Zonar helps ensures GDPR and Schrems II compliance by enhancing privacy and data protection

Zonar Systems is a leading smart fleet management and mobility solutions company that has been serving fleets of all sizes and industries for more than 20 years. Part of the Continental AG family, Zonar is headquartered in Seattle, Washington, from where it serves its global customer base. This year Zonar started to bring its products to market in Europe under the Continental banner.

Customer privacy and data protection is essential for any responsible company. Zonar takes this customer responsibility seriously as it builds out new technology solutions for the European market. To achieve both end goals, Zonar wanted to ensure that its current systems comply with privacy protections of the GDPR and Schrems II for U.S.-Europe data transfers. And it saw the opportunity to add an additional layer of protection for its European customers to help ensure privacy safeguards, even when that data is in use.

Protecting against today's data security threats

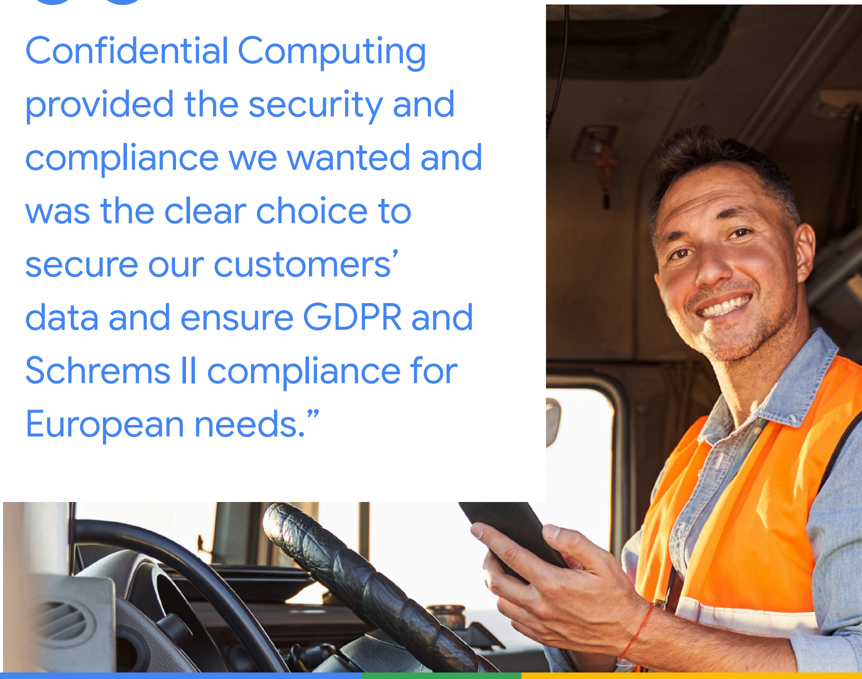
Data breaches, ransomware, and privacy hacks pose serious threats to customer privacy as well as to the company's reputation. Knowing how important additional protections are for its European customers, Zonar chose Google Cloud's Confidential Computing platform to support its GDPR and Schrems II compliance efforts.

Encrypting data in use, in the cloud

As a Google Cloud customer, Zonar engaged Confidential Computing, a new technology by Google Cloud that encrypts data in the cloud, while it's being processed.

Gordon Waddell, Senior Vice President of Software Development at Zonar, headed up the evaluation and implementation. "As expected, we had to do a lot of research around the latest trends in privacy and encryption," he says. "We looked at other solutions, which were very software-heavy and felt inelegant. Confidential Computing provided the security and compliance we wanted and was the clear choice to secure our customers' data and ensure GDPR and Schrems II compliance for European needs."

> Confidential Computing provided the security and compliance we wanted and was the clear choice to secure our customers' data and ensure GDPR and Schrems II compliance for European needs."



Moving from the data center to the cloud - securely

Zonar is currently completing a move from its legacy data center environment to a cloud-native environment with Google Cloud. Zonar elected to implement Confidential Computing to help secure data "extensively in our European deployment, to ensure the privacy of customer information in light of the regulatory environment there," says Waddell.

Data in the cloud exists in three states, two of which are typically encrypted: *at rest* and *in transit*. Google Cloud Confidential Computing addresses the third state, which is typically unencrypted: *in use*. For this state, Google Cloud takes advantage of AMD Secure Encryption Virtualization on AMD EPYC™ CPUs. This hardware-accelerated memory encryption uses keys to keep data encrypted, even when it's being accessed, indexed or searched. These keys are the held within the AMD Secure Processor on an EPYC CPU, and not even Google can read them.

The company also uses Google Cloud External Key Management with a European-hosted external key to help ensure that data at rest is protected by regional keys, which Zonar's compliance and privacy team considers vital. Waddell adds, "We use Confidential Computing in most Google services that support it, but primarily in our use of GKE [Google Kubernetes Engine] using N2D nodes."

Zonar uses Terraform to deploy infrastructure as code into Google Cloud, with regional deployments resident in North America and one in Europe. "By having infrastructure as code in Terraform," says Waddell, "we're able to ensure the same infrastructure is deployed in both regions and manage differences in a very easy way — in this case, the Terraform for Europe-specified N2D hardware enables Confidential Computing features where it can."

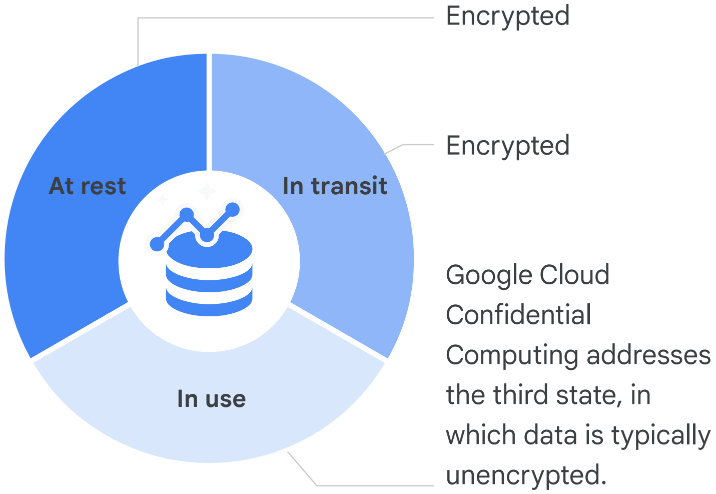
How companies can enable Confidential Computing

Confidential Computing helps protect data in use with the help of hardware-based Trusted Execution Environments (TEEs), a security standard defined by the Confidential Computing Consortium. A TEE is a secure area within a main processor that runs an isolated environment parallel to the main operating system. Through this isolation, the TEE guards data and code from malicious agents while in use.

Confidential Computing is enabled by the click of a button when customers create a Confidential VM. Adding Confidential Computing requires no changes to existing applications or code, and tools and workflows are not affected.

When Confidential GKE nodes are deployed on top of Confidential VMs, the contents in memory on the VMs are encrypted, and clusters with confidential GKE nodes are enabled, which enforce the use of Confidential VM for all nodes. All workloads running on these nodes are encrypted while in use.

Data in the cloud exists in three states


Encrypted
Encrypted
At rest
In transit
In use
Google Cloud Confidential Computing addresses the third state, in which data is typically unencrypted.

Zonar Confidential Computing deployment details

- ✓ Confidential VMs
- ✓ Hosted on AMD EPYC™ processors
- ✓ Confidential GKE Nodes
- ✓ N2D machine types
- ✓ European-hosted keys
- ✓ Terraform in U.S. and Europe
- ✓ Transport Layer Security and other known standards
- ✓ The project will scale when Confidential Computing is live in both regions

Waddell is pleased with the use of Confidential Computing. "By having Confidential Computing as a feature in Google Cloud managed services, such as the ability to enable it in GKE, and Google's strong support for Terraform-based deployments, we're able to use it without any significant change to our strategy."

Plus, having achieved compliance with privacy protections of GDPR and Schrems II, Zonar enjoys strengthened trust from its European customer base. "It is important to us that our customers know Zonar is doing everything in its power to protect their data," says Waddell.

Waddell sees Confidential Computing providing a basis for other deployments over time as Zonar accelerates toward its cloud-native future. "When Confidential Computing is widely available in the market, we can use the flexibility of Google Cloud and our platform to scale to meet demand."

Zonar experienced no performance or latency issues with the project, added Waddell: "Confidential Computing is doing exactly what we want it to do. It's running really well on top of our managed infrastructure, and we cannot tell the difference in performance. To look at it, you don't even know it's there." For Zonar Confidential Computing delivers greater data security without missing a step in performance.

To learn how Google Cloud's Confidential Computing platform powered by AMD can help protect your sensitive data, visit us at cloud.google.com/confidential-computing.