



WHITEPAPER

Security and compliance in Compliant Cloud



cleura 

Introduction

Except for the ability to digital innovation, the traditional reasons of why an organization turns to the public cloud is cost savings or to augment their private cloud capacity. Although these reasons are still valid, a more important reason is on the rise, namely security. Organizations are coming to realize that providers can invest and specialize far more in people and processes to deliver a secure infrastructure. At Cleura we have an expressed goal and business strategy to deliver better security than traditional on-premises solutions.

But security in itself is not good enough. Highly regulated industries and organizations are hesitant to step into a public cloud because of all the regulatory demands they are facing these days. Basel, Solvency and GDPR to name a few. This is the main reason why Cleura has created a specific service targeted towards regulated organizations. It is our goal to provide our customers with all the benefits from a public cloud while at the same time ensuring that they can meet all the regulatory demands. We firmly believe that this is a sought after service in short supply. This is why security and compliance in combination with innovation are our primary

focus areas and this reflects in everything within our organization.

Making sure that customer data is both secure and compliant is our primary design criteria. It impregnates everything from how we build our data centers and design our hardware to our extensive training and hiring priorities. It shapes our daily operations and disaster planning and how we address threats and assess risks. We want to offer our customers a simple business model in a very regulatory and complex world.

This paper outlines the way we ensure that our customers can have top grade security and meet all their regulatory demands at the same time.

Security and compliance in Compliant Cloud

Cleura's Security Culture

As a strict IaaS provider our reason for being is to ensure information availability to our customers in a secure manner. Cloud security is not part of our business, cloud security is our business. Meeting regulatory demands is often associated with bureaucracy and slow processes but we are living proof that you can be quick, agile, secure and compliant at the same time. Solving modern demands for security and compliance is both creative and inspirational. Working with security at Cleura is fun.

Employee Screening

Each employee goes through a rigorous background check before being hired. The check includes criminal records and financial information such as current debt. Before an employee is promoted to work with our Compliant Cloud customers the background check is extended to include the employee's family and business associates.

Security Training For All Employees

All staff at Cleura have weekly training sessions in information security. These trainings range from practical exercises in locking computers and appliances to security awareness and information classifications. All staff take regular diagnostic tests to ensure that the training has the desired effect.

As an annual tradition we hold security hardening parties where we enjoy each others company, eat good food and make a complete overhaul of our personal security measures. For instance we change and strengthen our passwords and make sure that all our discs are encrypted. Anyone who wants to join us in celebrating new and innovative security

solutions are welcome to join in.

Cleura houses one of the nations foremost authorities on social hacking and our staff is specially trained to withstand social hacking.

Our Dedicated Security Team

The security team at Cleura consists of people with extensive experience in information security with backgrounds ranging from white hat hackers, military intelligence and military special forces.

Top Grade Physical Security

Your data is stored in top grade infrastructure in state of the art facilities. We follow all recommendations from the Civil Contingencies Agency, even the optional recommendations. In many cases we exceed the recommendations¹.

Our European data centers and every installed appliance is fully compliant with Uptime Institutes definition of a Tier IV data center.²

Our datacenters are certified to be compliant with all demands from PCI-CPP, HIPAA, ISO 27001 and ISO 27018.

¹ "Vägledning för fysisk informationssäkerhet i it-utrymmen" ISBN: 978-91-7383-401-8

² <https://uptimeinstitute.com/research-publications/asset/tier-standard-topology>

We Customize Agreements

We do not use standard agreements other than as templates. We shape legal agreements that ensures compliance if they are scrutinized by our customers control agencies like the Financial Supervisory Authority, the Data Protection Agencies, the Data Inspection Board and the Civil Contingencies Agency.

Limited Subcontractors

Our aim is to keep the number of subcontractors to a minimum and no subcontractor has remote access to customer information. All physical storage is completely owned and managed by Cleura. Data ownership is secured and can be contractually guaranteed even in case of a bankruptcy. We are vendor independent in all aspects of our business and have backup vendors prepared for emergencies. We work in accordance with ISO 22301 and have defined a backup plan for each of our subcontractors.

Intense Continuity Planning

Our Compliant Cloud service is ISO 22301 certified and we have extensive plans to ensure that we do not have any single points of failure. This includes both technical, personnel and business perspectives. Our continuity policy is available upon request.

Transparency

A smart security implementation does not require a lot of secrecy to be secure. We welcome audits to verify that we live the way we preach. We have an annual audit event for our customers to come and visit and review our processes and facilities. We are also open to, and welcome all audits from regulatory authorities. We go through great lengths to shape our policies so that they can be reviewed by external parties without requiring a NDA. Our aim is to publicly publish all reports from certification bodies as complete as we can without breaking confidentiality. If your company would like to invest in sending an auditor from an accredited organ to review us, you would make us really happy.

One Legal Authority

We are a Swedish company and all our Compliant Cloud administrators are EU citizens. This effectively means that our customers only have to account for Swedish contract law when signing an agreement with Cleura. As a member nation in EU all EU regulations is also valid in Swedish agreements.

Stable Owners With Long Term Strategies

The owners of Cleura have a long term strategy and see Cleura as the European leader in compliant cloud infrastructure.

Good Business

We have an extensive quality control system to ensure that our customers will be met with the outmost professionalism and enjoy the very best services we have to offer. Cleura is ISO 9001 and ISO 14001 certified and focus heavily on constantly improving the level of quality in all aspects of the business. Please have a look at our sample from our employee handbook that illuminated how we work with our management processes.

Sustainability

As a company, we strive to be good role models for our society. Therefore, we base our work on the UN's 17 global goals for economically, socially and environmentally sustainable development. For example, in the area of environment, we work to reduce our customers' climate footprint by offering a modern digital infrastructure for their digitization, which runs from data centers where energy efficiency is in focus. Another focus area for us is to increase gender equality in our industry by getting girls and young women interested and familiar with the IT industry.

Certifications And Rules We Comply With

It is a fairly straight forward task to become regulatory compliant and to us it was a natural step to take. The real challenge lies in making sure that our customers are regulatory compliant when they use our services. This is precisely why we go through great lengths to ensure and show that our customers are fully compliant when using our services.

- ISO 9001 - QMS ✓
- ISO 14001 - EMS ✓
- ISO 22301 - BCMS ✓
- ISO 27001 - ISMS ✓
- ISO 27010 - ISP ✓
- ISO 27013 - ITIL ✓
- ISO 27017 - Cloud Sec ✓
- ISO 27018 - Privacy ✓
- Compliance Controls Catalogue (C5) ✓
- SOC 2 ✓
- PCI-DSS ✓
- PCI-CPP ✓

About Cleura

Cleura is a leading global supplier of IT infrastructure cloud services based on OpenStack. The company delivers public, compliant and private clouds.

Cleura is certified according to ISO 9001, 14001, 27001, 27010, 27013, 27017 and 27018 – internationally recognized standards for quality, sustainability and information security. Its services are available from more than 20 data centers around the world. With its compliant cloud, Cleura ensures that customers adhere to demands originating from specific laws and regulations concerning auditing, reputability, data handling and data security, such as Basel, Solvency and GDPR. Cleura is a part of Iver.