

Anlage zum HANDELSFAKTOR SaaS-Vertrag

Datenschutzvereinbarung zur Auftragsdatenverarbeitung

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Handelsfaktor SaaS-Vereinbarung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten. Auftragnehmer ist die TELENORMA AG.

Das Rechenzentrum der TELENORMA wird von der GBC GmbH, Steingrüble 9, 72336 Balingen betrieben. Alle in dieser Vereinbarung beschriebenen technischen und organisatorischen Maßnahmen i.S.v. Art 32 DS-GVO werden von dem Subunternehmen GBC GmbH und der Hetzner Online GmbH erbracht und datenschutzrechtlich gewährleistet.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus der Handelsfaktor SaaS-Vereinbarung ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
- (2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28

Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

- (2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dabei hat er den Stand der Technik, die Implementierungskosten, Art und Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Der zusätzliche Aufwand der rechtlichen Prüfung und der technischen Umsetzung ist dem Auftragnehmer durch den Auftraggeber zu erstatten.
- (3) Der Auftragnehmer wird ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einsetzen. Eine Änderung dieser Maßnahmen bleibt dem Auftragnehmer insbesondere im Rahmen des technischen Fortschritts vorbehalten, soweit das in der Anlage vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen wird der Auftragnehmer dem Auftraggeber in Textform mitteilen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Auf Anfrage wird der Auftragnehmer dem Auftraggeber weitere Einzelheiten dieses Verfahrens mitteilen. Der Aufwand der entsprechenden Mitteilung ist dem Auftragnehmer durch den Auftraggeber zu erstatten.
- (4) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Der Aufwand ist dem Auftragnehmer zu vergüten.
- (5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- (6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
- (7) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

- (8) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- (9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. Der dem Auftragnehmer hierdurch entstehende Aufwand ist dem Auftragnehmer zu erstatten.
- (10) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Die Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart. Der dem Auftragnehmer hierdurch entstehende Aufwand ist dem Auftragnehmer durch den Auftraggeber zu erstatten.
- (11) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
- (12) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Der dem Auftragnehmer hierdurch entstehende Aufwand ist dem Auftragnehmer durch den Auftraggeber zu erstatten.

§ 4 Pflichten des Auftraggebers

- (1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- (2) Im Falle einer Inanspruchnahme des Auftragsverarbeiters durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 12 entsprechend. Der dem Auftragnehmer hierdurch entstehende Aufwand ist dem Auftragnehmer durch den Auftraggeber zu erstatten.
- (3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.
- (4) Der Auftragnehmer verpflichtet sich in den unter § 3, § 6, an anderer Stelle oder im Hauptvertrag aufgeführten Fällen dem Auftragnehmer den entstandenen Aufwand zu Vergüten. Der Auftragnehmer hat das Recht Leistungen zu verweigern, sollte der Auftraggeber mit Zahlungen im Verzug sein.

§ 5 Anfragen betroffener Personen

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

§ 6 Nachweismöglichkeiten

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

Zum Nachweis der Einhaltung der vereinbarten Pflichten, kann der Auftragnehmer, dem Auftraggeber folgende Informationen zur Verfügung vorlegen:

- Durchführung eines Selbstaudits
- Unternehmensinterne Verhaltensregeln einschließlich eines externen Nachweises über deren Einhaltung
- Zertifikat zu Datenschutz und/oder Informationssicherheit
- Genehmigte Verhaltensregeln nach Art. 40 DS-GVO
- Zertifikate nach Art. 42 DS-GVO

Der Auftraggeber kann Nachweise vorgeben. Der Aufwand der rechtlichen Prüfung, der technischen und organisatorischen Umsetzung und der entsprechenden Nachweispflicht ist dem Auftragnehmer durch den Auftraggeber im Voraus zu marktüblichen Preisen zu erstatten. Im Falle der Nichtzahlung hat der Auftragnehmer ein Zurückbehaltungsrecht bzw. kann den Nachweis in der vom Auftraggeber gewünschten Nachweisen verweigern.

- (2) Sollten gemäß Absatz 1 im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Der Auftraggeber stimmt der Benennung eines unabhängigen externen Prüfers durch den Auftragnehmer zu, sofern der Auftragnehmer eine Kopie des Auditberichts zur Verfügung stellt. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine marktübliche Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.
- (3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

- (1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
- (2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
- (3) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber mit einer Vorankündigungsfrist von 7 Tagen. In nachweislichen technischen Notfällen beträgt die Frist 12 Stunden. Bei Gefahr im Verzug entfällt die Vorankündigungsfrist.
- (4) Der Auftraggeber kann der Änderung – innerhalb der Vorankündigungsfrist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.
- (5) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
- (6) Mit Vertragsschluss stimmt der Auftraggeber den zum Zeitpunkt des Abschlusses des Hauptvertrages bereits für den Auftragnehmer tätigen Subunternehmen zu, dazu zählen insbesondere die Hetzner Online GmbH, die GBC GmbH, die TELENORMA Holding AG und die weiteren Unternehmen der TELENORMA Gruppe (Unternehmen mit einer Mehrheitsbeteiligung der TELENORMA Holding AG). Der Auftraggeber kann hier den Nachweis eigener durchgängiger Auftragsdatenverarbeitungs- und Datenschutzvereinbarungen verlangen.

§ 8 Informationspflichten, Schriftformklausel

- (1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
- (2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

§9 Verarbeitungsort

Die Verarbeitung findet derzeit in Deutschland statt.

Die Verarbeitung der Daten hat ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum stattzufinden. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn durch den Auftragnehmer die obigen Bedingungen und die sonstigen Bedingungen der DS-GVO eingehalten werden.

§10 Rechtswahl

Es gilt deutsches Recht.

§11 Haftung und Schadensersatz

Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung und den damit verbunden Allgemeinen Geschäftsbedingungen) vereinbarte Haftungsregelung gilt mit deren Beschränkungen auch für die Auftragsverarbeitung.

Anlagen Vereinbarungen Auftragsdatenverarbeitung Rechenzentrum nach Art.28 DS-GVO
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Albstadt, den 01.05.2018


TELENORMA
Telnorma AG
An der Technologiewerkstatt 1
72635 Albstadt
TELENORMA AG Albstadt

Auftragnehmer

Auftraggeber

Auftrag gemäß Art. 28 DS-GVO

Vereinbarung

zwischen (der)

TELENORMA Holding AG, An der Technologiewerkstatt 1, 72461 Albstadt, DE
- nachstehend Auftraggeber genannt -

und der

Hetzner Online GmbH, Gunzenhausen
- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

Gegenstand und Dauer des Auftrags bestimmen sich vollumfänglich nach den im jeweiligen Vertragsverhältnis gemachten Angaben.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber i.S.v. Art.4 Nr.2 und Art.28 DS-GVO auf Grundlage dieses Auftrags.

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

Der Umfang, die Art und der Zweck einer etwaigen Erhebung, Verarbeitung oder Nutzung personenbezogener Daten, die Art der Daten und der Kreis der Betroffenen werden dem Auftragnehmer durch den Auftraggeber gemäß der vom Auftraggeber ausgefüllten Anlage 1 beschrieben, soweit sich das nicht aus dem Vertragsinhalt der in Ziffer 1 beschriebenen Vertragsverhältnisse ergibt.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3. Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO (Art.28 Abs.3 Satz 2 lit.c DS-GVO)

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und

dem Auftraggeber zur Prüfung zu übergeben (siehe Anlage 2). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 Satz 2 lit.c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

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

4. Berichtigung, Sperrung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- Als Datenschutzbeauftragte ist beim Auftragnehmer Frau Margit Müller, Head of Data Protection, +49 (0)9831 505-216, data-protection@hetzner.com bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechen Art. 28 Abs. 3 Satz 2 lit. c, 32 DSGVO und Anlage 2.
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- Dokumentation der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber, die gemäß Ziffer 3 unter <https://www.hetzner.com/AV/TOM.pdf> abrufbar sind.

6. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Wenn der Kunde beim Produkt Dedicated Server, Colocation Server und Hetzner Cloud einen Standort außerhalb Deutschlands auswählt, erklärt er sich mit einem Rechenzentrumsbetreiber als Subunternehmer an diesem Standort einverstanden. Eine produktspezifische Liste der eingesetzten Subunternehmer am jeweiligen Standort finden Sie unter: <https://www.hetzner.com/AV/subunternehmer.pdf>.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann wahlweise erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS- GVO, die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS- GVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) und/oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer gibt dem Auftraggeber auf Anfrage hin Auskunft zur Natur und dem Zeitpunkt der Löschung.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Sonstige Vereinbarungen

11.1. Entgelte

Ein Entgelt für diesen Auftrag wird nicht gefordert.

Soweit der Auftraggeber Unterstützung nach Ziffer 4 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

Soweit der Auftraggeber nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung vom Auftragnehmer abgestellten Mitarbeiters.

Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

11.2. Vertragsdauer

Diese Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig diese Vereinbarung.

Das Recht zur isolierten, außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte konkret für die Vereinbarung bleiben hierdurch unberührt.

11.3. Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland.

11.4. Gerichtsstand

Die Parteien vereinbaren als Gerichtsstand den Sitz des für Gunzenhausen zuständigen Gerichts.

Unterschriften

Albstadt, den 01.05.18


 **TELENORMA**

Auftraggeber Telenorma AG
An der Technologiewerkstatt 1
72461 Albstadt

Gunzenhausen, den 16.03.18


HETZNER
ONLINE
Hetzner Online GmbH | Industriestr. 25
91710 Gunzenhausen | www.hetzner.com

Auftragsnehmer

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

Gegenstand der Zusatzvereinbarung sind folgende Datenarten und -Kategorien:

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

Kreis der Betroffenen

Der Kreis der durch diese Zusatzvereinbarung Betroffenen umfasst:

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

**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.

- 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.

- 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 (Virens Scanner, 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.

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

- Das Datenschutz-Managementsystem und das Informationssicherheitsmanagementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).
- Auftragskontrolle
 - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
 - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
 - Die Hetzner Online GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.

Anlage zum Vertrag im Zuge der Umsetzung der DSGVO

zwischen



Telenorma AG
An der Technologiewerkstatt 1
72461 Albstadt

- Auftraggeber -

und

GBC GmbH
Internet Service Center
Steingröße 9
72336 Balingen

- Auftragnehmer -

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

Präambel. Diese Anlage findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag des Auftragsgebers mit dem Auftragnehmer in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung

- ☒ 1. Domain- und Nameserver-Verwaltungsdienste
- ☒ 2. Hosten eines WEB Dienstes und/oder eines (S)FTP Dienstes
- ☒ 3. Versenden und Speichern von E-Mail im laufenden Geschäftsbetrieb
- ☒ 4. Homeing eines WEB Dienstes, wenn erweiterter Support vereinbart ist

- ☒ 5. selbständige Cloudlösungen (DAV, Nextcloud, Owncloud u.a.)
- ☒ 6. Gruppenlösungen unserer allg. Cloud-Umgebung
- ☒ 7. Wartung/Pflege kundeneigener Geräten (Switches, Router, Firewalls etc.)
- ☒ 8. Erweiterte Dienste wie Passwortserver, Zeitserver etc.
- ☒ 9. Internetrelays und -gateways und oben nicht weiter explizit aufgeführten weitere Dienste

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

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art.4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür,

dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(3) Der Auftragnehmer unterstützt, soweit vereinbart, den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

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

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

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

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

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

(9) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

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

§ 4 Pflichten des Auftraggebers

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

Bestimmungen feststellt.

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

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

§ 5 Anfragen betroffener Personen

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

§ 6 Nachweismöglichkeiten

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

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

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

§ 7 Subunternehmer

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung

beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung. Eine Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer erfolgt nicht.

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

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

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

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

(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart.

Ort, Datum:
Balingen, 01.05.2018

GBC GmbH
INTERNET SERVICE CENTER

STEINGRÜBLE 9
72336 BALINGEN
TEL.: 07433 / 99260
FAX.: 07433 / 992619

Name / Unterschrift Auftraggeber

Ort, Datum:
Ailsbach, 02.05.2018

TELENORMA

Telenorma AG
An der Technologiewerkstatt 1
72461 Ailsbach

Name / Unterschrift Kunde

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

GBC GmbH
Steingrueble 9
72336 Balingen

Stand - 01.05.2018

1. Vertraulichkeit gem Art 32 Abs 1 DSGVO

1.1 Zutrittskontrolle

- Alarmanlage
- Manuelles Schließsystem
- Sicherheitsschloesser
- Schlüsselregelung/-liste
- Absicherung der Gebäudeschächte
- Besucher nur in Begleitung von Mitarbeitern
- Sorgfalt bei Auswahl Reinigungspersonal

1.2 Zugangskontrolle

- Login Benutzer/Passwort
- Antiviren Server/Clients
- Mehrstufige Packet Firewall
- Mehrstufige App. Firewall incl IDS, IPS
- Passwort Server incl 2FA

1.3 Zugriffskontrolle

- Aktenschredder Cross Cut
- Tresor
- Protokollierung Zugriffe

1.4 Trennungskontrolle

- Trennung Produktiv-/Testumgebung
- Mandantenfähigkeit relevanter Anwendungen
- Berechtigungskonzepte, Rechtevergabe, Attributsvergaben

1.5 Pseudoanonymisierung (Art 25 Abs1, Art 32 Abs. 1 lit)

- Pseudoanonymisierung nach DSGVO Richtlinien

2. Integritaet

2.1 Weitergabekontrolle

Email Verschlüsselung, verschlüsselte Verbindungen wie https, sftp, TLS...etc.
VPN, Signaturverfahren
Protokollierung sicherheitsrelevanter Zugriffe nach DSGVO

2.2 Eingabekontrolle

Protokollierung sicherheitsrelevanter Zugriffe
Rechtevergabekonzept incl. manueller und automatischer Kontrolle

3. Verfuegbarkeit/Belastbarkeit (Art 32 Abs. 1)

Feuer-/Rauchmeldeanlage
Feuerloescher Serverraume
Serverraumueberwachung Temperatur und Feuchtigkeit
redundante USV
mehrfach redundante Server- und Plattensystemumgebung bis HA Qualitaet
mehrstufiges Sicherungskonzept incl Backup-/Recovery

4. Verfahren zur regelmaessigen Ueberpruefung (Abs 32 Abs1, Art 25-1)

4.1 Datenschutz-Management

Dokumentiertes Sicherungs-/Sicherheitskonzept
Formalisierter Prozess fuer Auskunftsanfragen Betroffener
benannter Sicherheitsbeauftragter

4.2 Incident Response Management

FW, Spamfilter, Virens Scanner, IDS, IPS
Ticketsystem fuer alle Vorfaelle
Prozess zur Erkennung und Meldung von Sicherheitsvorfaellen
Prozess zur Erkennung und Meldung von Datenpannen

4.3 Datenschutzfreundliche Voreinstellung / Datensparsamkeit

Datensparsamkeit auf allen Arbeitsebenen

4.4 Auftragskontrolle / Outsourcing an Dritte

Kein Outsourcing von Prozessen, welche mit Datenschutz und Datensicherheit korrelieren.

Erhoben vom Sicherheitsbeauftragten der Fa. GBC

Juergen Hahn
Balingen 01.05.2018