centron®

centron

Making IaaS as easy and accessible as possible - for everyone.

centron helps companies through IaaS, PaaS and SaaS services and products to outsource the entire IT infrastructure to concentrate on the essential things: their business. In 1999, centron was founded as a web hosting provider by Wilhelm and Monika Seucan, and in 2014 it started with the construction of its own data centre at the location in Hallstadt. 2023 centron, together with 50 employees, successfully supports approx. 2400 global customers with managed services, cloud services, cloud solutions and more.

centron Trust Center

The safety and security of your data is our top priority. In addition to our own **rigorous safeguards**, centron adheres to the **published standards** listed here.

ISO 27001

centron products & services are certified to be compliant with the ISO27001 standard. To be accredited the certification, centron had to prove that our **infrastructure services** meet the specified security standards to an external auditor. ISO 27001 certification demonstrates **centron's clear commitment to Information Security Management** and ensures that there are adequate processes in place to lessen the risk of data breach.

ISO 14001

In today's world, where **environmental concerns** have become a top priority, demonstrating one's commitment to sustainability is more important than ever. The ISO 14001 certified **centron data center in Hallstadt, Germany** proves our commitment to do our part.

ISO 9001

This certification provides a framework for implementing a **quality management system** that ensures consistent and high-quality service delivery. By achieving this certification, centron demonstrates its commitment to **delivering high quality services**, while also complying with environmental regulations and implementing sustainable practices in combination with the regulations of the **ISO 27001** and **ISO 14001**.

EU GDPR

GDPR compliance is a **shared responsibility**. centron products & services offers a wide set of controls to keep GDPR compliance. For centron that already has a high standard of data protection practices on its cloud products & services, **GDPR is a chance to enhance the practices**, and to tighten things up further.

Access Control

Access Control (Physical)

Access control system

- **Door security** in the office building
- Additional **biometric access** security to the data center and electronic door security for two-stage access control.
- Establishment of **protection zones** and **access rules**
- **Visitor regulations**
- **360° video surveillance** of the building exterior with sabotage detection and recording
- **video surveillance** of the data center interior.
- **Intrusion alarm** system with security service

Separation Control

Measures to ensure that data collected for different purposes can be processed separately

- All data can be **processed separately** from one another
- Exclusive use of software that provides **multi-tenancy**
- **Separation** of the processing systems
- Separation of the systems in **production** and **test** environment
- Customers have **no mutual access** to systems

Access Control (virtual)

Measures to prevent data processing systems from being used by unauthorized persons

- Granting of **authorizations**
- **Logged** allocation of authorizations
- Internal **password guidelines** are implemented by MS-AD
- The local systems of the employees are updated **as soon as updates are available**
- Automatic **blocking**
- Upstream connection of a physical firewall with **IDS** and **IPS**
- Use of **virus scanners**
- **Physical separation** of networks
- **Monitoring** of network traffic

Transport Control

Transfer Control

Measures to ensure that personal data cannot be read, copied, changed or removed by unauthorized persons

- A transfer of personal data takes place only at the **request** of **authorized** persons or institutions
- If **personal data** is transferred to authorized persons or institutions, it is **encrypted**, and unencrypted at the express request of the customer
- Data carriers that contain personal data are **cleaned** several times using different **erasure methods**
- when the data **carrier** is disposed of, then the data carrier is **destroyed** and **properly disposed** of.

- **Logging** of the system activities by a **monitoring** system
- Semi-automated **evaluation** of log files
- Logging of all work in the **ITIL-compliant ticket system**
- New personal data can only be entered by **authorized** persons
- Access to the **data processing system** is logged (see point access control).

Input Control

Measures to ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed

Order Control

Measures to ensure that personal data that can only be processed in accordance with the instructions of the client

- Orders by customers who request the processing of personal data are logged in a **ticket system**; an access control is configured for the ticket system
- Electronic orders are only possible from **verified** contact addresses
- Orders can also be sent by post in written form only through **verified addresses**
- Persons who place orders must have been **authorized** by the contractual partner to place orders

Reliability Control

Availability Control

Measures to ensure that personal data are protected against accidental destruction or loss

- **RAID** (redundant data writing on hard drives)
- **Rhythm**: daily or according to customer requirements
- **Retention period**: redundant, 1-5 weeks
- **File format**: binary, proprietary encrypted
- The **place of storage** is, depending on the order, the client's dedicated storage or server systems in their own or third-party data centers or the contractor's global storage systems
- RAID (mirroring of the hard disks), **redundant power supply units**
- Regular checking of the backups for **functionality**
- Implementation of the **disaster** and **recovery concept**, emergency concept and recovery plan
- **Data center**: Uninterruptible power supply (UPS), emergency diesel system, redundant air conditioning, early fire detection system, regular fire-fighting training for employees

Access Control (internal)

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization

- The password is only issued by **authorized personnel** to persons named by the client
- The communication of instructions takes place on the part of the contractor via an **ITIL compliant ticket system**
- The authorization to process personal data is controlled and logged by the **Active Directory**
- Logging of the logins on the **systems**
- Destruction of data carriers according to the **data carrier destruction concept**

centron Managed Backup

What is being secured?

Data carriers (HDD, SSD, etc.) of the operating system, all other data carriers and **partitions** or even complete Exchange databases are backed up. **Daily dumps** are generated by other databases, which - depending on their size - **remain locally** on the system for up to **seven days**.

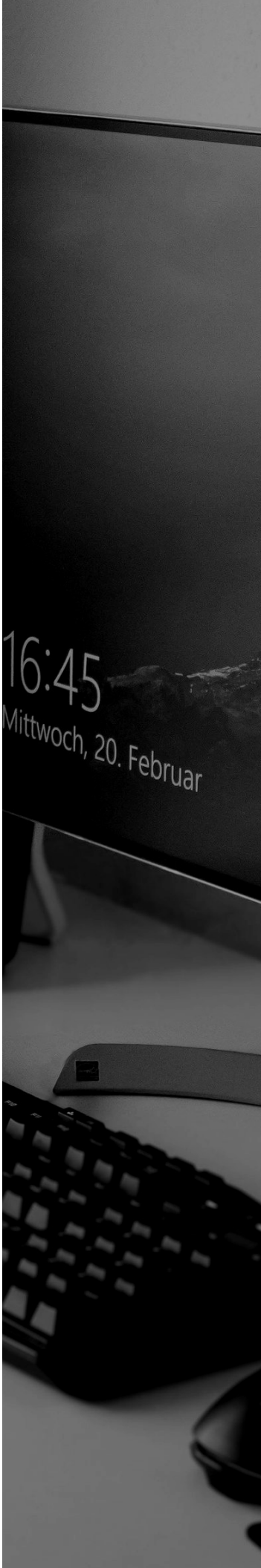
In this way we ensure an even **faster recovery**. These dumps are also kept in the **daily backup**. Temporary data is excluded, as these are created by the system itself during operation and are not relevant for a restore. We will record agreements that differ from this in a joint discussion.

Where is my backup going?

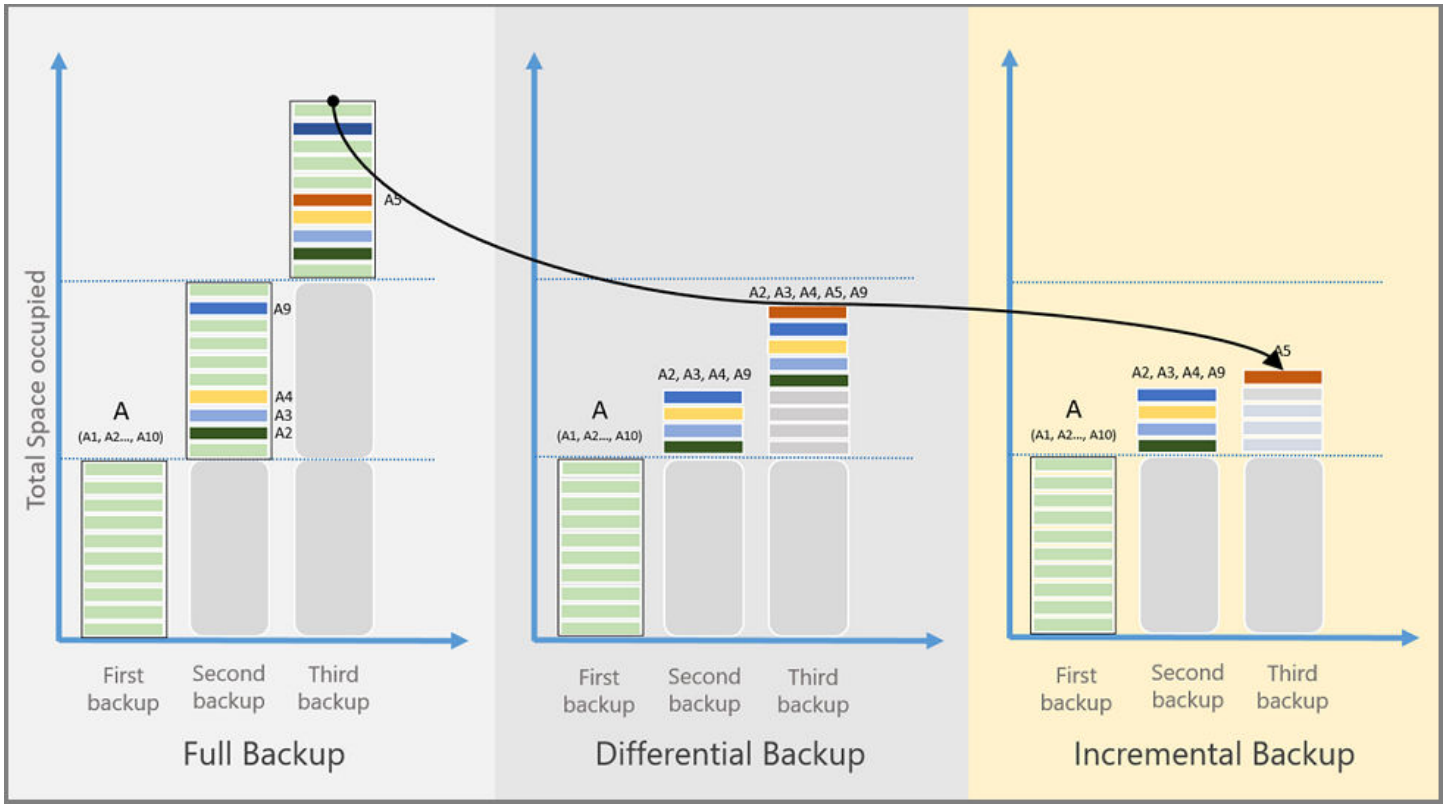
In order to **minimize** the **risk** of physical influences, the backup data at centron is mirrored to at least one other **fire protection site** of the data center. If your system shows hardware damage, your data backup can be provided on replacement hardware. It is also possible to outsource your backup to a second data center (**redundant storage**).

How is it secured?

At centron, the backups of the systems are stored according to the **generation principle**, also known as the **grandfather-father-son** principle. This means a **monthly full backup** of your system on which **weekly and daily backups** are based. This security chain is kept until its expiry date (**EOL = End Of Life**) is reached. If an error in a file is not discovered until later, it is possible to **restore** a version **other than the most recent** version. However, this is not a version management.



centron Managed Backup



Done every 4 weeks	Done weekly	Done daily
Kept for 4 weeks	Kept for 2 week from last Full	Kept for 1 week

centron Backup-as-a-Service

Thanks to our new backup landscape, we can reliably offer you the backup of your data in a **resource-saving** and **cost-effective** manner. With regard to data backup, you have the following **options**:

- Securing in **another fire compartment** (configured by default)
- Exclusive **target** for your server landscape
- **Georedundant backups** at different locations

Our backup Infrastructure is separated from centron's productive systems by rigorous network security measures. The productive infrastructure is **backed up itself** and tested in regular intervals through **restore tests**.

Contact

centron GmbH
Heganger 29
96103 Hallstadt, Deutschland
Phone: +49 951 968340
E-mail: info@centron.de
Website: https://www.centron.de

Copyright