HRorganizer B.V.
Binnenhaven 1
6709 PD Wageningen
+31 317 465 460
info@hrorganizer.com
www.hrorganizer.com

Last updated: 30 March 2021

Security and reliability

From laying the first foundations of HRorganizer, system security and reliability have been taken into account. Security to ensure that data may only be used by those entitled to do so. Reliability, allowing users to always have access to the system. This has resulted in:

- 99.98% uptime since 2013
- no attempt at digital theft has ever succeeded

System requirements

To use our software-as-a-service, we advise and support the use of systems that meet the following requirements:

Internet

768 kbps DSL (or faster)

Browser & Operating System

One of the following browser and operating system combinations:

- Internet Explorer 11.0 (or higher) op Windows 8.1 / Windows 10
- Edge op Windows 10
- Firefox 30.0 (or higher) op Windows 8 or higher / MacOS X or higher
- Chrome 36.0 (or higher) op Windows 8 or higher / MacOS X or higher
- Safari 8.0 (or higher) op MacOS X 10.10 or higher
- Android 4.4 (or higher)
- iOS 8.0 (or higher)

Measures

Security and reliability have been taken into account at all levels.

User-level

- Secure access with personal access details. This is stored in our system in encrypted form and is therefore not known, including to us.
- A strictly automated procedure for the recovery of access when the password is lost.
- May be extended on request using digital certificates or one-off access codes (whose functioning may be time-bound).

Mobile and Web-Application level

- Fully secured connection (https, ssl).
- All data is stored in pseudonymised form. Only the application and 3 of HRorganizer's IT employees have access to the key.
- Database and back-ups are encrypted continuously (using Transparent Data Encryption)
- Designed to keep licensees' data strictly separated.
- Designed to be able to resist all known methods of attack (e.g. sql-injection).
- Monitoring of availability and performance both from within and externally.
- 99,8% guaranteed availability.

Physical connection level

- This lies in the trusted hands of ArchiLogiQ (www.archilogiq.nl)
- Data centres fully connected in duplicate to the network infrastructure administered by ArchiLogiQ.
- This infrastructure includes several redundant internet connections (Gigabit Ethernet backbone).
- The data centre partner is certified according to the following standards: ISO 9001, ISO 27001, ISAE3402

Central computer (physical location) level

- This lies in the trusted hands of Equinix (www.equinix.nl).
- Power supply: multiple implementations, scalable high capacity, permanently guaranteed through Uninterruptible Power Supply (UPS) systems and on-site back-up diesel generators.
- Fire detection and control: Very Early Smoke Detection Apparatus (VESDA) installed in every space, connected to the Building Management System (BMS) continuously

monitored from a network operations centre. Fire is detected at a very early stage and immediately extinguished with minimum damage to equipment, connected to a firefighting system based on environmentally-friendly gas or water mist. Loss of data and interruption of operations is in this way avoided.

- Air conditioning: all data centre floors are at a constant temperature and have relatively low humidity.
- Physical security: physical security limits, 24x7x365 monitoring by on-site staff who check everyone entering the building, CCTV surveillance systems and alarm activation in case of break-in.
- Access: individually programmable access cards and visual identification, access only when the on-site engineer has approved our request. Responsible standard procedures ensure that we obtain quick access to the equipment, day and night.

Central computer level (ArchiLogiQ)

- Several computers with hardware and software virtualisation.
- Automatic 'failover' of virtual servers to other physical machines in case of hardware failure.
- Automatic distribution of the resources of virtual servers across the physical host servers.
- Multiple implementations of data storage via FC SAN (Fibre Channel Storage Area Network).
- Much of the data consulted is automatically transferred to fast SSD storage.

Central virtual server level (ArchiLogiQ)

- In case of planned maintenance to hardware, servers may be moved during the operation (by virtualisation) to other hardware without this affecting availability.
- Only accessible remotely from Binnenhaven 1 in Wageningen, where separate networks are used for employees and guests.
- Nightly differential database back-up, weekly full back-up, hourly transaction log back-up.
- Easily upscalable.