

## Rechenzentrum - Kurzbeschreibung

Das Rechenzentrum der PI Informatik im traditionsreichen Industriegebiet PankowPark wurde 2001 neu errichtet und bietet u.a. folgende Rahmenbedingungen für den Betrieb von Serversystemen und Anwendungen:

- ISO 27001:2008 sowie ISO 9001:2008 Zertifizierung
- Primärlokation mit 100m<sup>2</sup> Stellfläche
- Co-Lokation (Backup-Rechenzentrum) in separatem Gebäude (300m entfernt) integriert im Campus Backbone (Ringnode). Das Backbone des PankowPark (ca. 22km Fiber, ca. 400km Kupfer) befindet sich komplett im Eigentum der PI Informatik.
- Physisch getrennte, redundante Außenanbindungen in den Campus Backbone
- Zugang für Kundennetze über zwei unabhängige Versorgungspunkte (A0-Punkte) der Deutschen Telekom (Carrier wahlfrei)
- Eigenes autonomes System mit derzeit 2 Peering-Partnern\*
- Getrennte Hauptstromversorgung für Primär- und Co-Lokation
- USV- und Notstromversorgung für Primär- und Co-Lokation
- Redundante Klimatechnik in aktiver Kalt- und Warmgangausprägung und energieeffizienter Außenluftkühlung
- Einsatz von Wachschutz, Zutrittskontrolle, Alarm- und Brandmeldesysteme
- 3-Schichtbetrieb (24/7), Zentrales Management und Überwachung
- Möglichkeit, kundenspezifische Dienste in Überwachung zu integrieren
- Komplett unabhängiges Online Backup-Netzwerk (Backup to Disk to Mirror) mit redundanter Datenhaltung in getrennten Lokationen. Optional Spiegelung an eine dritte Lokation oder Auslagerung auf Tape.
- Bei optionaler Tape-Sicherung: Feuersichere (S120DIS) Lagerung von Backup-Datenträgern in getrennten Brandabschnitten.
- ITIL-konforme Prozeßorganisation des Servicemanagements (z.B. Incident und Change Management)
- Kundenspezifische Risiko- und Verfügbarkeitsanalysen nach der RiskPriorityMethod (RPM) können durchgeführt werden.
- Aufgrund des Kompetenzspektrums ist Kombination von Accomodation sowie Basis- und Applikationsbetrieb in einer Hand möglich.
- SLA können kunden- oder dienstspezifisch vereinbart werden und sind nicht zwingend an feste Schema gebunden („nur so viel Verfügbarkeit wie für den Geschäftsprozeß nötig“).
- Einsatz von langjährig erfahrenem Betriebspersonal.
- Kontinuierliche Rotation zwischen 1st und 2nd Level-Support zur Sicherstellung bestmöglicher Kompetenz und hoher 1st Level-Lösungsquote am Help Desk
- Datenschutz- und Datensicherheit werden durch geschultes / zertifiziertes Personal sichergestellt. Die Sachkundenachweise werden nach Ulmer Modell erbracht.

\*) Die PI Informatik ist seit 2001 Mitglied im RIPE

Status: März 2016 | Version 2016-02

Mit den zwei Lokationen unseres RZ können HV-Lösungen bis zu einer Verfügbarkeit von bis zu 99,5% effizient und flexibel abgebildet werden.

Für spezifische HV-Anforderungen, wie z.B. georedundante Architekturen, kooperieren wir mit einem Spezialunternehmen, welches an verschiedenen Standorten in Deutschland Hochsicherheits-Rechenzentren betreibt. Weiterhin können wir auf diesem Weg bei Bedarf Lösungen mit einer technischen Verfügbarkeit von 99,9x % anbieten.

## **Allgemeine Standards Auftragsdatenverarbeitung und Providerdienste**

Sämtliche RZ Leistungen der PI Informatik werden auf der Grundlage der Auftragsdatenverarbeitung (§ 11 Bundesdatenschutzgesetz) in Deutschland erbracht.

### *Einhaltung des Bundesdatenschutzgesetzes (BDSG)*

Die PI Informatik beachtet uneingeschränkt die Vorschriften des Bundesdatenschutzgesetzes für die Auftragsdatenverarbeitung. Alle Mitarbeiter sind nach § 5 BDSG schriftlich auf das Datengeheimnis verpflichtet. Alle RZ- und Service- Mitarbeiter werden zusätzlich auf das Fernmeldegeheimnis nach § 88 TKG verpflichtet. Die Erfordernisse des BSDG hinsichtlich der Auftragsdatenverarbeitung, insbesondere die Regelungen gem. §11, werden im Rahmen des SLA-Managements vertraglich mit den Kunden fixiert und sind als Vertragsanlage obligatorischer Bestandteil des jeweiligen Betriebskonzeptes. Dies kann durch kundenspezifische Bestimmungen zusätzlich ergänzt und erweitert werden. Diese Festlegungen finden Anwendung auf alle Leistungen, welche die PI Informatik gegenüber dem Auftraggeber erbringt und auf alle Tätigkeiten, bei denen deren Mitarbeiter oder durch uns beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

Die BDSG-Anforderungen [Technisch / organisatorische Maßnahmen (TOM) gem. § 9 BDSG] hinsichtlich

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

werden wie folgt (soweit kundenunabhängig zutreffend) gewährleistet:

- Das Industrieareal, auf denen sich Rechenzentrum und Co-Lokation befinden, wird durch Videoüberwachung sowie ein Wachschutzunternehmen 24/7 kontrolliert.
- Mechanische sowie elektronische Zutrittssysteme zu den Gebäuden sowie zu den Firmenräumen selbst

- Internes hierarchisches Schließsystem zur Vermeidung des unbefugten Zutritts zum Rechenzentrum selbst.
- Alarmgesicherte Bereiche für Rechenzentrum, Co-Lokation sowie für sämtliche relevanten Netzzugangspunkte und Infrastruktursysteme
- Laufende Protokollierung zur Nachweisführung (Betriebstagebuch)

Darüber hinaus vereinbaren wir jeweils in kundenindividueller Ausprägung spezifische Maßnahmen wie z.B.:

- Software-Zugangsmechanismen auf den Servern
- Mitarbeiterunabhängige Paßwortverwaltungsverfahren
- Kundenspezifische Konfiguration von OS-Schutzmechanismen (Paßwort, Benutzer-ID, Gruppenzugehörigkeit)
- Kundenspezifische und bedarfsgerechte Applikations-Zugriffsmechanismen (Berechtigungsprofile, Rollenkonzepte, Paßwörter etc.)
- Mehrstufige Firewall- und DMZ-Konzepte
- Einsatz von Verschlüsselungs- und IRM-Techniken
- Mehrstufige Genehmigungs- und Freigabeverfahren
- Mandantengestützte Datentrennungsvverfahren
- Spezifische Protokoll- und Nachweisverfahren
- Berufsständische Vertraulichkeitsregelungen etc.

## Qualitätsmanagement, Zertifizierung, Auditierung

**ISO 9001** Es erfolgt eine jährliche Konformitätskontrolle der Abläufe durch die ISOCERT GmbH. Innerhalb eines Prüfungs- und Auswahlverfahren erfolgt längstens alle 3 Jahre eine erneute Zertifizierung.

**ISO 27001** Es erfolgt eine jährliche Konformitätskontrolle der Abläufe durch die ISOCERT GmbH. Innerhalb eines Prüfungs- und Auswahlverfahren erfolgt längstens alle 3 Jahre eine erneute Zertifizierung.

Der Datenschutzbeauftragte der PI Informatik wirkt im regionalen Arbeitskreis ERFA Berlin-Brandenburg der GDD e.V. mit. Damit ist jederzeit aktuelles Fach- und Praxiswissen auf dem Gebiet des Datenschutzes gewährleistet. Der DSB des Kunden erhält im Rahmen des Service Level Agreements die Kontrollrechte gem. §11 BDSG. Die Datenschutzberater der PI Informatik erwerben Ihren Sachkundenachweis mit der Prüfung nach dem Ulmer Modell.



Die PI Informatik ist Gründungsmitglied des Trusted Cloud Kompetenznetzwerkes e.V. Die von uns angebotenen Lösungen erfüllen die Kriterien des Trusted Cloud Labels des BMWi.

Darüber hinaus können jederzeit kundenspezifische Audit- und Sicherungsverfahren vereinbart werden.