Data Protection and Security

AGNITAS
e-mail & marketing automation

Highest IT Security Standard for maximized Data Security

For AGNITAS the topics of data protection and data security have top priority. Since the company's founding in 1999 we have observed the highest security standards for physical, electronic, and legal data protection measures. With the implementation of a management system for information security conforming to the ISO 27001 norm, AGNITAS ensures the confidentiality, integrity and availability of information within the sphere of influence of the entire organization.

Information Security Management System according to ISO 27001

With the ISO certification for the newest standard of 27001:2013, the DEKRA declaved AGNITAS the highest IT security standard for the whole company. The existing certification has been extended by two further norms, ISO 27017:15 for maximum data security in the cloud and ISO 27018:2014 for data protection in the cloud.
The ISO 27001 norm defines the requirements for manufacturing, commissioning, operation, monitoring, maintenance and improvement of a documented information security management system (ISMS), taking into account IT risks within the entire organization.

Business Continuity Management

for interruption-free business activity

Information Security Forum

for administration and monitoring

Monitoring Programs

for system and data base administration

This involves the following measures amongst others:

- ✔ Information Security Management Forum
- ✔ Business Continuity Management:
  - Protection against interruptions business activities
  - Protection against major faults in information systems and against catastrophes
  - Emergency plans for earliest possible resumption of all business activities
- ✔ Security training for all employees
- ✔ Comprehensive monitoring systems and checklists for system and database administration
- ✔ Special rules for software development (code changes, source code management etc.) to ensure smooth and fault-free processes

General rules for data security

- ✔ Strict behavioral rules for all employees to ensure that information in the security area is handled correctly and is not modified without authorization
- ✔ Strict access rules for all AGNITAS staff and visitors
- ✔ Data encryption system and special guidelines on external data exchange

Data protection

- ✔ Written obligation to confidentiality according to the German Federal Data Protection Act (BDSG) Clauses 5 and 11 for all employees
- ✔ Externally operating data protection officer from a recognized law chancellery
- ✔ Deposition of the „Data Processing“ obligation statement by AGNITAS in accordance with the German Dialog Marketing Association (DDV) directives
- ✔ Signing of the „DDV Code of Ethics for e-mail marketing“ regarding voluntary self-restriction

Our data center

Physical access protection

- Access is only possible for authorized employees, without exceptions
- Access control through security staff, access only after legitimation via ID
- Camera and motion sensors
- Sealed hosting area containing individually lockable computer racks

Electronic access protection

- Exclusive use of public/private keys with passphrases
- Encrypted exchange of data
- Firewalls continuously monitored by administrators, all access recorded in log files
- Professional hosting of all DNS servers by a commercial provider

Legal protection of data

- Use of Enterprise-class commercial servers running the Red Hat Enterprise Linux operating system for all mission-critical applications
- Oracle database management system (DBMS)
- In case of DBMS failure an active DBMS standby will take over
- Full data redundancy (raids and hard disks mirroring) and system redundancy (e.g. redundant power supply)
- Storage unit with standby hard disks that come into operation immediately on disk failure
- Standby server hardware to cope with capacity peaks during e-mail transmission
- Emergency supply of electricity through multiple uninterruptible power supplies (UPSs)

- Redundant power supply through two independent power lines and use of in-house diesel generators on supply failure
- Multiple redundant high-speed connections to different suppliers

Preventative measures

- Daily fully-automatic backup of all data (databases, log files, etc.) to disk and tape during operation
- Software system for monitoring of all critical systems such as servers and DBMS that automatically informs system administrators of failure by phone and e-mail
- 24-hour onsite standby service in data center
- mobile 14-hour standby by AGNITAS
- Redundant room- and rack air-conditioning
- Early detection smoke and fire alarm system
- Inert gas extinguisher system
- Without use of subcontractors
- Permanent training for our expert stuff

Security rules for e-mail transmission utilizing EMM

- ✔ Extensive and detailed checklists for trouble-free sending of mails
- ✔ Preventative measures and emergency plans should EMM-infrastructure be attacked and should database servers and systems fail
- ✔ Access protection for data contained in E-Marketing Manager
  - Secure access through password protection and encrypted data transmission
  - High minimum requirements for password that must be changed every three months
  - Log-in block after three failed login attempts
  - 2-way authentication for new devices: Prevents third parties who are in unauthorized possession of access data from accessing EMM
  - Release function in association with user rights
  - Activity log for administrators: What activities have been carried out by which user within a specific period
  - Protection against brute force attacks, internal XSS scripting and SQL injection attacks
  - Encryption algorithms for link coding that are currently believed to be unbreakable

CSA Certified Senders Alliance

DDV Qualitätsstandard E-Mail Marketing

Informationssicherheits-management ISO 27001 www.dekra-siegel.de DEKRA zertifiziert

Software Hosted in Germany Bundesverband IT-Mittelstand e.V.

In addition, AGNITAS was one of the first members of the „Certified Senders Alliance“ (CSA). Both the CSA membership and the E-Mail Marketing Code of Ethics require that regulations concerning the protection of customers and consumers, as well as their person-related data, are adhered to. These go much further than normal requirements.

Contact us for more information:
AGNITAS AG | Werner-Eckert-Str. 6 | 81829 Munich | sales@agnitas.de | www.agnitas.de