Vereinbarung

zwischen

_____ **(Unternehmensname)**

_____ (Straße und Hausnummer)

_____ **(PLZ und Ort)**

- nachfolgend Auftraggeber genannt -

und

kantiko GmbH
Am Kiebitzberg 15
14532 Kleinmachnow
- nachfolgend Auftragnehmer genannt –
- gemeinsam auch „Parteien“ -

über

die Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Präambel

Zwischen den Parteien besteht ein Auftragsverhältnis. Der Auftraggeber hat die Leistungen des Produktes kontool vom Auftragnehmer am _____ (Datum) beauftragt.

Diese Vereinbarung und ihre Anlagen konkretisieren die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus einer Auftragsdatenverarbeitung des Auftragnehmers für den Auftraggeber ergeben. Des Weiteren regelt sie die Mindestanforderungen zum Datenschutz und zur IT-Sicherheit, die durch den Auftragnehmer anzuwenden sind. Sie findet Anwendung auf alle Tätigkeiten, die mit einer Auftragsdatenverarbeitung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen oder sonstigen Daten des Auftraggebers in Berührung kommen können.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Auftragsverhältnisses, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

§ 1 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Finanzdaten des Kunden, die auf die Server von kontool übertragen und für ein webbasiertes Berichts- und Planungswesen gespeichert und aufbereitet werden. Hierbei werden lediglich Summen- und Salden aus der Buchhaltungssoftware übertragen.
Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber jederzeit auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Herausgabe oder Löschung der Daten verlangen.

(3) Der Auftragnehmer erhält keine Zugriffsrechte zu den elektronischen Systemen und den Daten des Auftraggebers. Gleichwohl ist dem Auftragnehmer die Überprüfung der IT-Systeme des Auftraggebers für Kontroll- und Wartungszwecke in Notfällen sowie für beauftragte Aufgaben möglich.

§ 2 Leistungsgegenstand, Art, Zweck, Umfang, Art der Daten, Betroffene

(1) Die einzelnen Tätigkeiten und die Dauer des Auftrages sind im o.g. Vertrag konkretisiert.
Gegenstand der Vereinbarung:

a) Verarbeitung von Geschäftszahlen, Finanz- und Buchhaltungsdaten zur Aufbereitung statistischer Auswertungen auf der Onlineplattform des Auftraggebers.

(2) Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:

a) Der Auftragnehmer erhält keine Zugriffsrechte auf die Daten, die auf der untergebrachten Hardware des Auftragnehmers liegen. Eine Verarbeitung von Metadaten für ausschließlich administrative Zwecke ist möglich.

(3) Art der Daten:

a) Elektronisch gespeicherte Daten des Auftraggebers.
Bei der Art und Kategorien der gespeicherten Daten handelt es sich im Wesentlichen um Geschäftszahlen, Finanz- und Buchhaltungsdaten.

(4) Kreis der Betroffenen:

a) Der Kreis der Betroffenen sind die Kunden des Auftraggebers sowie die in den Finanzdaten und buchhalterischen Informationen bzw. Auswertungen enthaltenen Kreditoren und Debitoren. Diese sind dem Auftragnehmer nicht bekannt.

Finanzdaten und buchhalterische Informationen und Auswertungen des Auftraggebers Der Kreis der Betroffenen, Kunden, Kreditoren, Debitoren auf ist dem Auftragnehmer nicht bekannt

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für ihn einschlägigen Datenschutzgesetze verantwortlich. Er darf die zur Auftragsdurchführung erforderlichen Daten ausschließlich nach der Weisung des Auftraggebers erheben, verarbeiten oder nutzen, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Weisungen des Auftraggebers bedürfen der Schriftform. Mündlich erteilte Weisungen sind zumindest per E-Mail zu bestätigen/dokumentieren. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.
Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Für die dadurch entstehenden Aufwände wird die Vergütungsregelung nach §10 angewendet.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Für alle nicht im Vertrag vereinbarten Aufwände und Einzelbeauftragungen wird die Vergütungsregelung nach §10 angewendet.
In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart. (Anmerkung: Im Vertrag können die Parteien hierzu eine Vergütungsregelung treffen.)

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Für die dadurch entstehenden Aufwände wird die Vergütungsregelung nach §10 angewendet.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber

beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung gemäß §10 verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Datenlöschung

(1) Überlassene Dokumente und Datenträger sowie Kopien derselben sind grundsätzlich nach Beendigung des Auftrags zurückzugeben. Der Auftraggeber kann auch vorher jederzeit die Herausgabe verlangen. Der Auftraggeber kann auch die Löschung bzw. Vernichtung von Dokumenten und Datenträgern sowie Kopien derselben verlangen.
(2) Soweit Daten vom Auftragnehmer berichtigt, gelöscht oder gesperrt werden sollen, erfolgt dies ausschließlich auf Weisung des Auftraggebers. Die Vorgänge sind mit Angabe von Datum und durchführender Person zu protokollieren. Die Protokolle sind dem Auftraggeber auf Verlangen zur Verfügung zu stellen.
(3) Erfolgt eine Datenlöschung beim Auftragnehmer hat der Auftragnehmer sämtliche löschbaren elektronischen Datenträger, die Daten des Auftraggebers enthalten, datenschutzgerecht und nicht wieder herstellbar zu löschen.

§ 8 Kontrollrecht

(1) Der Auftraggeber kann sich nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten - zu den üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs - von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

§ 9 Unterauftragnehmer

1) Der Auftraggeber stimmt hiermit zu, dass der Auftragnehmer Unterauftragnehmer hinzuziehen darf, die in der Liste der zugelassene Unterauftragnehmer (siehe Anlage 2) aufgeführt sind.

(2) Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

§10 Vergütungsregelung

(1) Entstehen dem Auftragnehmer bei der Unterstützung des Auftraggebers im Hinblick auf Datenschutzfragen Aufwände, sind diese dem Auftraggeber in Rechnung zu stellen. Dazu wird ein Stundensatz von 150,00 Euro zzgl. MwSt. festgelegt.

§11 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es

sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

(5) Gerichtsstand ist Potsdam.

§12 Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung. Es wird darüber hinaus eine Haftungshöchstgrenze von 30.000,00 Euro vereinbart.

Auftraggeber	Auftragnehmer
Ort, Datum _____	Ort, Datum _____
_____	_____
Unterschrift	Unterschrift

Anlagen:
Anlage 1: Technische und organisatorische Maßnahmen (TOM)
Anlage 2: Verantwortliche Ansprechpartner
Anlage 3: Zugelassene Unterauftragnehmer

Anlage 1 Technische und organisatorische Maßnahmen

gemäß Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g) und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d) für den oben genannten Auftragnehmer.

Die nachstehenden Angaben beziehen sich auf die:

kantiko GmbH

Am Kiebitzberg 15

14532 Kleinmachnow

- Auftragnehmer -

Die Firma kantiko GmbH betreibt keine eigenen Server sondern hat die Datenhaltung- und -verarbeitung an ein externes TÜV-zertifiziertes Rechenzentrum mit Datenhaltung in Deutschland ausgelagert.

Bei dem Rechenzentrum handelt es sich um:

STRATO AG

Pascalstraße 10

10587 Berlin

- Rechenzentrum -

Der Auftragnehmer hat mit dem Rechenzentrum eine separate Vereinbarung zur Auftragsdatenverarbeitung nach Art 28. Abs. 3 geschlossen.
Darin werden folgende Maßnahmen aufgeführt:

Anlage – technisch-organisatorische Maßnahmen (TOM)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
1.1 Zutrittskontrolle
Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.

- Festlegung von Sicherheitsbereichen
- Realisierung eines wirksamen Zutrittsschutzes
- Protokollierung des Zutritts
- Festlegung Zutrittsberechtigter Personen
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Begleitung von Fremdpersonal
- Überwachung der Räume

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

- Festlegung des Schutzbedarfs
- Zugangsschutz
- Umsetzung sicherer Zugangsverfahren, starke Authentisierung
- Umsetzung einfacher Authentisierung per Username Passwort
- Protokollierung des Zugangs

- Monitoring bei kritischen IT-Systemen
- Gesicherte (verschlüsselte) Obertragung von Authentisierungsgeheimnissen
- Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
- Festlegung befugter Personen
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Automatische Zugangssperre und Manuelle Zugangssperre

1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen

1.4 Verwendungszweckkontrolle

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

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze
- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Test- und Entwicklungsumgebung

1.5 datenschutzfreundliche Voreinstellungen

Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

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

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, Kopie 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.

- Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Protokollierung von Übermittlungen gemäß Protokollierungskonzept
- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Wartung der Backendsysteme
- Beschreibung der Schnittstellen

- Umsetzung einer Maschine-Maschine-Authentisierung
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Einführung eines Prozesses zur Datenträgerverwaltungen
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery

3.1 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Brandschutz
- Redundanz der Primartechnik
- Redundanz der Stromversorgung
- Redundanz der Kommunikationsverbindungen
- Monitoring
- Ressourcenplanung und Bereitstellung
- Abwehr von systembelastendem Missbrauch
- Datensicherungskonzepte und Umsetzung
- Regelmäßige Prüfung der Notfalleinrichtungen

3.2 Desaster Recovery - Rasche Wiederherstellung nach Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Melde- und Freigabeprozess
- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung
- Beachtung von Funktionstrennung und –zuordnung
- Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragnehmer nach geeigneten Garantien
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit STRATO

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Informationssicherheitsmanagement nach ISO 27001
- Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen

- Prozess Sicherheitsvorfall-Management
- Durchführung von technischen Überprüfungen

Anlage 2 zur Vereinbarung nach Art. 4 Nr. 7 DS-GVO

Liste der Ansprechpartner/Verantwortlichen

Verantwortliche und weisungsberechtigte Personen des Auftraggebers und Auftragnehmers.

Auftraggeber

Weisungsberechtigte Funktionen	**Name**	**E-Mail**	**Tel.**

Sonstige Funktionen	**Name**	**E-Mail**	**Tel.**

Auftragnehmer

Weisungsempfänger	**Name**	**E-Mail**	**Tel.**
Geschäftsführer	Stefan Jürgens	juergens@kantiko.com	+49 (0) 30 83212 360
Geschäftsführer	Benjamin Panke	panke@kantiko.com	+49 (0) 30 83212 360
Geschäftsführer	Mirko Behnken	behnken@kantiko.com	+49 (0) 30 83212 360

Sonstige Funktionen	**Name**	**E-Mail**	**Tel.**
Datenschutzbeauftragter	Mirko Behnken	behnken@kantiko.com	+49 (0) 30 83212 360
Leiter Entwicklung	Lukas Possegger	possegger@kantiko.com	+49 (0) 30 83212 360

Anlage 3 zur Vereinbarung nach Art. 28 Abs. 2-4 DS-GVO

Liste der zugelassenen Unterauftragnehmer

Nachstehend aufgeführte Unterauftragnehmer übernehmen für den Auftragnehmer Teilaufgaben des Auftrags.

Nr.	Firma, Adresse	Aufgabe	Ansprechpartner, Weisungsempfänger, Datenschutzbeauftragter	Kontaktdaten
1	STRATO AG Pascalstraße 10 10587 Berlin	Hosting Dienstleister, eine separate ADV i.S. Art. 28 DS-GVO liegt vor und kann auf Anforderung nachgewiesen werden.	Dr. Karin Dreher Datenschutzbeauftragte	Telefon: + 49 (0)30 - 886 15 3620 Telefax: + 49 (0)30 - 886 15 363 E-Mail: dreher@strato.de Website: http://www.strato.de/

Vor Aufnahme der Tätigkeit ist die schriftliche Zustimmung durch den Auftraggebers einzuholen.