ratiokontakt
CLOUD FOR AMAZING CUSTOMERS

TOM

Technische und organisatorische Maßnahmen nach § 64 BDSG neu und Art. 32 DS-GVO

Der Auftragnehmer gewährleistet im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die nach § 64 BDSG-neu BDSG und Anlage gesetzlich geforderten Sicherheitsmaßnahmen und wird sie auf Verlangen des Auftraggebers nachweisen. Folgende besondere technische und organisatorische Maßnahmen werden bei der Verarbeitung eingehalten:

1. Zutrittskontrolle

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Video- und Alarmanlagen gesichert.
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
- Umgang mit betriebsfremden Personen
    - Private Besuche am Arbeitsplatz sind grundsätzlich untersagt
    - Geschäftliche Besuche unterliegen einer durchgängigen Aufsicht
    - Lieferanten werden persönlich vom Eingangsbereich abgeholt und stehen durchgängig unter Aufsicht

2. Zugangskontrolle

- bei Root Systemen und „Colocation“
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter sollten vordefinierte Richtlinien erfüllen. Bei zusätzlichen Maßnahmen können wir den Auftraggeber gerne kostenpflichtig unterstützen.
- bei Managed Systemen
    - Zugang ist passwortgeschützt, Zugriff besteht nur für Mitarbeiter von Auftragnehmer; verwendete Passwörter müssen komplexen Vorgaben entsprechen und eine Mindestlänge haben

3. Zugriffskontrolle

- Allgemein
    - Firewalls vor allen Systemen, die besondere Schutzmaßnahmen benötigen
- bei internen Verwaltungssysteme des Auftragnehmers
    - Sicherheitsupdate- und Backupmanagement (nach dem jeweiligen Stand der Technik) stellen sicher, dass unberechtigte Zugriffe verhindert werden.
    - Abgestufte Berechtigungsvergabe für Mitarbeiter des Auftragnehmers
    - Firewalls vor allen Systemen, die besondere Schutzmaßnahmen benötigen
- bei Root Systemen und „Colocation“
    - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber, da unsere Mitarbeiter auftragsbedingt keinen Zugriff haben

- bei Managed Systemen
  - Durch regelmäßige Sicherheitsupdates des Betriebssystems und der Standardsoftware und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
  - Verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers

4. Weitergabekontrolle

- Alle Mitarbeiter sind auf das Datengeheimnis nach § 53 BDSG (neu) bzw. § 5 BDSG verpflichtet.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Sichere und verschlüsselte Verbindungen für alle Verbindungen zwischen den Standorten
- Für Kunden-Services werden sichere Zugangskanäle angeboten

5. Eingabekontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- bei Root Systemen und „Colocation“
  - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
  - Bei diesen Systemen haben unsere Mitarbeiter keinerlei Zugriffsmöglichkeit. Wir nehmen Sperrungen aus rechtlichen oder technischen Gründen sowie im Falle des Zahlungsverzuges vor.
- bei Managed Systemen
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Unsere Mitarbeiter dürfen grundsätzlich ohne expliziete Anweisung des Auftraggebers nicht auf Ihre Daten zugreifen bzw. Daten eingeben, verändern oder löschen.

6. Auftragskontrolle

- Auf Wunsch Vertrag zur Datenverarbeitung
  - schriftliche Festlegung der weisungsbefugten Mitarbeiter des Auftraggebers
  - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datenschutzgeheimnis
  - Schriftliche Hinweise an die Mitarbeiter zum Datenverarbeitungszweck. Sie erhalten schriftliche Weisung zum Umgang mit personenbezogenen Daten.
  - Wirksame Kontrollrechte gegenüber dem Auftragnehmer
  - Laufende Überprüfung der Verfahren des Auftragnehmers
  - Eindeutige Vertragsgestaltung
- Formalisierte Auftragserteilung
  - Auftragsformular
  - Aufträge sind nur von verifizierten Kontaktadressen möglich (E-Mail und Fax)
  - Schriftliche Fassung und Dokumentation von Änderungen

7. Verfügbarkeitskontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
  - Backup- und Recovery-Konzept mit Sicherung aller relevanten Daten in angemessenen Intervallen.
  - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
  - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
  - Monitoring aller relevanten Server.
  - Einsatz unterbrechungsfreier Stromversorgung.
  - Maßnahmen gegen DDoS und sonstige Angriffe gegen die Systeme nach dem Stand der Technik
- bei Root Systemen und „Colocation“
  - Datensicherung obliegt dem Auftraggeber.
  - Hilfe und Beratung bei Schutzmaßnahmen gegen mögliche Angriffe, der Schutz liegt aber im verantwortungsbereich des Auftraggerbers
- bei Managed Systemen
  - Backup- und Recovery-Konzept mit Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
  - Einsatz von Festplattenspiegelung.
  - Einsatz unterbrechungsfreier Stromversorgung.
  - Einsatz von Softwarefirewall und Portreglementierungen.
  - Maßnahmen gegen DDoS und sonstige Angriffe gegen die Systeme nach dem Stand der Technik
- Allgemein
  - Firewalls
    - Restriktive Einstellungen - nur sichere und erlaubte Dienste sind erreichbar
    - Hardware-Firewall
    - Software-Firewall
  - Intrusion-Detection/Prevention-Systeme
  - Anti-Viren-Software
  - 24/7 Monitoring sämtlicher Dienste
  - 24/7 Bereitschaftstechniker auf Abruf verfügbar
    - erreichbar über Ticketsystem/E-Mail und zwei verschiedene Mobilfunknetze
  - Stromversorgung
    - 2 Trafostationen auf dem Gelände
    - Unterbrechungsfreie Stromversorgung (USV) 320 kW
    - Notstrom-Dieselgenerator 500 kW
    - Redundante Netzteile für Server buchbar
  - N + 1 redundante Klimatisierung
  - Geräte zur Überwachung von Temperatur in den Serverräumen
  - Feuer- und Rauchmeldeanlagen
  - Feuerlöschgeräte
  - Schutzsteckdosenleisten in den Server-Racks
  - Blitz- und Überspannungsschutz
  - Notfallpläne

8. Trennungskontrolle

- bei internen Verwaltungssysteme des Auftragnehmers
  - Datenverarbeitung erfolgt grundsätzlich auf je nach Zweck getrennten Systemen
  - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.
- bei Root Systemen und „Colocation“
  - Die Trennungskontrolle obliegt dem Auftraggeber.
- bei Managed Systemen
  - Je nach Paket werden Ihre Daten physikalisch oder logisch / virtuell von anderen Daten getrennt. Die Datensicherung erfolgt auf physikalisch oder virtuell getrennten Einheiten.

Impressum

Kontakt

ratiokontakt GmbH
Biegenhofstr. 13
96103 Hallstadt
Telefon: 09 51 / 9 35 35 – 0
Telefax: 09 51 / 9 35 35 – 9 02
E-Mail: info@ratiokontakt.de
Website: www.ratiokontakt.de