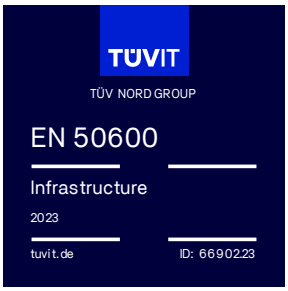
TÜVIT

Certificate



The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

Deutsche Rentenversicherung Bund
Berner Straße 1
97084 Würzburg, Germany

Certificate validity:
2023-07-25 – 2025-07-31

to confirm that its security area

Rechenzentrum Würzburg

fulfils all requirements of

EN 50600
Availability Class 2, Protection Classes 1-3,
Granularity Level 2

using Trusted Site Infrastructure Criteria Catalog TSI.STANDARD V4.3 of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate with the ID 66902.23 and consists of 5 pages.

Essen, 2023-07-25

Dr. Christoph Sutter, Head of Certification Body

To Certificate

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen, Germany
tuvit.de

TÜVNORDGROUP

Certification scheme

The certification body of TÜV Informationstechnik GmbH performs its certification based on the following certification scheme:

- German document: “Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH”, version 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation report

- German document: “Evaluierungsbericht – Trusted Site Infrastructure (TSI.STANDARD), Rechenzentrum Würzburg”, Version 1.0 as of 2023-07-14, TÜV Informationstechnik GmbH

Evaluation requirements

The evaluation requirements are defined in the following standards:

- EN 50600-1; Information technology – Data centre facilities and infrastructures – Part 1: General concepts; German version EN 50600-1:2019-08
- EN 50600-2-1; Information technology – Data centre facilities and infrastructures – Part 2-1: Building construction; German version EN 50600-2-1:2021-09
- EN 50600-2-2; Information technology – Data centre facilities and infrastructures – Part 2-2: Power supply and distribution; German version EN 50600-2-2:2019-08
- EN 50600-2-3; Information technology – Data centre facilities and infrastructures – Part 2-3: Environmental control; German version EN 50600-2-3:2019-08
- EN 50600-2-4; Information technology – Data centre facilities and infrastructures – Part 2-4: Telecommunications cabling infrastructure; German version EN 50600-2-4:2015-07
- EN 50600-2-5; Information technology – Data centre facilities and infrastructures – Part 2-5: Security systems; German version EN 50600-2-5:2021-09
- EN 50600-3-1; Information technology – Data centre facilities and infrastructures – Part 3-1: Management and operational information; German version EN 50600-3-1:2016-08
- EN 50600-4-2, Information Technology – Data centre facilities and infrastructures – Part 4-2: Power Usage Effectiveness; German version EN 50600-4-2:2016 + AC:2017 + A1:2019

and were checked applying the evaluation requirements:

- "TSI.STANDARD Criteria Catalog, TSI.STANDARD V4.3" as of 2021-04-01, TÜV Informationstechnik GmbH

The evaluation requirements are summarized at the end. Not applicable requirements are printed in grey.

Evaluation target

Evaluation target is the security area "Rechenzentrum Würzburg" of Deutsche Rentenversicherung. It is detailed in the evaluation report.

Evaluation result

The evaluation target fulfils all applicable requirements of the above-mentioned standards with regard to

- Availability Class 2,
- Protection Classes 1-3,
- Granularity Level 2.

Summary of the Evaluation Requirements

The requirements for Trusted Site Infrastructure, TSI.STANDARD V4.3, which contain the requirements of EN 50600:

1 ENV – Environment

Surrounding hazard potentials have been avoided. The decision on the location is based on risk assessments according e. g. floods, explosions, seismic events, shock waves, danger of collapse or pollutants.

2 CON – Construction

Walls, doors and windows offer protection against access, fire and debris. The building is protected against lightning. The security area is located in a separate fire protection area and not directly adjacent to the public and dangerous next-door production processes. IT and technical equipment are separated. A constructive fire and water prevention is given.

3 FIR – Fire Alarm & Extinguishing Systems

A fire alarm system has been installed in the complete security area and linked to an alarm receiving centre. Adjacent rooms, raised floors, suspended ceilings and air ducts are included in the fire monitoring. Apart from signalling an alarm, damage containment measures such as a gas extinguishing system in the security area are triggered. Furthermore appropriate hand fire extinguishers are available.

4 SEC – Security Systems & Organization

An access control system including appropriate access rules does exist. The protection against breaking and entering features several levels, and all security sensitive areas are monitored by means of an intrusion detection system. The security systems are fed by a main and an additional power source. The alarms are transmitted to a permanently manned security control room.

5 CAB – Cabling

Communication and data cables are laid with the necessary distance to each other and to power cables on separate cable routings in accordance with EN 50174-2. Data cables are not laid in any hazardous areas or they are specially protected. WAN trays are crossing-free, and connections to at least 2 providers are given from Level 3.

6 POW – Power Supply

The electrical installations are realized in accordance with the relevant standards and regulations. They are protected against over voltage and realized with adapted separations and with protection of the electric circuits. Failure of power components is handled by a redundant layout. The IT components and the security control room are connected to an emergency power unit and UPS systems. Commissioning procedures have been performed.

7 ACV – Air Conditioning & Ventilation

Air conditioning for the IT systems and infrastructure components is sufficiently given. It has been ensured that air temperature, humidity and dust content comply with specified limits. Dampers are installed according to the fire protection concept. The measured values are remotely controlled. Failure of air conditioning components are handled by a redundant layout. Commissioning procedures have been performed.

8 ORG – Organization

Periodical functional tests are carried out for all safeguards. A maintenance schedule defines methods and intervals for the wear parts of the infrastructure components. The data backup media is stored and protected against fire and access in an area separate from the security area.

9 DOC – Documentation

A DIM (Documentation of Infrastructure Measures) or a security concept has been provided. Rules of conduct exist, i.e. covering access control with respect to authorization or key / smart card distribution. Up-to-date drawings are available for the building and all infrastructure components, as well as schematics and data sheets. Furthermore a fire protection concept does exist and has been coordinated with the local fire brigade. Additionally emergency or recovery concepts are provided.

10 EN 50600

The supplementary requirements for holistic coverage of DIN EN 50600 have been implemented.

To achieve availability class X, all EN 50600 requirements relevant in level X as well as the TSI requirements in the areas of POW, ACV and CAB must be achieved at least in the corresponding TSI level X.

Granularity level 2 according to EN 50600-2-2 and -2-3 is confirmed if the TSI requirements are fulfilled in one of the levels 2, 3 or 4 together with the corresponding EN 50600 requirements.

Four different protection classes are defined. All areas and supply paths of the data center are assigned a protection class. They describe physical safeguards against the following events:

- unauthorised access
- internal environmental events
- external environmental events

With regard to unauthorised access, at least three protection classes must be implemented.

L Level

Level 1	Medium protection requirements (corresponds to the infrastructure requirements of the "IT-Grundschutz Catalogues" published by the German Federal Office for Information Security (BSI))
Level 2	Extended protection requirement (redundancies of critical supply systems, with supplementary requirements for the aforementioned assessment aspects)
Level 3	High protection requirement (complete redundancies of critical supply systems – no single point of failures in important central systems)
Level 4	Very high protection requirements (advanced access control, no adjacent hazard potentials, with minimal intervention times in the case of alarms)
Dual Site Level 2-4	both data centers individually reach at least one Level underneath the Dual Site Level.

E EFF - Energy Efficiency

The value for the Power Usage Effectivness (PUE) of the data center infrastructure was correctly determined and is below 1.5. The results of the continuous measurements over 12 months for the total energy demand and the IT energy demand as well as documentation for the measurement concept are available.