Auditbericht Datenschutz
02-2025

pcvisit Software AG

Manfred-von-Ardenne-Ring 20, 01099 Dresden, Deutschland

Inhaltsverzeichnis

1. Grundlagen und Methodik 3

2. Übersicht zur Bewertung von Abweichungen 4

3. Zusammenfassung / Ergebnis 5

4. Prüfung der technisch organisatorischen Maßnahmen (TOMs) 7

4.1 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO) 7

4.2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO) 7

4.2.1. Zutrittskontrolle Unternehmensräumlichkeiten 7

4.2.2 Zutrittskontrolle externe Serverräume 7

4.2.3 Zugangskontrolle 7

4.2.4 Zugriffskontrolle 8

4.2.5. Trennungsgebot 8

4.3 Integrität (Art. 32 Abs. 1 lit. b DSGVO) 8

4.3.1. Schwerpunktprüfung: Weitergabekontrolle 8

4.3.2. Eingabekontrolle 9

4.4. Verfügbarkeit / Belastbarkeit / rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO) 9

4.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DS-GVO; Art. 32 Abs. 1 lit. d DS-GVO) 9

4.5.1. Datenschutz-Management 9

4.5.2. Incident-Response-Management 10

4.5.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) 10

4.5.4. Auftragskontrolle 10

4.6 Prüfung der Unterauftragnehmer 10

4.7 Handlungsempfehlungen 11

1. Grundlagen und Methodik {#grundlagen-und-methodik}

Das interne Datenschutzteam der pcvisit Software AG hat im Zeitraum Januar 2025 - Februar 2025 gemäß Art. 32 (1) lit d (“ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung”) die technisch-organisatorischen Maßnahmen der pcvisit Software AG sowie deren Unterauftragnehmer (siehe auch AVV Punkt 6.5) geprüft. Die Prüfungen wurden hauptsächlich in Form von virtuellen Meetings und Gesprächen mit den beteiligten MitarbeiterInnen durchgeführt. Der Schwerpunkt der Prüfung lag bei dem Thema Weitergabekontrolle (Art. 32 Abs. 1 lit. b DS-GVO).

Folgende MitarbeiterInnen wurden befragt:

Tilo Müller	**IT, internes Datenschutzteam**
Katharina Fischer	Recht und Finanzen, Personal, QM, internes Datenschutzteam
Roberto Galz	Kunden-Support, Interner Helpdesk
Andreas Rombach	Kunden-Support
Edith Pistner	Buchhaltung, Vertragsverwaltung
Manuela Mrowetz	Backoffice, Personal

Als Prüf-/Auditgrundlage wurden verwendet:

- Datenschutz Grundverordnung (DSGVO)

- Anlage 1 zum AV-Vertrag (Version 1.8) Technische und organisatorische Maßnahmen im Sinne des Art. 32 DS-GVO (Link: siehe Footer Website www.pcvisit.de)

Das Audit wurde durchgeführt von:

Katharina Fischer	**geprüfte Qualitätsmanagerin (IHK) mit Weiterbildung Risikomanagement**
Tilo Müller	Weiterbildung zum Datenschutzbeauftragten

2. Übersicht zur Bewertung von Abweichungen {#übersicht-zur-bewertung-von-abweichungen}

Um eventuell festzustellende Abweichungen bzw. Mängel angemessen einzustufen, wurden sie in folgende Kategorien aufgeteilt:

Kritikalität	**Bewertung**	**Erläuterung**
Kein Mangel	0	Liegt vor, wenn keine Feststellungen und/oder Hinweise (Empfehlungen) vorhanden sind.
Nicht relevanter Mangel	1	Dies liegt vor, wenn es sich um rein formale nicht vorhandene Umsetzungen mit keinen oder nur unwesentlichen Folgen für die Rechte und Freiheiten Betroffener bzw. um **Verbesserungspotentiale** handelt.
Mäßiger Mangel	2	Ein mäßiger Mangel liegt vor, wenn zwingende formale Anforderungen nicht erfüllt wurden, wie z.B. das Fehlen von Richtlinien.
Schwerwiegender Mangel	3	Schwerwiegende Mängel sind erheblich, z.B. der nur teilweisen Nichtumsetzung von BSI-Vorgaben mit wesentlichen Auswirkungen.

Kritikalität	Bewertung	Erläuterung
Besonders schwerwiegender Mangel	4	Ein besonders schwerwiegender Mangel ist gegeben bei besonders erheblichen Mängeln, z.B. der vollständigen Nichtumsetzung von Mindestanforderungen des BSIs oder von Mängeln mit besonders hohen Auswirkungen auf die Rechte und Freiheiten Betroffener (natürlicher Personen).

3. Zusammenfassung / Ergebnis {#zusammenfassung-/-ergebnis}

Die pcvisit Software AG erbringt für den Kunden/Auftraggeber auf der Grundlage des bestehenden Servicevertrags über die **Bereitstellung einer Fernwartungs-Software** die dort näher bezeichneten Leistungen (siehe EULAS).
Die pcvisit Software AG verarbeitet verschiedene personenbezogene Daten von Interessenten, Kunden, Dienstleistern, Mitarbeitern, Bewerbern.

1. Personenstammdaten / Kontaktdaten:
   Name, Vorname, Anschrift, Firmenbezeichnung, Telefon, E-Mail, Profilbild (optional)

2. Vertragsstammdaten:
   Vertragsbeziehung, Produktnutzung, gekaufte Produkte, Bankverbindung

3. technische Daten:
   IP-Adresse, Gerät, Browser, Standort, Mac-Adresse, Produktversion

4. Benutzerkontoinformationen:
   Kundennummer, Firmen-ID, Anzeigename, Spracheinstellung, Berechtigungseinstellungen, Teammitglieder, Kontaktliste

5. zusätzliche Datenkategorien bei Support-Anfragen der Kunden des Auftraggebers über die pcvisit Services:
   Supportfall-ID, Bearbeiter, Beschreibung (Freitextfeld Notizen, Chat, Supportanfrage)

6. Verbindungsdaten:
   z.Bsp. Fernwartungsdauer, Anzahl der Fernwartungen und Ferndiagnosen, Fernwartungs-ID, Fernwartungskommentare (Freitextfeld) etc.

7. sonstige Daten:
   personenbezogene Daten im Zusammenhang mit der Anmeldung bei den pcvisit Services

Während des Audits wurden die technisch-organisatorischen Maßnahmen geprüft und bewertet (siehe Punkt 2). Die Prüfung und Nachweisführung erfolgte anhand von Stichproben der Dokumentationen, Schulungen, schriftlichen Regelungen, Produktnutzung, Protokolle, Monitoring etc.

Ergebnis:

Bei der Prüfung wurden keine relevanten Abweichungen (Bewertung 3 oder höher) festgestellt. Die von der pcvisit Software AG gemachten Angaben im Auftragverarbeitungsvertrag gemäß Art. 28 DS-GVO (Version 1.8) : *Anlage 1 Technische und organisatorische Maßnahmen im Sinne des Art. 32 DS-GVO* sind implementiert und entsprechen den vertraglich zugesicherten Maßnahmen.

Dresden, 25.02.2025

_____

Helge Betzinger, CTO und Vorstand pcvisit Software AG

4. # Prüfung der technisch organisatorischen Maßnahmen (TOMs) {#prüfung-der-technisch-organisatorischen-maßnahmen-(toms)}

4.1 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO) {#4.1-

pseudonymisierung-und-verschlüsselung-(art.-32-abs.-1-lit.-a-ds-gvo)}

Im Rahmen der Verarbeitung von personenbezogenen Daten kommen verschiedene Verschlüsselungsmechanismen (bspw. SSL/SSH-Verschlüsselung bei Übertragung; externer Zugriff per VPN) zum Einsatz. Zudem werden die Kundendaten auf den Datenverarbeitungssystemen zum Teil pseudonymisiert (Kundennummer bzw. Identitätsnummer), um einen noch höheren Schutz der Daten zu gewährleisten.

4.2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO) {#4.2-vertraulichkeit-(art.-32-abs.-1-lit.-b-dsgvo)}

4.2.1. Zutrittskontrolle Unternehmensräumlichkeiten {#4.2.1.-zutrittskontrolle-unternehmensräumlichkeiten}

Die in den TOMs aufgeführten Maßnahmen wurden geprüft, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen in Unternehmensräumlichkeiten, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Dazu zählen u.a. angemessene Sicherheitsschließsysteme, Wachschutz, Schulung aller MitarbeiterInnen, dokumentierte Schlüsselvergabe und Besucherregistrierung.

4.2.2 Zutrittskontrolle externe Serverräume {#4.2.2-zutrittskontrolle-externe-serverräume}

Die in den TOMs aufgeführten Maßnahmen wurden geprüft, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen in externen Serverräumen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.Das umfassende Sicherheitskonzept der von uns genutzten Rechenzentren garantiert, dass alle Daten vor Diebstahl oder Beschädigung durch Umwelteinflüsse geschützt sind. Die Rechenzentren sind ISO 27001 zertifiziert.

4.2.3 Zugangskontrolle {#4.2.3-zugangskontrolle}

Die in den TOMs aufgeführten Maßnahmen wurden ergriffen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dazu

zählen zum Beispiel

- Verbindliches Verfahren zu Vergabe und Entzug von Berechtigungen
- Die Datenübertragung von und zu den DV-Systemen wird bei kritischen Aktivitäten (z.B. bei Systempflege, Software-Updates, Backups, Fernwartung) durch verschiedene Maßnahmen gegen Nutzung durch Unbefugte gesichert: (z.B. Verschlüsselung, Überprüfung bekannter öffentlicher Schlüssel bei Kontaktaufnahme, Protokollierung der Systemnutzung)
- Eine Kennwortrichtlinie mit Vorgaben für den Passwort-Standard ist implementiert.
- Einsatz von Firewalls, Spamfilter und Virenschutz Programme
- Funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe) und Abschaltung von überflüssigen Diensten
- umfassendes Netzwerk-Monitoring mit entsprechenden Alarmierungen
- Patch- und Update-Management

4.2.4 Zugriffskontrolle {#4.2.4-zugriffskontrolle}

Die in den TOMs aufgeführten Maßnahmen gewährleisten, dass die Nutzer der Datenverarbeitungssysteme ausschließlich auf die entsprechend ihrer Zugriffsberechtigung zugeordneten Daten (und Programme) zugreifen können und personenbezogene Daten bei der Verarbeitung, Nutzung und nach Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies wird bspw. erreicht durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen, Verwendung von Multifaktor-Authentifizierung, regelmäßige Schulung von Datenschutz- Regeln / Einsatz von IT-Sicherheitsrichtlinien (u.a. bei der Nutzung von Wechselmedien, Umgang mit personenbezogenen Daten / Kundendaten, Passworteinsatz/ -vorgaben, Verschlüsselung, Ablage/ Speicherung von Daten) etc…

4.2.5. Trennungsgebot {#4.2.5.-trennungsgebot}

Die in den TOMs aufgeführten Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Dies wird bspw. erreicht durch softwareseitigen Ausschluss (Mandantenfähigkeit), Verwendung des Datenbank-Prinzips, zwischen Test- und Produktionsumgebung existiert eine Trennung mit dedizierten Datenbank- und Application-Server

Instanzen, Trennung über Zugriffsregelung, Funktionstrennung, Trennung von Entwicklungs- und Produktionsumgebungen, physische und logische Trennung von Daten und deren Datensicherungen.

4.3 Integrität (Art. 32 Abs. 1 lit. b DSGVO) {#4.3-integrität-(art.-32-abs.-1-lit.-b-dsgvo)}

4.3.1. Schwerpunktprüfung: Weitergabekontrolle {#4.3.1.-schwerpunktprüfung:-weitergabekontrolle}

Die getroffenen Maßnahmen gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, z.B. durch Verschlüsselung, umfangreichen Richtlinien zum Umgang mit personenbezogenen Daten, Hardware- und Software-Firewalls, Endpoint-Security, Dokumentation der Stellen, an welche eine Übermittlung vorgesehen ist, sowie der Übermittlungswege. Besonderes Augenmerk wurde auf die Schulung der MitarbeiterInnen bezüglich Cyber-Security gelegt.

4.3.2. Eingabekontrolle {#4.3.2.-eingabekontrolle}

Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann, sofern systemseitig unterstützt, nachträglich überprüft und festgestellt werden durch:
Benutzerprofile, Benutzeridentifikation, Berechtigungskonzepte, Protokollierung eingegebener Daten (Verarbeitungsprotokoll), Protokollierung der Eingabe, Änderung und Löschung von Daten, Protokollierung administrativer Tätigkeiten. Die pcvisit Software AG erhebt, verändert oder löscht personenbezogene Daten primär im Rahmen des eigenen Kundenverwaltungssystems (Bestands-, Nutzungsdaten, Endkundendaten) bzw. nur im Auftrag / nach Weisung des Kunden / Auftraggebers.

4.4. Verfügbarkeit / Belastbarkeit / rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO) {#4.4.-verfügbarkeit-/-belastbarkeit-/-}

rasche-wiederherstellbarkeit-(art.-32-abs.-1-lit.-b-und-c-ds-gvo)}

Daten werden gegen zufällige Zerstörung oder Verlust geschützt, gewährleistet wird dies unter anderem durch:

- Einsatz von RAID-Festplattensystemen
- externe Server werden nur bei ISO 27001-zertifizierten Unternehmen angemietet (Feuerschutz, Wachschutz, Katastrophenschutz, Redundanzkonzept etc.)
- Alle wichtigen DV-Systeme werden vom Backup-System abgedeckt.
- Konzept zur Rekonstruktion der Datenbestände (Backup/Restore-Konzept), Virenschutzprogramme/Anti-Malware Programme sind vorhanden und aktuell
- Notfallpläne sind vorhanden und werden regelmäßig geprobt

4.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DS-GVO; Art. 32 Abs. 1 lit. d DS-GVO) {#4.5-verfahren-zur-regelmäßigen-überprüfung,-bewertung-und-evaluierung-(art.-25-abs.-1-ds-gvo;-art.-32-abs.-1-lit.-d-ds-gvo)}

4.5.1. Datenschutz-Management {#4.5.1.-datenschutz-management}

Die pcvisit Software AG hat ein Datenschutzteam erstellt, welches ein Datenschutzmanagementsystem (DSMS) führt, in dem alle Maßnahmen, Verfahren, Tätigkeiten etc. abgebildet werden. Das DSMS beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen. Das DSMS wird fortlaufend gepflegt und aktualisiert.

4.5.2. Incident-Response-Management {#4.5.2.-incident-response-management}

Organisatorische und technische Prozesse zum Umgang mit Verdachtsfällen, potentiellen Schwachstellen, Datenschutz- und Sicherheitsvorfällen (incidents) sind

vorhanden.
Hierüber wird auch eine einheitliche Reaktion sowie ein prozessualisierter Umgang mit erkannten und vermuteten Sicherheitsvorfällen/ Störungen sichergestellt. Ebenfalls erfolgt im Rahmen dessen eine einheitliche Nachbereitung und Kontrolle im Sinne eines kontinuierlichen Verbesserungsprozesses.

4.5.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) {#4.5.3.-datenschutzfreundliche-voreinstellungen-(art.-25-abs.-2-ds-gvo)}

Grundsätzlich werden nur Daten erhoben und verarbeitet, welche für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden. Die pcvisit Software (pcvisit Services) kann vom Kunden selbst angepasst und verwaltet werden. Eine Löschung/ Berichtigung der Daten im System seitens des Kunden ist möglich.

4.5.4. Auftragskontrolle {#4.5.4.-auftragskontrolle}

- Die MitarbeiterInnen sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen unterzeichnet.
- Sollte die pcvisit Software AG bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DS-GVO i.V.m. Art 32 Abs. 1 DS-GVO.
- Vor dem Einsatz externer Dienstleister erfolgt eine dokumentierte Überprüfung.

4.6 Prüfung der Unterauftragnehmer {#4.6-prüfung-der-unterauftragnehmer}

Im Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO Punkt 6. “Unterauftragnehmer” verpflichtet die pcvisit Software AG ihre jeweiligen Unterauftragnehmer zu geeigneten technischen und organisatorischen Maßnahmen. Die TOMs der entsprechenden Unterauftragnehmer wurden mittels Vorlage eines geeigneten, aktuellen Testats oder Berichts (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder

Qualitätsauditoren) oder einer geeigneten Zertifizierung sowie zusätzlichen Dokumenten bzw. unter Bewertung der von der pcvisit Software AG zusätzlich getroffenen technischen und organisatorischen Maßnahmen. Ein Unterauftragnehmer wurde durch die pcvisit Software AG auditiert.

Unter Berücksichtigung (gemäß Art. 32 Abs. 1 DSGVO) der Stand der Technik, der Implementierungskosten, Art, Umfang, Umstände und Zweck der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere des Risikos für Rechte und Freiheiten natürlicher Personen sowie der zusätzlich getroffenen Maßnahmen bewertet die pcvisit Software AG die technisch-organisatorischen Maßnahmen aller Ihrer Unterauftragnehmer gemäß Punkt 6.5 des AVVs als ausreichend.

4.7 Handlungsempfehlungen {#4.7-handlungsempfehlungen}

Empfohlene Maßnahmen für festgestellte **nicht relevante Mängel (Bewertung = 1**):

Maßnahme	**Empfehlung**
Pseudonymisierung von Daten	weiter Augenmerk bei zukünftigen Entwicklungen, um Forderungen des EDSA umzusetzen
IT-Account-Prozess	Eine Erhöhung des Automatisierungsgrades wird zur Effizienzsteigerung empfohlen.
Zentrales Usermanagement	Eine Erhöhung des Automatisierungsgrades wird zur Effizienzsteigerung empfohlen.

Empfohlene Maßnahmen für festgestellte **mäßige Mängel:**
(Bewertung = 2 (siehe Punkt 2. “Übersicht zur Bewertung von Abweichungen”):

- Beim Audit 2023, 2024 und 2025 wurden keine Mängel der Stufe 2 oder höher festgestellt.
- Festgestellte Mängel mit der Bewertung 2 aus dem Audit 2022 wurden behoben.