Auftragsverarbeitungsvertrag

(gemäß Art. 28 DSGVO)

zwischen

Kunden (gemäß Bestellschein) (nachfolgend „**Auftraggeber**“)	und	vilisto GmbH Schellerdamm 22-24 21079 Hamburg (nachfolgend „**Auftragnehmer**“)

Inhalt

1. Vertragsgegenstand und Anwendungsbereich 1
2. Pflichten des Auftraggebers 1
3. Pflichten des Auftragnehmers 2
4. Kontrollrechte des Auftraggebers 3
5. Unter-Auftragsverarbeiter 3
6. Vergütung 4
7. Rückgabe und Löschung der Daten bei Vertragsende 4
8. Laufzeit 5
9. Schlussbestimmungen 5

Anhang 1 – Einzelheiten zur Auftragsverarbeitung
Anhang 2 – Genehmigte Unter-Auftragsverarbeiter
Anhang 3 – Technische und organisatorische Maßnahmen zur Datensicherheit

1. Vertragsgegenstand und Anwendungsbereich

1.1. **Vertragsgegenstand.** Der Auftragnehmer stellt dem Auftraggeber gemäß den AGB „Wartung einer vilisto Heizungssteuerung und Bereitstellung einer Online-Plattform“ (nachfolgend „**AGB**“) und dem Bestellschein (AGB und Bestellschein nachfolgend gemeinsam "**Hauptvertrag**") Wartungsleistungen sowie eine Online-Plattform bereit. Die Online-Plattform dient der Entgegennahme, Speicherung und aufbereiteten Darstellung von Daten einer vilisto Heizungssteuerung, zur Vornahme von Einstellungen für die Heizungssteuerung und zur Bereitstellung begleitender Funktionalitäten (nachfolgend „**Online-Plattform**“). Der vorliegende Vertrag zur Auftragsverarbeitung (nachfolgend "**Vertrag**") regelt die Verarbeitung personenbezogener Daten, die der Auftragnehmer im Zusammenhang mit der Durchführung des Hauptvertrages für den Auftraggeber in dessen Auftrag verarbeitet. Die Begriffe „**personenbezogene Daten**“, „**betroffene Person**“ (nachfolgend „**Betroffener**“) und „**Verarbeitung**“ haben in diesem Vertrag die in Art. 4 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „**DSGVO**“) beschriebene Bedeutung.

1.2. **Zustandekommen**. Der Auftragsverarbeitungsvertrag kommt durch Abschluss des Hauptvertrags, dessen Anlage und Bestandteil dieser Auftragsverarbeitungsvertrag ist, zustande, ohne dass es einer gesonderten Unterschrift bedarf.

1.3. **Inhalt der Auftragsverarbeitung.** Gegenstand, Art und Zweck der Verarbeitung sowie die Art der im Auftrag verarbeiteten personenbezogenen Daten (nachfolgend „**Daten**“) sowie die Kategorien Betroffener sind in ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG geregelt.

1.4. **Anwendungsbereich.** Dieser Vertrag gilt nur, wenn und soweit es sich um personenbezogene Daten handelt, die Verarbeitung im Auftrag erfolgt und der Auftraggeber oder Auftragnehmer gemäß Art. 3 und 4 DSGVO mit der Verarbeitung der Daten den Bestimmungen der DSGVO unterliegt.

2. Pflichten des Auftraggebers

2.1. **Datenschutzrechtliche Verantwortlichkeit.** Der Auftraggeber bleibt im Verhältnis zwischen Auftraggeber und Auftragnehmer alleiniger Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Der Auftraggeber ist während der Vertragslaufzeit allein verantwortlich, insbesondere

a) für die Wahrung der Datenschutzgrundsätze (Art. 5 DSGVO),
b) für die Rechtmäßigkeit der Datenverarbeitung (Art. 6 ff. DSGVO),
c) für die Erfüllung der Transparenzpflichten (Art. 12, 13, 14 und 21 DSGVO),
d) für die Wahrung der Rechte der Betroffenen (Art. 12, 15 bis 23 DSGVO),
e) für die Führung des Verzeichnisses der Verarbeitungstätigkeiten als Verantwortlicher (Art. 30 DSGVO),
f) für die Meldung von Datenschutzverletzungen (Art. 32, 33 DSGVO), und
g) für die Durchführung von Datenschutzfolgenabschätzungen (Art. 35, 35 DSGVO).

Unterstützungspflichten des Auftragnehmers nach diesem Vertrag bleiben unberührt.

2.2. **Weisungen.** Der Auftraggeber wird, soweit erforderlich, im Rahmen des Vertragsgegenstands des Hauptvertrags Weisungen zum Umgang mit den Daten geben, insbesondere im Hinblick auf die Zwecke und wesentliche Mittel der Verarbeitung. Weisungen müssen schriftlich (E-Mail genügt) erfolgen und sind ausschließlich an die im ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten Weisungsempfänger zu richten. Zu Weisungen auf Seiten des Auftraggebers sind neben den Nutzern der Online-Plattform mit den entsprechenden Berechtigungen ausschließlich die im ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten weisungsbefugten Personen berechtigt. Änderungen bei den Weisungsempfängern und Weisungsbefugten teilen sich die Parteien unverzüglich mit (E-Mail genügt).

3. Pflichten des Auftragnehmers

3.1. **Weisungsgebundenheit.** Der Auftragnehmer verarbeitet die Daten nur auf dokumentierte Weisung des Auftraggebers hin, sofern der Auftragnehmer nicht durch das Recht der EU oder der EU-Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. Im Falle einer solchen Verpflichtung teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Weisungen des Auftraggebers können sich auch auf die Übermittlung personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums beziehen, sofern dies durch diesen Vertrag nicht bereits festgelegt ist.

3.2. **Zweckbindung.** Der Auftragnehmer verarbeitet die Daten zu den in ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten Zwecken und nach den Weisungen des Auftraggebers.

3.3. **Hinweispflicht.** Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn eine vom Auftraggeber erteilte Weisung nach Meinung des Auftragnehmers gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder desjenigen Mitgliedstaates verstößt, in dem der Auftragnehmer seinen Sitz hat. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Eine Pflicht zur rechtlichen Prüfung von Weisungen besteht für den Auftragnehmer nicht.

3.4. **Betroffenenrechte**. Machen Betroffene ihre Rechte auf Auskunft (Art. 15 DGSVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSVO) oder Datenübertragbarkeit (Art. 20 DSGVO) geltend, erfüllt der Auftraggeber diese eigenständig und eigenverantwortlich. Gleiches gilt im Fall des Widerspruchs (Art. 21 DSGVO) oder Widerrufs von Einwilligungen. Ist dem Auftraggeber die Erfüllung von Betroffenenrechten unmöglich, so unterstützt der Auftragnehmer den Auftraggeber gemäß Ziffer 3.7. Für die Herausgabe und Löschung der Daten bei Vertragsende gilt vorrangig Ziffer 7. Anträge von Betroffenen leitet der Auftragnehmer an den Auftraggeber weiter.

3.5. **Datengeheimnis.** Der Auftragnehmer gewährleistet, dass sich die beim Auftragnehmer zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.6. **Meldepflicht.** Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO im Rahmen der Auftragsverarbeitung bekannt wird, und die Daten des Auftraggebers hiervon betroffen sind, meldet der Auftragnehmer dies dem Auftraggeber unverzüglich.

3.7. **Unterstützungspflicht.** Der Auftragnehmer wird den Auftraggeber angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen

dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 12 - 23 DSGVO genannten Rechte der Betroffenen nachzukommen. In Bezug auf die Online-Plattform gilt klarstellend: Eine Pflicht des Auftragnehmers die Online-Plattform über die Leistungsbeschreibung hinaus so bereitzustellen, dass Betroffenenrechte unter der DSGVO mittels integrierter Funktionen durch den Auftraggeber selbst erfüllt werden können, besteht nicht. Der Auftragnehmer wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Auftraggeber zudem bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Datensicherheit, Meldepflichten bei Datenpannen, Datenschutzfolgenabschätzung und Konsultation von Datenschutzbehörden) unterstützen.

3.8. **Datensicherheit.** Der Auftragnehmer trifft in seinem Verantwortungsbereich alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Die bei Vertragsbeginn vom Auftragnehmer getroffenen Maßnahmen sind im ANHANG TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN beschrieben. Der Auftragnehmer ist verpflichtet, diese auf ihre Angemessenheit hin zu prüfen und im Falle von Bedenken, diese dem Auftraggeber unverzüglich mitzuteilen. Der Auftragnehmer ist berechtigt, die Maßnahmen den jeweiligen Anforderungen entsprechend anzupassen, sofern hierdurch das Datenschutzniveau insgesamt nicht abgesenkt wird. Änderungen sind vom Auftragnehmer zu dokumentieren.

3.9. **Anfragen von Aufsichtsbehörden.** Anfragen von Aufsichtsbehörden (Art. 31 DSGVO) in Bezug auf eigenständige Pflichten des Auftragnehmers aus der DSGVO (vgl. Art. 30, 32, 44 ff. Abs. 1 DSGVO) beantwortet der Auftragnehmer eigenständig und informiert den Auftraggeber nur, soweit die Sache unmittelbare rechtliche Auswirkungen auf den Auftraggeber hat.

4. Kontrollrechte des Auftraggebers

4.1. **Kontrollen.** Der Auftraggeber ist in Bezug auf die Daten berechtigt, die Einhaltung

a) der gesetzlichen Vorschriften über den Datenschutz,

b) der Vereinbarungen dieses Vertrages, und

c) der Weisungen des Auftraggebers

beim Auftragnehmer in Benehmen mit dem Auftragnehmer zu kontrollieren. Kontrollen in den Betriebsstätten des Auftragnehmers muss der Auftraggeber rechtzeitig vorher ankündigen. Kontrollen sind zu den üblichen Geschäftszeiten und ohne wesentliche Beeinträchtigung des Geschäftsbetriebs des Auftragnehmers durchzuführen.

4.2. **Nachweis der Einhaltung des Art. 28 DSGVO.** Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung hierzu die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

4.3. **Nachweis genereller Maßnahmen**. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach Wahl des Auftragnehmers auch erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO,

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO, und

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren).

4.4. **Schutzwürdige Interessen des Auftragnehmers.** Soweit durch Kontrollen Betriebs- und Geschäftsgeheimnisse des Auftragnehmers offenbart oder geistiges Eigentum des Auftragnehmers gefährdet werden kann oder die Interessen des Auftragnehmers in ähnlicher Weise beeinträchtigt werden können, hat der Auftraggeber die Kontrollen durch einen fachkundigen und unabhängigen Dritten vornehmen zu lassen, der sich gegenüber dem Auftragnehmer vorab schriftlich zur Verschwiegenheit verpflichtet.

5. Unter-Auftragsverarbeiter

5.1. **Genehmigungserfordernis**. Der Auftragnehmer darf seinerseits weitere Auftragsverarbeiter (nachfolgend „**Unter-Auftragsverarbeiter**“) nur nach vorheriger schriftlicher Genehmigung des Auftraggebers (E-Mail genügt) einschalten. Die Genehmigung kann sich auf konkrete

Unternehmen beziehen (nachfolgend „**Einzel-Genehmigung**“) oder allgemein für eine Gruppe oder Art von Unternehmen erteilt werden (nachfolgend „**General-Genehmigung**“).

5.2. **Erteilte Genehmigungen**. Der Auftraggeber genehmigt hiermit die in ANHANG 2 – GENEHMIGTE UNTER-AUFTRAGSVERARBEITER genannten Unter-Auftragsverarbeiter.

5.3. **Information und Widerspruch bei General-Genehmigungen**. Im Fall einer General-Genehmigung gilt:

a) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Ersetzung eines bestehenden oder Hinzuziehung eines neuen Unter-Auftragsverarbeiters (Änderung) mit einer angemessenen Vorfrist, in der Regel mindestens vier Wochen. Die Information kann per E-Mail an den in ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG genannten Weisungsberechtigten des Auftraggebers erfolgen.

b) Der Auftraggeber hat das Recht, der Änderung des Unter-Auftragsverarbeiters schriftlich (E-Mail genügt) zu widersprechen. Im Falle eines Widerspruchs steht dem Auftragnehmer das Recht zu, diesen Vertrag und den Hauptvertrag außerordentlich mit Wirkung zum geplanten Inkrafttreten der Änderung außerordentlich zu kündigen (E-Mail genügt). Etwaig vorausbezahlte Vergütungen für den Zeitraum nach Wirksamwerden der Kündigung hat der Auftragnehmer dem Auftraggeber zu erstatten. Der Auftraggeber wird von seinem Widerspruchsrecht nur im Falle eines wichtigen Grundes Gebrauch machen. Ein wichtiger Grund liegt dann vor, wenn das berechtigte Interesse des Auftraggebers am Unterbleiben der Änderung dasjenige des Auftragnehmers an der Änderung wesentlich überwiegt.

5.4. **Vereinbarungen mit Unter-Auftragsverarbeitern.** Der Auftragnehmer wird Unter-Auftragsverarbeitern entsprechende Datenschutzpflichten auferlegen, so wie sie in diesem Vertrag festgelegt sind.

6. Vergütung

6.1. **Gesonderte Vergütung**. Die Leistungen des Auftragnehmers nach diesem Vertrag sind mit der im Hauptvertrag vereinbarten Vergütung abgegolten, jedoch mit folgenden Ausnahmen:

a) Den durch die Erfüllung der Unterstützungspflichten nach den Ziffern 3.4 und 3.7 verursachten Aufwand hat der Auftraggeber dem Auftragnehmer zu ersetzen.

b) Geht der Inhalt von Weisungen des Auftraggebers über dasjenige hinaus, was der Auftragnehmer dem Auftraggeber gemäß dem Hauptvertrag und dessen Leistungsbeschreibung explizit schuldet, hat der Auftraggeber die entsprechenden Aufwände dem Auftragnehmer gesondert zu vergüten.

c) Durch Kontrollen (insbesondere gemäß Ziffer 4.1) entstehende Aufwände wird der Auftraggeber dem Auftragnehmer erstatten, ausgenommen Aufwände im Rahmen des Nachweises genereller Maßnahmen nach Ziffer 4.3.

Die Vergütungspflicht entfällt, wenn, und soweit der Aufwand durch eine schuldhafte Pflichtverletzung des Auftragnehmers verursacht wurde.

6.2. **Arbeitszeit und Vorschüsse.** Die Aufwände nach Ziffer 6.1 umfassen neben Fremdkosten (z.B. Reisekosten) auch eine Vergütung der Arbeitszeit des vom Auftragnehmer in Anspruch genommenen Personals. Hierbei gilt ein Stundensatz von € 90,- (netto). Der Auftragnehmer kann bei umfangreicheren Arbeiten einen angemessenen Vorschuss vom Auftraggeber verlangen.

7. Rückgabe und Löschung der Daten bei Vertragsende

7.1. **Löschung**. Am Ende der Laufzeit dieses Vertrages wird der Auftragnehmer die Daten des Auftraggebers in seinem Produktionssystem und dessen Backups löschen, soweit der Auftragnehmer nicht durch das Recht der EU oder des Mitgliedsstaates, in dem er seinen Sitz hat, zur weiteren Speicherung verpflichtet ist. Soweit eine Löschung nur mit unverhältnismäßigem Aufwand möglich ist (z.B. in Archiven) kann eine vorübergehende Sperrung und endgültige Löschung im Rahmen des nächsten Löschturnus erfolgen.

7.2. **Anonymisierung**. Der Auftragnehmer ist berechtigt, die Daten in Form von Ziffer 6.6 und 6.7 der AGB weiter zu speichern und für die in Ziffer 6.5 AGB genannten Zwecke zu nutzen. Nach dem gemeinsamen Verständnis der Parteien handelt es sich bei diesen Daten ab Löschung der Daten im Produktionssystem um keine personenbezogenen Daten mehr, da kein Bezug mehr zu einer natürlichen Person herstellbar ist.

7.3. **Rückgabe.** Der Auftraggeber kann bei Vertragsende die Rückgabe der Daten vom Auftragnehmer heraus verlangen. Es gelten hierzu die Bestimmungen des Hauptvertrags (vgl. dort Ziffer 6.9 AGB).

8. Laufzeit

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Hauptvertrages Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.

9. Schlussbestimmungen

Ziffer 13 der AGB (Schlussbestimmungen) gelten auch für diesen Auftragsverarbeitungsvertrag.

ANHANG 1 – EINZELHEITEN ZUR AUFTRAGSVERARBEITUNG

1. Gegenstand, Art und Zweck der Verarbeitung

Bereitstellung einer Online-Plattform zur Entgegennahme, Speicherung und aufbereiteten Darstellung von Daten einer vilisto Heizungssteuerung, zur Vornahme von Einstellungen für die Heizungssteuerung und zur Bereitstellung begleitender Funktionalitäten gemäß Hauptvertrag.

Erbringung von Wartungsleistungen gemäß Hauptvertrag.

2. Art der personenbezogenen Daten

- Daten über Personen, die sich in Räumen mit ovis-Thermostaten aufhalten, insbesondere
  - ermittelte Anwesenheit einer Person in einem bestimmten Raum sowie zu Grunde liegende aggregierte Sensordaten, z.B.
    - Anzahl erkannter Bewegungen
    - Schallpegeldaten (keine Tonaufnahmen), z.B. Anzahl Überschreitungen eines Schallpegels in bestimmtem Zeitraum, höchster/durchschnittlicher Schallpegel)
    - Helligkeit, Luftfeuchte und Temperatur am Thermostat
  - Wahrscheinlichkeit der Anwesenheit einer Person in einem bestimmten Raum zu einer bestimmten Uhrzeit an einem bestimmten Wochentag (Kalenderdatei)
  - erkannte Fensteröffnung im Raum
  - erlernte Wohlfühltemperatur für Raum
  - vorgenommene Einstellungen (z.B. Einstellung Solltemperatur an ovis-Thermostaten, Anzahl der Nutzer-Interaktionen mit ovis-Thermostat)
- Daten über Nutzerkonten der Online-Plattform, deren Rollen und Berechtigungen sowie protokollierte Nutzeraktionen

3. Kategorien betroffener Personen

- Personen, die sich in Räumen mit ovis-Thermostaten aufhalten
- Nutzer der Online-Plattform

4. Weisungsempfänger und Weisungsberechtigte

a) Weisungsempfänger beim Auftragnehmer

Etwaige Weisungen des Auftraggebers an den Auftragnehmer sind an das Kundenmanagement unter folgender E-Mail-Adresse zu richten:

dsgvo-weisungen@vilisto.de

b) Weisungsbefugte Personen beim Auftraggeber

Die weisungsbefugten Personen sind im Hauptvertrag vermerkt.

5. Besondere Weisungen / Vereinbarungen

Die Verarbeitung erfolgt ausschließlich auf Datenverarbeitungsanlagen innerhalb des Europäischen Wirtschaftsraums.

ANHANG 2 – GENEHMIGTE UNTER-AUFTRAGSVERARBEITER

1. Einzel-Genehmigungen

Nr.	Firma, Anschrift, Land	Serverstandorte	erbrachte Leistungen	ggf. Anmerkungen
1	ALL-INKL.COM - Neue Medien Münnich Hauptstraße 68, 02742 Friedersdorf, Deutschland	Deutschland	Hosting der Online-Plattform	

2. General-Genehmigungen

Der Auftragnehmer darf für Hosting-Leistungen Unter-Auftragsverarbeiter mit Sitz im Europäischen Wirtschaftsraum einsetzen.

Technische und organisatorische Maßnahmen zur Datensicherheit

gemäß Art. 32 DSGVO (als Auftragsverarbeiter)

Inhaltsverzeichnis

1. Gegenstand **2**

2. Unter-Auftragsverarbeiter **2**

3. Vertraulichkeit (Art 32 Abs. 1 lit. b) DSGVO) **2**

2.1 ***Zutrittskontrolle*** *2*

2.2 ***Zugangskontrolle*** *2*

2.3 ***Zugriffskontrolle*** *3*

2.4 ***Datentrennung*** *4*

2.5 ***Verschlüsselung (Art 32 Abs. 1 lit. a) DSGVO)*** *4*

2.6 ***Pseudonymisierung (Art 32 Abs. 1 lit. a) DSGVO)*** *4*

4. Integrität (Art 32 Abs. 1 lit. b) DSGVO) **4**

2.7 ***Eingabekontrolle*** *4*

2.8 ***Weitergabekontrolle*** *4*

5. Verfügbarkeit (Art 32 Abs. 1 lit. b) DSGVO) **4**

6. Dokumenten-Historie **4**

1. Gegenstand

Dieses Dokument beschreibt die durch die vilisto GmbH (nachfolgend „**Unternehmen**“) getroffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten, soweit das Unternehmen als Auftragsverarbeiter handelt.

Die Maßnahmen beziehen sich auf folgende Verarbeitungen:

- Bereitstellung einer Online-Plattform für eine vilisto Heizungssteuerung
  - zur Entgegennahme, Speicherung und aufbereiteter Darstellung von Daten
  - zur Vornahme von Einstellungen für die Heizungssteuerung
  - zur Bereitstellung begleitender Funktionalitäten gemäß Hauptvertrag.

2. Unter-Auftragsverarbeiter

Das Unternehmen nutzt den Unter-Auftragsverarbeiter NEUE MEDIEN *MÜNNICH* die Technischen und Organisatorischen Maßnahmen des Unterauftragnehmers sind in einem eigenen Dokument erläutert. Dieses ist als **Anhang A1** – diesem Dokument angehängt. Die aufgeführten Unter-Auftragsverarbeiter werden gemeinsam als die **Unter-Auftragsverarbeiter** bezeichnet. Die dazugehörigen Anhänge gemeinsam „**Anhänge A**“

3. Vertraulichkeit (Art 32 Abs. 1 lit. b) DSGVO)

2.1 Zutrittskontrolle

Die nicht anonymisierten Daten werden ausschließlich in Rechenzentren unserer Unter-Auftragsverarbeiter gespeichert. Diese sind dort für die Zutrittskontrolle verantwortlich und beschreiben ihre Maßnahmen in den Anhängen A. vilisto speichert **anonymisierte Daten** auf seinen eigenen Servern in den eigenen Büroräumen. Dieser Server ist durch eine weitere verschlossene Tür innerhalb der vilisto Räumlichkeiten vor dem Zugriff Unbefugter geschützt. Einen Schlüssel hierfür besitzt ausschließlich ein stark eingeschränkter Personenkreis. Weiteren Mitarbeitern wird der Zugang nur zeitweise gewährt, um eventuell nötige Arbeiten durchzuführen.

2.2 Zugangskontrolle

a) Zugang auf Serverdaten

Direkten Zugriff zu den nicht anonymisierten Kundendaten (Serverzugriff, Datenbankzugriff) hat nur ein stark beschränkter Personenkreis. Für diese Systeme werden sichere Passwörter verwendet (mindestens 16 Zeichen zufällig generiert). Diese Passwörter werden mittels KeePass verschlüsselt gespeichert. Nur der stark eingeschränkte Personenkreis hat hierzu Zugang. Technische Mitarbeiter und Entwickler sind angewiesen keine Versuche zu unternehmen, Passwörter aus Quellcode oder Ähnlichem auszulesen. Es ist protokolliert wer zum eingeschränkten Personenkreis gehört. Sollte ein Mitarbeiter aus dem eingeschränkten Personenkreis ausscheiden, wird das Zugriffspasswort zur KeePass Datei umgehend geändert. Dieser Vorgang wird schriftlich festgehalten.

b) Zugang über die Online-Plattform durch vilisto

Alle anderen Mitarbeiter von vilisto (Support, Vertrieb, Technik) und Kunden haben ausschließlich über die vilisto Online-Plattform Zugriff auf die nicht anonymisierten Kundendaten. Die Online-Plattform ist durch Authentifizierung mittels eines Benutzernamens und eines Passwortes vor unberechtigtem Zugang geschützt. vilisto Mitarbeiter verwenden für den Zugriff ihre Domänenzugangsdaten. Die Vergabe und der Entzug von Zugängen für die Online-Plattform wird durch den Domänenserver der vilisto automatisch dokumentiert. Sollen Mitarbeiter aufgrund von Ausscheiden aus dem Unternehmen ihre Berechtigungen verlieren, wird dies durch ein komplettes Deaktivieren des Domänenkontos erreicht. Das Deaktivieren des Kontos ist bei vilisto Teil des normalen Offboarding-Prozesses. Die Mitarbeiter des Unternehmens sind angewiesen die Kundendaten als vertraulich zu behandeln. Die Mitarbeiter des Unternehmens sind angewiesen bei Abwesenheit ihre Computer zu sperren, sodass Besucher oder Mitarbeiter ohne Berechtigungen nicht zufällig Zugang erhalten. Nach 10 Minuten ohne Benutzung werden die Mitarbeiter außerdem automatisch aus der Online-Plattform ausgeloggt.

c) Zugang über die Online-Plattform durch den Kunden

Der Kunde erhält Zugang über Online-Plattform-Konten auf die Online-Plattform. Ein Kunde erhält dabei nur Zugriff auf die Daten, der bei dem Kunden installierten Thermostate und Gateways. Die Kundenkontos sind über Authentifizierungen mittels Benutzerkennung und Passwort geschützt. Jegliches Erstellen, oder Löschen von Konten sowie das Hinzufügen oder Entfernen von

Benutzerrechten durch vilisto oder den Kunden wird automatisch protokolliert. Diese Protokolle werden 180 Tage gespeichert. Für den sorgfältigen Umgang mit seinem Zugang zur Online-Plattform und mit weiteren Zugängen, die sich der Kunde erstellen kann, trägt der Kunde selbst die Verantwortung.

2.3 **Zugriffskontrolle**

a) Zugriffseinschränkungen

Die Konten können nach einem oder mehreren der folgenden Kriterien im Umfang der Daten auf, die sie zugreifen können, eingeschränkt werden:

(1) Alter der Daten, sodass nur Daten aus einer einzustellenden Periode eingesehen werden können.

(2) Thermostate die eingesehen werden können. Konten können so beschränkt werden, dass sie ausschließlich bestimmte Thermostate oder Thermostate bestimmter Kunden einsehen können.

(3) Sichtbarkeit einzelner Datensätze. Das Konto kann berechtigt werden verschiedene Datensätze angezeigt zu bekommen. Beispielsweise Temperaturen, Solltemperaturen, Luftfeuchtigkeit oder die Ventilstellung.

b) Rollen und Berechtigungen

Es sind folgende Rollen vorgesehen, die bestimmte Rechte haben:

(1) vilisto Administrator (stark eingeschränkter Personenkreis).

Zugriff auf alle Daten und die Möglichkeit alle Einstellungen anzupassen. Erstellen von Accounts, vergeben von Rechten.

(2) vilisto Support

Zugriff auf alle betreuten Thermostate, alle Datensätze der letzten 14 Tage. Einstellungen für Thermostate vornehmen.

(3) vilisto Entwickler

Zugriff nur auf Thermostate von Kunden die explizit zur Nutzung in der Weiterentwicklung zugestimmt haben sowie Zugriff auf anonymisierte Daten. (Verbot jedes Versuchs der De-Anonymisierung).

(4) *Hauptaccount Kunde*

Zugriff auf alle Daten der Thermostate des Kunden. Einstellungen vornehmen für alle Thermostate des Kunden. Festlegung der Speicherfristen für die Daten des Kunden.

(5) *Unteraccount Kunde*

Zugriff auf eine Teilmenge der Thermostate des Kunden, begrenzter Zeitraum und begrenzte Datensätze. Dies ist durch den Kunden definierbar.

c) Modifikationseinschränkungen

Im der Online-Plattform gibt es keine Möglichkeit Daten zu modifizieren. Lediglich das Ändern von Einstellungen ist möglich. Daten können nur durch den Hauptaccount eines Kunden manuell gelöscht werden. Sie werden regelmäßig automatisiert mit den durch den Kunden eingestellten Löschfristen gelöscht.

d) Überprüfung bei vilisto

vilisto überprüft mindestens alle 3 Monate ob allen ihren Mitarbeitern noch die richtigen Rollen zugewiesen sind. Diese Überprüfung wird protokolliert.

e) Überprüfung beim Kunden

Der Kunde ist selbst dafür verantwortlich die von ihm vergebenen Zugriffsrechte zu kontrollieren.

2.4 Datentrennung

a) Die Thermostate werden eindeutig durch das Gateway, mit dem sie verbunden sind, einem Kunden zugeordnet.

b) Kunden haben ausschließlich auf Thermostate ihrer Gateways Zugriff. Die Zuordnung der Gateways zu den Kunden erfolgt bei Installation und kann nur durch vilisto Administratoren- oder vilisto Support-Konten erfolgen.

c) Entwickler arbeiten, wenn möglich ausschließlich auf Testsystemen, die auf komplett getrennten Daten laufen.

d) Sollte es notwendig sein auf Systemen mit Kundendaten Tests durchzuführen, haben die Entwickler nur auf Daten der von den Kunden für Entwickler freigegebenen Thermostate bzw. Test-Thermostate Zugriff.

2.5 Verschlüsselung (Art 32 Abs. 1 lit. a) DSGVO)

a) Transportverschlüsselung bei der Sammlung der Daten:

Die Daten werden zwischen den Thermostaten und den Gateways via Funk des Standards ZigBee übertragen. Diese Übertragung ist durch das im ZigBee vorgesehene AES verschlüsselt. Zwischen Gateways und Server werden die Daten SSL-verschlüsselt übertragen.

b) Transportverschlüsselung bei der Anzeige der Online-Plattform

Die Daten, die über die Online-Plattform angezeigt werden, werden über HTTPS zum Web-Browser des Nutzers übertragen und sind somit per SSL verschlüsselt.

2.6 Pseudonymisierung (Art 32 Abs. 1 lit. a) DSGVO)

Die Datensätze werden pseudonymisiert gespeichert. Dies bedeutet, dass die Daten wie beispielsweise Temperaturverläufe ausschließlich mit einer ID identifiziert sind. Die Zuordnung von IDs zu Raumnamen erfolgt über eine getrennte Datenbanktabelle. Die Raumnamen/-Nummern können selbst auch noch als Pseudonym betrachtet werden. Ohne Zusatzinformationen, die den vilisto Mitarbeitern nicht zugänglich sind, kann aufgrund der Raumnummern bzw. -Namen nicht auf einzelne Personen geschlossen werden.

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

2.7 Eingabekontrolle

Das System erlaubt es nicht Personenbezogene Daten einzugeben oder zu ändern. Alle Personenbezogenen Daten werden durch die Thermostate aufgezeichnet. Für die Änderung von Einstellungen gelten die beschriebenen Zugangskontrollen und Protokollierungsmaßnahmen.

2.8 Weitergabekontrolle

Bei vilisto werden keine Personenbezogenen Daten weitergegeben. Jeglicher Zugriff auf Personenbezogene Daten erfolgt über die Online-Plattform.

5. Verfügbarkeit (Art 32 Abs. 1 lit. b) DSGVO)

Die Unterauftragnehmer des Unternehmens treffen gemäß ihren technischen und organisatorischen Maßnahmen in den Anhängen A entsprechende Maßnahmen.

6. Dokumenten-Historie

Version	Datum	Bearbeiter	Änderung
1.0	04.09.2019	Lasse Stehnken	Ersterstellung

Technische und organisatorische Maßnahmen
Auftragsverarbeitungsvertrag
Art. 32 Abs. 2 DS-GVO

0 Auftragsverarbeiter

0.1 Auftragsverarbeiter ist

ALL-INKL.COM - Neue Medien Münnich

Inhaber: René Münnich
Hauptstraße 68, 02742 Friedersdorf, Deutschland

0.2 Der Auftragsverarbeiter (Auftragnehmer des Auftragsverarbeitungsvertrags) hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die für eine Auftragsverarbeitung erforderlichen technischen und organisatorischen Maßnahmen getroffen, um bei der (Auftrags-)Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die (Auftrags-)Verarbeitung besonderer Kategorien personenbezogener Daten.

0.3 Die nachstehenden entsprechend dem Katalog aus § 64 BDSG (2017) beschriebenen Maßnahmen beziehen sich auf ergriffene Maßnahmen, die im Rahmen der Auftragsverarbeitung erforderlich sind. Aus Sicherheitsgründen erfolgt nachstehend nur eine allgemeine Beschreibung.

0.4 Sämtliche getroffenen Maßnahmen bauen auf der Mitverantwortung des Kunden (Auftraggeber des Auftragsverarbeitungsvertrags) auf, weil der Kunde im Rahmen der Webhosting-Dienstleistungen einen an das Internet angebundenen Speicherplatz zur Ablage von Informationen/ personenbezogenen Daten für Zwecke deren Verarbeitung erhält, der zunächst „leer“ ist. Die Zwecke des „ob“ und des „wie“ der Nutzung bestimmt ausschließlich der Kunde. Entsprechendes gilt für den zur Verfügung gestellten E-Mail-Server und die sonstigen technischen Dienste. Demzufolge hat der Auftragsverarbeiter zunächst originär keine vertragliche Befugnis, auf diese Daten des Kunden zuzugreifen, selbst wenn dies technisch möglich ist. Die erforderliche Software zur Datenverarbeitung wird durch den Kunden auf dem ihm zugewiesenen Speicherplatz hochgeladen bzw. dort aktiviert. Der Auftragsverarbeiter sorgt lediglich für die technische Einsatzbereitschaft der IT-Systeme entsprechend den vertraglichen Vereinbarungen. Der Kunde ist folglich im Rahmen der durch ihn durchgeführten Datenverarbeitungen der „Herr der Daten“.

0.5. Ausnahmsweise jedoch nimmt der Auftragsverarbeiter im Rahmen der getroffenen Vereinbarung zur Auftragsverarbeitung Weisungen des Kunden entgegen und verarbeitet nur dann personenbezogene Daten des Kunden auf den diesem zur Nutzung überlassenen IT-Systemen in dessen Auftrag und aufgrund dessen Weisung.

V e r t r a u l i c h k e i t

1 Zutrittskontrolle

Gewährleistungsziel: Verwehrung des Zutritts zu Verarbeitungsanlagen, mit denen die (Auftrags-) Verarbeitung durchgeführt wird, für Unbefugte.

Getroffene Maßnahmen:

1.1 Die Rechenzentren und das Servicezentrum befinden sich in Deutschland (Dresden und Friedersdorf). Das Webhosting erfolgt ausschließlich auf Datenspeichern in Deutschland.

1.2 Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den autorisierten Zutritt zum Rechenzentrum, in welchem die IT-Systeme für den Kunden vorgehalten werden, sowie zum Servicezentrum aus welchem die IT-Systeme administriert werden.

1.3 Zutritte von Besuchern werden stets durch Beschäftigte des Auftragsverarbeiters begleitet. Das Rechenzentrum ist 24/7 durch Beschäftigte besetzt. Unbegleitete Zutritte sind nicht möglich.

1.4 Es sind Videokameras zur Überwachung des Zutritts und Einbruchs- bzw. Kontaktmelder im Einsatz.

1.5 Zutrittsberechtigte Beschäftigte sind organisatorisch festgelegt, Magnetkarten bzw. Schlüssel werden nur entsprechend einer Organisationsanweisung vergeben. Über den Zutritt von Besuchern des Rechenzentrums werden Anwesenheitslisten geführt, Regelungen für Fremdpersonal und zur Begleitung von Gästen sind vorhanden.

2 Zugangskontrolle

Gewährleistungsziel: Verwehrung des Zugangs zu Datenverarbeitungssystemen, mit denen die (Auftrags-) Verarbeitung durchgeführt wird, für Unbefugte.

Getroffene Maßnahmen:

2.1 Der Zugang zu Datenverarbeitungssystemen ist nur durch Authentifizierung möglich, wenigstens durch ein System von Benutzername und Passwort.

2.2. Im Übrigen sind Zugänge durch ein Berechtigungskonzept (abgestufte Zugriffsberechtigungen) nur besonders autorisierten Beschäftigten vorbehalten.

3 Datenträgerkontrolle

Gewährleistungsziel: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von *Datenträgern*.

Getroffene Maßnahmen:

3.1 S.o. Ziffer 2.1 und 2.2.

3.2 Soweit auf Weisung des Kunden Daten im Auftrag verarbeitet und personenbezogene

Daten auf Festplatten-Speicherplätzen als Datenträger gespeichert sind, erfolgen Zugriffe des Auftragsverarbeiters durch ein System von Befugnissen abgestufter Zugriffsberechtigungen durch die Beschäftigten in den Abteilungen Technik (Administration), Support, Domainverwaltung und Kundenbuchhaltung. Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch) sind getrennt. Der Zugriff entsprechend Berechtigung wird auch bei Verfahren zur Wiederherstellung von Daten aus Backups gewahrt. Test- und Produktionsumgebung sind getrennt.

3.3 Es ist Sache des Kunden, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages durch geeignete Techniken (Software) zu verschlüsseln.

4 Speicherkontrolle

Gewährleistungsziel: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von *gespeicherten* personenbezogenen Daten.

Getroffene Maßnahmen:

4.1 Die Bereitstellung der dem Kunden zur Nutzung überlassenen IT-Systeme des Auftragsverarbeiters und die Anbindungen der vertraglich zugesicherten Dienste an das Internet erfolgt außerhalb eines Weisungsrechts des Kunden ausschließlich in Verantwortung des Auftragsverarbeiters.

4.2 Der Zugang des Kunden auf die Datenspeicher des Auftragsverarbeiters, mit welchen die Webhosting-Dienstleistungen erbracht werden, erfolgt ausschließlich von außerhalb der Betriebsgebäude über Datenleitungen bzw. das Internet durch ein System der Anmeldung des Kunden mit einem ihm vergebenen Benutzernamen und einem Passwort.

4.3 Je nach den Nutzungshandlungen, die der Kunde auf den ihm zur Nutzung überlassenen Datenspeichern vornimmt, ist es alleine seine Verantwortung zu verhindern, dass eine unbefugte Eingabe von personenbezogenen Daten sowie eine unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten erfolgt.

4.4. Soweit jedoch der Auftragsverarbeiter auf Weisung des Kunden tätig wird, personenbezogene Daten des Kunden auf den ihm überlassenen Datenspeichern zu verarbeiten, hat nur ausgewähltes technisches Personal Zugangsrechte auf die betroffenen IT-Systeme.

4.5. Im Übrigen ist es Sache des Kunden, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Speicherkontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren.

5 Benutzerkontrolle

Gewährleistungsziel: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von *Einrichtungen zur Datenübertragung* durch Unbefugte.

Getroffene Maßnahmen:

5.1 Soweit im Rahmen der Auftragsverarbeitung durch den Auftragsverarbeiter „Einrichtungen zur Datenübertragung“ in den IT-Systemen des Auftragsverarbeiters genutzt werden, werden diese Einrichtungen durch ein dem Stand der Technik entsprechendes Verschlüsselungsverfahren betrieben, wenn der Schutzbedarf eine Verschlüsselung erfordert.

5.2 Sämtliche Beschäftigte des Auftragsverarbeiters sind zum Personendatenschutz geschult und entsprechend zur Vertraulichkeit verpflichtet.

5.3 Im Übrigen ist es Sache des Kunden, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Benutzerkontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren.

6 Übertragungskontrolle

Gewährleistungsziel: Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Getroffene Maßnahmen:

6.1 Soweit der Auftragsverarbeiter Übermittlungen oder Zurverfügungstellungen auf Weisung des Kunden vornimmt, werden die betroffenen Übermittlungsstellen dokumentiert.

6.2 Soweit erforderlich werden die Daten gegen Zugriffe auf Netzwerkebene geschützt und Schnittstellen gegen unbefugten Datenexport gesichert.

6.3 Im Übrigen ist es Sache des Kunden, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Übertragungskontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren und durch eine Verschlüsselung, z.B. SSL/TLS, dafür zu sorgen, dass die von ihm zu
übertragenen Daten für Dritte nicht lesbar sind.

7 Zugriffskontrolle

Gewährleistungsziel: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Getroffene Maßnahmen:

Es ist Sache des Kunden, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Zugriffskontrolle zu unterziehen, insbesondere nur geeigneten Dritten (z.B. Webagenturen, Administratoren) Zugang und Zugriff zu gewähren.

8 Eingabekontrolle

Gewährleistungsziel: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.

Getroffene Maßnahmen:

8.1 Es ist Sache des Kunden, ggf. personenbezogene Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einzugeben und dazu, insbesondere nur geeignete Dritte einzusetzen (z.B. Webagenturen, Administratoren). Die Beschäftigten des Auftragsverarbeiters dürfen grundsätzlich nicht auf diese Daten zugreifen bzw. Daten eingeben, verändern oder löschen.

8.2 Das Verarbeiten von personenbezogenen Daten erfolgt somit grundsätzlich durch den Kunden, so dass durch den Auftragsverantwortlichen nicht nachträglich überprüft werden und festgestellt werden kann, welche personenbezogenen Daten der Kunde zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert hat.

8.3 Nur im Rahmen seiner Tätigkeiten nach Weisung protokolliert der Auftragsverarbeiter diese Eingaben und Veränderungen in angemessener Weise und dokumentiert die Uhrzeit und den Eingebenden.

8.4 Muss der Auftragsverarbeiter aus gesetzlichen Gründen Informationen entfernen oder den Zugang zu ihnen sperren (etwa im Falle der Nutzung vom Kunden auf den IT-Systemen für Dritte bereit gehaltenen Telemediendiensten bzw. elektronischen Kommunikationsdiensten), wird die Sperrung bzw. die Entfernung von Inhalten protokolliert. Die Protokolldaten werden aufbewahrt und enthalten die Mitarbeiterkennung. Die Löschung erfolgt nach dem Vertragsende automatisiert und wird protokolliert.

9 Transportkontrolle

Gewährleistungsziel: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Getroffene Maßnahmen:

9.1 Die Gewährleistung der Vertraulichkeit der Übermittlung von personenbezogenen Daten wird durch SSL/TLS-Verschlüsselungen über die Webseiten des Auftragsverarbeiters gewährleistet. Soweit nach der Art des personenbezogenen Datums eine Integritätswahrung erforderlich ist, setzt der Auftragsverarbeiter ein Prüfsummenverfahren ein.

9.2 Die Datenträgerentsorgung geschieht durch zertifizierte Entsorgungsdienstleister.

9.3 Im Übrigen ist es Sache des Kunden, die Daten auf dem ihm vertragsgemäß überlassenen Speicherplatz für die Dauer des Vertrages einer geeigneten Transportkontrolle zu unterziehen und geeignete Verschlüsselungstechniken einzusetzen.

10 Pseudonymisierung

Getroffene Maßnahmen:

Es ist Sache des Kunden, personenbezogene Daten auf dem ihm überlassenen Speicherplatz selbst zu pseudonymisieren, soweit dies gesetzlich erforderlich ist.

11 Klassifikationsschema für Daten

Getroffene Maßnahmen:

Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim, vertraulich, intern, öffentlich, normaler Schutzbedarf, durchschnittlicher Schutzbedarf, hoher Schutzbedarf, sensibles Datum).

I n t e g r i t ä t

12 Datenintegrität

Gewährleistungsziel: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Getroffene Maßnahmen:

12.1 Es erfolgt die Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen und Transaktionshistorien sowie die Dokumentation der Syntax von Daten.

12.2 Es bestehen Reparaturstrategien und Ausweichprozesse.

12.3 Schreib- und Änderungsrechte sind eingeschränkt.

12.4 Erforderlichenfalls erfolgt der Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptografiekonzepts.

12.5 Es erfolgt ein Monitoring des Sollverhaltens von Prozessen. Es werden regelmäßig Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen durchgeführt.

12.6 Das Sollverhalten von Abläufen bzw. Prozessen wird festgelegt. Es erfolgt eine regelmäßige Durchführung von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen.

12.7 Über die Maßnahmen Ziffer 12.1 bis 12.6 hinaus, die der Auftragsverarbeiter für seine Daten und Systeme ergreift, ist es Sache des Kunden, für die Datenintegrität des Datenbestandes auf dem ihm überlassenen Speicherplatz selbst Sorge zu tragen.

V e r f ü g b a r k e i t u n d B e l a s t b a r k e i t

13 Verfügbarkeitskontrolle

Gewährleistungsziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Getroffene Maßnahmen:

13.1 Die Stromversorgung der Rechenzentren erfolgt über eigene Trafostationen. Die Stromversorgung und Netzersatzanlagen garantieren höchste Ausfallsicherheit.

13.2 Die unmittelbare Stromversorgung der Server ist typenabhängig, so dass bei der Verwendung entsprechender Typen zusätzlich eine redundante Stromversorgung über ein redundantes Netzteil (2 Netzteile) gewährleistet ist.

13.3 Der gesamte Energieverbrauch der Rechenzentren wird über unterbrechungsfreie Stromversorgungen (USV) sichergestellt. Im Falle eines Stromausfalls garantieren die USV-Anlagen eine unterbrechungsfreie Umschaltung auf eines der Notstrom-Dieselaggregate. Daneben filtern die USV-Anlagen vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes.

13.4 Leistungsstarke Netzersatzanlagen (Dieselaggregate) versorgen bei Stromausfall die Rechenzentren und die Kühlsysteme mit konstanter Energie.

13.5 Es erfolgt eine gerätegestützte Überwachung der Temperatur und der Feuchtigkeit im Rechenzentrum.

13.6 Es ist ein flächendeckendes Brand- und Frühwarnsystem im Einsatz.

14 Wiederherstellbarkeit

Gewährleistungsziel: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Getroffene Maßnahmen:

Die eingesetzten Systeme sind technisch redundant vorhanden. Der Datenbestand unterliegt einer regelmäßigen Sicherung. Es ist Sache des Kunden, seinen Datenbestand auf dem ihm überlassenen Speicherplatz selbst durch geeignete Sicherungsmaßnahmen vor Datenverlust zu schützen.

15 Trennbarkeit

Gewährleistungsziel: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Getroffene Maßnahmen:

15.1 Es erfolgt eine getrennte Verarbeitung und/oder Lagerung von Daten mit

unterschiedlichen Verarbeitungszwecken.

15.2 Es ist ein System von Befugnissen abgestufter Zugriffsberechtigungen durch die Beschäftigten in den Abteilungen Technik (Administration), Support, Domainverwaltung und Kundenbuchhaltung errichtet.

15.3 Es ist Sache des Auftraggebers, für die Trennung von personenbezogenen Daten auf dem ihm überlassenen Speicherplatz, selbst Sorge zu tragen.

16 Zuverlässigkeit

Gewährleistungsziel: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Getroffene Maßnahmen:

Die Verfügbarkeit der IT-technischen Systeme unterliegt einem 24/7 Monitoring.

A u f t r a g s v e r a r b e i t u n g

17 Auftragskontrolle

Gewährleistungsziel: Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Getroffene Maßnahmen:

17.1 Es erfolgt eine Kennzeichnung des Auftragsverarbeitungs-Status gegenüber dem Status der weisungsfreien Datenverarbeitung mit hinterlegtem Auftragsverarbeitungsvertrag und den dazugehörigen Anlagen in der Kundenmaske. Beschäftigte - insbesondere im Rahmen des Telefon-Support - haben somit ständig Kenntnis über das Vorliegen/Nichtvorliegen eines Auftragsverarbeitungsvertrags.

17.2 Es erfolgt eine Verarbeitung im Auftrag mit standardisierten Vertragsformularen des Auftragsverarbeiters, um eine gleichbleibende Qualität der Auftragsverarbeitung zu gewährleisten. Davon ggf. abweichende Formulare des Auftraggebers werden ggü. den betroffenen Beschäftigten des Auftragsverarbeiters besonders gekennzeichnet, um Abweichungen in den Standards der Arbeitsabläufe zu erfassen.

V e r f a h r e n z u r r e g e l m ä ß i g e n Ü b e r p r ü f u n g, B e w e r t u n g u n d E v a l u i e r u n g

18 Prüfung, Bewertung Evaluierung

Gewährleistungsziel: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung.

Getroffene Maßnahmen:

18.1 Datenschutz-Management

18.2 Regelmäßige Schulung der Beschäftigten.

18.3 Der Auftragsverarbeiter setzt einen Kernbestand an langjährig und dauerhaft beschäftigtem Technikerpersonal mit DV-technischer Erfahrung und Expertise ein.

- - -