

Höchster IT Sicherheitsstandard für maximale Datensicherheit

Für AGNITAS haben die Themen **Datenschutz und Datensicherheit** oberste Priorität. Bereits seit der Gründung 1999 gelten bei uns höchste Sicherheitsstandards mit **physikalischen, elektronischen und rechtlichen Maßnahmen zum Datenschutz**. Mit der Implementierung des **Management Systems für Informationssicherheit nach ISO Norm 27001** stellt AGNITAS die **Vertraulichkeit, Integrität und Verfügbarkeit der Informationen im Einflussbereich der gesamten Organisation** sicher.



Information Security Management System nach ISO 27001

Die DEKRA bescheinigt der AGNITAS AG mit der Zertifizierung nach 27001:2013 den höchsten IT-Sicherheitsstandard für das gesamte Unternehmen. Die bestehende Zertifizierung wurde zudem um zwei weitere Normen, ISO 27017:2015 für maximale Datensicherheit in der Cloud und ISO 27018:2014 für Datenschutz in der Cloud, erweitert.

Die ISO-Norm 27001 definiert die Anforderungen für die Herstellung, die Einführung, den Betrieb, die Überwachung, die Wartung und die Verbesserung eines dokumentierten Informationssicherheits-Managementsystems (ISMS) unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation.



- ✓ Information Security Management Forum
- ✓ Business Continuity Management:
 - Schutz vor Unterbrechungen der Geschäftsaktivitäten
 - Schutz vor größeren Störungen von Informationssystemen und vor Katastrophen
 - Notfallpläne zur frühestmöglichen Wiederaufnahme aller Geschäftsaktivitäten
- ✓ Sicherheits- und Datenschutzs Schulungen für alle Mitarbeiter
- ✓ Umfangreiche Überwachungssysteme und Checklisten für System- und Datenbank-Administration
- ✓ Spezielle Regelungen für die Software-Entwicklung (bzgl. Codeänderungen, Quellcodeverwaltung, etc.) zur Gewährleistung von reibungslosen und fehlerfreien Abläufen

Allgemeine Regelungen zur Datensicherheit

- ✓ Strikte Verhaltensregeln, um Informationen im Sicherheitsbereich entsprechend zu behandeln und nicht unzulässig zu modifizieren
- ✓ Strikte Zugangsregeln für alle Mitarbeiter und Besucher der AGNITAS
- ✓ Daten-Verschlüsselungs-System und besondere Richtlinien zum externen Datenaustausch

Datenschutz

- ✓ Schriftliche Verpflichtungserklärung zur Geheimhaltung von Daten nach §5 und §11 BDSG für alle Mitarbeiter
- ✓ Externer Datenschutzbeauftragter einer renommierten Anwaltskanzlei
- ✓ Abgabe der Verpflichtungserklärung „Datenverarbeitung“ durch AGNITAS gemäß DDV-Vorgabe (Deutscher Dialogmarketing Verband e.V.)
- ✓ Unterzeichnung des „Ehrenkodex eMail-Marketing des DDV“ zur freiwilligen Selbstbeschränkung
- ✓ DSGVO-konform: Zahlreiche Features in der Software zur Erfüllung der EU-Datenschutzgrundverordnung

Unser Rechenzentrum

Physikalischer Zugriffsschutz

- Zugang nur für autorisierte Mitarbeiter möglich
- Zugangskontrolle durch Wachpersonal, Zugang nur nach Legitimierung durch Personalausweis
- Kameras und Bewegungsmelder
- Abgeschlossener eigener Hostingbereich und darin einzeln abschließbare Rechnerschränke (Racks)

Elektronischer Zugriffsschutz

- Ausschließliche Verwendung von Public/Private Keys mit Passphrases
- Verschlüsselter Datenaustausch
- Firewall, die ständig von Administratoren überwacht wird, mit Protokollierung aller Zugriffe in Logdateien
- Professionelles Hosting aller DNS-Server

Extrem hohe Ausfallsicherheit

- Einsatz von professionellen Marken-Servern der Enterprise-Klasse mit Betriebssystem Red Hat Enterprise Linux für alle mission-critical Anwendungen
- Datenbankmanagementsystem (DBMS) von Oracle
- Volle Datenredundanz (durch Raids und gespiegelte Festplatten) und Systemredundanz (z.B. doppelt vorhandene Netzteile)
- Storage-Einheit mit Standby-Festplatten, die bei Plattenausfällen im laufenden Betrieb einspringen
- Standby-Server-Hardware zum Ausgleich von Kapazitätsspitzen beim E-Mail-Versand
- Unterbrechungsfreie Notstromversorgung durch mehrere USVs

Vorbeugende Maßnahmen in Form von

- Tägliche, vollautomatische Sicherung aller Daten (Datenbanken, Log-Dateien, etc.) im laufenden Betrieb auf Band
- Software-System zur Überwachung aller systemkritischen Systeme wie Server und DBMS, das im Störfall automatisch die Systemadministration per Telefon und E-Mail informiert
- 24-Stunden-Bereitschaft vor Ort im Rechenzentrum, mobile 14-Stunden-Bereitschaft von AGNITAS
- Redundante Raum- und Schrank-Klimatisierung
- Rauch- und Brandfrühsterkennung
- Edelgas-Löschanlage
- Kein Einsatz von Subunternehmern
- Ständige Schulung des Fachpersonals

Sicherheitsregeln für den Mail-Versand mit dem EMM

- ✓ Ausführliche Checklisten für den einwandfreien Mail-Versand
- ✓ Vorbeugende Maßnahmen und Notfallpläne bei Angriffen auf die EMM-Infrastruktur und bei Ausfällen von Datenbank-Servern und -Systemen
- ✓ Zugriffsschutz für die Daten im E-Marketing Manager
 - Gesicherter Zugriff über Passwort-Schutz und verschlüsselte Datenübertragung
 - Hohe Mindestanforderungen an das Passwort, das alle 3 Monate geändert werden muss
 - Login-Sperre nach drei fehlgeschlagenen Login-Versuchen
 - 2-Wege-Authentifizierung für neue Geräte: Dritte, die unberechtigt in Besitz der Zugangsdaten gekommen sind, können so nicht auf den EMM zugreifen
 - Freigabe-Funktion in Verbindung mit Benutzerrechten
 - Aktivitätsprotokoll für Administratoren: Übersicht über die Aktionen einzelner Benutzer innerhalb eines bestimmten Zeitraums
 - Schutz vor Brute-Force-Angriffen, vor internen XSS-Scripting- und SQL-Injection-Angriffen
 - Verschlüsselungs-Algorithmen für Link-Codierung, die derzeit als unknackbar gelten



DDV
Qualitätsstandard
E-Mail Marketing



Darüber hinaus war die AGNITAS AG eines der ersten Mitglieder der “Certified Senders Alliance” (CSA). Sowohl die CSA-Mitgliedschaft als auch der Ehrenkodex E-Mail-Marketing erfordern die Einhaltung von Regelungen zum Schutz von Kunden und Verbrauchern sowie deren personen-bezogene Daten, die weit über die üblichen Anforderungen hinausgehen.

Für mehr Informationen wenden Sie sich an uns:

AGNITAS AG | Werner-Eckert-Str. 6 | 81829 München | sales@agnitas.de | www.agnitas.de