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

1.1. **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	NETWAYS GmbH Deutschherrnstr. 15-19 90429 Nürnberg	Unter Auftragsverarbeiter 3,4,5	Cloud-Infrastruktur (Kubernetes) für die Online-Plattform für ovis2020	
2	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen	Deutschland	Hostinginfrastruktur (Strom, Uplink, Housing, Sicherheit)	ISO27001
3	noris network AG Thomas-Mann-Straße 16 - 20 90471 Nürnberg	Deutschland	Hostinginfrastruktur (Strom, Uplink, Housing, Sicherheit)	ISO27001
4	Core-Backbone GmbH Hans-Sachs-Str. 14 93138 Lappersdorf	Deutschland	Uplink Bereitstellung	

2. General-Genehmigungen

Der Auftragnehmer darf für Hosting-Leistungen Unter-Auftragsverarbeiter mit Sitz und Serverstandort im Europäischen Wirtschaftsraum einsetzen. Zusätzlich muss vilisto beim Einsatz von Rechenzentrumsbetreibern als Unter-Auftragsverarbeiter sicherstellen, dass diese nach ISO27001 zertifiziert sind.

Technische und organisatorische Maßnahmen zur Datensicherheit (ovis2020)

gemäß Art. 32 DSGVO (als Auftragsverarbeiter)

Inhaltsverzeichnis

1. Gegenstand

Dieses Dokument beschreibt die durch die vilisto GmbH (nachfolgend „**vilisto**“ oder „**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 für **ovis2020**
  - zur Entgegennahme, Speicherung und aufbereiteter Darstellung von Daten
  - zur Vornahme von Einstellungen für die Heizungssteuerung
  - zur Bereitstellung begleitender Funktionalitäten gemäß Hauptvertrag.
- Sie beziehen sich ausdrücklich nicht auf die Bereitstellung der Online-Plattform für ovis2017

2. Unterauftragsverarbeiter

Das Unternehmen nutzt den Unter- Auftragsverarbeiter Netways GmbH und deren Unter-Auftragsverarbeiter. Die Technischen und Organisatorischen Maßnahmen des Unterauftragnehmers und seiner Unterauftragnehmer sind in eigenen Dokumenten erläutert. Diese sind als **Anhänge A1-A4** diesem Dokument angehängt. Die aufgeführten Unterauftragsverarbeiter werden gemeinsam als die **Unter-Auftragsverarbeiter** bezeichnet. Die dazugehörigen Anhänge gemeinsam „**Anhänge A**“

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

3.1 Datenspeicherung und Verarbeitung

Die Daten der Online-Plattform werden ausschließlich in den Rechenzentren auf den Servern der Unter-Auftragsverarbeiter gespeichert. Auf Computern von vilisto erfolgt nur der Zugriff auf die Daten zum zwecke der Wartung, Fehlerbehebung, Einsparanalyse oder anderen im Hauptvertrag definierten Zwecken. Dieser Zugriff erfolgt in der Regel über das Browser-basierte Dashboard, kann jedoch auch über andere Zugänge zur Online-Plattform erfolgen. Diese Zugriffe sind gemäß 3.3 gesichert. Auf Servern oder Computern von vilisto werden **keine** personenbezogenen Daten dauerhaft gespeichert.

3.2 Zutrittskontrolle

Da vilisto keine personenbezogenen Daten auf eigenen Servern lagert, gibt es keine Hardware, zu der der Zutritt geregelt werden muss. Für die Server gelten insbesondere die TOMs der Unterauftragnehmer Hetzner Online GmbH und noris network AG.

3.3 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*e Mitarbeiter*in aus dem eingeschränkten Personenkreis ausscheiden, wird das Zugriffspasswort zur KeePass Datei umgehend geändert. Dieser Vorgang wird schriftlich festgehalten.
Zusätzlich haben Mitarbeitenden der Unter-Auftragnehmer entsprechend ihrer TOMs Zugriff auf die Daten in den zugrunde liegenden Serverstrukturen.

b) Zugang über die Online-Plattform durch vilisto

Alle anderen Mitarbeitenden 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 Mitarbeitende verwenden für den Zugriff ihre Domänenzugangsdaten. Die Mitarbeitenden des Unternehmens sind angewiesen die Kundendaten als vertraulich zu behandeln. Die Mitarbeitenden des Unternehmens sind angewiesen bei Abwesenheit ihre Computer zu sperren, sodass Besuchende oder Mitarbeitende ohne Berechtigungen nicht zufällig Zugang erhalten. Nach 10 Minuten ohne Benutzung werden die Mitarbeitenden 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. Die Kundenkontos sind über Authentifizierungen mittels Benutzerkennung und Passwort geschützt. Für den sorgfältigen Umgang mit seinem Zugang zur Online-Plattform und mit weiteren Zugängen trägt der Kunde selbst die Verantwortung.

3.4 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) Zugehörigkeit zu einem Kunden

b) Rollen und Berechtigungen

Es sind folgende Rollen vorgesehen, die bestimmte Rechte haben:

*(1) vilisto Administrator*in (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, Erstellen von Kundenaccounts.

*(3) vilisto Entwickler*in*

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

In der Online-Plattform gibt es keine Möglichkeit Daten zu modifizieren. Lediglich das Ändern von Einstellungen ist möglich. Eine Löschung der Daten kann durch den Kunden beauftragt werden.

d) Überprüfung bei vilisto

vilisto überprüft mindestens alle 3 Monate, ob allen ihren Mitarbeitenden 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.

3.5 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 Administrator*innen oder vilisto Support-Konten erfolgen.

c) Entwickler*innen 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*innen nur auf Daten der von den Kunden für Entwickler*innen freigegebenen Thermostate bzw. Test-Thermostate Zugriff.

Entwickler*innen haben dabei immer ausschließlich Zugriff auf die pseudonymisierten Daten (nach 3.7).

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

a) Transportverschlüsselung bei der Sammlung der Daten:
   - Die Daten der Thermostate werden von den Thermostaten bis zum Server mittels DTLS Ende-zu-Ende verschlüsselt. Es wird dabei die DTLS-Cipher-Suite ECDHE-ECDSA-AES128-CCM verwendet.
   - Zusätzlich sind die Daten bei der Übertragung vom Gateway zum Server mittels TLS 1.2 oder neuer verschlüsselt.
   - Die Certification Authority (CA) für die Zertifikate für die Server, die für den Aufbau der gesicherten Verbindung mit Thermostaten notwendig sind, liegt ausschließlich gesichert bei vilisto. Zertifikate werden gesichert auf die Server übertragen und haben eine Gültigkeit von höchstens einem Jahr.
   - Die Certification Authority (CA) für Herstellung von Zertifikaten für Thermostate und Gateways liegt gesichert bei den Produzenten und bei vilisto. Diese Zertifikate sind aber nicht geeignet, um Daten von Thermostaten zu empfangen.

b) Transportverschlüsselung bei der Anzeige der Online-Plattform:

   Die Daten, die über die Online-Plattform angezeigt werden, werden über HTTPS zum Web-Browser der*s Nutzer*in übertragen und sind mittels TLS 1.2 oder neuer verschlüsselt.

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

Die Daten werden in der vilisto Online-Plattform pseudonymisiert gespeichert und verarbeitet. Dazu erhält jedes Thermostat eine zufällig generierte Pseudo-Id. Für jegliche interne Verarbeitung, zur Regelung, Präsenzerkennung oder Speicherung der Daten auf dem Server wird ausschließlich die Pseudo-Id verwendet.
Die echte Thermostat-Id wird lediglich während der Thermostat-Server-Kommunikation und zur Anzeige im Dashboard verwendet. Identifizierende Informationen wie Raumnamen, oder Kommentare werden mit der Thermostat-Id gespeichert. Die Zuordnung von Thermostat-Id und Pseudo-Id erfolgt in einer von den restlichen Informationen getrennten Datenbank. Für weitere Ids, wie Raum-Ids und Stockwerk-Ids, wird die gleiche Art der Pseudonymisierung verwendet.

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

4.1 Eingabekontrolle

Das System erlaubt es nicht personenbezogene Daten einzugeben oder zu ändern. Alle personenbezogenen Daten werden durch die Thermostate gesammelt. Für die Änderung von Einstellungen und Metainformationen zu den Thermostaten (bspw. Standort und Raumnamen) gelten die beschriebenen Zugangskontrollen und Protokollierungsmaßnahmen.

4.2 Weitergabekontrolle

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

5. Wiederherstellbarkeit

Das System läuft in einem Kubernetes Cluster Hardware-unabhängig und wird bei Ausfall einzelner Hardwarekomponenten automatisch auf redundant vorhandener Hardware beim Unter-Auftragnehmer neu gestartet. Der Unter-Auftragnehmer speichert auch die Daten redundant in mindestens zwei Rechenzentren. Siehe auch die TOMs des Unterauftragnehmers.
Zusätzlich sichert vilisto die Daten regelmäßig wie folgt: Es werden regelmäßig, mindestens wöchentlich, Kopien der Datenbanklaufwerke erstellt, und beim Unter-Auftragnehmer auf einem Backuplaufwerk gesichert. Es werden mehrere alte Kopien der Datenträger vorgehalten.

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

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

7. Dokumenten-Historie

Version	Datum	Bearbeiter	Änderung
1.0	04.09.2019	Lasse Stehnken	Ersterstellung
2.0	3.12.2020	Lasse Stehnken	Änderungen für ovis2020
2.1	29.12.2020	Lasse Stehnken	Korrekturen + Clean

NETWAYS GmbH
Deutschherrnstr. 15-19
90429 Nürnberg

Tel.: +49 911 92885-0
Fax: +49 911 92885-77
E-Mail: info@netways.de
http://www.netways.de

Anlage der technischen und organisatorischen Maßnahmen (TOM)
i.S.d. Art. 32 DS-GVO

Gültig für die NETWAYS GmbH und ihren Töchtern
Stand vom 30.04.2018

In Verbindung mit dem Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO verpflichten sich die Vertragsparteien – der Verantwortliche und der Auftragsverarbeiter - in Ihrem jeweiligen Verfügungsbereich und bezogen auf den Vertragsgegenstand, gem. Art. 28 Abs. 3 lit. c DS-GVO 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, durch geeignete technische und organisatorische Maßnahmen ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Im Einzelnen handelt es sich hierbei um folgende Maßnahmen:

1. Vertraulichkeit gem. Art 32 Abs. 1 lit. b DS-GVO

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Der Zugang zu den Lokationen ist ausschließlich in Begleitung eines NETWAYS Mitarbeiters erlaubt und der Zutritt ist ausschließlich mit personalisierten Chipkarten, ggf. mit biometrischer Überprüfung oder elektronisches Codeschloss sowie durchgehender Kameraüberwachung möglich. Ein durchgehender Perimeterschutz ist durch Einfriedungsanlagen und Personal gewährleistet.

Einzelne Verarbeitungsanlagen (Racks) sind zusätzlich durch manuelle Schließsysteme gesichert welche mit Tresoren verwaltet werden. Entsprechende Schlüsselregelung inklusive Zugriffsbeschränkung sind implementiert.

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Sicherung von Server- und Clientsystemen erfolgt durch Login mit Benutzername und Passwort, Fernzugriff mindestens durch asymmetrische Verschlüsselungsverfahren für Konsolen- und VPN-Zugänge durchgeführt. Portzugriffe auf exponierte Dienste werden durch redundante Firewall-Systeme / Netzwerkgeräte eingeschränkt. Zentralverwaltete Benutzerberechtigungen, Richtliniensystem für die Einhaltung des Datenschutzes, Passwortvergaberichtlinie, arbeitsrechtliche Geheimhaltungsvereinbarungen und Konsolenunterweisung sind implementiert.

NETWAYS GmbH
Deutschherrnstr. 15-19
90429 Nürnberg
Tel.: +49 911 92885-0
Fax: +49 911 92885-77
E-Mail: info@netways.de
http://www.netways.de

1.3 Zugriffskontrolle

Es ist Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Verschlüsselungsqualität und Sicherheitsprotokolle werden nach der Möglichkeit des Auftraggebers implementiert. Grundsätzlich sind Server bzw. allgemein Netzwerkdienste aus dem Internet nicht erreichbar.

Die Anzahl der Administratoren sind auf ein Minimum beschränkt und Benutzerprofile durch ein zentrales Berechtigungssystem verwaltet. Änderungen können durch revisionssichere Snapshots des Festplattenspeichers, ein zentrales Log- oder Konfigurationsmanagement System nachvollzogen werden.

Token- und VPN Zugangssysteme werden durch Tresor- und Zugriffsregellungen geschützt. Vernichtung und Löschung gemäß DIN 66399 und DIN 32757 in den Sicherheitsstufen P5 und T4 auf Wunsch des Auftraggebers. Löschkonzept auf Anfrage einsehbar.

1.4 Trennungskontrolle

Es ist Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Werden Konfigurations-Management oder virtuelle Ressourcen des Auftragnehmers in Anspruch genommen, so sind diese einer Funktionstrennung unterzogen und durchlaufen Test- und Produktionsphase.

Vom Auftragnehmer werden für die Speicherung der Daten nur eigene, physische Möglichkeiten zur Verfügung gestellt. Die logische Trennung der Daten liegt in der Verantwortung des Auftraggebers.

1.5 Pseudonymisierung (Art. 32. Abs. 1 lit. a DS-GVO)

„Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen.

Eine Pseudonymisierung erfolgt auf Weisung des Auftraggebers entsprechend der Weitergabekontrolle (2.1) oder ggf. im Rahmen einer Sicherung (Privacy by Design). Interne Richtlinien, personenbezogene Daten im Falle einer Weitergabe zu anonymisieren / pseudonymisieren sind implementiert.

NETWAYS GmbH
Deutschherrnstr. 15-19
90429 Nürnberg
Tel.: +49 911 92885-0
Fax: +49 911 92885-77
E-Mail: info@netways.de
http://www.netways.de

2. Integrität gem. Art 32 Abs. 1 lit. b DS-GVO

2.1 Weitergabekontrolle

Es ist Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Der Auftraggeber bekommt eine dedizierte, verschlüsselte Zugriffsmöglichkeit für seine Umgebung welche ggf. in einem eigenständigen VLAN betrieben wird.

Für einmaligen Transport oder Support werden verschlüsselte Verbindungen bereitbestellt, z.B. HTTPS oder SFTP. Eine Speicherung auf Datenträger für den Transport wird nur auf ausdrücklichen Wunsch des Auftraggebers vorgenommen und kann nur durch persönliche Übergabe geschehen. Jeder außerordentliche Transport wird vorher durch den Auftraggeber angeordnet und entsprechend dokumentiert. Weiterhin können ggf. Verschlüsselung und Pseudonymisierung vereinbart werden.

2.2 Eingabekontrolle

Es ist Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Es werden von virtuellen Ressourcen, Serversystemen oder Containern revisionssichere Snapshots des Festplattenspeichers angelegt. Ggf. können Änderungen durch ein zentrales Log-Management System nachvollzogen werden. Änderungen und Eingaben werden durch den Auftraggeber eingestellt und entsprechend dokumentiert.

3. Verfügbarkeit und Belastbarkeit gem. Art 32 Abs. 1 lit. b DS-GVO

3.1 Verfügbarkeitskontrolle

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vermietete Server-Systeme des Auftraggebers sind mit redundanten Plattensubsystemen ausgestattet (Mindestanforderung RAID1) und ggf. mit einem Supportvertrag des Serverherstellers versehen. Die Stromversorgung ist redundant ausgelegt und durch USV / Generatoren gegenüber ausfällen des EVU geschützt.

Der Auftragnehmer betreibt ein Datensicherungssystem welches ggf. durch den Auftragnehmer genutzt werden kann. Die Sicherung wird standardmäßig einmal am Tag durchgeführt, wobei einmal pro Woche eine Vollsicherung, an den verbleibenden Tagen eine differentielle Sicherung durchgeführt wird. Das Datensicherungssystem wird als verteiltes System ggf. über zwei Standorte betrieben und einer regelmäßigen Überprüfung unterzogen.

NETWAYS GmbH
Deutschherrnstr. 15-19
90429 Nürnberg
Tel.: +49 911 92885-0
Fax: +49 911 92885-77
E-Mail: info@netways.de
http://www.netways.de

Virtuelle Server Systeme und Container werden ggf. per revisionssichere Snapshots des Festplattenspeichers auf das oben beschriebene System gesichert. Die Aufbewahrungszeit beträgt 7 Tage.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DS-GVO und Art. 25 Abs. 1 DS-GVO

4.1 Datenschutz-Management

Gewährleistung der Nachhaltigkeit des Datenschutzes.

Dokumentation des Datenschutzes vorhanden mit Zugriffsmöglichkeiten für Mitarbeiter nach Bedarf. Regelmäßige Überprüfung der Wirksamkeit erforderlicher Schutzmaßnahmen wird durchgeführt. Die Mitarbeiter sind geschult auf Vertraulichkeit und sind dem Datengeheimnis verpflichtet.

Der Auftragnehmer kommt den Informationspflichten nach Art. 13 und 14 DS-GVO nach. Interner Datenschutzbeauftragter im Unternehmen:

datenschutz@netways.de

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Der Auftragnehmer setzt Firewall-, Netzwerk und Spamfiltersysteme in redundanter Form für Umgebungen des Auftragnehmers ein. Die Funktionsweise wird durch regelmäßige Kontrolle und Wartung sichergestellt. Projekte und Umgebungen des Auftraggebers werden dokumentiert und der aktuelle Verlauf oder allgemeine Informationen in einem Ticketsystem protokolliert. Sicherheitsvorfälle werden dokumentiert und ein DSB mit einbezogen.

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

Privacy by design / Privacy by default

Es werden nicht mehr personenbezogene Daten erhoben, bearbeitet oder verwendet als für den jeweiligen Zweck erforderlich. Eine einfache Ausübung des Wiederrufrechts des Betroffenen ist möglich.

NETWAYS GmbH
Deutschherrnstr. 15-19
90429 Nürnberg

Tel.: +49 911 92885-0
Fax: +49 911 92885-77
E-Mail: info@netways.de

http://www.netways.de

4.4 Auftragskontrolle

Es ist eine weisungsgemäße Auftragsverarbeitung zu gewährleisten.

Alle Weisungen des Auftraggebers erfolgen schriftlich per E-Mail an unser Ticketsystem, wodurch eine lückenlose Nachvollziehbarkeit gewährleistet ist. Mündliche Absprachen werden im Ticketsystem protokolliert und dem Auftraggeber zur Kontrolle übersendet. Arbeitsanweisung werden durch Mitarbeiter des Auftragnehmers einer Plausibilitätsprüfung unterzogen. Die Mitarbeiter unterliegen einer Geheimhaltungsvereinbarung. Alle Prozesse werden von den jeweiligen Abteilungsleitern und der Geschäftsführung regelmäßig überprüft und bewertet.

Der Auftragnehmer gewährleistet zu jederzeit eine einfache Wahrnehmung der Kontrollrechte des Auftraggebers um das Schutzniveau regelmäßig zu überprüfen.

Es werden grundsätzlich keine weiteren Subunternehmer beauftragt, sofern nicht auf ausdrücklichen Wunsch des Auftraggebers.

Nach Beendigung des Vertrages werden alle Daten des Auftraggebers übergeben oder gelöscht. Ein Löschkonzept kann auf Anfrage eingesehen werden.

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

- **Zutrittskonstrolle**
  - **Datacenter-Parks in Nürnberg, Falkenstein und Helsinki**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenter-Park
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters
  - **Verwaltung**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen
- **Zugangskontrolle**
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem

Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.

- für Managed Server, Webhosting und Storage Share
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert

- **Zugriffskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
    - für Managed Server, Webhosting und Storage Share
        - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
        - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.
- **Datenträgerkontrolle**
    - **Datacenter-Parks in Nürnberg, Falkenstein und Helsinki**
        - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
        - Defekte Festplatten, die nicht sicher gelöscht werden können,

werden direkt im Rechenzentrum (Falkenstein) zerstört (geschreddert).

- **Trennungskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
  - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Trennungskontrolle obliegt dem Auftraggeber.
  - für Managed Server, Webhosting und Storage Share
    - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
    - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- **Pseudonymisierung**
  - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
  - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
  - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
  - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.
- **Eingabekontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

- für Dedicated Server, Colocation Server, Cloud Server und Storage Box
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
- für Managed Server, Webhosting und Storage Share
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
        - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
        - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
        - Monitoring aller relevanten Server.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - für Dedicated Server, Colocation Server, Cloud Server und Storage Box
        - Datensicherung obliegt dem Auftraggeber.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - Für Managed Server, Webhosting und Storage Share
        - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
        - Einsatz von Festplattenspiegelung.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Einsatz von Softwarefirewall und Portreglementierungen.

- Dauerhaft aktiver DdoS-Schutz.

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

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

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- **Auftragskontrolle**
  - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
  - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
  - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

Anlage 1: Technische und organisatorische Maßnahmen

Im Rahmen der Leistungen der noris network AG 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, verzeichnet[2] dieser Anhang die von der noris network AG getroffenen angemessenen technischen und organisatorischen Maßnahmen, die sich aus der im Leistungsvertrag in seinen Einzelheiten beschriebenen Datenverarbeitung ergeben, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten.

Vertraulichkeit

- Zutrittskontrolle gemäß ISO/IEC 27001 A.11
- Zugangskontrolle/Zugriffskontrolle gemäß ISO/IEC 27001 A.9
- Trennungskontrolle gemäß ISO/IEC 27001 A.6.1.2
- Pseudonymisierung liegt im Verantwortungsbereich des Auftraggebers (Je nach Vorgabe des Applikations-Designs)

Integrität

- Weitergabekontrolle liegt im Verantwortungsbereich des Auftraggebers (Je nach Vorgabe des Applikations-Designs)
- Eingabekontrolle liegt im Verantwortungsbereich des Auftraggebers (Je nach Vorgabe des Applikations-Designs)

Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle gemäß ISO/IEC 27001 A.17 und A.12.1.3

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management (Anlage 2) gemäß ISO/IEC 27001 A.18.1.4
- Incident-Response-Management gemäß ISO/IEC 27001 A.16
- Datenschutzfreundliche Voreinstellungen ("privacy by design") liegt im Verantwortungsbereich des Auftraggebers (Je nach Vorgabe des Applikations-Designs)
- Auftragskontrolle gemäß ISO/IEC 27001 A.12.1.1 und A.12.1.2.

[2] Für eine detaillierte Beschreibung aller vom Auftragnehmer getroffenen Maßnahmen s. **Anlage: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO, § 64 BDSG (neu) der noris network AG.**

Anlage 2: Datenschutz-Management-System

Das Datenschutzmanagement ist in das Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001 eingebettet. Das Management ist hierbei auf die Anforderungen aus A.18.1.4 („Privatsphäre und Schutz von personenbezogener Information") abgestimmt. Es kommen die Maßgaben aus den Anweisungen („Policies"), Verfahren („SOPs") und detaillierten Dokumentationen zur Anwendung, nach Rollen und Verantwortlichkeiten gemäß Organigramm mit entsprechenden Verantwortlichkeiten und Befugnissen in der Organisation. Darüber hinaus entsprechender Planung mit Maßnahmen zum Umgang mit Chancen/Risiken und die Ausstattung mit angemessenen Ressourcen, Kompetenzen, Awareness und Kommunikation. Die Überwachung, Messung, Analyse und Bewertung, zusammen mit internen Audits und Managementbewertungen finden zur fortlaufenden Verbesserung des Managementsystems kontinuierlich statt. Den Rahmen bei diesen Vorgehensweisen bildet das Integrierte Managementsystem des Auftragnehmers.

Anlage 3: Unterauftragnehmer (Subunternehmer)

ARNDT – Sicherheit und Service GmbH & Co. KG

Industriestraße 42, D-90765 Fürth

Objektschutz durch Schutz-/Sicherheitskräfte gemäß § 34a GewO

Core-Backbone GmbH · Hans-Sachs-Str. 14 · 93138 Lappersdorf

CORE BACKBONE

KEINE KOMPROMISSE. EINFACH ZUVERLÄSSIG.

Lappersdorf, 19.04.2018

Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO: Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung Art der Daten

Gegenstand der Zusatzvereinbarung sind folgende Datenarten und -Kategorien:

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Protokolldaten

Kreis der Betroffenen

Der Kreis der durch diese Zusatzvereinbarung Betroffenen umfasst:

- Kunden und Interessenten des Auftraggebers
- Mitarbeiter und Lieferanten des Auftraggebers

ANSCHRIFT
Core-Backbone GmbH
Hans-Sachs-Str. 14
93138 Lappersdorf
Deutschland

KONTAKT
Tel.: +49 (0)911-310432-00
Fax: +49 (0)911-310432-99
info@core-backbone.com
www.core-backbone.com

BANKVERBINDUNG
Raiffeisenbank
Regensburg eG
BIC/SWIFT: GENO DEF1 R02
IBAN:DE55 7506 0150 0000 1609 70

UNTERNEHMEN
GF: Daniel Maresch
Registergericht: Regensburg
Registernummer: HRB 10189
USt-IdNr.: DE249028038

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

1. Zutrittskontrolle
    a. elektronisches Zutrittskontrollsystem mit Protokollierung
    b. dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für sein Colocation Rack)
    c. Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    d. Videoüberwachung der Serverräume des Rechenzentrums
2. Zugangskontrolle
    a. bei „Rootserver" und „Colocation" Aufträgen durch Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind.
3. Zugriffskontrolle
    a. bei internen Verwaltungssysteme des Auftragnehmers
        i. Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    b. bei „Rootserver" und „Colocation" Aufträgen
        i. Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
4. Datenträgerkontrolle
    a. Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
    b. Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt zerstört.
5. Weitergabekontrolle
    a. Alle Mitarbeiter sind auf das Datengeheimnis i.S.d. Art. 32 Abs.4 DS-GVO verpflichtet.
    b. Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

ANSCHRIFT
Core-Backbone GmbH
Hans-Sachs-Str. 14
93138 Lappersdorf
Deutschland

KONTAKT
Tel.: +49 (0)911-310432-00
Fax: +49 (0)911-310432-99
info@core-backbone.com
www.core-backbone.com

BANKVERBINDUNG
Raiffeisenbank
Regensburg eG
BIC/SWIFT: GENO DEF1 R02
IBAN:DE55 7506 0150 0000 1609 70

UNTERNEHMEN
GF: Daniel Maresch
Registergericht: Regensburg
Registernummer: HRB 10189
USt-IdNr.: DE249028038

6. Eingabekontrolle
    a. bei internen Verwaltungssysteme des Auftragnehmers
        i. Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
        ii. Änderungen der Daten werden protokolliert.
    b. bei „Rootserver" und „Colocation" Aufträgen
        i. Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
7. Auftragskontrolle
    a. Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
    b. Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
8. Verfügbarkeitskontrolle
    a. bei internen Verwaltungssysteme des Auftragnehmers
        i. Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
        ii. Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
        iii. Einsatz von Festplattenspiegelung bei allen relevanten Servern.
        iv. Einsatz unterbrechungsfreier Stromversorgung.
    b. bei „Rootserver" und „Colocation" Aufträgen
        i. Datensicherung obliegt dem Auftraggeber.
        ii. Einsatz unterbrechungsfreier Stromversorgung.
9. Maßnahmen zur Datensicherung (physikalisch/logisch)
    a. bei internen Verwaltungssysteme des Auftragnehmers
        i. Die Datensicherung erfolgt auf logisch und/oder physikalisch getrennten Systemen.
    b. bei „Rootserver" und „Colocation" Aufträgen
        i. Die Trennungskontrolle obliegt dem Auftraggeber.