Public Sector – RFQ Data Protection

„The organization achieved a 20% quicker internal RFQ process.“

Customer Case Study

eperi

Eperi GmbH
Gutenbergstr. 4-6
64319 Pfungstadt
Germany
sales@eperi.com
eperi.com
+49 6157 956 39 00

Customer Case Study

Public Sector – RfQ Data Protection

On-premises

- Encryption of RfQ process to protect against internal and external attacks
- Protect administrators from suspicion

- 20% Quicker internal RfQ process
- 40% Higher internal adoption of email collaboration tools

> With a streamlined and secure RfQ process that includes eperi's data protection solution, we are able to increase our internal efficiency while staying compliant with our company security standards.

Customer

Public Sector Information Technology Institution

Project

Protection of RfQ Data from unauthorized internal usage

Problem

Responsible for highly protected **RfQ processes involving millions**, our customer needed a solution to protect sensitive RfQ data against unauthorized usage. The enterprise required protection for its on-premise email and calendar solution including a centralized **enterprise key management** tool to protect the RfQ information. The users need to be able to work on any device (mobile, Outlook, 3rd party tools, web interface) from anywhere and with all the functionality.

Solution

The eperi Gateway has been installed as centralized enterprise key management tool encrypting e-mails and calendars as well as mobile device data. **Via a centralized data security solution**, the customer is able to secure the sensitive RfQ data against internal and external data breaches and misuse. All e-mail and calendar data is encrypted from end to end and the **Exchange administrators** are not able to see any data in plain text. All authorized users can work from any device and anywhere with all functionalities **retained**. The administrators are also able to work **in their usual way** – but only on encrypted data.