industry standards, such as SAML2 (allowing users to sign in via their Active Directory accounts) and OpenID, through to social accounts, such as Google, Twitter or Facebook.

Passwords

Passwords are protected using sophisticated hashing and salting techniques; Cezanne HR only ever stores hashes of password, never the passwords themselves.

Customers can set rules in the system to enforce a strong password policy, including:

- Mandatory inclusion of at least one upper and lowercase letter, one number and one symbol
- Minimum and maximum passwords
- Expiry date reminders
- Password history to prevent users re-using their passwords within a customer-defined period
- Maximum number of failed login attempts before the account is temporarily locked.

User authorisation

User authorisation is controlled through dynamic roles-based security. Users are allocated to roles, such as HR administrator, restricted HR administrator, line manager or self service employee. The system then dynamically allocates permissions to individual users to view, change or delete information, or access different areas of functionality, based on their responsibilities in the company. For example, line managers can see more information about the employees that report to them than those employees who do not.

Importantly, Cezanne HR has been developed with embedded business intelligence functionality. This means that access to dashboards, queries and data exports are controlled by the same rules as those that govern access to features or information in the database.

Return of data

Should you decide to stop using the Cezanne HR service, you have the option to use the system's standard query functionality to export your data, or you can ask us to export your data for you. Exported data is provided in csv format via a secured process. Your data will be removed from our servers following the end of your subscription contract.

State-of-the-art-hosting

We have chosen to host the Cezanne HR software service with AWS (Amazon Web Services) at their European data centres based in Ireland. AWS is acknowledged as the world-leading Cloud Infrastructure as a Service provider. Its data centres are proven, secure and reliable and their certifications cover ISO27001, SOC 1/SSAE 16 (previously SAS70), SOC 2, SOC 3 and more. AWS has confirmed that they will comply with GDPR when it becomes enforceable on May 25, 2018, as will Cezanne HR.

The AWS infrastructure also has a number of built-in security features, such as distributed denial of service (DDoS) protection and password brute-force detection on AWS accounts.

Hosting your data in Europe is especially important in the light of the ruling on October 6th 2015, when the European Court of Justice determined that the 15-year-old US-EU Safe Harbor framework is no longer valid for the transfer of personal data from the European Economic Area (EEA) to the US.

For further information about AWS EU data protection compliance please visit: https://aws.amazon.com/compliance/eu-data-protection/

Operating system security

Operating system instances are hardened by disabling or removing any non-essential tools, utilities and other system administration options that might provide potential backdoor entry to the system, and by disabling or removing any unnecessary users, protocols, and processes. Our installation and configuration procedures are based on industry-recognised standards and tools.

Server management security

Cezanne HR does not have physical access to the data centre or physical machines as this is prohibited by Amazon. Cezanne HR can access the virtual machine instances for the purpose of; maintenance, applying security updates, monitoring and ensuring backups are running successfully. This is limited to senior and long-serving members of Cezanne HR's Managed Services team.

Resilience

When purchasing a Software as a Service (SaaS) solution, it is critical that the service is resilient and reliable. To ensure high availability the Cezanne HR software service includes:

- Installation in multiple EU data centres – your Cezanne HR software will continue to operate if a machine or data centre fails
- 24 hour monitoring – the availability of the system is monitored continuously and an alert sent to the support team if a problem occurs
- Elastic load balancing – extra computing resources are added dynamically if needed, for example during times of peak usage
- External monitoring from locations around the globe to alert Cezanne HR to unexpected latency or DNS problems
- Monitoring of resources including CPU, disk and memory usage so we can scale as and when required.

Data protection and ownership

Data controllers and data processors

It's important to know that you not only own your data, but are the data controller as defined by data protection legislation. Cezanne HR merely acts as a data processor; will only process data in accordance with the instructions of the data controller; and will maintain, together with our hosting providers, sufficient technical and organisational measures to safeguard personal data.

That means that as well as considering the service and security that we provide, you should look at your own environment and processes in order to ensure that you comply with the relevant legislation. This may extend to your company's data security, password policies, employees' use of their own devices and browsers, as well as the IT infrastructure you have in place – such as firewalls and anti-virus software.

As required by data protection legislation, Cezanne HR Limited is registered with the Information Commissioner's Office. Registration reference: Z362387X

For information about your responsibilities under the Data Protection act please visit: https://ico.org.uk/

cezanne™