



The eBusiness Solution Company.

RECHENZENTRUM SICHERHEITSMERKMALE



www.prodatis.com

RECHENZENTRUM

In unserem Rechenzentrum steht Ihnen die ideale Infrastruktur für Ihre Anwendungen zur Verfügung. Unternehmen und Verwaltungen, die besonders hohe Anforderungen an die Verfügbarkeit ihrer geschäftskritischen Anwendungen stellen, finden im PRODATIS Rechenzentrum den idealen Standort.

› INFRASTRUKTUR

Gesicherte, redundante und kreuzungsfreie WAN- /Strom-Trasse

Geordnete Verlegung im Doppelboden

Wartungsprotokolle für alle Anlagen

Regelmäßige Wartung der Anlagen

ISDN-Übertragungswege

Temperaturüberwachung

Unterbrechungsfreie Wartung

Kennzeichnungsmaßnahmen

Zertifizierung/Abnahme durch Zertifizierungsstelle

Wartungs- und Alarmpläne

Wartungspläne für Klima, EMA, BMA und Energie

› RESSOURCEN

Vollklimatisierung

Äußerer Blitzschutz

Notfallplan/Back-Up-Lösung

Verfügbarkeitsanforderungen

› BRANDSCHUTZ

Meidung brennbarer Ausbaustoffe und Möbel, keine Verkleidungen

Aufteilung in einzelne Funktions-, Brand-, Rauchabschnitte

Brandschutz, Melde- und Löschtechnik

Brandmeldeanlage

Brandmelder optisch + akustisch

Brandmeldezentrale (BMZ)

Handfeuermeldern

Automatische Brandmelder

Abnahmeprotokoll Feuerwehr

VDS-Löschanlage

TÜV Löschanlage

Brandfrühsterkennung durch Ansaugrauchmelder

Rauchmelderdichte mit 2-Melderabhängigkeit

Argon-Löschanlage

Handfeuerlöscher

Eigener Brandabschnitt mit mehreren Meldelinien

› ZUGANG

Absicherung Türen, Fenster, Abschlüsse gegen Einbruch

Gestützte Energieversorgung der Meldeanlage

Alarmorganisation

Öffnungs-, Glasbruch- und Bewegungsmelder

EMA-Wartung

Feste Bauweise mit hohem Widerstand (Steine über 120 mm Dicke und Beton über 100 mm Dicke)

Sicherheitssysteme und -organisation

Einbruchmeldeanlage (EMA) Typ B

VDS-Attest Einbruchmeldeanlage

Meldebereiche

Gestützte Energieversorgung der Einbruchmeldeanlage (EMA)

Zutrittskontrollanlage durch Zoneneinteilung, Auswertungsmöglichkeiten, Auswertungen Notstromversorgung/USV

Regelm. Sicherheitsbegehungen

Zutrittsregelung über Schlüssel und Transponder-System & telefonische Anmeldung außerhalb der Kernzeiten

Sicherheitsunterweisung

Alarmplan / Eskalationspläne für den Wachdienst



WEITERE SERVICES

- _ Telefonsupport
- _ 24 x 7 Monitoring
- _ mehrstufige Backuplösungen
- _ ISDN Mehrgeräteanschluss
- _ Fax, Mail und SMS Server zur
- _ Integration in Ihre Anwendungen

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN GEMÄSS § 9 BDSG

Nachstehend erfolgen eine Aufstellung und eine Beschreibung der wesentlichen Maßnahmen von PRODATIS zur Einhaltung der Datensicherheitsvorschriften gemäß der Anlage zu § 9 BDSG (Kontrollziele Nummern 1 bis 8). Hierbei ist einschränkend darauf hinzuweisen, dass ein Rechenzentrum verständlicherweise nicht alle Sicherheitsvorkehrungen offenlegen kann; vielmehr ist gerade im Interesse des Datenschutzes und der Datensicherheit der Verzicht auf vertrauliche und detaillierte Beschreibungen unabdingbar.

Durch freiwillige Datenschutzaudits gemäß § 9a BDSG wird auch der Nachweis erbracht, dass der Datenschutz bei PRODATIS nach den Vorgaben des BDSG gesetzeskonform gestaltet und wirksam bei Canaletto umgesetzt wird.

Die Mitarbeiter von PRODATIS sind mit den Vorschriften des BDSG vertraut und auf das Datengeheimnis verpflichtet.

› ZUTRITTSKONTROLLE

Die Betriebsareale, die in mehrere Sicherheitsbereiche mit differenzierten Zutrittsberechtigungen aufgeteilt sind, werden rund um die Uhr durch den Betriebsschutz überwacht. Der Zutritt zu den baulich extrem abgeschotteten und elektronisch überwachten Sicherheitszonen des Rechenzentrums ist nur autorisierten Personen möglich.

› ZUGANGSKONTROLLE

Der Zugang kann nur über ein Zugangskontrollsystem erfolgen. Beim elektronischen Datenaustausch zwischen dem PRODATIS Rechenzentrum und den Kunden besteht das Sicherungssystem aus vielschichtigen und komplexen Prüfungen. Weitere technische Absicherungen erfolgen über Firewalls und Proxyserver. Soweit technisch möglich und wirtschaftlich vertretbar, werden hierzu geeignete Verschlüsselungstechnologien eingesetzt.

› ZUGRIFFSKONTROLLE

Eine Reihe von Hardware- und Software-Identifikationsmaßnahmen, die Verschlüsselung der Daten bei der Datenübertragung sowie ein mehrstufiges Zugriffs- und Nutzungskontrollverfahren schließen den unbefugten Zugriff auf die gespeicherten Datenbestände und die unberechtigte Kenntnisnahme aus. Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen. Soweit technisch möglich und wirtschaftlich vertretbar, werden hierzu geeignete Verschlüsselungstechnologien eingesetzt.

› WEITERGABEKONTROLLE

Beim elektronischen Datenaustausch besteht das Sicherungssystem aus vielschichtigen und komplexen Prüfungen. Strenge Sicherheitsvorkehrungen im Rechenzentrum gewähr-

leisten, dass ein unbefugtes Entfernen von Datenträgern aus den Sicherheitsbereichen verhindert wird. Entsorgungsgut mit schutzwürdigem Inhalt wird durch hausinterne Shredder unter Beachtung des Vier-Augen-Prinzips vernichtet.

› EINGABEKONTROLLE

Ein mehrstufiges Protokoll- und Auditingverfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können.

› AUFTRAGSKONTROLLE

Die zur Verarbeitung eingereichten Daten werden entsprechend den gesetzlichen Vorschriften nur im Rahmen der Weisungen des jeweiligen Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben. Der Weisungsrahmen ist insbesondere durch den schriftlich geschlossenen Vertrag zur Datenverarbeitung im Auftrag unter Berücksichtigung der Pflichtinhalte gemäß § 11 Abs.

2 BDSG sowie ferner durch die Anwendungsbeschreibung der PRODATIS-Programme eindeutig vorgegeben. Gleiches gilt für auftragsbezogene Auskünfte; sie werden ausschließlich an den Auftraggeber oder im Rahmen seiner Weisungen erteilt. Ausnahmen vom konkreten Weisungsrahmen gelten für technisch bedingte Verarbeitungen, z.B. für die interne Datensicherung.

› VERFÜGBARKEITSKONTROLLE

Zahlreiche Datensicherungsmaßnahmen gewährleisten, dass personenbezogene und andere schutzwürdige Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Besonders umfangreich sind die Brandschutz-, Verlustsicherungs- und Katastrophenschutzmaßnahmen. Hierzu gehören unter anderem die Absicherung sämtlicher EDV-Räume und deren Umgebung durch Brandmelde- und stationäre Feuerlöschanlagen, die mehrfache maschinelle und gegen unbefugten Zugriff gesicherte Auslagerung von Datensicherungsbeständen, die Notstromversorgung zur unterbrechungsfreien Überbrückung von Stromausfällen sowie der 24-Stunden-Bereitschaftsdienst von Einsatz- und Evakuierungsleitung.

› TRENNUNGSGEBOT

In allen wichtigen Bereichen besteht das Prinzip der Funktionstrennung – 4-Augen-Prinzip; das heißt, alle in die Datenverarbeitung eingebundenen Abteilungen sind funktionell, organisatorisch und räumlich getrennt. Das Prinzip der Funktionstrennung ist auch weitgehend innerhalb der Organisationseinheiten verwirklicht;

schutzwürdige Daten werden den Mitarbeitern nur in dem Umfang zur Verfügung gestellt, wie es für die zugewiesene rechtmäßige Aufgabenerfüllung unbedingt erforderlich ist. Zur Sicherstellung werden definierte Rechteprofile für die verschiedenen Funktionsbereiche zugeteilt und zentral administriert. Zahlreiche Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken und für unterschiedliche Ordnungsbegriffe (z. B. Mitglieds- und Mandantenummer) erhobene bzw. gespeicherte Daten getrennt verarbeitet werden können.

PRODATIS

Stand: 30.04.2010