IT für Gesundheit und Soziales RZV

# RZV GmbH
# Ergänzende Normen und Prüfungsstandards

Ergänzend zu den Zertifikaten **ISO 27001, TÜViT TSI** und **SAP PCoE** (Partner Center of Expertise) erfüllt die RZV GmbH inhaltlich die Anforderungen der Normen **ISO 27701, ISAE 3402** und **IDW PS 951**.

Wetter, 06.05.2024

gez. Dr. Stefan Wolf
Geschäftsführer

gez. Martin Backhaus
Geschäftsführer

Dieses Schreiben wurde maschinell erstellt und ist ohne Unterschriften gültig.

## Inhalt

## 1 Vorbemerkung zu unseren Zertifikaten ISO 27001 und TÜViT TSI

Die **Wirksamkeit unseres integrierten RZV Managementsystems,** insbesondere unseres Prozesses **Informationssicherheit und Datenschutz, wird jährlich durch folgende externe Institutionen begutachtet** und alle 3 Jahre nach **ISO/IEC 27001** erneut zertifiziert:

1. DQS GmbH (Deutsche Gesellschaft zur Zertifizierung von Managementsystemen)

**Ergänzend zu der jährlich wiederkehrenden Wirksamkeitsüberprüfung** im Rahmen unserer ISO/IEC 27001 Zertifizierungen, werden unsere Prozesse und Vorgaben zur **Informationssicherheit und zum Datenschutz** regelmäßig von zwei weiteren neutralen externen Institutionen begutachtet:

2. TÜV Informationstechnik GmbH zur regelmäßigen Überprüfung der IT-Infrastruktur unserer beiden Rechenzentren hinsichtlich der Anforderungen des **TÜViT-Prüfkataloges "Trusted Site Infrastructure (TSI)**"

3. PERGON Unternehmensberatung e. K. mit Herrn Jürgen Bühse als unserem **extern benannten RZV Datenschutzbeauftragtem gemäß Art. 37 DS-GVO** zur kontinuierlichen Aufgabenwahrnehmung gemäß Art. 39 DS-GVO.

## 2 Erläuterungen zu ergänzenden Normen und Prüfungsstandards

### 2.1 ISO 27701 (oder vergleichbare Standards)

Die **ISO/IEC 27701** ist eine Erweiterung von **ISO/IEC 27001** (Informationssicherheits-Managementsystem (ISMS)) und **ISO/IEC 27002** (Security Controls) um Datenschutzkriterien. Die internationale Norm bietet Leitlinien für den Schutz der Privatsphäre und zum Umgang von Unternehmen mit personenbezogenen Daten. Sie hilft beim Nachweis der Einhaltung von Datenschutzbestimmungen weltweit.

Im Unterschied zur ISO/IEC 27001 spricht die Managementnorm **ISO/IEC 27701** statt von „Informationssicherheit“ von „**Informationssicherheit und Datenschutz**“. Darüber hinaus gibt es weitere inhaltliche Ergänzungen: So müssen unter anderem bei der Betrachtung des Kontextes der Organisation relevante Datenschutzgesetze und gerichtliche Entscheidungen berücksichtigt werden. Ebenso gilt es, bei der Risikobeurteilung Kriterien der Verarbeitung von personenbezogenen Daten zu berücksichtigen.

ISO 27701 ist heute - auch wenn sie auf ISO 27001 aufbaut - noch nicht zertifizierbar. Zertifiziert wird ein ISMS nach ISO/IEC 27001. Es ist aber möglich, die erweiterten Anforderungen im Rahmen eines Audits, wie den ISO/IEC 27701-komformen Umgang mit personenbezogenen Daten, überprüfen zu lassen. Hierfür steht RZV ihren Kunden und Interessenten selbstverständlich jederzeit gern zur Verfügung.

### 2.2 ISAE 3402 (international) = IDW PS 951 (DE) = SSAE 18 - SOC1, SOC2 (USA)

**ISAE 3402** (international) **= IDW PS 951** (DE) **= SSAE 18 - SOC1, SOC2** (USA) sind Prüfungsstandards der Wirtschaftsprüfer zur Überprüfung des Aufbaus sowie der Angemessenheit des dienstleistungsbezogenen, internen Kontrollsystems (**IKS**) für IT-Prozesse mit Kundenbezug.

Wir, RZV haben den Aufbau und die Angemessenheit unseres dienstleistungsbezogenen internen Kontrollsystems (IKS) für die Dienstleistungen Rechenzentrumsdienstleistungen, Betriebssystem Administration, Datenbank Administration, Applikationsbetreuung, Benutzerbetreuung, Management von LAN- und WAN-Netzwerken, Systemverfügbarkeit und Katastrophenvorsorge, IT-Sicherheit, Datensicherung und -wiederherstellung überprüfen lassen und ein entsprechendes Testat erhalten.

## 3 Erfüllung der ergänzenden Normen und Prüfungsstandards

Der Aufbau sowie die Angemessenheit unseres internen Kontrollsystems (IKS) für ausgelagerte Funktionen wurde im Juli 2014 durch eine der größten unabhängigen Wirtschaftsprüfungsgesellschaften Deutschlands, der Firma Ebner Stolz GmbH & Co. KG, gemäß den Anforderungen des Prüfungsstandards des Instituts der Wirtschaftsprüfer (IDW PS 951 Typ A) geprüft und durch das entsprechende Testat bestätigt.

Der zugehörige IDW PS 951 Prüfbericht kann auf Anfrage Kunden und Interessenten zur Einsichtnahme zur Verfügung gestellt werden.

Eine jährlich wiederkehrende IDW PS 951 Prüfung Typ A sowie eine Prüfung nach IDW PS 951 Typ B sind entbehrlich, da die Prozessbeschreibungen, Richtlinien, Dokumente und Aufzeichnungen unseres **integrierten RZV Managementsystems ISO/IEC 27001 (Informationssicherheitsmanagement) die wesentliche Grundlage für die Beschreibung unseres internen Kontrollsystems (IKS) bilden**. Zur Vermeidung doppelter Prüfungsaufwände wurde und wird auf eine erneute Prüfung verzichtet.

Insbesondere unser Prozess "**Informationssicherheit und Datenschutz**" ist zentraler Kern in unserem **integrierten RZV Managementsystem**. Damit erfüllen wir die Normen **ISO/IEC 27001** und **ISO/IEC 27701** sowie die Anforderungen **für technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 Datenschutz-Grundverordnung der Europäischen Union (DS-GVO)**, § 27 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD), § 26 Gesetz über den Kirchlichen Datenschutz (KDG) und § 64 Bundesdatenschutzgesetz (BDSG).

Selbstverständlich sind wir jederzeit bereit, die Ordnungsmäßigkeit unseres Datenschutzmanagementsystems (**ISO 27701**) sowie unseres internen Kontrollsystems (IKS) (**ISAE 3402/ IDW PS 951**) durch geeignete Prüfungshandlungen unserer Kunden und Interessenten beurteilen zu lassen.

## 4 Nachweise und Quellen

### 4.1 Nachweise

- RZVZertifikat - ISO 27001
- RZVZertifikat - TÜViT TSI ARZ
- RZVZertifikat - TÜViT TSI RZ-Betrieb
- RZVZertifikat - SAP PCoE
- RZVZertifikat - IDW PS 951 Typ A Prüfbestätigung

**Vgl. RZV Internet-Portal:** https://www.rzv.de/unternehmen/zertifikate

### 4.2 Quellen

**zu 2.1** vgl. etwa: https://www.dqs.de/de/audits/produkte/iso-27701/, abgerufen 18.04.2024, 11:11 Uhr

**zu 2.2** vgl. etwa: https://de.wikipedia.org/wiki/ISAE_3402, abgerufen 18.04.2024, 11:30 Uhr sowie verschiedene Veröffentlichungen namhafter Wirtschaftsprüfungsgesellschaften