TECOSIM specialises in engineering services for all aspects of product development. The company is a market leader in computer aided engineering (CAE) and a provider of development processes and software. In September 2017, TECOSIM Technische Simulation GmbH obtained ISO 27001 certification from TÜV Rheinland Cert GmbH to demonstrate the compliance of its IT-supported business processes. TECOSIM has compiled important information on data security at the company for its customers, below.

**CLASSIFICATION OF INFORMATION**
For us, all customer data and information belong to the „Secret“ information class; in other words, they are subject to the most stringent security standards in every respect.

**DATA EXCHANGE**
Your data reach us solely via the exchange portal you have provided. If you do not have your own portal, we will be happy to provide you with a secure transmission channel. The results are supplied via the same, secure pathway.

**NETWORK ARCHITECTURE**
Your data are stored locally on a RAID system at the branch of TECOSIM Technische Simulation GmbH that is carrying out the project.

**ACCESS CONCEPT**
Authorisations are organised on a specific customer basis. Therefore, your data can only be accessed by employees who are working for you on your projects.

**BACKUP STRATEGY**
We make backups everyday as a safeguard against technical breakdowns.

**EMPLOYEES**
Our employees receive regular training and testing to ensure compliance with our technical safety standards, and are under obligation to maintain this compliance.

**IT SECURITY**
Maximum safety standards protect our IT against attacks from outside, harmful software and loss of data for technical reasons.

**BUILDING SECURITY**
The offices of TECOSIM Technische Simulation GmbH are protected to prevent unauthorised parties from accessing or seeing into them. All buildings are equipped with intruder and fire alarm systems. A comprehensive zone concept provides special protection for those areas where project work is taking place.

**ARCHIVING**
On completion of the project, all customer data are permanently deleted. We can archive project data and results for up to five years after the end of a project, if you so wish. We will discuss the safekeeping period with you.

ISO 27001 is the internationally recognised standard for the active management of information security in organisations. It describes the requirements for establishing and documenting an information security management system (ISMS). An ISMS in accordance with ISO 27001 minimises risks and establishes security procedures relating to information security, which help to achieve lasting optimisation of the quality of systems in organisations.

More information: www.tuv.com