

■ CASE STUDY

# AWO Rheingau-Taunus embeds **security and compliance** into its infrastructure with enclave

How the welfare organisation uses Confidential Computing to keep its email communications and document storage fully encrypted – while also reducing costs



300

PERMANENT STAFF

150

VOLUNTEERS

Four

DAY-CARE CENTRES

20+

SCHOOLS

## 01

## Overview

## Overview

**When it comes to digitalisation, organisations in the public sector often have to balance high data protection standards, limited budgets and a shortage of IT specialists. At the same time, there is a growing desire for greater digital independence from major foreign providers.**

AWO Kreisverband Rheingau-Taunus faced these very challenges. The independent organisation within the wider AWO association employs 300 permanent staff and works with a further 150 volunteers, operating four day-care centres and more than 20 schools across the Rheingau-Taunus district in Hesse, Germany, and the state capital Wiesbaden. In 2023, for reasons of cost and data protection, the organisation decided to move away from operating its own server and migrate its email communications and entire digital infrastructure, including all data, to an open-source solution. As part of the project, enclaive implemented a Confidential Computing architecture.

## 02

## Challenge

## Challenge: Sensitive data and stringent requirements

As a service provider for all-day childcare and school social work facilities, AWO RTK manages highly sensitive personal, health and incident-related data concerning several thousand children, as well as contact, payment and contractual information relating to parents and partner organisations. All of this information needs to be processed securely.

**“The worst-case scenario for us would be data getting into the wrong hands,”**

explains Michael Weigelt, Chairman of the Executive Board of the district association. “The information we process is highly private and personal. We would risk losing a great deal of trust among local authorities and families – not to mention failing to comply with statutory requirements.”

## 02

## Challenge

However, a historically grown IT environment, combined with limited IT expertise and awareness, had created challenges in terms of usability, data protection and costs. The existing setup, based on remote access technology from a major US provider including its operating system and application suite, resulted in high peak loads and an often sluggish user experience. There were also compliance concerns, particularly around insufficiently protected communications and data handling, especially with regard to requirements such as Social Code Book VIII (SGB VIII) – Child and Youth Welfare, the Hessian School Act, the Hessian Child and Youth Welfare Code and the GDPR.

At the same time, the AWO Rheingau-Taunus had grown rapidly within a short period, both in terms of headcount and revenue. This also made it necessary to rethink the existing setup from a cost perspective.

## REQUIREMENTS IN SCOPE

- Social Code Book VIII (SGB VIII) – Child and Youth Welfare
- The Hessian School Act
- The Hessian Child and Youth Welfare Code
- The GDPR

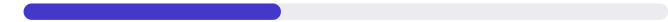
# 02

## Challenge

“We needed a solution that would meet our strict compliance requirements while remaining economically viable. Anyone familiar with the relevant providers will also know their licensing models – from the basic enterprise licence to applications including an email client, plus additional charges for storing data in Europe. And those licences are only valid for three years. On top of that, you always need the latest, and therefore expensive, PCs simply to run the current operating system,” says Weigelt, describing the cost challenge. “Our licences were costing around €40,000 for just under 100 existing users, while new devices would have cost us almost €100,000. That is why a fellow board member and I initiated the move to open-source software and decided to introduce new processes and a new security architecture at the same time.”

### THE COST OF THE PREVIOUS MODEL

Licences, just under 100 existing users ≈ €40,000



New devices almost €100,000



LICENCE VALIDITY • THREE YEARS

Weigelt has many years of experience in senior positions in the IT industry, including more than 30 years at IBM. Drawing on this expertise, he took the lead in planning the new IT infrastructure.

## 03

## Solution

## Solution: Encrypted data processing closes security and compliance gaps

The migration began in 2025 with the replacement of the hardware and the installation of Linux on the new PCs. To process its sensitive data securely and in accordance with compliance and data protection requirements, the district association chose enclave's Confidential Computing technology. This involved rebuilding both the email server and the document storage environment while ensuring that data remained encrypted throughout.

For AWO Rheingau-Taunus, it was particularly important that most of the implementation could be handled by external experts. The district association has only two IT employees, whose responsibilities are focused on user-facing systems.

### “enclave was a major help to us here”

says Weigelt. “Setting up your own email system is no small task. Servers need to be resilient and protected against data leakage. With mailcow, we had to install around a dozen system components, including SOGo, Dovecot, Postfix and spam filters – and all of them are now completely secure inside enclave's ‘blackboxes’.”

# 03

## Solution

AWO Rheingau-Taunus' email server and its individual components now run in what are known as Trusted Execution Environments (TEEs, also called enclaves): encrypted environments within the CPU. This hardware-based isolation, combined with control over its own encryption keys, provides effective protection against external attackers and unauthorised access by privileged insiders. Remote attestation – a tamper-proof cryptographic verification mechanism – also provides technical proof that data is being processed confidentially.

enclave uses the same technology to secure the district association's document storage in a Nextcloud instance. Only authorised users can access this Nextcloud and the individual documents, while even the operations team and infrastructure provider are systematically prevented from accessing them. HKN GmbH, a cloud service provider specialising in sovereign workspace solutions, was brought in to handle the day-to-day management of the Nextcloud user interface.

### THE CONFIDENTIAL ARCHITECTURE

EVERY EMPLOYEE · ANY PC OR MOBILE DEVICE



CPU

TRUSTED EXECUTION  
ENVIRONMENT · ENCLAVE

MAILCOW · EMAIL SERVER

S0Go

Dovecot

Postfix

Spam  
filters

DOCUMENT STORAGE

Nextcloud

DATA STAYS ENCRYPTED –  
AT REST, IN TRANSIT, IN  
USE

AWO-HELD  
KEYS



REMOTE  
ATTESTATION



TECHNICAL  
PROOF

× NO ACCESS

OPERATIONS TEAM · INFRASTRUCTURE PROVIDER

## 04

## Results

## Results & Benefits

By introducing Confidential Computing, AWO Rheingau-Taunus was primarily pursuing two objectives: comprehensive data security and consistent compliance with data protection requirements. With enclave, the district association benefits from several tangible advantages:

**Verifiable evidence of compliance:**

AWO Rheingau-Taunus actively uses the proof of secure data processing provided by remote attestation when engaging with data protection officers, during audits and in child safeguarding cases. This enables it to demonstrate its data security measures and duty of care beyond doubt.

**Secure communication without shadow channels:**

Every employee can now send messages securely via the encrypted email server from any PC or mobile device, effectively eliminating the need for alternative, insecure communication channels. Verifiably encrypted communications and document storage also simplify data exchange with doctors, public authorities and courts.

**No loss of performance:**

Previously, the district association frequently experienced an overloaded email system that would consequently become unavailable. In the new architecture, utilisation rarely exceeds 50 per cent, even at peak times. enclave's runtime encryption has little impact on performance, requiring only a few per cent of additional computing capacity.

# 04

## Results

Michael Weigelt is pleased that the increase in data security does not create additional work for employees:

**“enclave’s encryption is practically invisible, both in terms of computing performance and in day-to-day work. The only adjustment for our employees was setting up the new PCs and familiarising themselves with the new open-source applications.”**

The migration has also delivered the intended economic benefits. The new Linux-based architecture eliminates the district association’s high licensing costs and allows it to use older, refurbished hardware. As a result, the new setup reduces costs to around one third of the previous operating model.

### UTILISATION AT PEAK TIMES

50%



Rarely exceeded in the new architecture

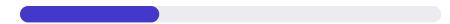
### COST OF OPERATION

1/3

PREVIOUS



NEW SETUP



New setup against the previous operating model

## 05

## Conclusion

## Conclusion & Outlook

**With enclave, AWO Rheingau-Taunus has successfully migrated its systems to a secure, compliant infrastructure. While the email server is already being used by all employees, the rollout of the confidential Nextcloud environment is still under way.**

This, however, is only the beginning. As part of its broader reorganisation, the district association is currently working on the introduction of an ERP system for contracts with parents and suppliers, among other initiatives. It also plans to migrate the entire architecture to a Kubernetes-based platform, allowing individual applications and system components to be managed more flexibly while maintaining high availability. Here too, the intention is to use enclave and Confidential Computing.

■ IN CLOSING

**“Our goal is very clear: we want to protect all of our data and system components and keep them fully encrypted,”**

---

says Michael Weigelt. “Once we’re ready, we will approach enclaive again to jointly implement a ‘Confidential ERP’ solution and migrate to a confidential Kubernetes architecture.”