Cezanne HR security and GDPR overview

Index

Secure by design

Advanced protection for your HR data

As a team, we have a long history of developing and delivering HR software solutions to customers of every size and in virtually every industry sector – including many of the world's most demanding organisations. We know what it takes to deliver robust, secure, international HR systems across the internet.

We not only designed our HR service for security, and to comply with EU data – and now GDPR – requirements, but have regular penetration testing by an expert third party, so you can be sure that our security is independently validated, and our system really does meet the high standard of security your HR data demands.

Built on best practice

Cezanne HR is designed to enable robust, fast, safe use across the internet, and to protect the security and integrity of your HR data and your HR system. From system architecture and data encryption to advanced options for user permissions, passwords and dual authentication, security is at the heart of what we design and deliver to you.

GDPR: General Data Protection Regulations

The GDPR introduces a major overhaul of the European data protection regulation. While the key principles of the GDPR are the same as those that have been in place since the introduction of legislation based on the European Directive of 1995, there is now a much greater emphasis on transparency and accountability.

This section details how Cezanne HR as the data processor complies with specific requirements of the GDPR.

To learn how Cezanne HR helps you with your own GDPR compliance, download this guide.

We are compliant with the provisions of articles 28(1), 32(1) and 32(2), in the sense that we have implemented "appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation". The measures implemented include, but are not necessarily limited to, the following:

- All data are encrypted both at rest and in transmission;
- All accesses to the system are monitored and logged (both successful logins and attempted logins);
- All modifications of personal data are timestamped and tracked in a log;
- Personal data belonging to the controller are only stored in cloud locations within the AWS service that offer high physical and logical access protection, including cyber security against viruses, malware and denial-of-service attacks;
- Ongoing confidentiality of data is assured by state-of-the-art authentication methods, which the controller can tune as required (in terms of password length, composition and duration);
- Ongoing availability of data is assured by constant monitoring of the system in multiple locations world-wide and rapid response processes in case of system stress or other performance issues;

- Resilience of processing systems is assured by use of multiple data centres and of mirror copies of databases;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident is assured by an appropriate backup/recovery procedure, which is periodically tested;
- The protection against unauthorised access to personal data is constantly checked through penetration testing performed by a reputable cybersecurity organisation;
- All security measures are regularly reviewed, also in light of the evolution of the technology and the cybersecurity industry.

We are compliant with the provisions of articles 28(2) and 28(3), because we have revised our Terms and Conditions to include all of the provisions that the law requires.

We are compliant for what concerns the physical location of data, as the agreement in place with our hosting provider, AWS guarantees that data will never leave the AWS region of Ireland, and the potential access to data by Cezanne HR's support personnel is in any case limited to access from the UK or from other EEA countries.

We have data processing agreements with all sub-processors are fully consistent with all the commitments we have with customers, including the assurance that no personal data is ever transferred or processed outside the EEA.

We are also compliant with other aspects of the GDPR, such as:

- We have procedures in place to manage potential data breaches.
- We are committed to assist our customers in case of data subject request.
- We are open to audits and inspections if requested.
- All our personnel that may have access to customers' personal data is fully trained in data security and protection and is bound by confidentiality agreements.
- We have procedures in place to return and/or erase all personal data of

customers that have terminated their subscription to the system.

Although the law doesn't strictly require it in our case, we maintain the formal records in accordance with art. 30(2) of GDPR.

We have appointed a data protection officer in accordance with art. 37(1) of GDPR. The appointment has been registered with the ICO.

Although it is not a GDPR requirement, but only a facilitator to prove compliance, we are actively working towards ISO27001 certification and are using the UK's leading accreditation body, bsi.

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. In order to access the system the user must either enter a username (e-mail address) and password or authenticate through an approved Single Sign-On (SSO) provider.

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

You 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 password length.
- Expiry dates with reminders.
- Password history to prevent users re-using their passwords within a custom-er-defined period.
- Maximum number of failed login attempts before the account is temporarily locked.
- You can also choose which, if any, of the SSO options – e.g. Google, Microsoft, Twitter, Facebook and OpenID – are available to your users. Only identifiers that are secured with SSL can be used when the OpenID SSO option is enabled.

User Authorisation

User authorisation is controlled through dynamic roles-based security. Employees 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.

World-class hosting

Your HR software on the world's leading platform

Your Cezanne HR software service is hosted within Amazon's AWS European data centres. 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 and more. 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.

In addition, our contract with AWS states that they will not move any content from the European region without first notifying us. If this happens we will, of course, both notify you and take steps to ensure your content remains within the EU. This is especially important in the light of the recent changes to data protection legislation.

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

Internal System Security

Inside the AWS environment, the systems are further safeguarded by firewalls between layers, IP and port restrictions, private subnets and network routing restrictions.

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,

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.
- 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.

Please note: The information on this page relates to the modules developed by Cezanne HR. It does not cover third-party modules marketed by Cezanne HR that may have a different hosting and security architecture.

The use of Cezanne HR's software service is subject to the terms and conditions of the Cezanne HR subscription agreement. Cezanne HR reserves the right to modify its security infrastructure in accordance with this agreement. Please contact us if you would like a copy of this agreement.

About Cezanne HR

We've built something special at Cezanne HR; a powerful, configurable HR software solution that's simple to deploy, easy to manage and remarkably cost-effective, whatever the size of your business. As a team, we've a long track record of delivering successful HR solutions to businesses worldwide. We've worked with companies of every size and across every business sector. That's why we decided from the very start to build an exceptionally robust and scalable SaaS platform for human resources management which, like our customer community, is growing all the time.