Vertrag zur Auftragsverarbeitung mit Comcodix

zwischen dem / der

_____

_____

_____

- Auftraggeber, nachstehend Verantwortlicher genannt -

und Comcodix GmbH, Kasernenstr. 38, 42651 Solingen

- Auftragnehmer, nachstehend genannt COMCODIX - zusammen auch – die Parteien – genannt

1. **Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung**
   1.1. Der Gegenstand und die Dauer der Auftragsverarbeitung (nachfolgend: Auftrag) zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ergeben sich aus dem Hauptvertrag. Gegenstand des Auftrags ist nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch COMCODIX für den Verantwortlichen. Im Zuge der Leistungserbringung von COMCODIX als IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Serversystemen des Verantwortlichen, kann ein Zugriff auf personen- bezogene Daten im Webspace des Verantwortlichen jedoch nicht ausgeschlossen werden.
   1.2. Die Laufzeit dieses Auftrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses Auftrags nicht darüberhinausgehende Verpflichtungen ergeben.
   1.3. Art der Daten:
   Zum Zwecke der Vertragserfüllung des Hauptvertrages kann ein Zugriff von COMCODIX
   - beim Hosting von Server-Systemen und dort betrieben Anwendungen (Datenbank-, Backup-, Web-Server, SAN-Umgebung),
   - bei der technischen Administration der Server-Systeme, inklusive der Installation von Plugins oder Arbeiten an den Datenbanken, die auf dem Webspace des Verantwortlichen genutzt werden,
   - bei sonstigen Support-Tätigkeiten für sämtliche Server-Systeme (z.B. im Rahmen des proaktiven Monitorings),

- im Rahmen der Auswertung von Log-Files, auf alle Daten des Verantwortlichen und seiner Kunden, die der Verantwortliche innerhalb der Comcodix-Hosting-Instanz verarbeitet, nicht ausgeschlossen werden, z.B.:

    - Kommunikationsdaten (z.B. Telefon, E-Mail)
    - Vertragsstammdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
    - Kundendaten (z.B. Name, Geburtsdatum, Anschrift)
    - Mitarbeiterdaten (z.B. Name)
    - Vertragsabrechnungs- und Zahlungsdaten
    - Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
    - Alle sonstigen Daten, die der Verantwortliche in der Comcodix-Hosting-Umgebung verarbeitet. Kreis der Betroffenen:

1.4. Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen, umfasst alle Personen, deren Daten von dem Verantwortlichen mit der Comcodix-Hosting-Instanz verarbeitet werden, z.B.:

- Kunden
- Interessenten
- Beschäftigte (z.B. Arbeitnehmer, Bewerber)
- Lieferanten
- Handelsvertreter
- Ansprechpartner
- Alle sonstigen Personen, deren Daten von dem Verantwortlichen mittels der Comcodix-Umgebung verarbeitet werden.

1.5. COMCODIX hostet den Service Comcodix-Hosting in deutschen Rechenzentren der Firma Hetzner Online GmbH und Vautron Rechenzentrum AG (nachfolgend gemeinsam: SERVERANBIETER).

1.6. Die SERVERANBIETER organisieren die Sicherheit des jeweiligen Rechenzentrums selbst und werden diesbezüglich als Unterauftragsverarbeiter gemäß Ziffer 6 dieses Vertrags für COMCODIX tätig.

1.7. Hierfür wurde jeweils ein Vertrag zur Auftragsverarbeitung zwischen COMCODIX und den SERVERANBIETERN abgeschlossen. COMCODIX gewährleistet, dass dem Verantwortlichen die Rechte aus diesen Verträgen zur Auftragsverarbeitung mit den SERVERANBIETERN in gleichem Umfang zustehen. Im Fall widersprüchlicher Regelungen zwischen diesem Auftragsverarbeitungsvertrag und den Verträgen zur Auftragsverarbeitung mit den SERVERANBIETERN haben die vertraglichen Regeln aus diesem Auftragsverarbeitungsvertrag Vorrang.

1.8. Neben dem Comcodix-Hosting-Dienst findet eine Datenverarbeitung der betroffenen Daten am Standort von COMCODIX in Solingen nicht statt. Ein Zugriff durch COMCODIX auf die innerhalb von Comcodix-Hosting gespeicherten Daten ist nur mittels einer verschlüsselten Verbindung möglich. Details hierzu ergeben sich aus den technischen und organisatorischen Maßnahmen in Anlage 1 dieses Vertrages.

2. **Anwendungsbereich und Verantwortlichkeit, Haftungsfreistellung**
   2.1. COMCODIX verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen. Dies umfasst Tätigkeiten, die im Hauptvertrag und im Auftrag konkretisiert sind. Der Verantwortliche ist im Rahmen dieses Auftrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an COMCODIX sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO), soweit nicht das anwendbare Datenschutzrecht ausdrücklich eine eigenständige Verantwortlichkeit oder Haftung von COMCODIX vorsieht; für die Einhaltung solcher Bestimmungen bleibt COMCODIX (ggf. neben dem Verantwortlichen) verantwortlich.
   2.2. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in einem dokumentierten elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
   2.3. Soweit COMCODIX gemäß den Weisungen des Verantwortlichen handelt und die technischen und organisatorischen Maßnahmen und die sonstigen ihm durch diese Vereinbarung auferlegten Verpflichtungen beachtet, stellt der Verantwortliche COMCODIX auf erstes Anfordern von allen rechtlichen Ansprüchen, Schäden und Kosten frei, soweit diese dadurch entstehen, dass Dritte oder betroffene Personen aus der Datenverarbeitung resultierende Ansprüche gegen COMCODIX geltend machen. Hiervon umfasst sind insbesondere auch die Kosten der notwendigen Rechtsverteidigung einschließlich sämtlicher Gerichts- und Anwaltskosten in der jeweiligen gesetzlichen Höhe, sowie Bußgelder in tatsächlich festgesetzter Höhe in dem Umfang, in dem der Verantwortliche Anteil an der Verantwortung für den durch das Bußgeld sanktionierten Verstoß trägt. Gegenstand der Freistellung sind demnach insbesondere Ansprüche aufgrund von rechtswidrigen Weisungen des Verantwortlichen gemäß Art. 28 Abs. 3 S. 3 DSGVO sowie nicht ausreichender technisch-organisatorischer Maßnahmen, die gemäß Ziffer 3 dieser Vereinbarung vom Verantwortlichen freigegeben wurden. Dem Verantwortlichen bleibt im Nachgang vorbehalten, nachzuweisen, dass die gegen COMCODIX gerichteten, vorgenannten Ansprüche und Bußgelder nicht auf Weisungen oder Pflichtverletzungen des Verantwortlichen beruhen.

3. **Technisch-organisatorische Maßnahmen**
   3.1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und COMCODIX geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
   3.2. COMCODIX hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Der Verantwortliche hat die technischen und organisatorischen Maßnahmen zu prüfen und COMCODIX Änderungswünsche mitzuteilen. COMCODIX ist berechtigt, Änderungswünsche

abzulehnen und/oder unter den Vorbehalt der Kostenübernahme durch den Verantwortlichen zu stellen. Soweit die technischen und organisatorischen Maßnahmen gem. Anlage 1 von dem Verantwortlichen akzeptiert werden, werden diese ausschließliche Grundlage des Auftrages i.S.d. Ziffer 2.12.3. Soweit die Prüfung des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.3. Der Verantwortliche ist im Rahmen dieser Vereinbarung allein verantwortlich für die Beurteilung der Angemessenheit der technischen und organisatorischen Maßnahmen. COMCODIX setzt die vom Verantwortlichen geprüften Maßnahmen entsprechend dem gemäß Ziffer 3.2 dokumentierten Umfang um.

3.4. Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen, die den angemessenen Schutz der personenbezogenen Daten des Verantwortlichen sicherstellen sollen und die den Anforderungen der DSGVO (Art. 32) genügen. Diese Maßnahmen werden wie folgt festgelegt, sind entsprechend zu dokumentieren und dem Verantwortlichen vorzulegen: Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie die Einhaltung des Trennungsgebots. Darüber hinaus sind auch auftragsspezifische Maßnahmen umzusetzen, insbesondere im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand. Die Maßnahmen schließen unter anderem Folgendes ein: die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

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

3.6. Der Verantwortliche und COMCODIX unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4. **Anfragen Betroffener, Berichtigung, Sperrung und Löschung von Daten; Unterstützung durch COMCODIX**

4.1. COMCODIX hat nur nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an COMCODIX zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird COMCODIX dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten. Die Prüfung der Anfrage obliegt ausschließlich dem Verantwortlichen.

4.2. COMCODIX verpflichtet sich, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen in Ansehung der Art der Verarbeitung dabei zu unterstützen, seiner Pflicht zur Beantwortung von Antragen auf Wahrnehmung der in Kapitel III der Datenschutzgrundverordnung genannten Rechte der betroffenen Person nachzukommen.

4.3. Ist der Verantwortliche auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, oder ist der Verantwortliche zur Berichtigung, Löschung, Einschränkung der Verarbeitung oder zur Datenübertragung verpflichtet, wird COMCODIX den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung dieser Rechte nachzukommen.

4.4. Der Verantwortliche wird COMCODIX schriftlich oder in einem dokumentierten elektronischen Format zur Mitwirkung auffordern, sofern solche Mitwirkungshandlungen von COMCODIX erforderlich sind. Der Verantwortliche stellt COMCODIX auf erste Anforderung von den durch diese Unterstützung entstandenen Kosten frei, soweit COMCODIX dem Verantwortlichen vorab den Kostenrahmen schriftlich oder in Textform mitgeteilt hat.

4.5. COMCODIX wird keine Auskunftsverlangen oder anderweitige Anfragen bezüglich der Rechte Betroffener beantworten und den Betroffenen insoweit an den Verantwortlichen verweisen.

4.6. Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an COMCODIX, wird COMCODIX den Betroffenen an den Verantwortlichen verweisen.

4.7. Die Parteien werden für alle vorstehenden Tätigkeiten – soweit sie keiner gesetzlichen Verpflichtung entsprechen - ein angemessenes Entgelt vereinbaren, soweit erkennbar wird, dass hierfür der Aufwand von COMCODIX das übliche Maß überschreitet.

5. **Kontrollen und sonstige Pflichten von COMCODIX**

COMCODIX hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37 bis 39 DSGVO ausüben kann. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- COMCODIX gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet COMCODIX, 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.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 32 DSGVO.
- Unterstützung des Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der COMCODIX zur Verfügung stehenden Informationen bei

der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zur Sicherheit der Verarbeitung (z.B. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Durchführung einer Datenschutz-Folgenabschätzung oder der vorherigen Konsultation der Aufsichtsbehörde). COMCODIX wird diese unterstützenden Tätigkeiten – soweit sie keiner gesetzlichen Verpflichtung entsprechen – nur gegen ein angemessenes Entgelt durchführen. Die Parteien werden im Einzelfall ein entsprechendes Entgelt miteinander abstimmen.

- Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit die Datenverarbeitungsprozesse, die von COMCODIX für den Verantwortlichen ausgeführt werden, betroffen sind. Dies gilt auch, soweit eine zuständige Datenschutz-Aufsichtsbehörde bei COMCODIX ermittelt.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch COMCODIX im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen. Hierzu kann COMCODIX auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit z.B. i.S.d. Art. 40, 42 DSGVO vorlegen.
- Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Verantwortlichen sind nicht Gegenstand der von COMCODIX zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

6. **Unterauftragsverhältnisse**

6.1. Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten von COMCODIX Unterauftragsverarbeiter einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- Die Einschaltung von Unterauftragsverarbeitern ist grundsätzlich nur mit schriftlicher Zustimmung des Verantwortlichen gestattet. Ohne schriftliche Zustimmung kann COMCODIX zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragsverarbeiter mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Verantwortlichen vor Beginn der Verarbeitung oder Nutzung mitteilt und der Verantwortliche hierdurch die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
- COMCODIX hat die vertraglichen Vereinbarungen mit dem / den Unterauftragsverarbeiter/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen dem Verantwortlichen und COMCODIX entsprechen, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten

technischen und organisatorischen Maßnahmen so durchgeführt werden, dass sie den gesetzlichen Anforderungen des Datenschutzrechts entsprechen.

- Bei der Unterbeauftragung sind Kontroll- und Überprüfungsrechte des Verantwortlichen entsprechend dieser Vereinbarung beim Unterauftragsverarbeiter einzuräumen. Dies umfasst auch das Recht des Verantwortlichen, von COMCODIX auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

6.2. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die COMCODIX bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. COMCODIX ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

6.3. COMCODIX wird die nachfolgend aufgeführten Unterauftragsverarbeiter zur Erfüllung seiner vertraglich geschuldeten Leistungen einsetzen. Eine aktuelle Liste der Unterauftragsverarbeiter ist unter folgendem Link aufrufbar: https://comcodix.de/hosting/subunternehmer-comcodix-gmbh. Der Verantwortliche wird sich dort regelmäßig über Änderungen informieren.

7. **Kontrollrechte des Verantwortlichen**

7.1. Der Verantwortliche überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von COMCODIX und dokumentiert das Ergebnis.

- Hierfür kann er z.B. Auskünfte von COMCODIX einholen,
- sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen
- oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu COMCODIX steht.

7.2. COMCODIX verpflichtet sich, dem Verantwortlichen auf Anforderung in Textform innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen und Prüfungen – einschließlich Inspektionen - , die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen oder dazu beizutragen, die zur Durchführung einer Kontrolle erforderlich sind.

8. **Mitteilung bei Verstößen von COMCODIX**

8.1. COMCODIX unterrichtet den Verantwortlichen unverzüglich bei schwerwiegenden Verstößen von COMCODIX oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder die in diesem Vertrag getroffenen Festlegungen.

8.2. COMCODIX trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Verantwortlichen ab.
8.3. COMCODIX unterstützt den Verantwortlichen bei der Erfüllung der Informationspflichten nach Art. 33 DSGVO.

9. **Weisungsbefugnis des Verantwortlichen**

9.1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen in dem zu Grunde liegenden Vertrag und diesem Auftragsverarbeitungsvertrag und nach dokumentierter Weisung von dem Verantwortlichen. Der Verantwortliche behalt sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.
9.2. Auskünfte an Dritte darf COMCODIX nur nach vorheriger schriftlicher Zustimmung des Verantwortlichen erteilen.
9.3. Der Verantwortliche wird mündliche Weisungen unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. COMCODIX verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
9.4. Die vorstehenden Beschränkungen der Ziffern 9.1 bis 9.3 bezüglich der Verarbeitung personenbezogener Daten gelten nur, sofern COMCODIX nicht durch das Recht der Union oder der Mitgliedstaaten, dem COMCODIX unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt COMCODIX dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
9.5. COMCODIX hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. COMCODIX ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.
9.6. Bezüglich der Weisungsbefugnis wird Folgendes vereinbart:

Die Parteien verpflichten sich, Ansprechpartner für die Weisungen im Nachgang gesondert zu benennen. Bei Wechsel oder längerfristiger Verhinderung des jeweiligen Ansprechpartners haben die Parteien unverzüglich schriftlich oder in einem dokumentierten elektronischen Format einen Nachfolger bzw. Vertreter zu benennen, wobei die Benennung nicht zwingend namentlich zu erfolgen hat, sondern sich auf eine bestimmte Funktion im Unternehmen beziehen kann, z.B. den Leiter der IT-Abteilung. Mitglieder der Geschäftsführung sind stets weisungsbefugt bzw. zuständige Weisungsempfänger.

Weisungsberechtigte Personen des Verantwortlichen sind:

Name	Funktion	Telefon / E-Mail-Adresse

Weisungsempfänger bei COMCODIX sind:

Name	Funktion	Telefon / E-Mail-Adresse
Felix Bornmann	Geschäftsführer	+49 212 223310 fb@comcodix.de
Christopher Gertig	Serveradministration	+49 212 223310 cg@comcodix.de

9.7. Die Parteien verpflichten sich, bei Wechsel oder längerfristiger Verhinderung des jeweiligen Ansprechpartners unverzüglich schriftlich einen Nachfolger bzw. Vertreter gemäß den Vereinbarungen in Ziffer 9.6 zu benennen.

10. **Löschung von Daten und Rückgabe von Datenträgern**

10.1. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Vertrages hat COMCODIX sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Verantwortlichen an den Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

10.2. Eine Löschung von Daten erfolgt aber nur sofern nicht nach dem Unionsrecht oder dem anwendbaren Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Das Protokoll der Löschung ist von COMCODIX auf Anforderung vorzulegen.

11. **Informationspflichten, Schriftformklausel, Rechtswahl**

11.1. Sollten die Daten des Verantwortlichen bei COMCODIX durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat COMCODIX den Verantwortlichen unverzüglich darüber zu informieren. COMCODIX wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Verantwortlichen als »verantwortlicher Stelle« im Sinne des Bundesdatenschutzgesetzes bzw. als »Verantwortlicher« im Sinne der Datenschutzgrundverordnung liegen.

11.2. Änderungen und Ergänzungen dieses Auftrages und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen von COMCODIX – bedürfen einer schriftlichen Vereinbarung 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.

11.3. Bei etwaigen Widersprüchen gehen Regelungen dieses Auftragsverarbeitungsvertrages zum Datenschutz, ggf. bestehenden datenschutzrechtlichen Regelungen des Hauptvertrags vor. Sollten einzelne Teile dieses Auftragsverarbeitungsvertrags unwirksam sein, so berührt dies die Wirksamkeit dieses Vertrags im Übrigen nicht.

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

11.5. Die folgende Anlage ist Vertragsbestandteil:

Anlage 1 – Technische und organisatorische Maßnahmen

Ort: _____ Ort: _____

Datum: _____ Datum: _____

_____ _____

COMCODIX Verantwortlicher

Anlage 1:
zum AV-Vertrag vom: _____

Technische und organisatorische Maßnahmen gem. Art.32 DSGVO

Die Comcodix-Hosting-Dienste basieren auf einer Serverinfrastruktur. Für diese gilt das Prinzip der geteilten Verantwortung. Hierbei sind die SERVERANBIETER für die relevanten Maßnahmen zur Sicherheit der Serverinfrastruktur als solche und COMCODIX für die Sicherheit der Daten innerhalb dieser Serverinfrastruktur verantwortlich. Daher verweist COMCODIX für die relevanten Maßnahmen zur Sicherheit der Serverinfrastruktur an die jeweiligen, im Vertrag zur Auftragsdatenverarbeitung unter Ziffer 6 genannten SERVERANBIETER.

Die Haftung von COMCODIX gemäß den vertraglich vereinbarten Regelungen wird durch das Prinzip der geteilten Verantwortung nicht berührt.

Die nachfolgenden TOMs beschreiben die technischen und organisatorischen Maßnahmen der COMCODIX am Standort Solingen sowie die TOMs der SERVERANBIETER jeweils unter einem eigenen Unterpunkt.

I. Technische und organisatorische Maßnahmen der COMCODIX am Standort Solingen

1. **Zutrittskontrolle**

   Um die Zutrittskontrolle zu gewährleisten und Unbefugten den Zutritt zu Datenverarbeitungsanlagen, zu verwehren sind folgende Maßnahmen getroffen worden:

   - Das Gebäude wird durch eine Alarmanlage geschützt. Die Büros werden bei aktivierter Alarmanlage durch Bewegungsmelder überwacht. Sie lösen einen lauten Alarm aus, der auch direkt an mehrere Verantwortliche durchgeschaltet wird.
   - Sämtliche Zugänge so wie die Flur- und Treppenbereiche sind durchgehend videoüberwacht.
   - Die Reinigung der Betriebsräume wird nur von hauseigenem Personal vorgenommen. Während der Reinigung können keine vertraulichen Unterlagen eingesehen werden.

2. **Zugangskontrolle**
   a. *Benutzer-Authentifikation*
      - Nur authentifizierte Benutzer haben Zugang zu den Endgeräten (Clients), über die ein Zugriff auf die Server in den Rechenzentren der SERVERANBIETER möglich ist. Zusätzlich sind diese PCs passwortgeschützt und die Daten darauf verschlüsselt.
      - Der Zugang zu der Server-Infrastruktur der SERVERANBIETER erfolgt mittels einer verschlüsselten SSH-Verbindung, die durch Benutzername und Passwort abgesichert ist.

   b. *Serversysteme*
      - Die Serversysteme werden von eigenem Personal konfiguriert und gepflegt.
      - Die Kennungen der Administratoren, denen besondere Eindringungstiefen zugebilligt sind werden durch Username und Passworte geschützt. Die Administratoren andern ihre Passwörter regelmäßig.

   c. *Monitore*
      - Die Monitore der Entwickler Administratoren besitzen eine Bildschirmsperre mit automatischer Aktivierung und passwortgeschützter Aufhebung.

   d. *Internet*
      - Der Zugriff auf den Application-Server ist nur mit Username und Passwort durch die berechtigten Administratoren möglich. Das Passwort wird regelmäßig geändert uns ist nur den Administratoren bekannt.
      - Der Zugang zum Internet ist mit einer Firewall abgesichert.

   e. *Firewall*
      - Die Regeln der Firewall sind durch Parameter einstellbar, dafür gibt es eine eigene Administrationsoberfläche. Die Administration der Firewall erfolgt ausschließlich durch den Netzwerkadministrator. Der Zugriff auf die Firewall ist nur mit Username und Passwort durch die berechtigten Administratoren möglich. Das Passwort wird regelmäßig geändert und ist nur den Administratoren bekannt. Die Firewall wird mit den neuesten Patches, Updates und Virendefinitionen aufgewertet, sobald diese dem Administrator zugänglich sind. Dies kann sogar stündlich geschehen, wenn es nötig ist.
      - Es werden alle Zugriffsversuche, zulässige und unzulässige protokolliert und die IP-Adressen aufgezeichnet.

   f. Datenbank
      - Die Daten von COMCODIX werden ausschließlich in Datenbanken gehalten.
      - Für die Datenbankverwaltung gibt es einen ausschließlich und auf Dauer beauftragten Admin. Er ist nicht nur für die Konsistenz der Datenbanken verantwortlich, sondern auch für die Zuweisung von Speicherplatz, die in Zusammenarbeit mit den Administratoren vorgenommen wird.
      - Zugriff auf die Datenbanken haben ausschließlich nur die Administration und der Datenbank-Admin. Der Zugriff auf die Datenbank ist nur mit Username und Passwort durch die berechtigten Administratoren möglich.
      - Jeder der Zugriffsberechtigten ändert sein Passwort in regelmäßigen Abständen.

3. **Zugriffskontrolle**
   a. *Administratoren*
      - Die Administratoren haben Zugriff auf das gesamte System.
      - Die Administratoren genießen, wie auch in anderen Unternehmen einen hohen Vertrauensvorschuss. Ihre Verhaltensweisen werden von Selbstdisziplin und Verantwortungsbewusstsein geprägt Die berechtigten Administratoren sind hochgradig vertrauenswürdig.
      - Administratoren sind genau wie System Verwalter, Netzverwalter oder Privilegien Verwalter Personen mit besonderen Zugriffsmöglichkeiten zu allen Ressourcen der Datenverarbeitung. Sie stehen immer im Spannungsfeld zwischen den Handlungen, die ihnen möglich wären und dem, was sie tun dürfen und müssen.
      - Mit der Kenntnis des Usernamens und des Passwortes eines Administrators stehen ihm alle Systemressourcen offen. Er hat eine nahezu unbeschränkte Eindringtiefe in das jeweilige System und damit auch in die Anwendungen. Damit kann er alle Anwendungspassworte, die Berechtigungstabellen, die individuellen Erlaubnisse und Verbote einsehen und auch verändern. Er kann sämtliche systemeigenen Schutzrechte umgehen und auf alles zugreifen, was möglicherweise als Verursacher eines Fehlers auftreten könnte. Er kann neue Benutzer einrichten und ihnen Erlaubnisse erteilen, vorhandene Benutzer löschen oder ihre Berechtigungen ganz oder teilweise sperren. Er kann ihre Systempassworte zwar in den meisten Systemen nicht lesen, wohl aber löschen und neue zuweisen. Alle diese Tätigkeiten muss er ausführen können, um bei Systemfehlern reagieren zu können, um aus dem System die höchstmögliche Leistung herauszuholen und um die Nutzer auf die ihnen erlaubte Ausbreitung im System einzuschränken.
      - Aufgrund dieser Funktionsvielfalt ist ihm das System im oben erwähnten Umfang geöffnet und die hohe Eindringtiefe ermöglicht.
      - Die Administratoren haben aufgrund ihrer Funktion die Möglichkeit, alle Daten der Datenbank einzusehen oder evtl., auch zu verändern. Auf der anderen Seite sind für jemanden anderen, der sich unberechtigterweise Zugang zur Datenbank verschaffen sollte, die Hürden sehr, sehr hoch, denn er müsste außerdem den richtigen Servernamen, den richtigen Datenbank-Dateinamen und den Usernamen und das Passwort für die entsprechende Datei kennen.
      - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
      - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
      - Anzahl der Administratoren auf das „Notwendigste“ reduziert
   b. *User*
      - Das System basiert auf einer strikten Trennung zwischen der User-Schicht und der Datenbank-Schicht.
      - Die Abfrage eines Kunden / Externen-Users läuft wie folgt ab:
        - Login des Users mit Benutzername und Kennwort in der betreffenden (branchenspezifischen) Web-Anwendungssoftware. Der Zugriff auf die Comcodix-Dienste in den Rechenzentren der SERVERANBIETER erfolgt über eine mittels HTTPS abgesicherte Weboberfläche.

- Es ist jederzeit sichergestellt, dass der Kunde nur seine bzw. die für ihn bestimmten Daten selektieren kann.
- Bei Abfragen interner Anwender (Mitarbeiter) erfolgt der Zugriff gesteuert über die Unix/Windows Anmeldung mit eigenem Benutzernamen und Passwort, sowie auf Applikationsebene mit Benutzernamen und zweitem Passwort.
- Ein direkter Zugriff, oder ein unmittelbarer Zugriff auf Datenbankebene ist jedem Anwender verwehrt, und erfolgt ausschließlich über eigene Anwendungsapplikationen.

c. Sicherheit des Zugangs zu Applikationen:

- Zugang zu den Applikationen ist nur den dafür freigeschalteten Benutzern möglich. Zugang zu den eigentlichen Anwendungen des Produktionssystems wird zusätzlich noch durch ein zweistufiges Passwort (System/Programme) geschützt, welches nur den betreffenden Entwicklern bekannt ist.

d. Zeitliches Sicherheitsmanagement

- Das Authentifizierungs-/Autorisierung-Modul veranlasst nach außen hin bei Nichtaktivität eine automatische Unterbrechung der Verbindung nach 30 Minuten.

4. **Gewährleistung, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können**

- COMCODIX stellt dies durch eine zertifizierte SSL-Verbindung (HTTPS) sicher (s.o.). Sobald diese Verbindung durch eine korrekte Authentifizierung des Benutzers (übereinstimmende ID-Tags wie Benutzererkennung und Passwort, etabliert wurde, ist es nur dem eingeloggten (befugten) Benutzer möglich die Daten zu sehen (nur Leserechte).
- Für alle anderen ist diese verschlüsselte Verbindung nicht „einsehbar“. Jeglicher ungeschützter Verbindungsversuch über HTTP führt zu einem Verbindungsabbruch und zur Termination der Session.
- Sämtliche Datenträger der PC- und Notebook Systeme, die zum Zugriff auf das Rechenzentrum der SERVERANBIETER berechtigt sind, sind vollständig verschlüsselt.

5. **Weitergabekontrolle**
   - COMCODIX gewährleistet die Weitergabekontrolle, d.h. dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch folgende Maßnahmen:
     - Es laufen diverse Protokolle, die alle Programmaufrufe dokumentieren (wer sich wann und wie oft eingeloggt hat) und die es ermöglichen zu überprüfen, ob und welche Dateneingaben, Datenbewegungen oder/und ein Datendruck erfolgt sind.
     - Jeder Zugriff (wer, wann, wie oft etc.) und jede Veränderung der Datenbank werden mitgeloggt. Diese Daten werden in Logfiles abgelegt.
     - Einrichtungen von Standleitungen bzw. VPN Tunneln zur Weitergabe von Daten in anonymisierter oder pseudonymisierter Form.

6. **Eingabekontrolle**
    - Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
        - COMCODIX kann dies feststellen, da grundsätzlich protokolliert wird welche Daten, wann geändert wurden, wie auch systemintern mitgeloggt wird, wer zuletzt welche Daten geändert hat.
        - Eingehende Requests und an Clients zurückgesendete Responses des Application-Servers werden in Logdateien protokolliert. Die Logdateien werden je nach Last/Frequenz/Platzbedarf einen angemessenen Zeitraum (1 Woche bis 1 Monat) lang aufbewahrt und dann endgültig von einem Applicationserver-Admin gelöscht.
7. **Auftragskontrolle**
    - Die Auftragskontrolle bedeutet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen.
    - Dies wird von COMCODIX dadurch gewährleistet, dass nur Berechtigte zugreifen können.
    - Ausschließlichkeit: Es erhält nur der ausdrücklich Berechtigte Zugriff zu den Daten. Durch diese strikte Trennung wird sichergestellt, dass auf die Daten nicht zugegriffen werden kann, um sie weiterzuverarbeiten.
    - Eine Neuentwicklung oder Programmänderung im Authentifikations- / Autorisierungsmodul erfolgt stets nur bei Vorliegen eines schriftlichen Auftrages, dessen Gültigkeit durch den Geschäftsführer bestätigt werden muss. Diese Aufträge werden ohne zeitliche Beschränkung aufbewahrt. Die Weisungsgebundenheit, Hinweispflichten und Prüfungsrechte sind vertraglich geregelt.
    - Weisungen werden grundsätzlich schriftlich erteilt. In Ausnahmefällen können die bevollmächtigten Personen Weisungen auch mündlich erteilen, wobei eine schriftliche Bestätigung erfolgen muss.
    - Gewährleistung, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
8. **Verfügbarkeitskontrolle / Datensicherung**
    - Alle Daten werden in einem einheitlich festgelegten Konzept gesichert.
    - Die Sicherung erfolgt auf eigens dafür angelegte Sicherungsserver mittels verschlüsselter Übertragung. Zudem werden die zu sichernden Daten vorher lokal ebenfalls verschlüsselt. Sie sind somit nur verschlüsselt auf dem Sicherungsserver gespeichert.
    - Am Wochenende findet eine Vollsicherung der Dateisysteme statt. Von Montag bis Freitag werden sie inkrementell gesichert, d.h., nur die Änderungen im Datenbestand werden gesichert.
    - Zur Rekonstruktion von Daten liegen sehr ausführliche Anweisungen vor. Nur die Systemadministration ist befugt, aus den Sicherungen zerstörte Dateiinhalte zurückzuholen. Die Rekonstruktion kann nur in den Administrationskennungen ausgeführt werden. In dieser Kennung wird die Recovery-Funktion der Sicherungssoftware benutzt, in der auch die richtigen Datenträger benannt werden.

- Der Systemadministrator führt solche Arbeiten in Eigenverantwortung aus, sein Vertreter auf ausdrückliche Anweisung.

9. **Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden**
    - Die verschiedenen Datenbereiche sind logisch voneinander getrennt.
    - Die Benutzerverwaltung (Stammdaten) ist von der Produktionsdatenverwaltung getrennt. Die Daten der Comcodix-Dienste in den Rechenzentren der SERVERANBIETER werden gesondert auf anderen Servern als die Stammdaten gespeichert.
    - In der jeweiligen Auftrags-Verwaltung können nur die zugehörigen Kunden eingesehen und verwaltet werden. Dies wird durch festgelegte Benutzerrechte sichergestellt.
    - Zum anderen werden separat von der Benutzerverwaltung in der Prozessdatenverwaltung die Login-Daten und die Protokollierungen festgehalten. Es findet keine Weitergabe an Dritte oder sonstige Datenverarbeitung statt. COMCODIX speichert die Daten nur und verwendet Sie nur zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber dem Auftraggeber.

HETZNER

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

I. Vertraulichkeit

- Zutrittskontrolle
  - 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.

III. Technische und organisatorische Maßnahmen der Microsoft Corporation

Microsoft hat für die Kundendaten in den Kern-Onlinediensten die folgenden Sicherheitsmaßnahmen getroffen und wird diese beibehalten, die in Verbindung mit den Sicherheitsverpflichtungen in den OST (einschließlich der Bestimmungen der DSGVO) die einzige Verantwortung von Microsoft in Bezug auf die Sicherheit dieser Daten darstellen.

Bereich	Praktiken
Organisation der Informationssicherheit	**Verantwortung für die Sicherheit.** Microsoft hat einen oder mehrere Sicherheitsbeauftragte bestimmt, die für die Koordination und Überwachung der Sicherheitsvorschriften und -verfahren verantwortlich sind. **Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit.** Mitarbeiter von Microsoft mit Zugriff auf Kundendaten unterliegen Vertraulichkeitsverpflichtungen. **Risikomanagementprogramm.** Microsoft hat vor der Verarbeitung der Kundendaten oder der Einführung des Service für Onlinedienste eine Risikobewertung vorgenommen. Microsoft bewahrt ihre Sicherheitsdokumente in Übereinstimmung mit ihren Anforderungen an die Aufbewahrung auf, nachdem diese nicht mehr wirksam sind.
Inventarverwaltung	**Inventarisierung.** Microsoft pflegt ein Bestandsinventar aller Medien, auf denen Kundendaten gespeichert sind. Der Zugriff auf die Bestände dieser Medien ist Mitarbeitern von Microsoft vorbehalten, die schriftlich zu diesem Zugriff ermächtigt wurden. **Handhabung von Beständen** - Microsoft teilt Kundendaten in Kategorien ein, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs auf Kundendaten zu ermöglichen. - Microsoft ordnet Beschränkungen für das Drucken von Kundendaten an und verfügt über Verfahren für die Entsorgung von gedruckten Materialien, die Kundendaten enthalten. - Mitarbeiter von Microsoft müssen die Genehmigung von Microsoft erhalten, bevor sie Kundendaten auf tragbaren Geräten speichern, remote auf Kundendaten zugreifen oder Kundendaten außerhalb der Einrichtungen von Microsoft verarbeiten.
Sicherheit im Personalwesen	**Sicherheitsschulungen.** Microsoft informiert ihre Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Aufgaben. Außerdem informiert Microsoft ihre Mitarbeiter über mögliche Konsequenzen beim Verstoß gegen die Sicherheitsvorschriften und -verfahren. Microsoft verwendet in Schulungen ausschließlich anonyme Daten.
Physische Sicherheit und Sicherheit der Umgebung	**Physischer Zugang zu Einrichtungen.** Microsoft beschränkt den Zugang zu Einrichtungen, in denen ihre Informationssysteme, die Kundendaten verarbeiten, befinden, auf benannte autorisierte Personen. **Physischer Zugang zu Komponenten.** Microsoft führt Unterlagen über die eingehenden und ausgehenden Medien, die Kundendaten enthalten, einschließlich Art des Mediums, autorisierte(r) Absender/Empfänger, Datum und Uhrzeit, Anzahl der Medien und Arten von Kundendaten, die sie enthalten. **Schutz vor Störungen.** Microsoft verwendet unterschiedliche Systeme nach Branchenstandard, um den Verlust von Daten aufgrund von Stromversorgungsausfällen oder Leitungsstörungen zu verhindern. **Entsorgung von Komponenten.** Microsoft verwendet Verfahren nach Branchenstandard, um Kundendaten zu löschen, wenn sie nicht mehr benötigt werden.
Kommunikations- und Betriebsmanagement.	**Betriebsrichtlinie.** Microsoft führt Sicherheitsdokumente, in denen die Sicherheitsmaßnahmen und die relevanten Verfahren und Verantwortlichkeiten ihrer Mitarbeiter, die Zugriff auf Kundendaten haben, beschrieben sind. **Verfahren zur Datenwiederherstellung** - Microsoft erstellt fortlaufend, jedoch keinesfalls seltener als einmal pro Woche (es sei denn, es wurden in dem Zeitraum keine Kundendaten aktualisiert) mehrere aktuelle Kopien von Kundendaten, von denen Kundendaten wiederhergestellt werden können, und bewahrt diese auf. - Microsoft bewahrt Kopien von Kundendaten und Datenwiederherstellungsverfahren an einem anderen Ort auf als an dem Ort, an dem sich die primären Computergeräte, die die Kundendaten verarbeiten, befinden. - Microsoft verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von Kundendaten regeln. - Microsoft prüft die Datenwiederherstellungsverfahren mindestens alle sechs Monate, mit Ausnahme der Verfahren für Azure-Dienste für die Verwaltung, die alle zwölf Monate geprüft werden. - Microsoft protokolliert Datenwiederherstellungsmaßnahmen, einschließlich der verantwortlichen Person, der Beschreibung der wiederhergestellten Daten, gegebenenfalls der verantwortlichen Person sowie welche Daten (gegebenenfalls) beim Datenwiederherstellungsverfahren manuell eingegeben werden mussten. **Malware.** Microsoft verfügt über Antimalwarekontrollen, um zu verhindern, dass Malware unbefugten Zugriff auf Kundendaten erhält, einschließlich Malware aus öffentlichen Netzwerken. **Grenzüberschreitende Daten.** - Microsoft verschlüsselt Kundendaten oder versetzt den Kunden in die Lage, Kundendaten zu verschlüsseln, die über öffentliche Netzwerke übertragen werden. - Microsoft beschränkt den Zugriff auf Kundendaten in Medien, die ihre Einrichtungen verlassen. **Event-Logging.** Microsoft zeichnet den Zugriff und die Nutzung von Informationssystemen auf, die Kundendaten enthalten, indem die Zugriffs-ID, Zugriffszeit, gewährte oder verweigerte Autorisierung und entsprechende Aktivität registriert wird, oder versetzt den Kunden dazu in die Lage.

Bereich	Praktiken
Zugriffskontrolle	**Zugriffsrichtlinie.** Microsoft führt Unterlagen über Sicherheitsberechtigungen einzelner Personen, die auf Kundendaten zugreifen. **Zugriffsautorisierung** - Microsoft führt und aktualisiert Unterlagen zu den Mitarbeitern, die für den Zugriff auf Microsoft-Systeme, die Kundendaten enthalten, autorisiert sind. - Microsoft deaktiviert Anmeldedaten, die über einen Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden. - Microsoft benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen. - Wenn mehrere Personen Zugriff auf die Systeme haben, auf denen Kundendaten enthalten sind, stellt Microsoft sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen. **Geringste Berechtigung** - Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist. - Microsoft beschränkt den Zugriff auf Kundendaten nur auf die Personen, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen. **Integrität und Vertraulichkeit** - Microsoft weist ihre Mitarbeiter an, Administrationssitzungen zu deaktivieren, wenn sie Einrichtungen unter der Kontrolle von Microsoft verlassen oder wenn Computer anderweitig unbeaufsichtigt gelassen werden. - Microsoft speichert Kennwörter so, dass sie während ihres Geltungszeitraums nicht lesbar sind. **Authentifizierung** - Microsoft verwendet Verfahren nach Branchenstandard, um Nutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen. - Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass die Kennwörter regelmäßig erneuert werden müssen. - Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt Microsoft vor, dass das Kennwort mindestens acht Zeichen umfassen muss. - Microsoft stellt sicher, dass deaktivierte oder abgelaufene Kennungen keiner anderen Person gewährt werden. - Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf die Informationssysteme zu verschaffen, oder versetzt den Kunden dazu in die Lage. - Microsoft unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die beschädigt oder versehentlich offengelegt wurden. - Microsoft verwendet Verfahren nach Branchenstandard zum Schutz von Kennwörtern, einschließlich Verfahren, die die Vertraulichkeit und Integrität von Kennwörtern wahren sollen, wenn sie zugewiesen und verteilt werden sowie während der Speicherung. **Netzwerkdesign.** Microsoft verfügt über Kontrollen, um zu verhindern, dass Personen, die Zugriffsrechte, die ihnen nicht zugewiesen wurden, annehmen, sich Zugriff auf Kundendaten verschaffen, ohne hierfür autorisiert zu sein.
Management von Informationssicherheitszwischenfällen	**Verfahren für die Reaktion auf Zwischenfälle** - Microsoft führt Unterlagen über Sicherheitsverletzungen unter Angabe einer Beschreibung der Verletzung, des Zeitraums, der Konsequenzen der Verletzung, des Namens der Person, die den Zwischenfall gemeldet hat, und der Person, der der Zwischenfall gemeldet wurde, sowie des Verfahrens zur Wiederherstellung von Daten. - Für jede Sicherheitsverletzung, die ein Sicherheitsvorfall ist, erfolgt eine Meldung durch Microsoft (wie im Abschnitt „Sicherheitsvorfallmeldung“ weiter oben beschrieben) ohne schuldhaftes Zögern, auf jeden Fall aber innerhalb von 72 Stunden. - Microsoft untersucht Offenlegungen von Kundendaten, einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage. **Dienstüberwachung.** Die Sicherheitsmitarbeiter von Microsoft prüfen mindestens alle sechs Monate Protokolle, um bei Bedarf Verbesserungsmaßnahmen vorzuschlagen.
Business Continuity-Management	- Microsoft unterhält Notfallpläne für die Einrichtungen, in denen sich Microsoft-Informationssysteme, die Kundendaten verarbeiten, befinden. - Der redundante Speicher von Microsoft sowie ihre Verfahren zur Wiederherstellung von Daten sind so konzipiert, dass versucht wird, Kundendaten in ihrem ursprünglichen oder ihrem zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren.

Anlage zum Vertrag über Auftragsdatenverarbeitung nach DS-GVO
Technische und organisatorische Maßnahmen

1. Zutrittskontrolle

- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Dokumentierte Schlüsselvergabe an Mitarbeiter
- Richtlinien zur Begleitung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung von Serverräumen
- Rechenzentren sind alarmgesichert (Einbruch, Sabotage) mit Aufschaltung an einen externen Sicherheitsdienst
- Rechenzentren sind nicht als solche gekennzeichnet (neutrale Schilder)

2. Zugangskontrolle

- Root-Server (dedicated, virtual)
  - Serverpasswörter, welche vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden können und der Auftragnehmerin in der Regel nicht bekannt sind.
  - Auf Wunsch des Kunden Supportzugänge für die Mitarbeiter, die über ein zentrales SSH-Gateway erfolgen. Die Zugänge sind über Zwei-Faktor-Authentifizierung streng abgesichert, der Zugriff auf die Server findet verschlüsselt statt
  - Das Passwort zum Kundencenter wird per zugesandtem Link vom Auftraggeber selbst sicher generiert und dem Auftraggeber direkt angezeigt. Zusätzlich sind die wichtigsten Funktionen mit Zwei-Faktor-Authentifizierung abgesichert (SMS-Tan).
- Managed Server (dedicated, virtual)
  - Root-Zugang nur für Mitarbeiter der Auftragnehmerin über das zentrale SSH-Gateway. Die Zugänge sind über Zwei-Faktor-Authentifizierung streng abgesichert, der Zugriff auf die Server findet verschlüsselt statt

3. Zugriffskontrolle

- Interne Verwaltungssysteme der Auftragnehmerin
  - Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt die Auftragnehmerin sicher, dass unberechtigte Zugriffe verhindert werden.
  - Die Übertragung von Backups findet verschlüsselt statt
  - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter der Auftragnehmerin.
- Root-Server (dedicated, virtual)
  - Die Verantwortung der Zugriffskontrolle obliegt ausschließlich dem Auftraggeber.
- Managed Server (dedicated, virtual)
  - Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt die Auftragnehmerin sicher, dass unberechtigte Zugriffe verhindert werden.
  - Die Übertragung von Backups findet verschlüsselt statt

- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter der Auftragnehmerin.
- Für übertragene und installierte Daten / Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.

4. Weitergabekontrolle

- Alle Mitarbeiter sind auf das Datengeheimnis nach § 5 BDSG verpflichtet.
- Rückgabe oder datenschutzgerechte Löschung der Daten nach Auftragsbeendigung, es erfolgt eine Protokollierung von Daten- und Festplattenvernichtungen
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Vertrages zur Verfügung gestellt.

5. Eingabekontrolle

- Interne Verwaltungssysteme der Auftragnehmerin
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
- Root-Server (dedicated, virtual)
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
- Managed Server (dedicated, virtual)
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

6. Auftragskontrolle

- 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 Datenschutzerklärung enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Die Datenschutzerklärung enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
- Es ist ein betrieblicher Datenschutzbeauftragter bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.

7. Verfügbarkeitskontrolle

- Interne Verwaltungssysteme der Auftragnehmerin
  - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten (verschlüsselte Übertragung).

- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
- Einsatz von Festplattenspiegelung bei allen relevanten Servern.
- Monitoring aller relevanter Server.
- Einsatz unterbrechungsfreier Stromversorgung.
- Dauerhaft aktiver DDoS-Schutz.

- Root-Server (dedicated, virtual)
  - Datensicherung obliegt dem Auftraggeber.
  - Einsatz unterbrechungsfreier Stromversorgung.
  - Mehrfach redundate Klimatisierung, Alarmierung bei Ausfall der Klimatisierung
  - Redundante Netzwerkaussenanbindungen und Peerings, Alarmierung bei Ausfall des Netzwerks
  - Dauerhaft aktiver DDoS-Schutz.
- Managed Server (dedicated, virtual)
  - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Vertrages (verschlüsselte Übertragung)
  - Einsatz von Festplattenspiegelung je nach gebuchten Leistungen des Vertrages.
  - Einsatz unterbrechungsfreier Stromversorgung.
  - Mehrfach redundate Klimatisierung, Alarmierung bei Ausfall der Klimatisierung
  - Redundante Netzwerkaussenanbindungen und Peerings, Alarmierung bei Ausfall des Netzwerks
  - Einsatz von Softwarefirewall und Portreglementierungen.
  - Dauerhaft aktiver DDoS-Schutz.

8. Trennungskontrolle zur Datensicherung (physikalisch / logisch)

- Interne Verwaltungssysteme der Auftragnehmerin
  - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.
- Root-Server (dedicated, virtual)
  - Die Trennungskontrolle obliegt dem Auftraggeber.
- Managed Server (dedicated, virtual)
  - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.