pcvisit Software AG
- Datenschutz -
Manfred-von-Ardenne-Ring 20
01099 Dresden

per E-Mail an: datenschutz@pcvisit.de

Bitte **nicht** per Fax senden.

Die DS-GVO betrifft alle Unternehmen sowie Selbständige in Europa und regelt den Umgang mit personenbezogenen Daten im Unternehmen. Da wir für Sie ein Auftragsverarbeiter im Sinne der DS-GVO sind, ist es rechtlich notwendig, zwischen Ihnen und der pcvisit Software AG einen Auftragsverarbeitungsvertrag (AVV) abzuschließen.

Bitte tragen Sie auf

- **Seite 2: Ihre Unternehmensdaten sowie**
- **Seite 11: Ihre Kontaktpersonen ein.**

Den ausgefüllten und unterzeichneten Vertrag senden Sie uns bitte per E-Mail zurück an **datenschutz@pcvisit.de** .

Ihr pcvisit-Team

AUFTRAGSVERARBEITUNG gemäß Art. 28 DS-GVO

Stand: 29.02.2024 Version 1.8

zwischen dem Verantwortlichen

_____ **(Unternehmen)**

_____ **(ggf. pcvisit Kundennummer)**

_____ **(ggf. Ansprechpartner)**

_____ **(Straße / Haus-Nr.)**

_____ **(PLZ / Ort / Land)**

im Folgenden „Auftraggeber“

und dem Auftragsverarbeiter

pcvisit Software AG
Manfred-von-Ardenne-Ring 20
01099 Dresden
im Folgenden „Auftragnehmer“

Der Auftragnehmer verpflichtet sich als Anbieter gegenüber dem Auftraggeber nach Maßgabe der folgenden Bestimmungen:

1. **Gegenstand dieser Vereinbarung und Laufzeit**

1. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Bereitstellung der vertraglichen Leistungen durch den Auftragnehmer ergeben. Die Regelungen dieser Vereinbarung gelten, soweit durch den Auftragnehmer Leistungen gemäß der bereits bestehenden oder künftig abzuschließenden Verträge zwischen dem Auftraggeber und dem Auftragnehmer (im Folgenden die „Leistungsvereinbarung“) erbracht werden, und dabei ein Zugriff auf personenbezogene Daten des Auftraggebers (im Folgenden „Daten“) nicht ausgeschlossen werden kann. Nicht-personenbezogene Daten des Auftraggebers sind nicht Gegenstand dieser Vereinbarung.

2. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Leistungsvereinbarung.

2. **Art und Zweck der vorgesehenen Verarbeitung von Daten**

    1. Der Auftragnehmer erbringt für den Auftraggeber auf der Grundlage des bestehenden Servicevertrags über die Bereitstellung einer Fernwartungs-Software die dort näher bezeichneten Leistungen (siehe EULAS). Bei der Erbringung der Leistungen kann nicht vollständig ausgeschlossen werden, dass der Auftragnehmer Daten des Auftraggebers zur Kenntnis nehmen kann, insbesondere im Rahmen und zum Zwecke der

1. Bereitstellung aller pcvisit-Services
2. Support beim Auftraggeber
3. allgemeine Fehlerbehebung und Behebung von Störungen
4. Tests bei Anpassung von Programmen
5. Tests bez. Erstellung von neuen Programmen und Änderungen von Programmen
6. Unterstützung des Auftraggebers
7. Fehleranalyse auf Basis von Logfiles oder Reproduktion von Fehlern
8. Bereitstellung von Speicherkapazitäten auf virtuellen und physischen Servern
9. Unterstützung der Leistungsanpassung/ Nutzungsoptimierung Produkt und Service

    Neben der Pflicht zu regelmäßigen Datensicherungen trägt der Auftraggeber auch Sorge dafür, dass der Auftragnehmer bei der Erbringung der Leistungen möglichst wenig mit Daten des Auftraggebers in Berührung kommt.

    Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

    Datenverarbeitungen in anderen Ländern dürfen nur erfolgen, sofern der Auftraggeber zuvor schriftlich zugestimmt hat und zusätzlich die Voraussetzungen der Art.44 bis 47 DS-GVO erfüllt sind oder eine Ausnahme nach Art.49 DS-GVO vorliegt. Vereinzelt werden Leistungen (z.B. Tool zur Onlineschulung, Chatportal etc.) von Firmen aus dem Drittland bezogen. Diese sind im Punkt 6 “Unterauftragnehmer” dargelegt und erfüllen die besonderen Voraussetzungen der Art. 44 ff. DS-GVO. Jede weitere Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2. Bei folgenden Arten von Daten des Auftraggebers findet in Zusammenhang mit den in Punkt 2.1 beschriebenen Leistungen eine Datenverarbeitung beim Auftragnehmer statt:

Datenkategorien:

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

11. **Vertragsstammdaten:**
    Vertragsbeziehung, Produktnutzung, gekaufte Produkte, Bankverbindung

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

13. **Benutzerkontoinformationen:**
    Kundennummer, Firmen-ID, Anzeigename, Spracheinstellung, Berechtigungs- einstellungen, Teammitglieder, Kontaktliste

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

15. **Verbindungsdaten:**
    Fernwartungsdauer, Anzahl der Fernwartungen und Ferndiagnosen, Fernwartungs-ID, Fernwartungskommentare (Freitextfeld), Aufzeichnung von Fernwartungen, Logfiles, Teilnehmer, Bild- und Dateitransfer (nur Übertragung, keine Speicherung)

16. **sonstige Daten:**
    personenbezogene Daten im Zusammenhang mit der Anmeldung bei pcvisit Services

3. Der Kreis der in datenschutzrechtlicher Hinsicht Betroffenen sind:

17. der Auftraggeber,

18. Mitarbeiter des Auftraggebers

19. hinzugezogene Experten des Auftraggebers

20. Kunden des Auftraggebers (soweit es sich um natürliche Personen handelt)

21. möglicherweise personenbezogene Daten von Dritten, die während einer Fernwartung über den übertragenen Bildschirm, das Chatfenster, beim Dateitransfer, im Rahmen der Fernwartungsprotokollierung oder bei Supportanfragen übermittelt werden.

4. Der Auftragnehmer nimmt die in 2.2 genannten Daten des Auftraggebers ausschließlich zur Erbringung der Leistungen und nach den in dieser Vereinbarung festgelegten Weisungen des Auftraggebers zur Kenntnis. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, ihm ggf. überlassenen Daten des Auftraggebers ohne Zustimmung des Auftraggebers an Dritte weiterzugeben, soweit nicht die Leistungsvereinbarung mit dem Auftraggeber etwas anderes vorsieht (zu “Unterauftragnehmern” siehe Punkt 6.).

5. Der Auftragnehmer verpflichtet sich der RiLi 2000/31/EG, insbesondere den Artikeln (12) bis (15), freier Dienstleistungsverkehr, als Grundlage für das reibungslose Funktionieren des Binnenmarktes. Darauf bezieht sich der Artikel 2 (4) DS-GVO explizit.

3. **Grundsätze zu technischen und organisatorischen Sicherheitsmaßnahmen**

    1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Auftraggeber und der Auftragnehmer geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

    2. Die vom Auftragnehmer zu treffenden technischen und organisatorischen Sicherheitsmaßnahmen sind in der Anlage 1 dieser Vereinbarung geregelt, insbesondere auch Verfahrensanweisungen des Auftragnehmers zur Gewährleistung der betrieblichen IT-Sicherheit und des Datenschutzes. Desweiteren sind in Anlage 1 Sicherheitsmaßnahmen speziell bei Fernwartung und bei Supportanfragen festgelegt. Der Auftraggeber hat die technischen und organisatorischen Maßnahmen zu prüfen und dem Auftragnehmer Änderungswünsche mitzuteilen. Der Auftragnehmer ist berechtigt, Änderungswünsche abzulehnen und/oder unter Vorbehalt der Kostenübernahme durch den Auftraggeber zu stellen. Soweit die technischen und organisatorischen Maßnahmen gemäß Anlage 1 von dem Auftraggeber akzeptiert werden, werden diese ausschließliche Grundlage des Auftrages i. S. d. Punktes 3.3.

    3. Für den Fall, dass Dritte oder betroffene Personen (weder Auftraggeber noch Auftragnehmer) aus der Datenverarbeitung resultierende Ansprüche gegen den Auftragnehmer geltend machen und diese Ansprüche entweder

- aufgrund von rechtswidrigen Weisungen des Auftraggebers gemäß Art. 28 Abs. 3 S. 3 DS-GVO oder
- aufgrund nicht ausreichender technisch-organisatorischer Maßnahmen (welche gemäß Punkt 9. dieser Vereinbarung vom Auftraggeber freigegeben wurden),

entstanden sind, stellt der Auftraggeber den Auftragnehmer auf erstes Anfordern von allen rechtlichen Ansprüchen, Schäden und Kosten frei.

Dem Auftraggeber bleibt im Nachgang vorbehalten, nachzuweisen, dass die gegen den Auftragnehmer gerichteten, vorgenannten Ansprüche und Bußgelder nicht auf Weisungen oder Pflichtverletzungen des Auftraggebers beruhen.

4. Der Auftraggeber hat dafür Sorge zu tragen, dass seine Datenverarbeitungssysteme in ihrer Gesamtheit so gestaltet sind, dass auch bei der Durchführung der Leistungen folgende Prinzipien sichergestellt sind:

- Vertraulichkeit (Schutz vor unbefugtem Zugriff),
- Integrität (Schutz vor unbefugten Veränderungen, Verlust, Zerstörung),
- Verfügbarkeit,
- Authentizität,
- Revisionsfähigkeit und Transparenz.

Insbesondere hat der Auftraggeber seine Datenverarbeitungssysteme untereinander dermaßen zu gestalten und die Systemumgebungen so voneinander abzuschotten, dass bei der Wartung durch den Auftragnehmer zu wartender Datenverarbeitungssysteme nicht auf Daten anderer Datenverarbeitungssysteme zugegriffen werden kann.

Eine Sicherheitsmaßnahme ist insbesondere, wenn der Auftraggeber seine Daten mit einem dem Stand der Technik entsprechenden Verfahren verschlüsselt. Verschlüsselung ist das Ersetzen von

Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann.

5. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. **Berichtigung, Einschränkung und Löschung von Daten**

    1. Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und nicht direkt beantworten. Die Prüfung der Anfrage obliegt ausschließlich dem Auftraggeber.

    2. Der Auftragnehmer verpflichtet sich, den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen in Anbetracht der Art der Verarbeitung dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in der Datenschutz-Grundverordnung genannten Rechte der betroffenen Person nachzukommen.

    3. Der Auftraggeber fordert den Auftragnehmer in Textform zur Mitwirkung auf, insofern eine Mitwirkung des Auftragnehmers erforderlich ist. Für alle sich daraus ergebenden Tätigkeiten beim Auftragnehmer - soweit sie keiner gesetzlichen Verpflichtung entsprechen - wird ein angemessenes Entgelt vereinbart, soweit erkennbar wird, dass das übliche Maß überschritten wird.

7. **Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

    Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrages gesetzliche Pflichten und gewährleistet insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer hat einen fachkundigen Datenschutzbeauftragten schriftlich bestellt. Der Datenschutzbeauftragte und die Kontaktmöglichkeiten zu diesem können im Impressum der Website des Auftragnehmers eingesehen werden.
b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass diese gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen (siehe Anlage 1).
d) Auftraggeber und Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei dem Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. **Unterauftragnehmer**

    1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, welche sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, welche der Auftragnehmer z.B. als Telekommunikations- und Informationsleistungen, Post-/Transportdienstleistungen, im Zahlungsverkehr (Banken, Kreditkarteninstitute), Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

    2. Der Auftragnehmer ist berechtigt, Unterauftragnehmer einzusetzen. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragnehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO). Wenn und soweit diesen Unterauftragnehmern personenbezogene Daten des Auftraggebers zugänglich werden, setzt der Auftragnehmer diese Unterauftragnehmer erst nach vorheriger Zustimmung des Auftraggebers ein. Der Auftraggeber wird seine Zustimmung erteilen, wenn nicht schwerwiegende datenschutzrechtliche Gründe entgegenstehen. Die Zustimmung gilt als erteilt, wenn der oder die Betroffene nicht innerhalb der Frist widerspricht. Können sich Auftraggeber und Auftragnehmer nach Ausübung des 2-wöchigen Widerspruchsrechts nicht auf eine einvernehmliche Lösung einigen, kann jede Seite den Hauptvertrag innerhalb von 4 Wochen nach Scheitern der Verhandlungen kündigen (Sonderkündigungsrecht).

    3. Wenn und soweit den Unterauftragnehmern des Auftragnehmers personenbezogene Daten des Auftraggebers zugänglich sind bzw. werden, verpflichtet der Auftragnehmer den jeweiligen Unterauftragnehmer zu geeigneten technischen und organisatorischen Maßnahmen. Die Weiterleitung von personenbezogenen Daten des Auftraggebers durch den Auftragnehmer an den Unterauftragnehmer erfolgt erst, nachdem der Unterauftragnehmer entsprechend verpflichtet wurde.

    4. Erbringt der Unterauftragnehmer die vereinbarten Leistungen außerhalb der EU / des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

5. Der Auftraggeber erteilt hiermit seine Zustimmung für die Unterstützung des Auftragnehmers durch folgende Unterauftragnehmer:

Unterstützung bei Hauptleistungen:

Firma Unterauftragnehmer	**Anschrift**	**Leistung**	**Datenschutz-maßnahmen**
PlusServer GmbH	Venloer Straße 47 50672 Köln	Rechenzentrums-leistungen	ISO 27001 zertifiziert, AVV
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen	Rechenzentrums-leistungen	ISO 27001 zertifiziert, AVV
billwerk GmbH	Mainzer Landstraße 51a 60329 Frankfurt am Main	Prozessautomatisierung für wiederkehrende RG & Zahlungen	AVV
HostPress GmbH	Bahnhofstraße 34 66571 Eppelborn	Managed Web Hosting	AVV
Mailjet SAS	4, rue Jules Lefebvre, 75009 Paris, France	DS-GVO-konformer E-Mail-Service	ISO 27001 zertifiziert, AVV
Auth0 by Okta (Region Europe)	100 1st Street, Suite 600 San Francisco, California 94105 United States	Identity as a Service (IDaaS)	ISO 27001 zertifiziert, EU-U.S. Data Privacy Framework zertifiziertes Unternehmen (TADPF)
Amazon Web Services, Inc	410 Terry Avenue NortSeattle WA 98109 United States	Hosting und Serviceleistungen	ISO 27001-, 27017- und 27018 zertifiziert, CISPE Code of Court[^1], EU-U.S. Data Privacy Framework zertifiziertes Unternehmen (TADPF)
toolhouse DV-Systeme GmbH & Co. KG	Türltorstraße 16-20 D-85276 Pfaffenhofen/Ilm	Support- und Servicedienstleistung	ISO 9001 zertifiziert, AVV

Unterauftragnehmer zur Bereitstellung zusätzlicher Dienstleistungen: (Für nicht zur Hauptleistung gehörende (optionale) Nebenleistungen):

Firma Unterauftragnehmer	Anschrift	Leistung	Datenschutz-maßnahmen
LIVESTORM SAS	60, rue François 1er 75008 Paris France	Online-Schulungen und Präsentationen	AVV
Userlike UG	Probsteigasse 44-46 50670 Köln	interaktiver Websupport	AVV
UserVoice	121 2nd St, Fl 4 San Francisco, CA 94105	Feedback-Forum	Server ist SSAE16 / ISAE Type II compliant, ISO 27001, ISO27017, ISO27018 certified, and PCI DSS v3.2 compliant, EU-U.S. Data Privacy Framework zertifiziertes Unternehmen (TADPF)
Typeform	B65831836, Bac de Roda, 163; Barcelona 08018, Spain	interaktiver Websupport	AVV
Atlassian Pty Ltd	1098 Harrison Street Level 6, 341 George St, Sydney NSW 2000, Australia	Servicedesk, Wissensdatenbank	Data Processing Agreement-Vertrag including the standard contractual clauses, ISO 27001 und 27018 zertifiziert, SOC2

7. **Kontrollrechte des Auftraggebers**

Der Auftraggeber hat vor der Aufnahme der Datenverarbeitung den Auftragnehmer auch anhand der Geeignetheit der technischen und organisatorischen Maßnahmen des Auftragnehmers sorgfältig ausgewählt.

1. Der Auftragnehmer kann dem Auftraggeber die Einhaltung und Umsetzung seines internen Sicherheitskonzepts z.B. durch qualifizierte Selbstauskünfte und ggf. Testate von Sachverständigen auf schriftliche Anforderung des Auftraggebers nachweisen.

2. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der Anlage 1 (technischen und organisatorischen Maßnahmen), zu überprüfen.

   Nach Wahl des Auftragnehmers kann der Nachweis anstatt durch eine Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

Kommt es im Einzelfall zu einer Vor-Ort-Überprüfung durch den Auftraggeber oder einem von ihm beauftragten Prüfer, gilt Folgendes:
• Überprüfungen und Kontrollen finden auf eigene Kosten des Auftraggebers statt (zu den üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs beim Auftragnehmer, unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers)
• Überprüfungen und Kontrollen sind vorab unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 2 Wochen) beim Auftragnehmer anzumelden

3. Der Auftraggeber ist berechtigt, alle Zugriffe, die für die Erbringung der Leistungen erfolgen, in seinem System zu verfolgen und zu protokollieren (Einzelheiten siehe Anlage 1). Der Auftragnehmer verpflichtet sich, eine auftraggeberseitige Protokollierung nicht abzuschalten oder technisch zu unterbinden.

4. Auch bei seinen Kontrollen berücksichtigt der Auftraggeber seine Pflichten hinsichtlich Geheimhaltung zum Schutz des Auftragnehmers. Insbesondere ist der Auftraggeber verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen des Auftragnehmers und auftragnehmereigenem Know-How – auch soweit technische und organisatorische Sicherheitsmaßnahmen betroffenen sind – vertraulich zu behandeln.

5. Der Auftragnehmer verpflichtet sich, im Falle einer Kontrolle durch die für den Auftraggeber zuständige Datenschutzbehörde der prüfenden Datenschutzaufsichtsbehörde (nachfolgend „Behörde“) im gesetzlich erforderlichen Umfang Zugang zu den Arbeitsräumen zu gewähren und/oder Auskünfte zu erteilen. Er benachrichtigt den Auftraggeber, möglichst bevor eine solche angekündigte behördliche Kontrolle stattfindet.

2. **Mitteilung bei Verstößen des Auftragnehmers**

1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen.

2. Bei unrechtmäßiger Kenntniserlangung von Daten (siehe Punkt 2.2 a) durch Dritte, insbesondere Daten zu Bank- und Kreditkartenkonten, ist ausschließlich der Auftraggeber verpflichtet, eine unverzügliche Mitteilung an die zuständige Datenschutzaufsichtsbehörde und an die Betroffenen zu machen. Vor Abgabe dieser Mitteilung informiert der Auftraggeber den Auftragnehmer über den Inhalt. Auf Anfrage unterstützt der Auftragnehmer den Auftraggeber bei der Mitteilung gegen ggf. gesonderte Vergütung.

3. Stellt der Auftragnehmer mehr als nur unwesentliche Verstöße des Auftraggebers oder des Auftragnehmers sowie der bei ihm beschäftigten Personen gegen die Festlegungen dieses Vertrages oder gegen Datenschutzvorschriften fest, welche diese Datenverarbeitung im Auftrag unmittelbar betreffen (siehe Punkt 2.), informiert der Auftragnehmer den Auftraggeber unverzüglich.

3. **Weisungsbefugnis des Auftraggebers**

1. Die Beurteilung der Zulässigkeit der Datenverarbeitung sowie die Wahrung der Rechte der Betroffenen obliegt allein dem Auftraggeber. Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gemäß den Regelungen der Leistungsvereinbarung zu erteilen. Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung,

Löschung, Sperrung und Herausgabe von seinen personenbezogenen Daten verlangen. Entsteht dem Auftragnehmer dabei Mehraufwand, ist dieser dem Auftragnehmer zu vergüten.

2. Die datenschutzrechtlichen Weisungen des Auftraggebers beschränken sich im Prinzip auf die Regelungen in dieser Vereinbarung und ihrer Anlage 1 „Technische und organisatorische Maßnahmen“. Der Auftraggeber erteilt alle darüber hinausgehenden Aufträge oder Teilaufträge und Weisungen schriftlich (postalisch oder per E-Mail) und dokumentiert diese. Entsteht dem Auftragnehmer durch darüber hinausgehende Weisungen Mehraufwand, ist dieser dem Auftragnehmer zu vergüten.

3. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn dieser der Meinung ist, eine Weisung verstößt gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

4. **Löschung und Rückgabe von personenbezogenen Daten**

1. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, welche im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2. Nach Beendigung der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens aber mit Beendigung der Leistungsvereinbarung - wird der Auftragnehmer vom Auftraggeber überlassene Datenträger zurückgeben und Daten des Auftraggebers (siehe oben Punkt 2.2 a oder b) sowie davon erstellte Kopien löschen. Das Protokoll der Löschung wird der Auftragnehmer auf Anforderung vorlegen.

3. Von der Lösch- bzw. Rückgabepflicht ausgenommen sind Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung, zur Erfüllung von gesetzlichen Auskunfts- oder Aufbewahrungspflichten oder zu Beweissicherungszwecken, welche der Auftragnehmer zum Nachweis seiner Leistungen benötigt. Diese Daten wird der Auftragnehmer löschen, sobald die entsprechenden Speicherfristen abgelaufen sind.

5. **Weitere Bestimmungen**

1. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

2. Sollte Eigentum des Auftraggebers bei dem Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

3. Jegliche Nebenabreden, Änderungen und Ergänzungen dieses Auftrages und all ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingung handelt.

4. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

5. Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.

6. Die folgende Anlage ist Vertragsbestandteil:

Anlage 1 - Technische und organisatorische Maßnahmen im Sinne des Art. 32 DS-GVO

12. **Bestimmung der Kontaktpersonen**

    1. Bezüglich der Weisungsbefugnis (siehe Punkt 9) wird folgendes vereinbart:

1. weisungsberechtigte Personen des Auftraggebers sind:

Name 1 + Funktion		
E-Mail-Adresse		
Name 2 + Funktion		
E-Mail-Adresse		
Name 3 + Funktion		
E-Mail-Adresse		

2. Weisungsempfänger beim Auftragnehmer sind die Vorstände, die Prokuristen und der Datenschutzbeauftragte. Die jeweils aktuellen Kontaktmöglichkeiten sind auf der Website des Auftragnehmers leicht zugänglich hinterlegt.

    2. Der Wechsel bestehender und die Beauftragung weiterer Unterauftragnehmer beim Auftragnehmer wird dem Vertragsinhaber (Auftraggeber) angezeigt (siehe Punkt 6).

_____ _____

Ort, Datum Unterschrift Auftraggeber

Dresden, 29.02.2024 _____

Ort, Datum Unterschrift Auftragnehmer

Helge Betzinger - Vorstand pcvisit Software AG

Anlage 1: Technische und organisatorische Maßnahmen im Sinne des Art. 32 DS-GVO

Inhaltsverzeichnis

Dokumenteninformation 13

Versionshistorie 13

Sicherungsmaßnahmen 14

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO) 14

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) 14

Zutrittskontrolle Unternehmensräumlichkeiten 14

Zutrittskontrolle externe Serverräume 15

Zugangskontrolle 15

Zugriffskontrolle 16

Trennungsgebot 17

Integrität (Art. 32 Abs. 1 lit. b DSGVO) 17

Weitergabekontrolle 17

Eingabekontrolle 18

Verfügbarkeit / Belastbarkeit / rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO) 18

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 25 Abs. 1 DS-GVO; Art. 32 Abs. 1 lit. d DS-GVO) 19

Datenschutz-Management 19

Incident-Response-Management 19

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) 19

Auftragskontrolle 19

Sicherheitsmaßnahmen speziell bei Fernwartung (zwischen Auftragnehmer und Auftraggeber) 20

Sicherheitsmaßnahmen speziell bei Supportanfragen (zwischen Auftragnehmer und Auftraggeber) 20

1. Dokumenteninformation {#dokumenteninformation}

Die EU-Datenschutzgrundverordnung (DS-GVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

In diesem Dokument mit aufgenommen sind die jeweils für Ihren Anwendungsfall erforderlichen technischen-organisatorischen Maßnahmen der Unterauftragnehmer. Diese sind ebenfalls nach Art. 28 DS-GVO sorgfältig ausgewählt und werden laufend überprüft. Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DS-GVO. Diese Vorschriften verlangen, dass technische und organisatorische Maßnahmen getroffen werden, um den Schutz personenbezogener Daten zu gewährleisten. Für eine automatisierte Verarbeitung nennt die DS-GVO verschiedene Kontrollbereiche, welche jeweils noch verschiedene Unterpunkte beinhalten:

1. Pseudonymisierung und Verschlüsselung
2. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

3. Wiederherstellbarkeit der Daten
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der pcvisit Software AG im Rahmen der Verarbeitung der personenbezogenen Daten gemäß Punkt 2. des AVV betrieben werden. Die Server und Datenbanken sowie die Datensicherungen (Backups) aller AVV-relevanten Daten werden in einem professionell betriebenen Rechenzentrum gehostet und gewartet. Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung der Unterauftragnehmer fallen oder aus Gründen der Aufrechterhaltung der Sicherheit durch Vertraulichkeit nicht detailliert veröffentlicht werden. Die Unterauftragnehmer werden sorgfältig ausgewählt.

2. Versionshistorie {#versionshistorie}

Version	Status	Datum	Verantwortlich	Änderung
1.0	finale Version	15.04.2018	Datenschutzbeauftragter	Gegenprüfung / Ergänzung
1.1	finale Version	03.05.2018	Ergänzung Unterschrift Auftragnehmer	Ergänzung
1.2	finale Version	18.05.2018	Überarbeitung / Aktualisierung Punkt 6. Unterauftragnehmer in AVV	Aktualisierung
1.3	finale Version	27.06.2018	- Überarbeitung / Aktualisierung Punkt 3,5 und 6 AVV - neuer Unterauftragnehmer: Auth0 (Punkt 6.5 AVV)	Aktualisierung / Ergänzung
1.4	finale Version	04.03.2019	- Aktualisierung Unterauftragnehmer (neu: Livestorm SAS) - Ergänzung 7.2.”beauftragte Prüfer” - Ergänzung “Patchmanagement” unter TOM 3.2.3.	Aktualisierung / Ergänzung
1.5	finale Version	14.11.2019	- formale Korrektur AVV: 8.3 Auftraggeber statt Auftragnehmer - formale Korrektur AVV: 12.2 Beauftragung statt beauftragen - formale Korrektur TOM: pcvisit Software AG statt pcvisit Software GmbH	Aktualisierung
1.5a	finale Version	05.06.2020	- formale Korrektur AVV: Ergänzung pcvisit Kundennr. Seite 2	Aktualisierung
1.6	finale Version	10.02.2021	Aktualisierung der Datenschutzmaßnahmen bei Punkt 6.5 Unterauftragnehmer im AVV	Aktualisierung
1.7	finale Version	12.10.2021	Aktualisierung, z.Bsp. Punkt 2, Punkt 6.5 (Wegfall Unterauftragnehmer inxmail, tandemploy, domainfactory) und Punkt 7 (Wegfall der	Aktualisierung

Version	Status	Datum	Verantwortlich	Änderung
			Entgeltpflicht), allgemeine Überarbeitung / Anpassung an aktuelle Rechtslage	
1.8	finale Version		allgemeine Überarbeitung / Anpassung an aktuelle Rechtslage (Data Privacy Framework) -3.2.1: Entfernen Punkt Sicherheitsverglasung	Aktualisierung

3. Sicherungsmaßnahmen {#sicherungsmaßnahmen}

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

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) {#vertraulichkeit-(art.-32-abs.-1-lit.-b-ds-gvo)}

1. Zutrittskontrolle Unternehmensräumlichkeiten {#zutrittskontrolle-unternehmensräumlichkeiten}

- Alle Mitarbeiter wurden dokumentiert geschult, informiert und sensibilisiert. Die Schulungen werden regelmäßig durchgeführt.
- Es wird ein dem Schutzbedarf der Daten angemessenes Schließsystem verwendet (Schlüssel; Sicherheits-Schließsystem).
- Es ist eine verantwortliche Person für die Verwaltung der Zutrittsmittel bestimmt.
- Eine Dokumentation der Schlüsselvergabe wird geführt und laufend aktualisiert.
- Das Gebäude ist außerhalb der Geschäftszeiten verschlossen und kann nur manuell durch die Mitarbeiter geöffnet werden.
- Sicherung der Büro-/Geschäftsräume während der Arbeitszeit; auch wenn die Türen nicht abgeschlossen sind, können Sie nur mittels Schlüssel geöffnet werden (Türknauf; Klingel, Gegensprechanlage)

- Besucher müssen sich über Gegensprechanlage anmelden, und werden dann von einem Mitarbeiter abgeholt
- Besucher halten sich ausschließlich in Begleitung eines Mitarbeiters im Gebäude / den Büroräumen auf.
- In den Büroräumen von pcvisit wird ein Prozess zur Besucherregistrierung angewendet
- 24/7-Überwachung des Firmengeländes und Büroräumlichkeiten durch einen Sicherheitsdienst und interne Alarmbereitschaft.
- Ein abschließbares Archiv sowie abschließbare Schränke sind vorhanden. Restriktive Zugriffsberechtigungen kommen zum Einsatz. Die Schlüssel stehen nur den Berechtigten zur Verfügung.

2. Zutrittskontrolle externe Serverräume {#zutrittskontrolle-externe-serverräume}

Das umfassende Sicherheitskonzept der von uns genutzten Rechenzentren garantiert, dass alle Daten vor Diebstahl oder Beschädigung durch Umwelteinflüsse geschützt sind. Alle Data Center sind an 365 Tagen im Jahr 24 Stunden durch Wachpersonal besetzt. Zusätzlich werden die Eingangsbereiche und Außenanlagen sowie alle sensiblen Bereiche im Inneren durch Kameras überwacht. Durch ein modernes Zugangskontrollsystem, basierend auf einer Zwei-Faktor-Authentisierung, werden nur autorisierte Personen in das Gebäude gelassen. Zur ergänzenden Kontrolle führt das Wachpersonal regelmäßige Rundgänge durch. USV-Anlagen und Spannungsfilter sowie redundante Generatoren sorgen für die konstante Stromversorgung der Server und der Infrastruktur. Insgesamt stehen mehrere Tausend kVA pro Rechenzentrum an Notstromleistung zur Verfügung. Durch die Klimatisierung mittels energieeffizienter Klimageräte arbeiten die Server und Infrastruktur stets in einem optimalen Temperaturbereich. Zusätzlich überwacht die Gebäudeleittechnik permanent alle kritischen Werte.

Zugriffsbeschränkungen

- Colocation Racks mit Schlüssel- oder Kombinationsschlössern gesichert
- Private Cages auf Anfrage verfügbar
- Videoüberwachungsanlage mit Bewegungssensoren
- Identitäten aller Besucher werden vor Ort überprüft
- Biometrische Fingerabdruckscanner und/oder Zugriffskarten mit persönlichen PIN
- Automatische Alarmsysteme mit direkter Verbindung zum Sicherheitsdienst
- Sicherheitspersonal rund um die Uhr an 365 Tagen im Jahr

Zertifizierung

- Die Rechenzentren sind ISO 27001 zertifiziert.

3. Zugangskontrolle {#zugangskontrolle}

- Verbindliches Verfahren zu Vergabe und Entzug von Berechtigungen:
    - Regelung des Zugangs zu den Datenverarbeitungs-Systemen (DV-Systemen) über ein Benutzer-/Berechtigungskonzept

    - Vergabe personalisierter Benutzeraccounts und Hardware mit entsprechenden Kennwortrichtlinien (eindeutige Zuordnung von Benutzerkonten zu Benutzern)
    - Zuordnung der Mitarbeiter in eine oder mehrere Benutzergruppen, wobei die jeweiligen Benutzergruppen unterschiedliche Zugriffsrechte haben (Rechtebeschränkung Standardnutzer)
    - Zentrales Usermanagement
    - Protokollierung fehlerhafter Passworteingaben. Auswertung Protokolle bei Auffälligkeiten
    - Netzdienste werden nur im Rahmen der für die Aufgabe erforderlichen Nutzungsszenarien vergeben. (IT-Accountprozess)

- Die Datenübertragung von und zu den DV-Systemen wird bei kritischen Aktivitäten (z.B. bei Systempflege, Softwareupdates, Backups, Fernwartung) durch folgende Maßnahmen gegen Nutzung durch Unbefugte gesichert:

    - Überprüfung bekannter öffentlicher Schlüssel bei Kontaktaufnahme
    - Verschlüsselte Datenübertragung (SSL/SSH)
    - Zugriff auf System von außen über VPN-Verbindung oder sichere pcvisit-Remote2Office Fernwartungssoftware
    - Protokollierung der Systemnutzung
    - Zugang Fernwartungspersonal nur über sichere Fernwartungssoftware (pcvisit-Software). Fernwartungsmaßnahmen werden überwacht und können jederzeit abgebrochen werden.

- Eine Kennwortrichtlinie mit Vorgaben für den Passwort-Standard ist implementiert.
- Einsatz von Firewalls zur Verhinderung von Angriffen.
- Das Unternehmensnetzwerk ist durch eine umfassende Firewall-Architektur gegen Angriffe gesichert.
- Spamfilter und Virenschutzprogramme sind vorhanden und werden immer auf dem aktuellsten Stand gehalten.
- Funktionelle Beschränkung der Nutzung von Clientsystemen und Bildschirmarbeitsplätzen (restriktive Rechtevergabe) und Abschaltung von überflüssigen Diensten.
- Es ist ein umfassendes Netzwerkmonitoring mit entsprechenden Alarmierungen etabliert.
- Beschränkung der Server in den Rechenzentren auf die benötigten Dienste.
- Patch-und Updatemanagement (systematisierte Beschaffung, Test und Installation von Updates und Patches)
- Zusätzliche Maßnahmen:

    - Verschlüsselung von Datenträgern bei Transport
    - Sämtliche Arbeitsstationen werden bei Verlassen des Arbeitsplatzes vom Benutzer oder nach Inaktivität gesperrt (passwortgeschützte, automatische Bildschirmsperren)

- Reduktion der zugriffsberechtigten Personen auf ein Minimum.
- Jährliche Sicherheits-Audits werden vorgenommen.

4. **Zugriffskontrolle {#zugriffskontrolle}**

- Die Einschränkung der Zugriffsmöglichkeiten des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch:
    - spezifischem IT-Accountprozess, der die Vergabe, Änderung und Sperrung von IT-Zugängen regelt und dokumentiert.
    - Vergabe von personalisierten Benutzeraccounts und personalisierter Hardware mit entsprechenden Kennwortrichtlinien (eindeutige Zuordnung von Benutzerkonten zu Benutzern)
    - Zuordnung der Mitarbeiter in eine oder mehrere Benutzergruppen und /oder Rollen, wobei die jeweiligen Benutzergruppen/-rollen unterschiedliche Zugriffsrechte haben
    - Differenzierte Zugriffsberechtigung auf Anwendungsprogramme
    - Differenzierte Verarbeitungsmöglichkeiten (Lesen/ Ändern/ Löschen).
    - Verwendung von Multifaktor-Authentifizierung, wo es die Systeme unterstützen.
- Das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern wird verhindert durch:
    - Benennung Verantwortliche für die Herausgabe/ Prüfung von Hardware/ Datenträgern
    - Softwareseitigen Ausschluss (Berechtigungskonzept)
    - Konzept zur Laufwerksnutzung/-zuordnung
    - Gesicherte Schnittstellen/ Firewall
- Ein Verfahren zur Vergabe von Berechtigungen ist implementiert (restriktive Zugriffsberechtigung/ projektbezogene Zugänge). Die Beantragung und Vergabe von Berechtigungen erfolgt unter Einbeziehung des Vorgesetzten und mit Dokumentation der Berechtigungsvergabe im IT-Account Prozess.
- Personifizierter Admin-Account mit erhöhten Kennwortvorgaben
- regelmäßige Schulung von Datenschutz-Regeln/ Einsatz IT-Sicherheitsrichtlinien (u.a. Nutzung von Wechselmedien; Umgang mit personenbezogenen Daten/ Kundendaten, Passworteinsatz/ -vorgaben, Verschlüsselung, Ablage/ Speicherung von Daten etc.)

5. Trennungsgebot {#trennungsgebot}

- Zwischen Test- und Produktionsumgebung existiert eine Trennung mit dedizierten Datenbankservern und Applikationsserverinstanzen.
- Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für welchen sie ursprünglich erhoben wurden. Die unterschiedliche und getrennte Verarbeitung wird gewährleistet durch:
    - Softwareseitigen Ausschluss (Mandantentrennung)
    - Datenbank-Prinzip, Trennung über Zugriffsregelung
    - Trennung von Test- und Produktivdaten (Produktivdaten ausschließlich in ISO 27001-Hosting-Dienstleister)
    - Funktionstrennung
    - Trennung von Entwicklungs- und Produktionsprogrammen
    - Logische Trennung
    - Speicherung unterschiedlicher Datenkategorien in getrennten Datenbanken und Verarbeitung je nach Verwendungszweck mit geeigneter Software

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

1. Weitergabekontrolle {#weitergabekontrolle}

- Ein physischer Versand von Datenträgern ist nicht vorgesehen.
- Verbot des Einsatzes privater Datenträger.
- Nicht mehr benötigte Datenträger werden durch zertifizierte Dienstleister zerstört.
- Alle zum Transport oder für die Übertragung vorgesehenen sensiblen Daten werden verschlüsselt.
- Der Schutz personenbezogener Daten beim physischen Transport bzw. bei der elektronischen Übermittlung wird durch folgende Maßnahmen sichergestellt:
    - Transportverschlüsselung (SSL,SSH,VPN, sichere pcvisit-Remote2Office Fernwartungssoftware)
    - Verschlüsselung von Datenträgern
    - Ausschließliche Nutzung von durch die IT freigegebenen Systemen
    - SFTP-Server

Folgende Sicherheitsmaßnahmen existieren:

- Hardware- und Software-Firewall
- Programme, die das Eindringen von Viren verhindern bzw. das Eindringen erkennen (Endpoint-Security)
- Erkennung und Markierung von SPAM
- Nur freigegebene Dienste dürfen genutzt werden
- Für mobile Arbeitsplätze und Heimarbeitsplätze existieren VPN-Zugänge zum Unternehmensnetzwerk oder Zugang über sichere pcvisit-Remote2Office Software
- Dokumentation der Stellen, an welche eine Übermittlung vorgesehen ist, sowie der Übermittlungswege

2. Eingabekontrolle {#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. Verfügbarkeit / Belastbarkeit / rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DS-GVO) {#verfügbarkeit-/-belastbarkeit-/-rasche-wiederherstellbarkeit-(art.-32-abs.-1-lit.-b-und-c-ds-gvo)}

Dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind, wird gewährleistet durch:

- Einsatz von RAID-Festplattensystemen
- Einsatz von USV inkl. Überspannungsschutz und Notstromaggregat (zwei unabhängige Generatoren, die Energieversorgung bei mehrtägiger Stromunterbrechung gewährleisten können) und Blitzschutzeinrichtungen
- Feuerschutz: um die Daten unserer Kunden vor Brandschäden zu schützen, sind alle Rechenzentren mit speziellen Vorsorge-, Schutz- und Alarmsystemen ausgestattet. Diese umfassen: Hitze- und Rauchsensoren, Sensoren zur Partikelanalyse, Löschanlagen in mehreren Zonen.
- Betrieb einer Alarmanlage inkl. Weiterleitung an Leitstelle, Werkschutz, Feuerwehr, Wachdienst etc.
- Katastrophenschutz: An den erforderlichen Standorten sind die Rechenzentren mit Maßnahmen zum Schutz vor Hochwasser (Pumpen, spezielle Abwasserleitungen) und Erdbeben ausgestattet.
- Redundanzkonzept: Verteilung der Rechenleistung auf mehrere Server, zum Teil in getrennten Brandschutzbereichen innerhalb eines Rechenzentrums.
- Einsatz eines Wachdienstes.
- Mehrfache Datenbank- und Systembackups.
- Alle wichtigen DV-Systeme werden vom Backup-System abgedeckt.
- Konzept zur Rekonstruktion der Datenbestände (Backup/Restore-Konzept).
- Virenschutzprogramme/Anti-Malwareprogramme sind vorhanden und aktuell.
- Notfallpläne sind vorhanden und werden regelmäßig geprobt.
- Unterbrechungsfreie Stromversorgung (USV) in den Unternehmensräumlichkeiten mit ausreichend langer Überbrückungsdauer und ordnungsgemäßen Herunterfahren.

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

1. Datenschutz-Management {#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 laufend gepflegt und aktualisiert.

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

Ein organisatorischer und technischer Prozess zum Umgang mit Sicherheitsvorfällen (incidents) ist definiert und implementiert. 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.

3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) {#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 kann vom Kunden selbst angepasst und verwaltet werden. Eine Löschung/ Berichtigung der Daten im System seitens des Kunden ist möglich.

4. Auftragskontrolle {#auftragskontrolle}

- Die Mitarbeiter 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.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsverarbeitung zur Verfügung, welche entsprechende Regelungen zur Kontrolle enthält:
- Sorgfältige Auswahl des Auftragnehmers,
- Eindeutige Vertragsgestaltung, insbesondere Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer und Festlegung der durchzuführenden Kontrollmaßnahmen
- Klare und eindeutige Erteilung von Weisungen (schriftliche Form), sowie Festlegung der zur Erteilung und zum Empfang von Weisungen berechtigten Personen,
- Kontrolle der bei dem Auftragnehmer getroffenen technischen und organisatorischen Sicherheitsmaßnahmen,
- Regelung des Einsatzes von Unterauftragnehmern,
- soweit erforderlich, Bestellung eines Datenschutzbeauftragten bei dem Auftragnehmer

6. Sicherheitsmaßnahmen speziell bei Fernwartung (zwischen Auftragnehmer und Auftraggeber) {#sicherheitsmaßnahmen-speziell-bei-fernwartung-(zwischen-auftragnehmer-und-auftraggeber)}

- Sofern der Auftragnehmer für Wartungsmaßnahmen auf das System des Auftraggebers zugreifen muss, ist dieser Vorgang mit dem Auftraggeber vorab abzustimmen.
- Der Auftraggeber ergreift technische Maßnahmen, um die Zugriffe des Auftragnehmers auf sein System fortlaufend zu überwachen und zu protokollieren. Der Auftraggeber stellt durch Protokollierung der Fernwartungszugriffe sicher, dass alle Fernwartungszugriffe nach der Durchführung nachvollzogen werden können. Der Auftraggeber bewahrt die Dokumentation drei Jahre auf.
- Der Auftraggeber ist berechtigt, den Fernwartungsvorgang von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen. Sofern der Fernwartungsvorgang unterbrochen wird, wird der Auftragnehmer insbesondere von seinen Verpflichtungen bezüglich Reaktionszeit, Herstellungszeiten etc. entbunden.
- Der Auftragnehmer darf personenbezogene Daten im Wege einer Dateiübertragung oder Downloads für Zwecke der Fehleranalyse und -behebung nur dann von den Datenverarbeitungssystemen des Auftraggebers abziehen und auf sein eigenes kopieren, wenn er dafür zuvor die Zustimmung des Auftraggebers eingeholt hat.
- Personenbezogene Daten, die der Auftragnehmer beim Fernzugriff erhalten hat, wird der Auftragnehmer unverzüglich löschen oder dem Auftraggeber zurückgeben, wenn diese Daten für die Durchführung der Leistungen des Auftragnehmers nach dem Wartungsvertrag nicht mehr erforderlich sind. Etwaige dem Auftragnehmer übergebene Papierausdrucke mit personenbezogenen Daten muss der Auftragnehmer nach Abschluss der Wartungs-/Pflegearbeiten gemäß dem Wartungsvertrag unverzüglich zurückgeben oder mit Zustimmung des Auftraggebers datenschutzgerecht vernichten. Dies gilt nicht für Daten, die zur Dokumentationskontrolle und für Revisionsmaßnahmen der Fernwartung benötigt werden.

7. Sicherheitsmaßnahmen speziell bei Supportanfragen (zwischen Auftragnehmer und Auftraggeber) {#sicherheitsmaßnahmen-speziell-bei-supportanfragen-(zwischen-auftragnehmer-und-auftraggeber)}

- Namen von Mitarbeitern des Auftraggebers sowie personenbezogene Fehlermeldungen, Bedienungsfehler/ -probleme oder sonstige personenbezogene Störungen werden vom Auftragnehmer nur erhoben, verarbeitet und genutzt, soweit dies zur Bearbeitung von telefonischen oder E-Mail-Support-Anfragen gemäß der Leistungsvereinbarung erforderlich ist.
- Der Auftraggeber stellt sicher, dass Daten aus Log-Files von Datensicherungen oder sonstige personenbezogene Dateien nur insoweit an den Auftragnehmer weitergeleitet werden, soweit dies zur ordnungsgemäßen Erbringung der Support-Leistungen notwendig ist.
  Soweit möglich, hat der Auftraggeber vor Zusendung der für die Supportdienstleistungen

notwendigen Daten (Logfiles, Screenshots etc.) an den Auftragnehmer alle personenbezogenen Daten zu entfernen.

[^1]: CIPSE ist ein Zusammenschluss von Anbietern von Cloud-Infrastruktur (auch “Infrastructure as a Service” genannt) und bietet europäischen Kunden Cloud-Services. Mit dem CISPE Code of Conduct können Kunden und APN-Partner sicherstellen, dass ihr Cloud-Infrastrukturanbieter die erforderlichen Datenschutzstandards erfüllt, um ihre Daten gemäß der Datenschutz-Grundverordnung zu schützen.