Vertrag zur Auftragsverarbeitung personenbezogener Daten mit der PICTURE-Prozessplattform (Betriebsmodell „Software-as-a-Service“)

entsprechend DS-GVO

zwischen

_____

_____

_____

- Auftraggeber -

und

PICTURE GmbH

Friesenring 32

48147 Münster

- Auftragnehmer -

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Gegenstand dieses Auftrags ist in Ziffer 2 dieses Vertrags definiert. Hierbei hat der Auftraggeber den Auftragnehmer im Rahmen der Sorgfaltspflichten gemäß Art. 28 der Datenschutzgrundverordnung der Europäischen Union (DS-GVO) als Dienstleister ausgewählt. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den

schriftlichen Auftrag zur Auftragsverarbeitung im Sinne des Art. 28 DS-GVO und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung" oder „Verarbeitung" (von Daten) benutzt wird, liegt dieser Verwendung das Begriffsverständnis im Sinne des Art. 4 Nr. 2 DS-GVO zu Grunde.

(3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf darüber hinaus nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2. Gegenstand, Zweck und Art der Verarbeitung

(1) Dieser Vertrag ist an eine der folgenden Leistungsvereinbarungen gebunden, welche die Leistung des Auftragnehmers gegenüber dem Auftraggeber definiert und die Vergütungsaspekte regelt.

☐ AGB-Nutzungsbedingungen PICTURE-Prozessplattform („Software-as-a-Service")[1]

☐ _____ (vgl. Fußnote 1)

(2) Dieser Vertrag regelt die datenschutzrechtlichen Aspekte folgender Arbeiten und/oder Leistungen, welche der Auftragnehmer für den Auftraggeber erbringt:

- Betrieb des Softwareproduktes „PICTURE-Prozessplattform" (inkl. Einspielen von Updates und Upgrades). Die PICTURE-Prozessplattform ist ein webbasiertes Standardprodukt zum Prozessmanagement, das als „Software-as-a-Service" vom Auftragnehmer angeboten wird.
- Information der benannten technischen Ansprechpartner sowie der hierfür im Produkt registrierten Nutzer über Produktneuerungen, Updates, Upgrades, Systemausfällen, geplante Wartungsarbeiten sowie Änderungen bzgl. der Nutzung des Produktes.
- Support im Sinne von Unterstützung bei der Beantwortung von Bedienungsfragen per E-Mail und/oder Telefon. Eine Fernwartung durch den Auftragnehmer findet nicht statt.

(3) Die Verarbeitung personenbezogener Daten im Rahmen der Arbeiten / Leistungen gemäß Ziffer 2.1 und 2.2 erfolgt zu folgendem Zweck:

- Betrieb eines Informationssystems („Prozessregister") zur Dokumentation, Analyse und Verbesserung von Geschäftsprozessen (Arbeitsabläufen) in der Organisation des Auftraggebers

(4) Die Verarbeitung personenbezogener Daten im Rahmen der Arbeiten / Leistungen gemäß Ziffer 2.1 und 2.2 erfolgt auf folgende Art:

[1] Die zutreffende Option ist anzukreuzen; ggf. ist die abweichende Leistungsvereinbarung explizit zu benennen.

- Der Auftragnehmer stellt dem Auftraggeber ein webbasiertes Informationssystem in Form einer Standard-Software bereit. Das System wird durch den Auftragnehmer technisch administriert und in einer von seinen Unterauftragnehmern im Sinne von Ziffer 9 bereitgestellten technischen Infrastruktur betrieben. Die fachliche Administration des Systems sowie die Verarbeitung personenbezogener Daten in diesem System, insb. deren Erfassung, Nutzung und Löschung, erfolgt selbständig durch den Auftraggeber mittels der Standard-Funktionalität des Systems.
- Durch die Erbringung von Leistungen nach Ziffer 2.2 ist der Zugriff auf personenbezogene Daten durch den Auftragnehmer nicht auszuschließen.

(5) Im Rahmen der Arbeiten / Leistungen gemäß Ziffer 2.1 und 2.2 werden folgende Arten personenbezogener Daten verarbeitet:

Benutzerdaten (Stammdaten der Benutzerkonten):
☒ Benutzername (Login)
☒ E-Mail-Adresse
☒ Name
☒ Vorname
☒ Titel
☒ Anrede
☒ zugehörige Organisationseinheit

Nutzungsdaten:
☒ Zeitpunkt von Änderungen an den im System verwalteten fachlichen Informationsobjekten (Prozesse, Organisationseinheiten, Dokumente etc.)
☒ Verfasser von Änderungen an den im System verwalteten fachlichen Informationsobjekten (Prozesse, Organisationseinheiten, Dokumente etc.)
☐ Protokoll der durch Benutzer mit Administrator-Rechten vorgenommenen Konfigurationsänderungen im Verwaltungsmodul des Systems inkl. Zeitpunkt und durchführender Person (Audit-Log für administrative Tätigkeiten)[2]

Stellendaten[3]:
☒ Stellenbezeichnung

[2] Die Protokollierung der administrativen Tätigkeiten im Audit-Log ist optional und kann auf Wunsch des Auftraggebers jederzeit durch diesen selbständig deaktiviert werden. Macht der Auftraggeber von der Möglichkeit zur Deaktivierung keinen Gebrauch, so sind in diesem Vertrag sämtliche mit Verweis auf Fußnote 2 gekennzeichneten Optionen anzukreuzen.

[3] Solange der Auftraggeber nicht von der Option Gebrauch macht, die Stellen mit Stelleninhabern zu verknüpfen (vgl. folgende Fußnote), haben die verarbeiteten Stellendaten keinen direkten Personenbezug. Da in einigen Organisationseinheiten jedoch nur wenige Personen arbeiten und da einige Stellentypen nur durch einzelne Personen besetzt sind, könnten bei Kenntnis der Organisationsstruktur des Auftraggebers u.U. im Einzelfall Rückschlüsse auf konkrete Personen gezogen werden. Bei den Stellendaten solcher Organisationseinheiten handelt es sich daher um personenbeziehbare Daten, die vom Regelungsgegenstand dieses Vertrags erfasst sind.

☒ Organisatorische Einordnung der Stelle (Organigramm)
☒ Stellenart
☒ Anzahl der Stellen des jeweiligen Stellentyps
☒ Plankapazität der Stelle in Wochenarbeitsstunden
☒ Verknüpfung von Stellen mit den durch diese Stelle ausgeführten bzw. verantworteten Tätigkeiten in Prozessmodellen (grafische Darstellung von Arbeitsabläufen)
☐ Stellenbesetzung durch Personen (Stelleninhaber)[4]
☐ Vergütungsgruppe, mit der die Stelle tarifrechtlich bewertet ist[5]

Angaben zum Stelleninhaber (vgl. Fußnote 4):
☐ Name, Vorname, Anrede (vgl. Fußnote 4)
☐ E-Mail-Adresse (vgl. Fußnote 4)
☐ Telefonnummer (vgl. Fußnote 4)

Weitere Daten (optional):
☐ Der Auftraggeber macht von der Möglichkeit zur Verarbeitung weiterer Arten personenbezogener Daten Gebrauch (z.B. durch Erfassung in benutzerdefinierten Datenfeldern und/oder Freitextfeldern). Die Verarbeitung umfasst folgende weitere Arten personenbezogener Daten:

_____

_____

_____

(6) Von der Datenverarbeitung betroffen ist folgender Personenkreis:
☒ Alle Anwender der PICTURE-Prozessplattform beim Auftraggeber
☐ Alle Personen, über die Informationen in Form von Stellendaten in dem Softwareprodukt erfasst werden. Die Auswahl der Personen, die in dem Softwareprodukt hinterlegt werden, obliegt vollständig und ausschließlich der Verantwortung des Auftraggebers (vgl. Fußnote 4).

Weitere Personen (optional):
☐ Der Auftraggeber macht von der Möglichkeit Gebrauch, im Rahmen der Nutzung der PICTURE-Prozessplattform auch personenbezogene Daten weiterer Personenkreise

[4] Die Verarbeitung von Angaben zu den Stelleninhabern ist optional und kann auf Wunsch des Auftraggebers in der Software zentral deaktiviert werden. Macht der Auftraggeber von der Möglichkeit zur Deaktivierung keinen Gebrauch, so sind in diesem Vertrag sämtliche mit Verweis auf Fußnote 4 gekennzeichneten Optionen anzukreuzen.
[5] Die Verarbeitung von Angaben zu Vergütungsgruppen ist optional und kann auf Wunsch des Auftraggebers in der Software zentral deaktiviert werden. Macht der Auftraggeber von der Möglichkeit zur Deaktivierung keinen Gebrauch, so sind in diesem Vertrag sämtliche mit Verweis auf Fußnote 5 gekennzeichneten Optionen anzukreuzen.

zu verarbeiten, die über die oben genannten, üblicherweise betroffenen Personengruppen hinausgehen (z. B. in benutzerdefinierten Datenfeldern).
Von der Verarbeitung personenbezogener Daten sind daher zusätzlich folgende Personenkreise betroffen:

_____

_____

_____

3. Rechte, Pflichten und Weisungsbefugnisse des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher gemäß Art. 4 Abs. 7 DS-GVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DS-GVO obliegt allein dem Auftraggeber. Dem Auftragnehmer steht das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen. Die Regelungen aus Ziffer 5 Abs. 6 und 7 dieses Vertrages bleiben unberührt.

(2) Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Sicherstellung der datenschutzrechtlichen Anforderungen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber ist verpflichtet, das Ergebnis in geeigneter Weise zu dokumentieren.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen erfolgen per E-Mail an support@picture-gmbh.de.

(5) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich per E-Mail, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten besteht, ist ausschließlich der Auftraggeber für die Erfüllung der Pflichten verantwortlich. Die Verpflichtungen des Auftragnehmers zur Unterstützung des Auftraggebers zwecks Wahrung der Betroffenenrechte gemäß Ziffer 8 dieses Vertrags bleiben unberührt.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

(1) Weisungsberechtigte Personen des Auftraggebers sind:

a. _____
(Vor- und Nachname, Organisationseinheit, E-Mail, Telefon)

b. _____
(Vor- und Nachname, Organisationseinheit, E-Mail, Telefon)

c. _____
(Vor- und Nachname, Organisationseinheit, E-Mail, Telefon)

(2) Weisungsempfänger beim Auftragnehmer sind:

a. *Herr Dr. Thorsten Falk (Geschäftsführer)*

b. *Herr Malte Stockmann (Bereichsleiter Software-Lösungen)*

(3) Für die Erteilung von Weisungen sind folgende Kommunikationskanäle zu nutzen:

a. E-Mail (bevorzugt)

support@picture-gmbh.de

b. Postalisch

PICTURE GmbH
- (Name des Weisungsempfängers) -
Friesenring 32
48147 Münster

(4) Bei einem dauerhaften Wechsel oder bei längerfristiger Verhinderung der o.g. Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. Vertreter mitzuteilen.

(5) Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Abs. 1 gilt nicht sofern der Auftragnehmer zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall 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 (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(3) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen als die unter Abs. 1 und 2 genannten, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

(4) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Der Auftragnehmer hat einen Beauftragten für den Datenschutz i.S.d. Art. 37 DS-GVO bestellt. Der Datenschutzbeauftragte ist per E-Mail an datenschutz@picture-gmbh.de zu erreichen.

(6) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

(7) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

(8) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(9) Der Auftraggeber gestattet die Verarbeitung von Daten in Privatwohnungen im Rahmen der Telearbeit von Beschäftigten des Auftragnehmers. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicherzustellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

(10) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(11) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen.

(12) An der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten, bei erforderlichen Datenschutz-Folgenabschätzungen durch den Auftraggeber gemäß Art. 35 DS-GVO sowie ggf. in diesem Zusammenhang notwendigen vorherigen Konsultationen mit der Aufsichtsbehörde gemäß Art. 36 DS-GVO hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(13) Der Auftragnehmer sichert zu, für seine im eigenen Betriebsablauf durchgeführten Tätigkeiten zur Verarbeitung personenbezogener Daten – insbesondere derer, die im Auftrag des Auftraggebers durchgeführt werden - ein Verzeichnis der Verarbeitungstätigkeiten zu führen und dieses der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

6. Kontrollbefugnisse

(1) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren. Dies kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten und in

die verwendeten Datenverarbeitungssysteme, sowie durch Überprüfungen und Inspektionen - zu den jeweils üblichen Geschäftszeiten - vor Ort erfolgen (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

(2) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(3) Eine Einsicht des Auftraggebers in den Quellcode der in Ziffer 2 genannten Standardsoftware ist explizit, aus geheimhaltungs- und geschäftspolitischen Gründen des Auftragnehmers, ausgeschlossen.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DS-GVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist unverzüglich über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(5) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch in angemessenem Umfang geltend machen. Einzelheiten hierzu regeln die Vertragsparteien vor Abruf einer entsprechenden Leistung.

7. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich

- Störungen,
- Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie
- den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten

mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO.

(2) Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO).

(3) Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß Ziffer 4 dieses Vertrages durchführen.

8. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Rechte der von der Verarbeitung personenbezogener Daten betroffenen Personen nach Art. 12 bis 23 DS-GVO („Betroffenenrechte“) verantwortlich.

(2) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten Mitteln dabei, die Einhaltung der Betroffenenrechte zu gewährleisten.

(3) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung, Datenübertragbarkeit oder Widerspruch - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers ergreifen.

9. Unterauftragsverarbeiter

(1) Der Auftragnehmer ist berechtigt, Unterauftragsverarbeiter zur Verarbeitung von Daten des Auftraggebers einzusetzen.

(2) Der Auftragnehmer muss dafür Sorge tragen, dass er die Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(3) Eine Beauftragung von Unterauftragsverarbeitern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(4) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragsverarbeitern gelten. In dem Vertrag mit dem Unterauftragsverarbeiter sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragsverarbeiters deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragsverarbeiter eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragsverarbeitern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragsverarbeitern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(5) Der Vertrag mit dem Unterauftragsverarbeiter muss schriftlich oder in elektronischer Form abgefasst werden (Art. 28 Abs. 4 und Abs. 9 DS-GVO). Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Unterauftragsverarbeiter die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

(6) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragsverarbeiter den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

(7) Die zum Zeitpunkt des Abschlusses dieser Vereinbarung bestehenden Unterauftragsverhältnisse mit Unterauftragsverarbeitern sind in Anlage 1 mit Namen, Anschrift und Auftragsinhalt der bezeichneten Unterauftragsverarbeiter dokumentiert. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(8) Jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragsverarbeitern ist dem Auftraggeber spätestens acht Wochen vor dem geplanten Vollzug der Maßnahme durch den Auftragnehmer anzuzeigen. Eine Änderungsmitteilung muss Namen und Anschrift sowie die vorgesehene Tätigkeit des neuen Unterauftragsverarbeiters enthalten.

(9) Der Auftraggeber hat gemäß Art. 28 Abs. 2 DS-GVO das Recht, Einspruch gegen eine beabsichtigte Änderung einzulegen. Der Einspruch muss durch den Auftraggeber binnen vier Wochen nach Zugang der Information über die beabsichtigte Änderung der Unterauftragsverarbeiterverhältnisse erklärt werden.

(10) Eine Benachrichtigung über eine geplante Änderung gemäß Abs. 3 sowie eine Erklärung eines Einspruchs gemäß Abs. 4 ist gegenüber den in Ziffer 4 definierten Ansprechpartnern und über die dort festgelegten Kommunikationskanäle zu erklären.

(11) Im Falle eines wirksam erklärten Einspruchs erfolgt keine Bestellung des Unterauftragnehmers für die Verarbeitung der Daten des Auftraggebers. Dem Auftragnehmer steht in diesem Falle das Recht zu, die dieser Vereinbarung zu Grunde liegende Leistungsvereinbarung (vgl. Ziffer 2) sowie diese Vereinbarung selbst fristlos zu kündigen.

10. Datengeheimnis

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne von Art. 5 Abs. 1 lit. f) DS-GVO sowie Art. 32 Abs. 4 DS-GVO verpflichtet.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis verpflichtet werden.

(3) Der Auftraggeber verpflichtet sich, sofern er besonderen Geheimnisschutzregeln bezüglich der hier im Vertrag genannten relevanten Daten und Verarbeitungszwecken unterworfen ist, diese Geheimschutzregeln vor Vertragsabschluss dem Auftragnehmer anzuzeigen und vollständig bekannt zu machen. Unterlässt der Auftraggeber diese Anzeige und Bekanntmachung, so sichert der Auftraggeber damit zu, keinen besonderen Geheimschutzregeln unterworfen zu sein, die vom Auftragnehmer beachtet werden müssen.

11. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Diese Verpflichtung gilt auch nach Beendigung des Vertrages fort. Dies betrifft insbesondere Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12. Vergütung

(1) Die Vergütung des Auftragnehmers wird gesondert im Rahmen der zugrundeliegenden Leistungsvereinbarung vereinbart und hat unberührt der hier in diesem Vertrag definierten Rechte und Pflichten Gültigkeit.

13. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet.

(2) Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(3) Die umgesetzten technischen und organisatorischen Maßnahmen des Auftragnehmers sind in Anhang 2 dieses Vertrags beschrieben. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen der Unterauftragsverarbeiter des Auftragsnehmers ist jeweils als Anlage in den Verträgen zur Auftragsverarbeitung der Unterauftragsverarbeiter mit dem Auftragnehmer beigefügt. Diese Verträge werden dem Auftraggeber mit diesem Vertrag ausgehändigt.

(4) Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(5) Für die Sicherheit erhebliche Änderungen bzgl. der Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren wird der Auftragnehmer im Vorwege mitteilen. Solche Mitteilungen sind für die Dauer des Vertrages aufzubewahren. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer sowie der von seinen Unterauftragsverarbeitern getroffenen technischen und organisatorischen Maßnahmen anfordern.

(6) Sofern der Auftraggeber nicht binnen vierzehn Tagen einer mitgeteilten Änderung der technischen und organisatorischen Maßnahmen widerspricht, gilt die Maßnahme als angenommen.

(7) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Bei der Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen seiner Unterauftragsverarbeiter kann der Auftragnehmer insbesondere auf das Vorliegen einschlägiger gültiger und aktueller Zertifizierungen (z.B. Informationssicherheit gemäß der Norm ISO 27001) durch externe Gutachter abstellen.

(8) Das Prüfergebnis ist dem Auftraggeber auf Anfrage mitzuteilen.

14. Haftung

(1) Auf Art. 82 der DSGVO wird verwiesen.

15. Dauer des Auftrags

(1) Die Dauer dieses Vertrages ist an die Dauer der diesem Vertrage zugrundeliegenden Leistungsvereinbarung gebunden. Mit Kündigung und Beendigung der zugrundeliegenden Leistungsvereinbarung endet auch dieser Vertrag fristlos zu sofort.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Bestimmungen aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

(3) Der Auftragnehmer kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn in den Weisungen des Auftraggebers ein schwerwiegender Verstoß gegen die anzuwendenden Datenschutzvorschriften oder gegen Bestimmungen aus diesem Vertrag vorliegt oder der Auftraggeber Widerspruch gegen mitgeteilte Änderungen der technischen und organisatorischen Maßnahmen einlegt oder der Auftraggeber ergänzende Weisungen über Art, Umfang und Verfahren zur Datenverarbeitung gegenüber dem Auftragnehmer erteilt.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzkonform zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist ebenfalls unverzüglich datenschutzkonform zu löschen.

(2) Auf Wunsch des Auftraggebers händigt der Auftragnehmer nach Beendigung des Vertrages vor der Löschung entsprechend Absatz 1 sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber aus.

(3) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist von drei Wochen durch den Auftraggeber angekündigt werden.

17. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(4) Soweit sich nicht aus dem Hauptvertrag ein anderer Gerichtsstand ergibt, ist ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag beim Sitz des Auftragnehmers.

(5) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den	_____	_____, den	_____
(Ort)	(Datum)	(Ort)	(Datum)

_____	_____
- Auftraggeber -	- Auftragnehmer -

Anlage 1
Unterauftragsverarbeiter

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragsverarbeiter").

Dabei handelt es sich um nachfolgende Unternehmen:

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Deutschland

Der Unterauftragsverarbeiter Hetzner Online GmbH stellt die für den Betrieb notwendige Hardware, die Netzzugänge sowie Teile der eingesetzten Infrastruktur für redundante und räumlich verteilte Datensicherungen (Backups) bereit.

WIIT AG
Joachim-Erwin-Platz 3
40212 Düsseldorf
Deutschland

Der Unterauftragsverarbeiter WIIT AG stellt Teile der eingesetzten Infrastruktur für redundante und räumlich verteilte Datensicherungen (Backups) bereit.

Anlage 2
Technische und organisatorische Maßnahmen des Auftragnehmers zur Gewährleistung der Datensicherheit

Präambel

Diese Technischen und Organisatorischen Maßnahmen (TOMs) beschreiben die von der PICTURE GmbH umgesetzten Maßnahmen zum Schutz personenbezogener Daten im Rahmen des Betriebs der SaaS-Anwendung „PICTURE-Prozessplattform". Sie gelten für den Produktivbetrieb der Anwendung einschließlich der zugehörigen Administrations-, Support- und Entwicklungsprozesse sowie für alle Systeme und Komponenten, die zur Bereitstellung, Wartung und Absicherung des Dienstes eingesetzt werden.

Die im Auftrag verarbeiteten Kundendaten werden auf dedizierten Servern in einem Rechenzentrum verarbeitet. Virtuelle Server kommen ausschließlich für Infrastruktur- und Betriebsdienste (z. B. Monitoring, System-Management) zum Einsatz; auf diesen Systemen werden keine personenbezogenen Daten im Kundenauftrag verarbeitet.

Die beschriebenen Maßnahmen orientieren sich an Art. 32 DSGVO und folgen einem risikobasierten Ansatz unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. Bei wesentlichen Änderungen der Risiken, der eingesetzten Systeme oder der betrieblichen Verfahren werden diese TOMs überprüft und bei Bedarf angepasst.

Die Umsetzung der TOMs erfolgt arbeitsteilig durch die PICTURE GmbH als Auftragnehmerin sowie durch eingesetzte Unterauftragsverarbeiter. Die PICTURE GmbH bleibt für die ordnungsgemäße Auswahl, vertragliche Bindung und Kontrolle der Unterauftragsverarbeiter verantwortlich und stellt sicher, dass die beschriebenen Schutzziele insgesamt erreicht werden.

Die PICTURE GmbH ist Entwicklerin und Betreiberin der SaaS-Anwendung und verantwortet die softwareseitige Administration des Dienstes einschließlich der hierfür erforderlichen Infrastruktur-Dienste bis hinunter auf Betriebssystem-Ebene. Dies umfasst insbesondere Maßnahmen der Zugangs- und Zugriffskontrolle, der Änderungs- und Integritätskontrolle, der Protokollierung/Eingabekontrolle, der Anwendungssicherheit (Secure Development), der Datensicherung und Wiederherstellung sowie den organisatorischen Betrieb (u. a. Incident-, Patch- und Schwachstellenmanagement). Darüber hinaus verantwortet die PICTURE GmbH die Zutrittskontrolle an den Arbeitsplätzen des eigenen Personals sowie an der für Entwicklung und Administration eingesetzten IT-Infrastruktur.

Der Rechenzentrumsbetrieb der Produktivsysteme erfolgt durch den Unterauftragsverarbeiter Hetzner, der insbesondere für die physische Sicherheit des Rechenzentrums (Zutrittskontrolle, Gebäudesicherheit) sowie für Aspekte der Zugangskontrolle auf Netzwerkebene innerhalb der bereitgestellten Infrastruktur verantwortlich ist. Die geo-redundante Backup-Infrastruktur wird durch den Unterauftragsverarbeiter WIIT AG betrieben, der ebenfalls für die physische Sicherheit seiner Rechenzentrumsstandorte sowie für die Zugangskontrolle auf Netzwerkebene innerhalb seiner Infrastruktur verantwortlich ist.

Die in dieser Anlage 2 beschriebenen TOMs beziehen sich ausschließlich auf die von der PICTURE GmbH selbst implementierten Maßnahmen. Die mit den Unterauftragsverarbeitern vertraglich vereinbarten TOMs werden in Anlage 3 (Hetzner) und Anlage 4 (WIIT AG) zu Informationszwecken offengelegt.

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

Zutrittskontrolle (Kein unbefugter Zutritt zu Datenverarbeitungsanlagen)	• Mechanisches Schließsystem • Definierte Regeln zur Schlüsselvergabe inkl. deren Dokumentation • Zutrittskontrollsystem mit Chipkarten für ausgewählte Räume (z.B. Serverraum) • Begleitungsregeln von Besuchern gemäß Zonenkonzept
Zugangskontrolle (Keine unbefugte Systembenutzung)	• Authentifizierung mit Benutzername / Kennwort • Passwortrichtlinie inkl. Kriterien zur Vergabe sicherer Kennwörter (u.a. Sonderzeichen, Mindestlänge) • Zwei-Faktor-Authentifizierung für ausgewählte Dienste / Systeme • Automatische Sperrung bei wiederholter Falscheingabe von Zugangsdaten • Ausgabe von Zertifikaten zur Authentifizierung für besonders schutzbedürftige Systeme • Remote-Zugriff nur per VPN (mit 2FA) • Firewall • Regelmäßige Sicherheitsupdates / Patch-Management: Einspielen sicherheitsrelevanter Updates nach risikobasierter Priorisierung, um die Ausnutzung bekannter Schwachstellen zu verhindern. • Deaktivierung von Benutzerkonten/Zugangsdaten beim Ausscheiden (geregelter Offboarding-Prozess)
Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)	• Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte) • Definition von Rollen (Auswertungen, Kenntnisnahme, Veränderung, Löschung) • Anzahl der Personen mit Administrator-Berechtigungen auf das Notwendige reduziert • Protokollierung von Zugriffen in Log-Dateien

Trennungskontrolle / Verwendungszweckkontrolle (Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)	• Zweckbindung der Verarbeitung personenbezogener Daten • Logische Mandantentrennung (softwareseitig) • Separierung von Datenbanken • Trennung von Produktiv- und Testsystemen
Verschlüsselung	• Einsatz von Verschlüsselung während der Datenübertragung zwischen Auftraggeber und Auftragnehmer (Transportverschlüsselung bei der Datenübertragung über öffentliche Netzwerke) • Verschlüsselung bei der persistenten Speicherung (z.B. externe Backups im Rahmen der geo-redundanten Sicherung) • Verschlüsselte Datenträger auf den mobilen Endgeräten an den Arbeitsplätzen des Entwicklungs- und Betriebspersonals
Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)	Pseudonymisierung kommt im Zusammenhang mit der Löschung von Benutzerkonten zum Einsatz. Hierbei werden personenbezogene Daten (z. B. Vor- und Nachname, Login-Name, E-Mail-Adresse) entfernt. Der zugehörige Benutzerdatensatz bleibt ausschließlich mit einer internen technischen ID erhalten, um die referenzielle Integrität des Datenmodells (z. B. für Versionshistorien) sicherzustellen. Die technische ID wird in der grafischen Oberfläche (GUI) nicht exponiert; eine Zuordnung zu einer Person ist nach Löschung der personenbezogenen Daten nicht mehr möglich. In der GUI wird der Nutzer als „Gelöschter Benutzer“ dargestellt.

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

Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)	• Mitarbeitende werden gemäß Art. 32 Abs. 4 DSGVO unterwiesen und verpflichtet, personenbezogene Daten ausschließlich im Rahmen der Vorgaben datenschutzkonform zu verarbeiten und weiterzugeben. • Elektronische Datenübermittlungen erfolgen grundsätzlich verschlüsselt nach dem Stand der Technik. • Nach Beendigung des Auftrags erfolgt eine datenschutzgerechte Löschung der verarbeiteten Daten.

Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)	• Die Eingabe personenbezogener Daten erfolgt in der Regel durch den Auftraggeber bzw. dessen Mitarbeitende.
	• In Einzelfällen kann eine Eingabe/Änderung personenbezogener Daten stellvertretend durch den Auftragnehmer erfolgen (z. B. im Rahmen des technischen Supports, etwa bei der Unterstützung der Nutzerverwaltung). Für diese Fälle gelten folgende Maßnahmen:
	  ○ Protokollierung von Eingaben und Änderungen (Nachvollziehbarkeit, wer wann welche Daten angelegt, verändert oder gelöscht hat)
	  ○ Auswertung/Review der Protokolle bei Bedarf bzw. anlassbezogen (z. B. zur Aufklärung von Auffälligkeiten oder Fehlbedienungen)

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

Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)	• Backup- und Recovery-Konzept mit mindestens werktäglicher Sicherung aller relevanten Daten • Aufbewahrung von verschlüsselten Datensicherungen an sicheren, ausgelagerten Orten (Geo-Redundanz) • Einsatz von Schutzprogrammen zur Vermeidung von Sicherheitsvorfällen und Ausfällen (z. B. Malware-/Spam-Schutz, Firewalling) • Monitoring aller relevanten Server • Redundante Internet-Außenanbindung • Klimaanlage in Serverräumen • Geräte zur Überwachung von Temperatur und Feuchtigkeit im Serverraum
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen)	• Notfallmanagement inkl. Notfallpläne • Incident Management • Regelmäßige Tests der Wiederherstellbarkeit von Daten (Restore-Tests)

Technische und organisatorische Umsetzung des Rechts auf Löschung, "Recht auf Vergessenwerden" (Art. 17 DS-GVO)

Während der Vertragslaufzeit liegt die Verantwortung für die fachliche Löschung personenbezogener Daten beim Auftraggeber. Der Auftragnehmer stellt hierfür in der technischen Plattform geeignete Funktionen zur Identifikation und Löschung einzelner personenbezogener Datensätze innerhalb des jeweiligen Mandanten bereit. Es obliegt dem Auftraggeber, diese Funktionen im Rahmen seines fachlichen Löschkonzepts angemessen einzusetzen. Zusätzlich ist der Auftragnehmer während der Vertragslaufzeit für die fristgerechte Löschung nicht mehr benötigter Sicherheitskopien im Rahmen der definierten Backup- und Rotationsverfahren verantwortlich. Nach Beendigung des Vertragsverhältnisses geht die Verantwortung für die vollständige Löschung des Mandanten einschließlich sämtlicher Sicherheitskopien gemäß den festgelegten technischen und organisatorischen Verfahren auf den Auftragnehmer über.

Seitens des Auftragnehmers sind zur Erfüllung dieser Verantwortlichkeiten folgende Maßnahmen implementiert:

- Löschung personenbezogener Daten gemäß definiertem Löschkonzept mit festgelegten Löschklassen, Verfahren, Fristen und Verantwortlichkeiten; elektronische Daten werden nach dem Stand der Technik logisch gelöscht, sofern kein überschreibendes Verfahren erforderlich ist.
- Löschung personenbezogener Daten nach Beendigung eines Vertragsverhältnisses anhand eines dokumentierten mandantenbezogenen Löschprozesses einschließlich Nachweisführung.
- Automatisierte Löschung durch Ablaufmechanismen für Daten mit definierten Aufbewahrungsfristen; Backups unterliegen einer konfigurierten Frist zur sicheren Löschung über eine Rotationsstrategie.
- Vor Ausmusterung von Datenträgern (z.B. Festplatten) erfolgt eine überschreibende Löschung gemäß branchenüblichen Praktiken (z.B. Empfehlungen des BSI). Sofern dies nicht möglich ist (z.B. bei defekten Datenträgern) erfolgt eine physische Zerstörung.
- Sicherstellung einer datenschutzkonformen Vernichtung von Papierunterlagen durch Aktenvernichter bzw. Entsorgung durch einen externen Dienstleister („Datentonne“)
- Sicherstellung einer datenschutzkonformen Vernichtung von Datenträgern (z. B. Festplatten, USB-Speicher) vor Wiederverwendung oder Entsorgung, intern oder durch externen Dienstleister.
- Dokumentation von durchgeführten Löschmaßnahmen in geeigneten Systemen (z. B. Ticketsystem, Löschprotokolle).

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

- Integriertes Informationssicherheits- und Datenschutz-Management-System zur Steuerung und kontinuierlichen Verbesserung etabliert

- Regelmäßige Datenschutz-Unterweisungen und Verpflichtung der Mitarbeitenden gem. Art. 32 Abs. 4 DSGVO, insb. Kenntnis der Verfahrensanweisungen inkl. Weisungsrecht des Auftraggebers
- Incident-Response-Management inkl. regelmäßiger Überprüfung/Aktualisierung der Verfahren (z. B. Lessons Learned)
- Regelmäßige Überprüfung der TOM (mind. jährlich)
- Unterauftragnehmer-Management: vertraglich vereinbarte Kontrollrechte; regelmäßige Prüfung relevanter Nachweise (z. B. ISO 27001-Zertifikate)
- Datenschutz durch Technikgestaltung/Voreinstellungen: Berücksichtigung und Prüfung im Entwicklungsprozess (Art. 25 Abs. 2 DSGVO)

Anlage 3

Technische und organisatorische Maßnahmen des Unterauftragsverarbeiters Hetzner Online GmbH zur Gewährleistung der Datensicherheit

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 und Falkenstein
    - 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
  - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
    - 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.
  - bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
    - 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.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

        - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
        - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
    - bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
        - 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 und Falkenstein
        - 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.
    - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
        - Die Trennungskontrolle obliegt dem Auftraggeber.
    - bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
        - 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.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

        - 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.
        - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
            - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
        - bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
            - 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.
    - bei Hauptauftrag "Dedicated Server", "Colocation Server", "Cloud Server"
        - Datensicherung obliegt dem Auftraggeber.
        - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
        - Dauerhaft aktiver DDoS-Schutz.
    - bei Hauptauftrag "Managed Server", "Webhosting", "Storage Box"
        - 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.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

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.

Hetzner Online GmbH
Geschäftsführer: Martin Hetzner
Registergericht Ansbach, HRB 6089
USt-IdNr. DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bankverbindung:
Deutsche Bank AG Nürnberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

Anlage 4

Technische und organisatorische Maßnahmen des Unterauftragsverarbeiters WIIT AG zur Gewährleistung der Datensicherheit

Anhang 3

Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO

Nachfolgend werden die technischen und organisatorischen Maßnahmen dargestellt, welche die WIIT AG (nachfolgend: WIIT) zum Schutz der Daten ihrer Auftraggeber (nachfolgend: Kundendaten) getroffen hat. Die nachfolgend beschriebenen Kontrollen beziehen sich auf Dienste für deren Administration und Bereitstellung WIIT ausschließlich verantwortlich ist (bspw. Cloud-Dienste wie ASP-Hosting, Hosted Exchange, SharePoint oder shared Webhosting). Sofern WIIT dem Kunden Dienste bereitstellt, die dem Kunden volle Administrationsrechte auf Serversysteme einräumen (bspw. virtuelle oder dedizierte Server) gelten diese Ausführungen nur eingeschränkt, da der Kunde in erster Linie selbst für die Absicherung, Wartung, Datenablage, -verwaltung und -sicherung verantwortlich ist, sofern keine andere vertragliche Vereinbarung geschlossen wurde. Allerdings wird WIIT, sofern der Kunde einen administrativen Zugang auf seine Systeme zu Wartungszwecken eingerichtet hat, anfallende Arbeiten gemäß der folgenden beschriebenen Maßgaben vornehmen.

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

I. Zutrittskontrolle

(Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.)

Mit dem Begriff „Zutritt" ist der physische Zugang von Personen zu Gebäuden und Räumlichkeiten gemeint, in denen DV-Systeme betrieben und genutzt oder Datenbestände gelagert werden. Dies sind Rechenzentren, in denen Web-Server, Applikationsserver, Datenbanken, Speichersysteme betrieben wer-den und Arbeitsräume, in denen Mitarbeiter Arbeitsplatzrechner nutzen. Auch die Räumlichkeiten, in denen sich Netzkomponenten und Netz Verkabelungen befinden und verlegt sind, gehören hierzu sowie Archivräume.

Festlegung von Sicherheitsbereichen

Zu schützende Bereiche und deren Zutrittspunkte sind festgelegt. Die Kritikalität der Gebäude bzw. Räume wurden anhand der darin befindlichen IV-Anlagen sowie ggf. sonstiger Unterlagen festgestellt. Der Betrieb sämtlicher IT-Infrastrukturen erfolgt im selbstbetriebenen Rechenzentrum, das nach der Sicherheitsnorm ISO 27001 zertifiziert ist.

Außenanlagen

Von außen ist das Firmengelände der WIIT am Standort Limburgerhof durch einen 2 Meter hohen Gittermattenzaun mit Stachel-Draht-Rolle sowie vergitterten, abschließbaren Fenstern mit A4 Panzerglas gesichert. Daneben kommt eine Alarmanlage mit Polizeiaufschaltung und Aufschaltung zum Wachdienst sowie Videoüberwachung (Außenbereich) zum Einsatz (Zone1).

Die mit einer Türsicherung (elektrische Türöffner) ausgestatteten Eingangstüren werden stets verschlossen; es gibt drei Eingänge, geregelt über den Einsatz von Generalschlüsseln mit Chipkartenleser und differenzierten Schließgruppen. Ein Schlüsselmanagement ist vorhanden.

Büroräume

Sämtliche Mitarbeiter haben Zutritt zu den Büroräumen. Serverräume sind in den

Büroräumen nicht vorhanden (Zone 2). Ein Kundenbereich ist nicht vorhanden und Kundenbesuche sind nicht gewünscht bzw. erfolgen nur im Einzelfall mit Begleitung, Besucherausweis, Besucherbuch und Datenschutzerklärung.

Rechenzentrum

Der Zutrittsschutz der als besonders schutzwürdig deklarierten Räume Rechenzentrumsbereich, Serverraum und USV-Anlage wird durch WIIT selbst realisiert (Zone 3). Hier befinden sich die Server, daher wird der Schutzbedarf als hoch bewertet. Zutritt hat lediglich ausgewähltes und berechtigtes Personal. Besondere Sicherungsmaßnahmen bestehen durch den Einsatz von Bewegungsmeldern und einer separaten Schließanlage.

Zutritt, Festlegung zutrittsberechtigter Personen

Der Zutritt zu den Räumen, in denen personenbezogene Daten verarbeitet werden, erfolgt durch elektronische Zutrittskarten. Die Voraussetzungen sowie der Kreis der allgemein zutrittsberechtigten Personen sind festgelegt und die Zutrittsberechtigungen zu sicherheitsrelevanten Bereichen sind auf das notwendige Minimum beschränkt. Zutrittsmittel zu Gebäuden bzw. Räumlichkeiten sind grundsätzlich personengebunden vergeben und dürfen nicht an Dritte weitergegeben werden. Die Nutzer sind hierfür sensibilisiert.

Verwaltung und Dokumentation von Zutrittsberechtigungen

Ein Prozess zur Beantragung, Genehmigung, Ausgabe, Verwaltung und Rücknahme von Zutrittsmitteln bzw. zum Entzug von Zutrittsrechten ist eingerichtet und wird angewendet. Bei Ausscheiden bzw. Wechseln in einen anderen Aufgabenbereich, werden sämtliche Zutrittsmittel und -rechte zu allen bzw. zu im Rahmen der Aufgabenerfüllung nicht mehr erforderlichen Räumlichkeiten unverzüglich entzogen.

Alle Schlüssel für ein Gebäude werden für das jeweilige Gebäude zentral verwaltet. Dabei sind für jeden Schlüssel, der ausgegeben wird, mindestens die Person, die den Schlüssel erhalten hat und das Ausgabedatum des Schlüssels zu dokumentiert. Die Ausgabe ist vom Empfänger schriftlich zu quittieren und wird dokumentiert. Die Vergabe und Rücknahme von Zutrittsmitteln und Berechtigungen ist dokumentiert. Der Prozess stellt sicher, dass ausscheidende Mitarbeiter zwingend den Schlüssel abgeben müssen.

Es gibt Regelungen zum Zutritt für Firmenfremde, wie Gäste oder Lieferanten. Diese Regelungen beinhalten minimal, dass Firmenfremde ihren berechtigten Aufenthalt innerhalb der Gebäude jederzeit nachweisen können, z.B. mittels Gästeausweis, Besucherausweis oder Lieferantenausweis. Namen und Herkunft (Firmenzugehörigkeit, Geschäftsadresse oder Privatadresse) der Personen werden protokolliert.

Die Reinigung der Räumlichkeiten findet während der Betriebszeiten und damit unter Aufsicht statt. Bei einer erforderlichen Reinigung außerhalb der Betriebszeiten werden geeignete Regelungen (z.B. Anforderungen an das Reinigungspersonal) vereinbart.

Die Wartungsarbeiten durch Fremdpersonal vor Ort werden so durchgeführt, dass nur die beauftragten Arbeiten möglich sind. Dies kann z.B. durch Begleitung oder durch eine genaue Protokollierung/Aufzeichnung der Tätigkeiten erfolgen. In jedem Falle wird nur temporär der Zutritt gewährt, wo dies erforderlich ist.

II. Zugangskontrolle

(Maßnahmen, die verhindern, dass Datenverarbeitungssyteme von Unbefugten genutzt werden können.)

Kreis der Zugangsberechtigten

Der Kreis der Personen, die Zugang zu DV-Anlagen haben, auf denen Kundendaten verarbeitet und/oder gespeichert werden, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum beschränkt.

Die Verschlüsselung und Speicherung von Passwörtern in Abhängigkeit von Mitarbeiterberechtigungen der WIIT erfolgt über die Nutzung einer hierfür spezialisierten Software.

Identifikation und Authentisierung

Der Zugang zu den DV-Anlagen, auf denen Kundendaten verarbeitet werden, ist erst nach Identifikation und erfolgreicher Authentisierung möglich. Der Zugriff durch WIIT im Zuge der administrativen Tätigkeit wird protokolliert. Sämtliche Mitarbeiter der WIIT müssen sich mit starken Autentifizierungsmechanismen (min. Benutzernamen und Kennwort, bevorzugt Mehr-Faktor-Autentifizierung und Zertifikatsbasierte Autentifzierung) am System anmelden. Die Komplexität von Kennwörtern ist geregelt und entspricht dem Stand der Technik. Es besteht ein geregeltes Verfahren für die Rücksetzung von Passwörtern. Es werden passwortgeschützte Bildschirmschoner mit Sperrung bei mehr als 10 Minuten Abwesenheit eingesetzt.

III. Zugriffskontrolle

(Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten nach der Speicherung und bei der Verarbeitung, Nutzung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können)

Berechtigungskonzept

Jede Zugangsberechtigung ist mit einer Zugriffsberechtigung verknüpft durch die Verknüpfung mit einer oder mehreren im Berechtigungskonzept definierten Rollen. Hierbei darf jeder Zugangsberechtigte nur mit den Anwendungen und innerhalb dieser Anwendungen nur auf die Daten zugreifen, die er zur auftragsgemäßen Bearbeitung des jeweils aktuellen Vorgangs konkret benötigt und die in dem individuellen Berechtigungsprofil eingerichtet sind. Die Datenverarbeitung selbst ist so weit eingeschränkt, dass ausschließlich die minimal erforderlichen Funktionen für die Verarbeitung der personenbezogenen Kundendaten verwendet werden können. Der Zugriffsberechtigte muss sich gegenüber der Datenverarbeitungsanlage anhand von nachprüfbaren eindeutigen Merkmalen identifizieren.

Bei der Vergabe der Berechtigungen bzw. Zuweisung von Benutzerrollen werden immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Dabei ist sichergestellt, dass die im System abgebildete Funktionstrennung nicht durch kumulierte Berechtigungen aufgehoben wird. Das Berechtigungskonzept ergibt sich aus den Festlegungen zur Zutritt- und Zugangskontrolle. Diese sind schriftlich dokumentiert.

On- und Offboarding und Protokollierung Zugriff

Zugriffsberechtigungen werden beantragt und nach Genehmigung der zuständigen Stelle, vergeben. Sobald ein Administrator aus dem Dienst ausscheidet, werden

umgehend die Zutritts-, Zugangs- und Zugriffsberechtigungen aufgehoben.

Auch bei sonstigen Mitarbeitern der WIIT werden Zugriffsberechtigungen umgehend aufgehoben, wenn ein Mitarbeiter aus der jeweiligen Fachaufgabe ausscheidet. Die Erteilung oder Aufhebung von Zugriffsberechtigungen der Nutzer des jeweiligen Kunden obliegt der Verantwortung des Kunden. Es existiert ein Prozess zur Sperrung der Zugriffsmöglichkeit seitens des Kunden (z.B. bei Vertragsbeendigung).

Protokollierung Zugriff

Der Zugriff auf Kundendaten wird protokolliert und die Protokolle werden regelmäßig ausgewertet.

IV. Trennungskontrolle

(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können.)

Sparsamkeit bei der Datenerhebung

Es werden nur solche Daten erhoben, gespeichert oder verarbeitet, die unmittelbar dem Zweck dienen, die zur Erfüllung der Aufgabe oder Durchführung des Prozesses mindestens notwendig sind.

Getrennte Verarbeitung verschiedener Datensätze

Regelungen und Maßnahmen zur Sicherstellung der getrennten Verarbeitung und/ oder Lagerung von Daten und/ oder Datenträgern mit unterschiedlichen Verwendungszwecken werden angewendet.

Solche Maßnahmen sind:

- die Umsetzung einer Funktionstrennung,
- Richtlinien und Arbeitsanweisungen,
- Verfahrensdokumentation,
- Umsetzung von Regelungen zur Programmierung,
- Regelungen zur System- und Programmprüfung und
- Vorhandensein von Stellenbeschreibungen.

Personenbezogenen Daten werden nur während der Auftragsabwicklung bei WIIT gespeichert. Die Daten werden nach Auftraggeber und innerhalb dieser nach Auftrag getrennt gespeichert und verarbeitet.

Personenbezogene Daten können ausschließlich im Rahmen der Ablage durch den Auftraggeber auf dem zur Verfügung gestellten Speicherplatz/Systemen gespeichert werden. Eine getrennte Erhebung oder Auswertung der Daten ist möglich. Zugriff auf die Daten haben nur Personen, die über entsprechende Berechtigungsstufen verfügen. Die Löschung der personenbezogenen Daten erfolgt nach Weisung der Auftraggeber nach der Auftragsverarbeitung.

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

I. Weitergabekontrolle

(Maßnahmen, die gewährleisten, 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 welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen

ist.)

Weitergabe

Grundsätzlich werden KEINE Daten aus den WIIT-Systemen weitergegeben. Falls dies ausnahmsweise erforderlich sein sollte, so erfolgt die Weitergabe nur, soweit WIIT hierzu gesetzlich verpflichtet ist oder auf Anfrage/Weisung durch den jeweiligen Kunden.

Sichere Verbindung

Die Datenübertragungen zwischen Clients und Servern erfolgt generell verschlüsselt durch Verschlüsselung der Übertragungsstrecke. Sämtlicher Datenverkehr zwischen dem Browser (=Client) und den Produktivsystemen wird TLS-verschlüsselt übertragen. In Web-Oberflächen werden SSL-Zertifikate eingesetzt, die es den Anwendern ermöglichen, zu identifizieren, ob sie mit einem Server der WIIT interagieren.

Bei sogenannten Niederlassungsanbindungen werden statische VPN-Tunnel eingesetzt (S2S), welche Verschlüsselungsverfahren wie IPSEC, AES256 im Minimum verwenden.

Topologische Netzwerkstruktur

Sämtliche WIIT-Server liegen netztopologisch hinter entsprechenden Firewalls und Protection Systemen wie DDoS und WAF Gateways, der Zugriff auf die Systeme kann nur über diese erfolgen. Die Gateways lehnen Verbindungen, die aus einem nicht explizit freigeschalteten Netz kommen, ab. Diese Maßnahmen entsprechen stets dem aktuellen Stand der Technik. Es kommt eine HA-Firewall-Lösung zum Einsatz.

Aktualisierungen

Die Backendsysteme werden nach dem Stand der Technik gehärtet, damit sich ein Angreifer nicht aufgrund von Schwachstellen unbefugt Zugriff auf die Systeme und Daten verschaffen kann. Sowohl das Betriebssystem selbst als auch die darauf eingesetzte Software wird regelmäßig aktualisiert, um bekannt gewordenen Sicherheitslücken entgegenzuwirken.

Speicherung Kundendaten

Es werden keinerlei Kundendaten lokal auf Clients bei WIIT gespeichert. Bei WIIT werden außerdem keine externen physischen Datenträger zur Verarbeitung oder Speicherung von Daten der Auftraggeber verwendet. Falls ausnahmsweise auf expliziten schriftlichen Kundenwunsch(Weisung) Daten auf externe physische Datenträger kopiert werden, erfolgt dies nur nach Genehmigung und wird dokumentiert. Die Datenträger werden ummittelbar verschlüsselt und per Bote an den Auftraggeber verschickt, eine Aufbewahrung in den Räumen der WIIT findet grundsätzlich nicht statt.

Mobile Datenträger

Die Verwendung von mobilen Datenträgern wie z.B. USB-Sticks oder CDROMs zur Verarbeitung oder Speicherung von Kundendaten ist nur in Ausnahmefällen zulässig. Es ist insbesondere geregelt, dass grundsätzlich lediglich firmeneigene Datenträger verwendet werden dürfen.

Prozess zur Sammlung und Vernichtung von Daten- und Informationsträgern

Die Verarbeitung und Speicherung der Kundendaten erfolgt ausschließlich auf den Serverfestplatten. Sollte einer oder mehrere dieser physischen Datenträger ausgetauscht werden müssen (wegen Defekt der Festplatte oder Austausch des gesamten Serversystems), so ist ein Prozess zur Sammlung, Aufbewahrung und

späteren Entsorgung/Zerstörung der Festplatten eingerichtet.

Soweit Informationsträger in Papierform zum Einsatz kommen (bei der Belegerfassung) ist ein Prozess zur Sammlung, Aufbewahrung und Entsorgung eingerichtet. Es gibt Regelungen und Verfahren zur sicheren und datenschutzgerechten Sammlung und Vernichtung. Es werden hierbei Zerstörungsverfahren nach DIN 66399 bzw. ISO/IEC 21964 verwendet, die eine Rekonstruktion der Daten nur mit erheblichem Aufwand erlauben.

II. Eingabekontrolle

(Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt werden.)

Eingabeberechtigungen

Zugriffe durch Mitarbeiter der WIIT auf personenbezogene Daten der Kunden sind durch ihre Aufgabenstellung definiert (s.o.). Dies sind in der Regel Zugriffe aus Gründen des Supportes oder der Administration. Zugriffe auf die Daten, durch dazu berechtigte Nutzer des Kunden, werden durch eine im jeweiligen Vertrag definierte Vorgehensweise durch WIIT eingerichtet und freigegeben.

Zugriffe werden getrennt nach ihren Berechtigungen auf Betriebssystemebene, Datenbankebene oder Anwendungsebene. Innerhalb der Anwendungsebene können sowohl Kundenbenutzer als auch Mitarbeiter der WIIT-Zugriff bekommen.

Zugriffe auf Datenbankebene oder Betriebssystemebene sind nur möglich durch Administratoren der WIIT, nicht jedoch durch Kundenbenutzer. Zugriffe auf Datenbank- oder Betriebssystemebene werden zu Administrationszwecken benötigt.

Zugriffe der System-Administratoren dienen nicht der Verarbeitung oder dem aktiven Zugriff auf personenbezogene Daten, sondern der Pflege, Wartung und Aktualisierung der Server-Systeme an sich.

Protokollierung der Eingaben

Die Eingaben in die DV-Anlage werden auf der Anwendungsebene protokolliert (Mitarbeiter und Kunden). Die Protokolle werden für einen Zeitraum von 6 Monaten aufbewahrt, sofern keine Anhaltspunkte vorliegen, die eine längere Aufbewahrung erforderlich machen.

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

I. Verfügbarkeitskontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

Die Gewährleistung der Verfügbarkeit wird durch WIIT im Wesentlichen selbst sichergestellt und weist einen äußerst hohen Standard auf, u.a.:

- Anbindung an das öffentliche Stromnetz ebenso wie die Anbindung an die Internet-Backbones über zwei getrennte Gebäudeeinführungen,
- unterbrechungsfreie Stromversorgung inklusive Notstromversorgung für 24 Stunden Volllast,
- redundante Klimatisierung,
- Brandfrüherkennung.

Backup-Konzept

Um die Verfügbarkeit der Daten auch im Notfall sicherzustellen, werden die Daten täglich gesichert und die Festplatten gespiegelt sowie aktuelle Sicherungskopien ausgelagert. Zu diesem Zweck ist ein Backup-Konzept erstellt worden, das regelmäßig auf Aktualität geprüft wird. In dem Backup-Konzept ist festgelegt, nach welchem Schema regelmäßig Backups stattfinden. Es wird regelmäßig überprüft, ob das Zurückspielen der Daten vollständig und innerhalb der Zeitvorgaben möglich ist.

Es besteht eine USV-Anlage für den Serverraum. Für die Aufbewahrung der Daten gelten die gleichen Anforderungen und Sicherheitsstandards wie im laufenden Betrieb, d.h. es ist sichergestellt, dass die Anforderungen aus dem Zutritts-, Zugangs- und Zugriffschutz umgesetzt sind. Ebenso sind die Daten nach den geltenden Datenschutzrichtlinien zu vernichten/ zu löschen, wenn diese nicht mehr benötigt werden.

Im Rahmen der Auftragsdatenverarbeitung übermittelt der Auftragnehmer bis auf nachgeordnete Dienstleister selbst keine personenbezogenen Daten an Dritte durch Einrichtungen zur Datenübertragung. Übermittlungen personenbezogener Daten an Dritte oder Behörden erfolgen nur im Rahmen der entsprechenden Weisung aus dem Auftragsverhältnis oder aufgrund einer gesetzlichen Anforderung.

Es findet eine regelmäßige Prüfung von Notstromaggregaten und Überspannungsschutzeinrichtungen sowie eine permanente Überwachung der Betriebsparameter statt.

Disaster – Recovery, Notfallmanagement

Liegen Anzeichen für definierte Notfälle vor, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln vorgesehen. Hierzu ist ein Notfallkonzept festgelegt und beschrieben. Es finden regelmäßige Prüfungen der Notfalleinrichtungen wie z.B. Notstromaggregate und Blitz-/Überspannungsschutzeinrichtungen sowie eine permanente Überwachung der Betriebsparameter statt.

In den klimatisierten und mit Wassersensoren ausgestatteten Serverräumen ist eine Brand-/Rauchmeldeanlage verbaut, die bei Feststellung eines Brandes/ bei Rauch Alarm auslöst. Die Serverräumlichkeiten liegen in separaten Brandabschnitten. Die Unterbringung von Backupsystemen erfolgt in separaten Räumlichkeiten und Brandabschnitten. CO2 Feuerlöscher sind in unmittelbarer Nähe der Serverräumlichkeiten vorhanden.

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

(Hierunter fallen Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.)

I. Kontrollverfahren

Regelmäßige Prüfung durch den IT-Sicherheitsbeauftragten

Der IT-Sicherheitsbeauftragte überprüft in regelmäßigen Abständen die Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen. Dies erfolgt durch interne Audits auf Basis der internationalen Norm ISO/IEC 27001. Im Falle eines negativen Prüfungsergebnisses werden getroffene Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt.

Meldewesen

Vor Einführung neuer Datenverarbeitungsverfahren oder der Veränderung von Datenverarbeitungsverfahren erfolgt eine Meldung an den IT-Sicherheitsbeauftragten

und den betrieblichen Datenschutzbeauftragten.

Aktualisierung von Verfahrensverzeichnissen

Die Verfahrensverzeichnisse werden mindestens kalenderjährlich aktualisiert.

Datenschutzfreundliche Voreinstellungen

Bei der Entwicklung neuer IT-Lösungen werden datenschutz-freundliche Voreinstellungen gewählt. Hierdurch wird gewährleistet, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Incident-Response-Prozess

Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess).

Regelmäßige Zertifizierungen der Informationssicherheit durch externe Stellen

WIIT betreibt ein Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001, welches von einer externen Stelle zertifiziert wird.

II. Auftragskontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.)

Auftragsverarbeitung

WIIT vereinbart mit ihren Kunden einen Vertrag zur Auftragsverarbeitung mit Festlegungen zu den Weisungsbefugnissen des Auftraggebers. In der Vereinbarung werden über den Auftrag selbst die Verarbeitungsschritte spezifiziert. Wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden, so ist ein Vertrag zur Auftragsverarbeitung abzuschließen.

Regelungen zur Weisungserteilung und -entgegennahme

Aufträge werden in der Regel als Ticket erfasst. Es gibt eine eindeutige Zuordnung zwischen Ticket und Auftrag. Damit ist sichergestellt, dass jederzeit ersichtlich ist, auf Basis welchen Auftrags welche Tätigkeit im System durch wen durchgeführt wurde. Jede Kundenanforderung wird im Ticketsystem pro Kunde. Ein zentraler Dispatcher nimmt unabhängig von der Bearbeitung der Kundenanforderung das Ticket auf und übergibt es dann zur gesonderten Bearbeitung an den zuständigen Sachbearbeiter.

Die WIIT-Telefonzentrale überprüft die Kundenidentität anhand der hinterlegten Kundentelefonnummer und der übermittelten Telefonnummer. Sollten hierbei Unklarheiten bestehen, kontaktiert WIIT den Kunden anhand der hinterlegten Kundentelefonnummer /Kontaktdaten.

Zuständigkeiten und die daraus resultierende Bearbeitung von Weisungen sind definiert und als Verfahren hinterlegt. Insbesondere sicherheitskritische Verfahren werden über Checklisten dokumentiert und im Nachgang durch ein QM kontrolliert.

Tätigkeiten mit Auswirkungen z.B. der Überprüfung der Datensicherung, des Virenschutze oder die Entsorgung von Speichermedien unterliegen dem Vier-Augen Prinzip.

WIIT setzt im Bereich seiner Administration ein Passworttresorverfahren ein, so dass Mitarbeiter des UserHelpDesk keine Kenntnisse der Kundenpasswörter haben.

Regelungen/Beschränkungen der Auftragsausführung

Es ist sichergestellt, dass durch WIIT nur die Arbeiten durchgeführt werden, die in der zu erstellenden Leistungsbeschreibung enthalten sind. Alle darüber hinaus gehenden Arbeitsschritte werden vorher mit der zuständigen Stelle auf Seiten des Auftraggebers abgesprochen und schriftlich freigegeben.

WIIT informiert den Auftraggeber unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen, wenn Fehler festgestellt werden oder anderen Unregelmäßigkeiten beim Umgang mit Daten des Auftraggebers. Diese werden unverzüglich behoben.

Bei Beendigung des Auftragsverhältnisses erfolgt eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Daten, Unterlagen und Betriebsmittel.

Sonstiges, Innerbetriebliche Organisation

Alle Personen, die bei WIIT mit personenbezogenen Daten umgehen oder sonst an der Auftragsdurchführung beteiligt sind (z.B. externer Support), sind schriftlich zur Vertraulichkeit verpflichtet und werden u.a. zu den Grundsätzen des Datenschutzes sowie zum ordnungsgemäßen und sorgfältigen Umgang mit Daten geschult.

WIIT hat einen Datenschutzbeauftragten bestellt.