Vertrag

über die Verarbeitung personenbezogener Daten

- nachfolgend „Vertrag“ genannt -

zwischen

- nachfolgend „**Auftraggeber**“ oder „Verantwortlicher“-

und

QSC AG
Mathias-Brüggen-Straße 55
50829 Köln

- nachfolgend „**Auftragnehmer**“ oder „Auftragsverarbeiter“ -

einzeln oder gemeinsam auch „**Partei**“ und/oder „**Parteien**“

INHALTSVERZEICHNIS

1 BEGRIFFSBESTIMMUNGEN

Im Sinne dieses Vertrages bezeichnet der Ausdruck

(a) „Drittland“ Länder, die keine Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums sind.

(b) **„Hauptvertrag“** den in Ziffer 2 näher gekennzeichneten Leistungsvertrag.

(c) **„weiterer Auftragsverarbeiter oder Unterauftragsverarbeiter“** den Vertragspartner des Auftragsverarbeiters, der von diesem mit der Durchführung bestimmter Verarbeitungsaktivitäten für den Verantwortlichen beauftragt wird;

(d) **„Sub-Unterauftragsverarbeiter“** den Vereinbarungspartner des weiteren Auftragsverarbeiters oder Unterauftragsverarbeiters, der von Letzterem mit der Durchführung bestimmter Verarbeitungsaktivitäten im Regelungsbereich dieses Vertrags beauftragt wird.

2 GEGENSTAND DES VERTRAGS, RECHTSGRUNDLAGE

(1) Die Rechtsgrundlagen dieser Vereinbarung liegen den Bestimmungen der EU-Datenschutzgrundverordnung (DS-GVO) ab deren Geltungsdatum zugrunde.

(2) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragsverarbeiter für den Verantwortlichen in dessen Auftrag und nach dessen Weisung in Ergänzung des Vertrags / der Verträge gem. Bestellformular „Plusnet WebServer“ inkl. aller Zusatz- und/oder Ergänzungsvereinbarungen bzw. Vertragserweiterungen, (nachstehend „Hauptvertrag“ genannt).

(3) Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie die Kategorien der betroffenen Personen in Verbindung mit **Annex 1**. Der Verantwortliche gewährt dem Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen wie in **Annex 1** beschrieben.

3 RECHTE UND PFLICHTEN DES VERANTWORTLICHEN

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Verantwortliche verantwortlich. Der Verantwortliche wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z.B. durch Einholung von Einwilligungserklärungen) geschaffen werden, damit der Auftragsverarbeiter die vereinbarten Leistungen auch insoweit rechtsverletzungsfrei erbringen kann.

(2) Der Auftragsverarbeiter wird personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation — verarbeiten, sofern er nicht durch das Recht

der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zu der Verarbeitung verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Soweit im Hauptvertrag Vereinbarungen zu Leistungsänderungen getroffen wurden, gehen diese den Regelungen in diesem Absatz vor. Soweit keine Vereinbarungen zu Leistungsänderungen im Hauptvertrag getroffen wurden, werden Weisungen und Maßnahmen, die eine Abweichung zu den in diesem Vertrag oder im Hauptvertrag festgelegten Leistungen darstellen, als Antrag auf Leistungsänderung behandelt. Zusätzliche Weisungen und Maßnahmen, die über die vertraglich vereinbarten Leistungen hinausgehen, sind –soweit nicht ausdrücklich anders vereinbart- bei Mehraufwand für den Auftragsverarbeiter gesondert zu vergüten. Die Vertragsparteien werden sich in diesem Fall über eine angemessene Vergütung gesondert verständigen. Soweit nicht ausdrücklich anders vereinbart, werden Unterstützungsleistungen des Auftragsverarbeiters nach Ziffern 3 Abs. (4), (6) und 4 Abs. (4), (5), (7), (8) Satz 2), (9), (10) Satz 2), (11) dieser Vereinbarung gesondert vergütet.

(4) Der Verantwortliche kann auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz und der in diesem Vertrag niedergelegten Pflichten durch die Einholung von Auskünften und Abfragen der unter Ziffer 3 Abs. (5) angeführten Nachweise beim Auftragsverarbeiter in Hinblick auf die ihn betreffende Verarbeitung kontrollieren. Der Verantwortliche wird vorrangig prüfen, ob die in Satz 1 dieses Absatzes eingeräumte Möglichkeit der Überprüfung ausreicht. Der Verantwortliche kann darüber hinaus auf eigene Kosten die Einhaltung der Vorschriften über den Datenschutz vor Ort kontrollieren. Der Verantwortliche kann die Kontrollen selbst durchführen oder durch einen von ihm beauftragten Dritten auf seine Kosten durchführen lassen. Vom Verantwortlichen mit der Kontrolle betraute Personen oder Dritte sind mit Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Die vom Verantwortlichen mit der Kontrolle betrauten Personen oder Dritte werden dem Auftragsverarbeiter in angemessener Form vorangekündigt und in die Lage versetzt, ihre Legitimation zur Durchführung der Kontrollen nachzuweisen. Dritte im Sinne dieses Absatzes dürfen keine Vertreter von Wettbewerbern des Auftragsverarbeiters sein. Der Verantwortliche wird Kontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen.

(5) Dem Auftragsverarbeiter steht es frei, die hinreichende Umsetzung der Pflichten aus diesem Vertrag, insbesondere der technisch-organisatorischen Maßnahmen (Ziffer 5) und Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch folgende Nachweise zu belegen:

- die Einhaltung genehmigter Verhaltensregeln;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit;
- Eigenerklärung des Auftragsverarbeiters.

(6) Der Verantwortliche wird in Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten unverzüglich und vollständig informieren. Der Verantwortliche wird in Hinblick auf die ihn betreffende Verarbeitung den Auftragsverarbeiter bei der Prüfung möglicher Verstöße und bei Abwehr von Ansprüchen betroffener Personen oder Dritten sowie bei der Abwehr von Sanktionen durch Aufsichtsbehörden zeitnah und umfänglich unterstützen.

4 RECHTE UND PFLICHTEN DES AUFTRAGSVERARBEITERS

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich im Rahmen des getroffenen Vertrags und nach Weisung des Verantwortlichen entsprechend der Regelung der Ziffer 3 Abs. (2). Der Auftragsverarbeiter verwendet die personenbezogenen Daten für keine anderen Zwecke und wird die ihm überlassenen personenbezogenen Daten nicht an unberechtigte Dritte weitergeben. Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung der personenbezogenen Daten des Verantwortlichen befassten Mitarbeiter und andere für den Auftragsverarbeiter tätigen Personen diese personenbezogenen Daten nur auf Grundlage der Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

(2) Der Auftragsverarbeiter gewährleistet, einen unabhängigen, fachkundigen und zuverlässigen Datenschutzbeauftragten zu bestellen, sofern dies von dem anwendbaren Recht der Europäischen Union oder des Mitgliedsstaates, dem der Auftragsverarbeiter unterliegt, gefordert wird.

(3) Den Ort der Datenverarbeitung legen die Parteien in **Annex 1** vor der Datenverarbeitung fest. Änderungen des Orts der Datenverarbeitung werden die Parteien bei Bedarf unter Beachtung der in dieser Vereinbarung festgelegten Form vereinbaren. Eine Datenverarbeitung in sogenannten Drittländern wird unter Berücksichtigung der einschlägigen geltenden rechtlichen Bestimmungen der Europäischen Union vorgenommen. Der Auftragsverarbeiter wird bei einer möglichen Verwendung der EU-Standardvertragsklauseln diese im Namen und im Auftrag des Verantwortlichen abschließen. Die Vertretungsvollmacht hierfür wird hiermit durch den Verantwortlichen erteilt.

(4) Der Auftragsverarbeiter wird – im vertraglich vereinbarten Umfang unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen - den Verantwortlichen bei der Einhaltung seiner ihm nach den geltenden rechtlichen Bestimmungen obliegenden Pflichten unterstützen. Der Auftragsverarbeiter behält sich vor, bei umfangreicher Inanspruchnahme nach dieser Ziffer 4 die eigene Unterstützungsleistung kostenpflichtig nach vereinbartem Tages-/Stundensatz abzurechnen. Die Bewertung der Schwelle zur „umfangreichen Inanspruchnahme“ liegt im billigen Ermessen des Auftragsverarbeiters.

(5) Ist der Verantwortliche gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von personenbezogenen Daten zu geben, so wird der

Auftragsverarbeiter den Verantwortlichen darin unterstützen, diese Auskünfte zu erteilen, sofern diese Auskünfte die Datenverarbeitung gemäß diesem Vertrag betreffen. Der Auftragsverarbeiter wird den Verantwortlichen – soweit rechtlich zulässig - über an ihn als Auftragsverarbeiter gerichtete Mitteilungen der Aufsichtsbehörden (z. B. Anfragen, Benachrichtigung über Maßnahmen oder Auflagen) in Verbindung mit der Verarbeitung von personenbezogenen Daten nach diesem Vertrag informieren. Soweit rechtlich zulässig wird der Auftragsverarbeiter Auskünfte an Dritte, auch an Aufsichtsbehörden, nur nach schriftlicher Zustimmung durch und in Abstimmung mit dem Verantwortlichen erteilen.

(6) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Fälle von schwerwiegenden Betriebsstörungen, bei Verdacht auf Datenschutzverletzungen und/oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten.

(7) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung.

(8) Der Auftragsverarbeiter führt nach Maßgabe der einschlägigen geltenden rechtlichen Bestimmungen, denen der Auftragsverarbeiter unterliegt, ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung. Der Auftragsverarbeiter unterstützt den Verantwortlichen auf Anfrage und stellt dem Verantwortlichen die für die Führung seines Verzeichnisses von Verarbeitungstätigkeiten notwendigen Angaben zur Verfügung, soweit diese Angaben im vertraglich umschriebenen Verantwortungs- und Leistungsbereich als Auftragsverarbeiter liegen und der Verantwortliche keinen anderen Zugang zu diesen Informationen hat.

(9) Falls der Verantwortliche eine Datenschutz-Folgenabschätzung durchführt und/oder eine Konsultation der Aufsichtsbehörde nach einer Datenschutzfolgenabschätzung beabsichtigt, werden sich die Vertragsparteien bei Bedarf über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragsverarbeiters abstimmen.

(10) Abhängig von der Art der Verarbeitung wird der Auftragsverarbeiter den Verantwortlichen bei dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen unterstützen. Bei Bedarf werden sich die Vertragsparteien über Inhalt und Umfang etwaiger Unterstützungsleistungen des Auftragsverarbeiters abstimmen. Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, leitet der Auftragsverarbeiter die Anfragen der betroffenen Person zeitnah an den Verantwortlichen weiter.

(11) Soweit sich Speichermedien im Besitz des Verantwortlichen befinden, wird der Verantwortliche vor einer etwaig vorgesehenen Übergabe (z.B. zur Prüfung oder Abwicklung von Gewährleistungsansprüchen) an den Auftragsverarbeiter oder dessen Unter-Auftragsverarbeiter alle personenbezogenen Daten – soweit nicht anders vereinbart – löschen.

(12) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien, mit Ausnahme der aufgrund gesetzlicher Verpflichtung des Auftragsverarbeiters weiter vorzuhaltenden personenbezogenen Daten, werden – soweit nicht im Hauptvertrag und dessen Anlagen und Anhänge bereits geregelt und soweit nicht anders vereinbart – an den Verantwortlichen zurückgegeben oder auf Kosten des Verantwortlichen vernichtet bzw. gelöscht. Gleiches gilt für Test- und Ausschussmaterial.

(13) Sofern die Vertragsparteien eine ausdrückliche Vereinbarung zur Rückgabe und Löschung von personenbezogenen Daten bzw. Datenträgern getroffen haben, geht diese Vereinbarung den Regelungen in diesem Absatz vor. Soweit die Vertragsparteien keine ausdrückliche Vereinbarung zur Rückgabe von personenbezogenen Daten bzw. Datenträgern des Verantwortlichen getroffen haben kann der Auftragsverarbeiter personenbezogene Daten bzw. Datenträger des Verantwortlichen auf Kosten des Verantwortlichen zurückgeben. Wenn der Verantwortliche seiner Rücknahmepflicht nicht nachkommt, steht es dem Auftragsverarbeiter frei, die personenbezogenen Daten bzw. Datenträger auf Kosten des Verantwortlichen zu löschen/vernichten. Der Verantwortliche kann während des Bestehens des Vertragsverhältnisses oder mit Vertragsende schriftlich die personenbezogenen Daten, die nicht gemäß Abs. ((12) vernichtet bzw. gelöscht sind, auf seine Kosten heraus verlangen und dem Auftragsverarbeiter einen Zeitpunkt (längstens bis Vertragsende) für die Herausgabe nennen. Die Vertragsparteien werden sich nach Herausgabeverlangen auf die weiteren Modalitäten der Herausgabe (wie z.B. Format) verständigen. Das Herausgabeverlangen muss dem Auftragsverarbeiter einen Monat vor dem vom Verantwortlichen benannten Zeitpunkt bzw. ein Monat vor Vertragsende zugegangen sein.

5 TECHNISCHE UND ORGANISATORISCHE SICHERHEITSMAßNAHMEN

(1) Der Verantwortliche und der Auftragsverarbeiter werden geeignete technische und organisatorische Maßnahmen treffen, um ein, dem Risiko angemessenes Schutzniveau zu gewährleisten. Die derzeit als geeignet angesehenen Maßnahmen des Auftragsverarbeiters sind in **Annex 2** beschrieben. Der Verantwortliche hat die technischen und organisatorischen Maßnahmen im Zusammenhang mit etwaigen weiteren Maßnahmen in Hinblick auf ein angemessenes Schutzniveau bewertet. Diese Maßnahmen werden wie in **Annex 2** beschrieben, als geeignete Maßnahmen vereinbart.

(2) Die technischen und organisatorischen Maßnahmen können im Laufe des Vertragsverhältnisses angepasst werden. Die Sicherheit der Verarbeitung und die Angemessenheit des Schutzniveaus wird der Verantwortliche regelmäßig prüfen und dem Auftragsverarbeiter etwaigen Anpassungsbedarf unverzüglich mitteilen. Der Verantwortliche wird dem Auftragsverarbeiter hierzu alle erforderlichen Informationen zur Verfügung stellen. Der Auftragsverarbeiter seinerseits kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen. Der Verantwortliche ersetzt dem Auftragsverarbeiter, soweit nicht ausdrücklich anderweitig vereinbart, den durch die Anpassung der Schutzmaßnahmen an den technischen Fortschritt entstehenden Mehraufwand.

(3) Für die Überprüfungs- und Nachweismöglichkeiten gelten Ziffer 3 Abs. (4) und Ziffer 3 Abs. (5).

6 VERTRAULICHKEIT

(1) Der Auftragsverarbeiter wird im Zusammenhang mit der hier vereinbarten Verarbeitung personenbezogener Daten die Vertraulichkeit wahren. Er wird die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten, soweit diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Vereinbarungen im Hauptvertrag zur Wahrung der Vertraulichkeit, die nicht vom Anwendungsbereich dieses Auftragsverarbeitungsvertrags betroffen sind, bleiben unberührt.

(2) Der Auftragsverarbeiter wird Personen, die Zugang zu personenbezogenen Daten haben, mit den für sie maßgeblichen Datenschutzvorgaben und Weisungen dieser Vereinbarung im Voraus vertraut machen.

7 UNTERAUFTRAGSVERARBEITER

(1) Der Auftragsverarbeiter darf zur Erfüllung der in diesem Vertrag beschriebenen Aufgaben weitere Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter) einsetzen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Aufträge zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung erteilt und die keine Auftragsverarbeitungsleistung für den Verantwortlichen beinhalten. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind insbesondere Nebenleistungen zu verstehen, die der Anbieter z.B. als Post-/Transportdienstleistung, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahme zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(2) Für die in **Annex 3** aufgeführten Unterauftragsverarbeiter sowie die in **Annex 4** aufgeführten Sub-Unterauftragsverarbeiter und die dort genannten Aufgabenbereiche gilt die Genehmigung des Verantwortlichen als erteilt.

(3) Der Verantwortliche erteilt hiermit dem Auftragsverarbeiter die allgemeine Genehmigung für den künftigen Einsatz weiterer Auftragsverarbeiter (Unterauftrags- und Sub-Unterauftragsverarbeiter) nach Maßgabe des folgenden Absatz (4).

(4) Der Auftragsverarbeiter informiert den Verantwortlichen schriftlich oder per E-Mail über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter (Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter), wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen binnen 14 Tagen nach Zugang der Information beim Verantwortlichen Einspruch zu erheben. Die Vertragsparteien werden sich bei Bedarf über Art und Weise, hinzutretender oder alternativer Möglichkeiten der Information über den künftigen Einsatz oder Änderungen beim Einsatz weiterer

Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter verständigen. Dies kann z.B. die Vorhaltung und den Abruf einer Listung der Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter einschließen. Der Verantwortliche wird die Genehmigung zur Einbindung weiterer Unterauftragsverarbeiter und Sub-Unterauftragsverarbeiter nicht ohne wichtigen Grund verweigern.

(5) Dem Auftragsverarbeiter steht ein außerordentliches **Kündigungsrecht** des Hauptvertrages nach Maßgabe des Hauptvertrages – oder für den Fall, dass ein solches Kündigungsrecht im Hauptvertrag nicht eingeräumt wurde, ein außerordentliches Kündigungsrecht von 4 Wochen zum Monatsende – zu, wenn nach Auffassung des Auftragsverarbeiters der Verantwortliche die Einbindung des Unterauftragsverarbeiters und/oder Sub-Unterauftragsverarbeiters ohne wichtigen Grund verweigert oder dem Auftragsverarbeiter eine Leistungserbringung ohne den abgelehnten Unterauftragsverarbeiter und/oder Sub-Unterauftragsverarbeiters nicht möglich ist.

(6) Der Auftragsverarbeiter wird Unterauftragsverarbeiter auswählen, die hinreichende Garantien dafür bieten, dass die vereinbarten geeigneten **technischen und organisatorischen Maßnahmen** so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Der Auftragsverarbeiter wird mit Unterauftragsverarbeitern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieses Vertrags inhaltlich entsprechen. Der Auftragsverarbeiter wird mit dem Unterauftragsverarbeiter die technischen und organisatorischen Maßnahmen festlegen und die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen, vor Beginn der Datenverarbeitung und dann regelmäßig kontrollieren.

(7) Die Beauftragung von **Sub-Unterauftragsverarbeitern** durch den Auftragsverarbeiter ist nach Maßgabe der Abs. (1) bis Abs. (6) zulässig.

8 VERTRAGSDAUER, KÜNDIGUNG

Diese Vereinbarung gilt für die Dauer der tatsächlichen Leistungserbringung durch den Auftragsverarbeiter. Dies gilt unabhängig von der Laufzeit etwaiger anderer Verträge (insbesondere des Hauptvertrags), die die Parteien ebenfalls bzgl. der Erbringung der vereinbarten Leistungen abgeschlossen haben.

9 ANSPRECHPARTNER

(1) Datenschutzbeauftragter des Auftragsverarbeiters ist:

Datenschutzbeauftragter: Thomas Bösel
T +49 221 669-8000
datenschutzbeauftragter@qsc.de

(2) Der Verantwortliche benennt gegenüber dem Auftragsverarbeiter den Ansprechpartner für im Rahmen dieses Vertrages anfallende Datenschutzfragen. Wird kein Ansprechpartner vom Verantwortlichen benannt, gilt der Ansprechpartner des Hauptvertrages als benannt.

10 HAFTUNG UND FREISTELLUNG

(1) Der Verantwortliche gewährleistet in seinem Verantwortungsbereich die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Pflichten bei der Verarbeitung personenbezogener Daten.

(2) Es gelten die Haftungsbeschränkungen aus dem Hauptvertrag. Der Verantwortliche stellt den Auftragsverarbeiter von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragsverarbeiter aufgrund der vom Verantwortlichen beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer rechtswidrigen Verarbeitung der personenbezogenen durch den Auftragsverarbeiter beruht.

11 SONSTIGES

(1) Von der Ungültigkeit einer Bestimmung dieses Vertrags bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Sollte sich eine Bestimmung als unwirksam erweisen, werden die Parteien diese durch eine neue ersetzen, die dem von den Parteien Gewollten am nächsten kommt.

(2) Sämtliche Änderungen dieses Vertrags sowie Nebenabreden bedürfen der Schriftform (einschließlich in elektronischer Form). Dies gilt auch für das Abbedingen dieser Schriftformklausel selbst.

(3) Die Allgemeinen Geschäftsbedingungen des Verantwortlichen finden auf diesen Vertrag keine Anwendung.

(4) Der Gerichtsstand zu diesem Vertrag ist Köln. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes.

(5) Bei Widersprüchen zwischen den Bestimmungen dieses Vertrags und Bestimmungen sonstiger Vereinbarungen, insbesondere des Hauptvertrags, sind die Bestimmungen dieses Vertrags maßgebend. Im Übrigen bleiben die Bestimmungen des Hauptvertrags unberührt und gelten für diesen Vertrag entsprechend.

Annexe:

Nachstehende Annexe sind feste Bestandteile dieser Vereinbarung:
Annex 1: Einzelheiten der Datenverarbeitung
Annex 2: Technische und organisatorische Sicherheitsmaßnahmen
Annex 3: Genehmigte Unterauftragsverarbeiter
Annex 4: entfällt

Köln, Datum	, Datum
Unterschriften QSC AG / Auftragnehmer	Unterschrift(en) Auftraggeber
Namen in DRUCKBUCHSTABEN	Name(n) in DRUCKBUCHSTABEN
Funktion	Funktion

Annex 1

Einzelheiten der Datenverarbeitung

1. Datenkategorien, Datenarten, Zugriffsformen

a. Kategorien betroffener Personen:

Beispiele:

- ☐ Beschäftigte
- ☐ Kunden
- ☐ Lieferanten
- ☐ Abonnenten
- ☐ Interessenten
- ☐

b. Betroffene personenbezogene Daten:

Beispiele:

- ☐ Nachname/Vorname
- ☐ Anschrift
- ☐ Geburtsort
- ☐ Familienstand
- ☐ Kontaktdaten (z. B. Telefon, E-Mail)
- ☐ Unterschrift
- ☐ Verkehrsdaten (z.B. Anschlusskennung, Standortdaten, Anfang/Ende einer Telefonverbindung)
- ☐ Vertragsstammdaten
- ☐ Personalstammdaten
- ☐ Abrechnungsdaten
- ☐ Kundenhistorie
- ☐ Nationalität
- ☐ Beruf
- ☐ Bankverbindung
- ☐

c. Sensible Daten / Besondere Kategorien von Daten i.S.v. Art. 9 DSGVO

Beispiele:

☐ Gesundheitsdaten
☐ genetische Daten
☐ biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
☐ Gewerkschaftszugehörigkeit
☐

2. Leistungsbeschreibung

Der Gegenstand der Auftragsverarbeitung sowie Art und Zweck ist im Hauptvertrag, insbesondere in der jeweiligen produktspezifischen Leistungsbeschreibung, beschrieben. Im Wesentlichen erbringt der Auftragnehmer diese zum Zwecke der zur Verfügungsstellung von Server-Infrastruktur sowie ggf. zzgl. zur Verfügungstellung von Speichermedien (dedizierte oder virtuelle Server) und die Erbringung von servernahen Diensten zur Aufrechterhaltung der Funktionsfähigkeit (je nach Hauptvertrag).

3. Verarbeitungsort:

Die Verarbeitung der Daten findet an folgenden Standorten statt:

- Fahrenheitstr. 11, 28359 Bremen
- Grasweg 62 – 66, 22303 Hamburg
- Notkestraße 13 – 15, 22607 Hamburg
- Am Tower 5, 90475 Nürnberg
- Haus 23, Balanstraße 73, 81541 München

Annex 2

Technische und organisatorische Sicherheitsmaßnahmen

Dieser Anhang beschreibt die technischen und organisatorischen Maßnahmen des Anbieters zum Zeitpunkt des Vertragsschlusses. Sofern der Anbieter während der Vertragslaufzeit Änderungen vornimmt, wird der Kunde über diese informiert, außer sie sind nur von unwesentlicher Bedeutung für die beauftragte Leistung.

Der Geltungsbereich für die hier referenzierten Dokumente erstreckt sich – wenn nicht explizit anders genannt – über die gesamte Organisation des Anbieters sowie seiner Tochterunternehmen. Zusätzlich gelten sie auch für die Anteile von Kundenumgebungen, die sich vertraglich in Betriebsverantwortung des Anbieters befinden.

Richtlinien, Standards, Verfahrensbeschreibungen und die Dokumentation der Durchführung der Verfahren sind interne Dokumente des Anbieters, die grundsätzlich Kunden oder Dritten weder in Papierform noch elektronisch zur Verfügung gestellt werden. Sie werden im Rahmen von Audits (ISO-Standards) und Prüfungen des internen Kontrollsystems („**IKS**“) intern und extern auditiert. Die Zertifikate (ISO27001 und ISO9001) sowie der Prüfbericht zum IKS werden den Kunden auf Anfrage zur Verfügung gestellt.

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

a. Datenschutz-Management

Datenschutz-management	Anforderung	Status
Datenschutzmanagement System für den Schutz personenbezogener Daten	Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist hauptamtlich bestellt und dem Vorstandsvorsitzenden direkt unterstellt.
	Datenschutzrichtlinie	Eine Datenschutzrichtlinie ist vorhanden und kann in den Räumlichkeiten des Anbieters eingesehen werden. Die Kenntnisnahme ist durch die Mitarbeiter des Anbieters zu bestätigen.
	Nachhaltige Verbesserung des Datenschutzmanagement Systems	Das Datenschutzmanagement System ist an den PDCA Zyklus des ISMS nach ISO27001 angegliedert. Dadurch wird gewährleistet, dass die technischen und organisatorischen Maßnahmen überprüft und entsprechende Verbesserungen dokumentiert und nachverfolgt werden.

Datenschutz-management	Anforderung	Status
	Überprüfung der Maßnahmen zum Datenschutz	Die Überprüfung der Datenschutzmaßnahmen erfolgt im Rahmen der internen Audits für die anderen Managementsysteme. Der Datenschutzbeauftragte ergänzt entsprechende Prüfungsanforderungen, unterstützt fachlich die Audits und definiert notwendige Maßnahmen.

b. Organisationskontrolle

Organisation	Anforderung	Status
Allgemeine organisatorische Maßnahmen	Informationssicherheitsmanagementsystem („**ISMS**“)	Auf Basis der ISO27001 wird beim Anbieter ein ISMS betrieben. Die ISMS-Strategie und die Informationssicherheit („**ISi**“) sind in der ISi-Leitlinie beschrieben. Die Controls der ISO27001 werden über das Statement of applicability („**SOA**“) und über weitere themenspezifische Dokumente referenziert.
	ISMS-Beauftragter	Die Rolle des ISMS-Beauftragten ist definiert und ist organisatorischer Bestandteil des Bereichs Interne Revision & Compliance.
	BCM Beauftragter	Die Rolle des BCM-Beauftragten ist definiert und ist organisatorischer Bestandteil des Bereichs Interne Revision & Compliance.
	Verantwortlicher für Informationssicherheit	Die Verantwortung für Umsetzung der Maßnahmen aus Informationssicherheit und Datenschutz liegt beim Chief Information Security Officer (CISO). Die Prüfung der Umsetzung erfolgt durch die interne Revision & Compliance (Datenschutz, ISMS und BCM).
	ISi-Richtlinie	Eine ISi-Richtlinie ist für alle Mitarbeiter im Zugriff und wird regelmäßig oder bei Bedarf aktualisiert. Die Kenntnisnahme ist durch die Mitarbeiter des Anbieters zu bestätigen. Sie kann in den Räumlichkeiten des Anbieters eingesehen werden.
	Kennwortrichtlinie	Eine Kennwortrichtlinie ist vorhanden und kann in den Räumlichkeiten des Anbieters eingesehen werden.
	Internes Kontrollsystem („**IKS**“)	Das IKS des Anbieters wird jährlich durch eine externe Wirtschaftsprüfungsgesellschaft geprüft (IDW PS 951).
	Risikomanagement	Ein Konzern-Risikomanagement ist etabliert und berichtet regelmäßig an den Vorstand.

Organisation	Anforderung	Status
	Verpflichtung und Schulungen der Mitarbeiter	Die Mitarbeiter des Anbieters werden bei Einstellung auf die Einhaltung des Datengeheimnisses / Datenschutzes (Art. 39 DSGVO), des Fernmeldegeheimnisses (§ 88 TKG) und der ISi-Richtlinie verpflichtet. Zusätzlich - soweit notwendig - auf das Sozialgeheimnis. Eine Sensibilisierung zu mindesten den genannten Themen erfolgt bei Einstellung und wird entsprechend Aufgabenbereich (z. B. Administratoren insbesondere ISi) jährlich in Schulungen aktualisiert.

c. Incident-Response-Management

Incident-Response-Management	Anforderung	Status
Umgang mit Sicherheitsvorfällen im Umfeld personenbezogener Daten	Der Umgang mit Sicherheitsvorfällen ist geregelt.	Der Prozess zur Sicherheitsvorfallbehandlung ist definiert und umgesetzt. In der Richtlinie zur Sicherheitsvorfallbehandlung sind Sicherheitsvorfälle, ihre Kategorisierung und Eskalationsverfahren sowie grundlegende Anforderungen und notwendige Verfahren definiert. Dabei sind Sicherheitsvorfälle mit personenbezogenen Daten entsprechend hoch klassifiziert. Die Umsetzung wird im Rahmen der internen Audits überprüft.
	Sicherheitsvorfälle werden bemerkt, es wird angemessen auf sie reagiert und sie werden dokumentiert und erforderlichenfalls nach Art. 33 DSGVO gemeldet.	Die Sicherheitsvorfallbehandlung ist eng mit den betrieblichen Prozessen verzahnt (IT Service Management, prozessuale Umsetzung entsprechend ITIL). Sowohl Messverfahren, als auch Alarmierung, Meldung, Reaktion, Eskalation und Dokumentation sind unter Berücksichtigung der Vorgaben aus der Richtlinie Sicherheitsvorfallbehandlung implementiert.

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

Datenschutzfreundliche Voreinstellungen	Anforderung	Status
Vorgabe und Überprüfung der Berücksichtigung von Datenschutzanforderungen bei Entwicklung, Einführung oder Änderungen an Services oder Systemen	Die Betrachtung dieses Aspekts ist in Verfahren zur Entwicklung / Einführung und Änderungen berücksichtigt, die Durchführung ist dokumentiert.	Für die Einführung neuer Systeme oder Technologien existiert eine Richtlinie, die das Verfahren beschreibt und den Aspekt der datenschutzfreundlichen Voreinstellungen berücksichtigt. Die Durchführung des beschriebenen Verfahrens wird dokumentiert.

e. Auftragskontrolle

Auftrag	Anforderung	Status
Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen den Parteien; Maßnahmen, die die Einhaltung von Weisungen des Kunden sicherstellen	Kriterien zur Auswahl des Auftragnehmers	Evaluationsverfahren durch den Einkauf des Anbieters.
	Prüfungen bei potentiellen Auftragnehmern	Evaluationsverfahren durch den Einkauf des Anbieters.
	Bewertung der IT-Sicherheit vor Auftragsentscheidung	Eine Bewertung der IT-Sicherheit des Auftragnehmers erfolgt vor Auftragsvergabe durch den Einkauf und durch den Kunden bzw. durch die fachlich verantwortliche Stelle.
	Eindeutige Vertragsgestaltung	Eine eindeutige Vertragsgestaltung mit Abgrenzung der Rechte und Pflichten der Parteien wird mit formalisierten Verträgen und Auftragsformularen sichergestellt.
	Kontrolle der Vertragsausführung	Regelmäßige Überprüfung, Vorlage von Prüfungsberichten.
	Weisungen	Weisungen werden nur schriftlich oder bei Eilmaßnahmen mit schriftlicher Bestätigung entgegengenommen.

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

a. Zutrittskontrolle

Zutritt	Anforderung	Status
Allgemeine Regelung Zutrittskontrolle	Regelung des Zutritts zu Datenverarbeitungsanlagen	Die Maßnahmen zur Zutrittssicherheit sind abhängig vom Einsatzzweck der Räumlichkeiten und dem Schutzbedarf der Systeme, die sich in ihnen befinden. Sensible Datenverarbeitungsanlagen befinden sich immer in entsprechend geschützten Räumlichkeiten wie z. B. den Rechenzentren („**RZ**“) des Anbieters. Grundlegende Maßnahmen folgen im Weiteren und sind detailliert im Dokument Anforderungen Zutrittssicherheit definiert.
Schutz der Räume mit Datenverarbeitungsanlagen vor dem Zutritt Unbefugter	Eingezäuntes Betriebsgelände	Die Betriebsgelände der Rechenzentren sind umzäunt.
	Alarmanlage, Videoüberwachung	Sensible Gebäude bzw. Gebäudeteile werden mit einer Videoanlage, z. T. mit Bewegungsmeldern und einer Einbruchmeldeanlage überwacht.
	Personenkontrolle beim Gebäudezutritt	Es existieren technische und organisatorische Maßnahmen zur Beschränkung des Zutritts zu geschützten Bereichen für interne und externe Personen. Dies umfasst die Kontrolle der Zutritte per Besucherliste, Tragepflicht von Mitarbeiter- und Gästeausweisen und stete Begleitung von Gästen. Ebenso existiert ein Rechtesystem für den Zutritt zu besonders schützenswerte Bereichen (z. B. RZ).

Zutritt	Anforderung	Status
	Zutrittskontrollsystem	Die Zutrittssteuerung an den RZ-Standorten erfolgt über ein Zutrittskontrollsystem (Transponderkarten mit elektronischem Türöffner, bei RZ-Zutritt zusätzlich PIN). Das System regelt und kontrolliert den Zutritt zum Grundstück und zu den Gebäuden.
	Schlüsselregelung / Schlüsselbuch	Die Schlüsselausgabe erfolgt durch den Wachdienst oder das zentrale Gebäudemanagement. Jeder ausgegebene Schlüssel wird in einem Schlüsselbuch oder einem Schlüsselmanagementsystem vermerkt.
	Weitere Überwachungseinrichtungen	An RZ-Standorten: 7 x 24 Stunden Wachdienst inkl. regelmäßigen Kontrollgängen; Videoüberwachung und Bewegungsmelder in den RZ-Fluren

b. Zugangskontrolle

Zugang	Anforderung	Status
Schutz der Computersysteme gegen den Zugang für Unbefugte	Zugang zu Systemen nur über Zugangsberechtigungen	Zum Zugang zu Systemen muss sich der Nutzer grundsätzlich mittels eines Verfahrens auf dem aktuellen Stand der Technik authentisieren. Bei Systemen mit besonders hohem Schutzbedarf bzw. kritischen Zugriffswegen sind zusätzliche Verfahren, wie z. B. eine Zwei-Faktor-Authentifizierung, etabliert. Fernwartungszugriffe und hier notwendige zusätzliche Maßnahmen sind in der „Fernwartungsrichtlinie“ dokumentiert.
	Berechtigungen nur nach Genehmigung	Die Zugangsberechtigung wird beantragt und von dem verantwortlichen Vorgesetzten und / oder dem Informationseigner genehmigt. Besondere Berechtigungen (z. B. Systemadministrator) bedürfen zudem der Genehmigung durch Beauftragte. Je nach Vereinbarung ist zusätzlich eine Genehmigung durch den Kunden erforderlich.
	Bedarfsbezogene Berechtigung	Der Zugang zu Applikationen und zu Informationen erfolgt auf Basis von Rollen und dem konkreten geschäftlichen Bedarf der Benutzer (Prinzip der minimalen Berechtigung/Need To Know Prinzip).
	Kennwortverfahren	Das Kennwortverfahren ist in der Kennwortrichtlinie dokumentiert. Passwortlänge, Komplexität, Gültigkeit und Historie werden verbindlich vorgegeben und die Vorgaben werden kontinuierlich an aktuelle Anforderungen angepasst.
	Protokollierung und Kontrolle fehlerhafter Anmeldungen	Fehlerhafte Anmeldungen werden soweit sinnvoll und technisch machbar protokolliert und bei Bedarf oder nach Kundenvereinbarung ausgewertet.

Zugang	Anforderung	Status
	Automatische Sperrung PC (z. B. Kennwort oder Pausenschaltung)	Eine automatische Sperrung des PC erfolgt nach einem festgelegten Zeitraum.
	Zugang zu Netzwerken	Unsichere Netze („**untrusted**“, z. B. Internet) werden durch Security Gateways (Firewalls, Proxy, SMTP-Gateways etc.) separiert und überwacht.
	Zugang über mobile Geräte	Der Zugang über mobile Geräte bzw. deren Einsatz wird über die ISi-Richtlinie und über die „Regeln für mobile Devices“ reglementiert und gesteuert.

c. Zugriffskontrolle

Zugriff	Anforderung	Status
Schutz der Daten gegen den Zugriff durch Unbefugte	Zugriff auf Daten nur über Zugriffsberechtigungen	Zum Zweck der Zugriffskontrolle erfolgt die Autorisierung von Benutzern über ein Rechte- bzw. Berechtigungssystem.
	Berechtigungsvergabe und -Entzug	Die Zugriffsberechtigung muss beantragt und von dem verantwortlichen Vorgesetzten genehmigt werden. Besondere Zugriffsberechtigungen bedürfen zudem der Genehmigung durch Beauftragte. Vergabe und Entzug von Zugriffsberechtigungen werden durch einen elektronischen Workflow unterstützt und dokumentiert. Der Berechtigungsprozess beinhaltet den Entzug von Zugriffsberechtigungen im Falle eines Wechsels in der Verantwortung oder bei Ausscheiden eines Mitarbeiters aus dem Unternehmen. Je nach Vereinbarung ist zusätzlich eine Genehmigung durch den Kunden erforderlich.
	Kontrolle der Berechtigungsvergaben	Eine Kontrolle der Berechtigungsvergaben erfolgt anlassbezogen und regelmäßig im Rahmen interner und externer Audits.
	Kontrollierte Vernichtung von Daten und Ausdrucken	Die kontrollierte Vernichtung von Daten und Ausdrucken erfolgt durch spezialisierte, zertifizierte Dienstleister.

d. Trennungskontrolle

Trennung	Anforderung	Status
Trennung der Datenbestände, die zu unterschiedlichen Zwecken verarbeitet werden	Mandantentrennung der Systeme	Die Überprüfung, ob eine Mandantentrennung von Daten und Funktionen notwendig ist, wird bei der Auswahl und Implementierung von Systemen berücksichtigt und wenn gegeben eingehalten, dokumentiert und überprüft.

Trennung	Anforderung	Status
	Zweckbindung der Systeme	Die Systeme werden gemäß den im Leistungsvertrag skizzierten Anforderungen zweckgebunden verwendet.
	Zweckbindung der Daten	Die Daten werden gemäß den im Leistungsvertrag skizzierten Anforderungen zweckgebunden verarbeitet.
	Trennung Produktivdaten von Testdaten	Eine Trennung der Kundenproduktivdaten von den Kundentestdaten erfolgt gemäß Vorgaben des Kunden (s. Leistungsvertrag).

e. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Pseudonymisierung	Anforderung	Status
Verschlüsselung von personenbezogenen Daten	Schutzbedarfsermittlung	Für die von der QSC AG verarbeiteten oder gespeicherten personenbezogenen Daten wurde ein Verzeichnis der Verarbeitungstätigkeiten erstellt. In diesem wird auch erfasst, ob es sich dabei um besonders schützenswerte Daten (besondere Kategorien personenbezogener Daten) handelt Die so klassifizierten Daten werden – soweit technisch umsetzbar - verschlüsselt gespeichert und übertragen.
	Definition und Verfügbarkeit von Verschlüsselungsverfahren	Für die Verschlüsselung von temporär lokal gespeicherten Daten auf mobilen Geräten und die dauerhafte Speicherung auf Netzlaufwerken sind Anwendungen und Verfahren definiert, die dem für die Daten Verantwortlichen die Verschlüsselung ermöglichen. Die Verschlüsselung dieser Daten an sich und die Nutzung der Verfahren ist über die Informationssicherheitsrichtlinie der QSC AG vorgeschrieben.
Verarbeitung in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können	Präferierte Pseudonymisierung von personenbezogenen Daten	Bei der Erhebung und Verarbeitung von personenbezogenen Daten wird geprüft, ob der Personenbezug notwendig ist oder notwendige Informationen auch pseudonymisiert zur Weiterverarbeitung / Speicherung ausreichen. Dies wird vor allem auch im Bereich der Logdaten berücksichtigt. Ist in besonderen Fällen aber der Rückschluss auf Personenbezug notwendig, wird der Personenbezug durch Aufhebung der Codierung wiederhergestellt. Dafür wurde ein System bei dem Anbieter etabliert, welches diese Funktion zentralisiert zur Verfügung stellt. Die Nutzung dieses Systems und damit die Möglichkeit den Personenbezug herzustellen ist durch je nach Art der Daten durch Betriebsvereinbarungen (interner Personenbezug) oder durch vertraglich geregelt (externer Personenbezug, z.B. personenbezogene Daten der Kunden).

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

a. Weitergabekontrolle

Weitergabe	Anforderung	Status
Schutz der Daten bei der Speicherung oder Übermittlung gegen unbefugtes Kopieren, Verändern oder Löschen	Organisatorische Festlegungen zur Aufbewahrung von Datenträgern	Die organisatorischen Festlegungen zur Aufbewahrung von Datenträgern erfolgt gemäß Vorgabe des Kunden (s. Leistungsvertrag).
	Geschützte Räume zur Datenaufbewahrung	Die Lagerung der Datensicherungen erfolgt entweder in einem geschützten Raum (z. B. Datenschutzraum, Rechenzentrum) des Anbieters oder extern durch einen geeigneten Dienstleister. Eine Ausnahme bildet die Berücksichtigung von Vorgaben des Kunden (s. Leistungsvertrag).
	Schutzmaßnahmen für Datenübertragung übers Internet	Die Datenübertragung zwischen vertrauenswürdigen Netzen über öffentliche / nicht vertrauenswürdige Netze erfolgt verschlüsselt.
	Physischer Datentransport, z. B. Bänder, nur durch Fachunternehmen	Der physische Datentransport von Datenträgern mit sensiblen oder potentiell sensiblen Daten (z. B. Datenvernichtung ohne explizit klassifizierte Daten) erfolgt in verschlossenen Spezialtransportbehältern. Die Übergabe der Daten an das Fachunternehmen wird protokolliert.
	Verschlüsselung von Datenträgern	Anbieterintern werden Daten auf mobilen Datenträgern grundsätzlich verschlüsselt, bei anderen Datenträgern hängt die Verschlüsselung von Einsatzart und der Klassifizierung der Daten ab. Eine Verschlüsselung von Datenträgern des Kunden erfolgt nach Vorgabe (s. Leistungsvertrag).
	Weitergabe der Daten an Dritte	Eine Weitergabe der Daten zur Weiterverarbeitung an Dritte erfolgt nur in Absprache mit dem Kunden oder gemäß Weisung des Kunden /der vertraglichen Vereinbarungen bzw. der gesetzlichen Notwendigkeiten.

b. Eingabekontrolle

Eingabe	Anforderung	Status
Nachweis der Dateneingabe oder -veränderung	Einsatz von Systemen mit Protokollfunktionen	Es werden Systeme mit Protokollfunktionen für relevante Daten eingesetzt.
	Aufbewahrung von Systemprotokollen	Protokolle werden entsprechend Standards (ISO27001) bzw. nach gesetzlichen Vorgaben aufbewahrt. Zusätzliche Anforderungen gemäß Auftrag des Kunden (s. Leistungsvertrag) werden berücksichtigt.

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

a. Verfügbarkeit

Verfügbarkeit	Anforderung	Status
Schutz der Daten gegen zufällige Zerstörung oder Verlust	Regelmäßige Datensicherungen	Die regelmäßigen Datensicherungen erfolgen gemäß Auftrag des Kunden (s. Leistungsvertrag).
	Spiegeln von Festplatten, z. B. RAID-Verfahren	Spiegeln von Festplatten, z. B. RAID-Verfahren, erfolgt gemäß Auftrag des Kunden (s. Leistungsvertrag).
	Schutzmaßnahmen gegen Brand und Wasser	Gesetzliche Vorgaben zum Brand- und Wasserschutz werden in allen Gebäuden eingehalten. Die Rechenzentren sind ISO27001 und nach weiteren TÜV Standards zertifiziert und entsprechen hohen Anforderungen an Brand- und Wasserschutz.
	Unterbrechungsfreie Stromversorgung („**USV**“)	Die Rechenzentren des Anbieters sind durch getrennte USV-Anlagen mit Batteriepufferung und Dieselgeneratoren gegen Stromausfälle gesichert. Die Hauseinführungen sind redundant implementiert.
	Getrennte Aufbewahrung	Eine räumlich getrennte Aufbewahrung von Daten erfolgt gemäß Auftrag des Kunden (s. Leistungsvertrag).
	Einsatz von Firewalls sowie Anti Viren / Anti Malware Software- und Systemen	Maßnahmen zum Schutz von Systemen und Umgebungen gegen unberechtigte Zugriffe, Viren und Malware sind im Gesamtumfeld des Anbieters definiert (Anforderungen Virenschutz und Virenschutzkonzept) und implementiert. Die kundenspezifischen Maßnahmen erfolgen nach Auftrag (s. Leistungsvertrag).

b. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Rasche Wiederherstellbarkeit	Anforderung	Status
Wiederherstellung personenbezogener Daten	Notfallplan	Notfallplan und entsprechende Handbücher zur Aufrechterhaltung der Kernprozesse im Notfall und zur möglichst raschen Wiederherstellung des Normalbetriebs sind vorhanden und etabliert.
	Notfalltests	Die für die Erfüllung des Notfallplans notwendigen Übungen und Tests sind definiert, werden durchgeführt und die Durchführung sowie Verbesserungsmaßnahmen werden dokumentiert.

Annex 3

Angaben zu Unterauftragsverarbeitern

Der Auftragsverarbeiter setzt Unterauftragsverarbeiter ein. Die jeweils aktuelle Liste der Unterauftragsnehmer ist im Internet unter der folgenden Adresse abrufbar:

https://www.plusnet-webservices.de/index.php/dsgvo/unterauftragsverarbeiter

Ziffer 7 Absatz (4) bleibt unberührt.