Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 Datenschutz-Grundverordnung

zwischen dem

Kunden

- Verantwortlicher gem. Art. 24 DS-GVO -

- nachfolgend „**Auftraggeber**“ -

und der

x-ion GmbH
Marschnerstr. 52
22081 Hamburg

- Auftragsverarbeiter gem. Art. 28 DS-GVO -

- nachfolgend „**Auftragnehmer**“ -

- beide nachfolgend gemeinsam „**Vertragsparteien**“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen.

Präambel

Die Vertragsparteien gehen mit Abschluss eines Vertrages zur Nutzung der Services von xCloud ein Auftragsverarbeitungsverhältnis nach Art. 28, 29 DS-GVO sowie EG 81 ff. DS-GVO ein. Um die Rechte und Pflichten der Vertragsparteien zum Datenschutz aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

Der Vertrag findet Anwendung auf alle Tätigkeiten, die Gegenstand der zugrunde liegenden Customer Order und deren Anlagen oder einer vergleichbaren vertraglichen Vereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Auftraggeber die gemäß Art. 4 Nr. 7 DS-GVO verantwortliche Stelle ist.

§ 2 Begriffsbestimmungen

Personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO sind alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen.
Sofern in dieser Vereinbarung der Begriff “Datenverarbeitung” oder “Verarbeitung” (von Daten) benutzt wird, wird damit allgemein die Verwendung von personenbezogenen Daten verstanden. Eine Verwendung personenbezogener Daten gemäß Art. 4 Nr. 2 DS-GVO umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung, Löschung sowie das Pseudonymisieren und darüber hinaus das Verschlüsseln und die sonstige Nutzung von Daten. Eine inhaltliche Aufgabenübertragung wird mit dieser Vereinbarung nicht getroffen.
Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO, welcher alleine über die Zwecke und Mittel der Verarbeitung personenbezogener Daten nach dieser Vereinbarung entscheidet.
Der Auftragnehmer ist Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO, der ausschließlich personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

§ 3 Konkretisierung des Auftragsinhalts

(1) Gegenstand, Zweck und Dauer der Auftragsverarbeitung sind in der Customer Order, einschließlich der dazugehörigen Anlagen oder einer vergleichbaren vertraglichen Vereinbarung, niedergelegt. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag des Auftraggebers. Die Verarbeitungstätigkeit des Auftragnehmers beschränkt sich hierbei auf das Anbieten der Services von xCloud, in welcher die personenbezogenen Daten lediglich gemäß Art. 4 Nr. 2 DS-GVO erfasst und gespeichert werden. Es erfolgt weder ein Zugriff noch eine Kenntnisnahme des Inhalts sämtlicher Daten durch den Auftragnehmer. Im Rahmen einer Service- oder Support-Anfrage (Weisung) durch den Auftraggeber ist dem Auftragnehmer der Zugriff auf

bestimmte Daten ausnahmsweise gestattet, um der jeweiligen Anfrage nachzukommen. Die technische Umsetzung von xCloud ist in Anhang 2 beschrieben.

(2) Die Erbringung der vertraglich vereinbarten Verarbeitung findet ausschließlich in einem Mitgliedstaat 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. Das angemessene Schutzniveau wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DS-GVO).

(3) Gegenstand dieser Vereinbarung sind solche personenbezogenen Daten, die dem Auftragnehmer durch den Auftraggeber zur Verfügung gestellt werden. Für die Verarbeitung dieser Daten durch den Auftragnehmer ist die Art der Daten, die jeweilige Kategorie der Daten sowie die Kategorie der betroffenen Personen nicht relevant. Es bedarf somit keiner detaillierten Aufzählung.

§ 4 Weisungsbefugnis des Auftraggebers

(1) Weisungen durch den Auftraggeber werden anfänglich durch die dem Vertrag zugrunde liegende Customer Order, einschließlich der dazugehörigen Anhänge oder in einer vergleichbaren vertraglichen Regelung, festgelegt und können im weiteren Verlauf durch den Auftraggeber gegenüber dem Auftragnehmer oder eine durch den Auftragnehmer bezeichnete Stelle geändert, ersetzt oder ergänzt werden. Weisungen, welche im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

(2) Die Weisungen durch den Auftraggeber können in schriftlicher Form, elektronischer Form (Textform) oder mündlich erfolgen.

(3) Mündliche Weisungen sind unverzüglich durch den Auftraggeber schriftlich oder in elektronischer Form (Textform) zu bestätigen.

(4) Der Auftragnehmer ist dazu verpflichtet, jede durch den Auftraggeber erteilte Weisung in schriftlicher oder elektronischer Form (Textform) zu dokumentieren (Dokumentationspflicht des Auftragnehmers gemäß Art. 28 Abs. 3 S. 2 lit. a DS-GVO)

(5) Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf personenbezogene Daten ausschließlich im Rahmen des Auftragsverhältnisses sowie der erteilten Weisungen durch den Auftraggeber verarbeiten (Ausnahme: Art. 28 Abs. 3 S. 2 lit. a DS-GVO). Der Auftragnehmer darf die Daten für keine anderen Zwecke verwenden und ist insbesondere nicht berechtigt, die ihm überlassenen Daten an Dritte weiterzugeben.

(2) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO i.V.m. § 62 BDSG; insofern gewährleistet er insbesondere die Einhaltung folgender datenschutzrechtlicher Vorgaben:

1. Datenschutzbeauftragter

a. Schriftliche Benennung eines Datenschutzbeauftragten gemäß Art. 37 DS-GVO, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
b. Die Kontaktdaten des Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
c. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
d. Die jeweils aktuellen Kontaktdaten des Datenschutzbeauftragten sind veröffentlicht und in leicht zugänglicher Weise hinterlegt, gem. Art. 37 Abs. 7 DS-GVO.

2. Vertraulichkeit

a. Der Auftragnehmer gewährleistet, dass es den mit der Datenverarbeitung befassten Mitarbeiter und jeder anderen dem Auftragnehmer unterstellten Personen untersagt ist, eine Verarbeitung außerhalb der durch den Auftraggeber erteilten Weisung durchzuführen, i.S.d. Art. 28 Abs. 3 S. 2 lit. a DS-GVO, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
b. Der Auftragnehmer gewährleistet des Weiteren, dass sich die zur Datenverarbeitung befugten Personen sowie allen weiteren Personen, die entsprechend der vertraglichen Verpflichtung mit personenbezogenen Daten in Berührung kommen, zur Vertraulichkeit verpflichtet haben und vor dem Beginn ihrer jeweiligen Tätigkeit mit den für sie relevanten datenschutzrechtlichen Bestimmungen vertraut gemacht worden sind, gem. Art. 28 Abs. 3 S. 2 lit. b DS-GVO.

3. Sicherheit der Verarbeitung

a. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten sowie zur Minderung potentieller nachteiliger Folgen der jeweils betroffenen Personen und setzt sich hierzu unverzüglich mit dem Auftraggeber in Verbindung.
b. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 DS-GVO vollumfänglich nachzukommen, und solche Maßnahmen zur Sicherheit der Verarbeitung zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
c. Der Auftragnehmer verpflichtet sich zur Umsetzung und Einhaltung aller für den vorliegenden Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c DS-GVO, sowie zu einer regelmäßigen Überprüfbarkeit gemäß Art. 28 Abs. 3 S. 2 lit. e DS-GVO i.V.m. Art. 32 Abs. 1 lit. d DS-GVO [Einzelheiten in Anlage 1: TOMs]

4. Zusammenarbeit mit den Aufsichtsbehörden

   a. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen, gemäß Art. 31 DS-GVO.
   b. Der Auftragnehmer hat den Auftraggeber über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörden unverzüglich zu informieren, soweit sich diese auf den vorliegenden Auftrag beziehen.

5. Unterstützung des Auftraggebers

   a. Der Auftragnehmer hat den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen nach Kapitel III der DS-GVO sowie der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten nach bestem Wissen zu unterstützen.

6. Informationspflichten

   a. Der Auftragnehmer hat den Auftraggeber unverzüglich darüber zu informieren, soweit eine Ermittlung in Bezug auf die Auftragsverarbeitung durch eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten stattfindet.
   b. Der Auftragnehmer hat den Auftraggeber unverzüglich davon in Kenntnis zu setzen, soweit ihm Verletzungen personenbezogener Daten des Auftraggebers bekannt werden.
   c. Der Auftragnehmer hat den Auftraggeber nach bestem Wissen und Gewissen zu unterstützen, soweit der Auftraggeber seinerseits einer Kontrolle durch eine Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahrens, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, oder anderen mit der Auftragsverarbeitung zusammenhängenden Ansprüchen ausgesetzt ist.

7. Anfragen von Betroffenen

   a. Der Auftragnehmer hat den Auftraggeber nach bestem Wissen bei der Wahrnehmung von Betroffenenrechten zu unterstützen. Hierbei ist der Auftragnehmer dazu verpflichtet, mittels der jeweils geeigneten technischen und organisatorischen Maßnahmen den Auftraggeber bei Beantwortung der Anfragen von Betroffenen im Rahmen seiner rechtlichen und tatsächlichen Möglichkeiten zu unterstützen.

§ 6 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Der Auftragnehmer wird innerhalb seines Verantwortungsbereichs die innerbetriebliche Organisation so gestalten, dass diese den besonderen Anforderungen des Datenschutzes ausnahmslos gerecht wird. Hierbei wird er technische und organisatorische Maßnahmen zu einem angemessenen Schutz der zu verarbeiteten Daten treffen, welche den Anforderungen der Datenschutzgrundverordnung (Art. 32 DS-GVO) ausnahmslos und in vollem Umfang genügen.

(2) 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. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen so zu gestalten, dass Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung sichergestellt sind und ein dem Risiko der genannten Merkmale entsprechendes Schutzniveau gemäß Art. 28 Abs. 3 lit. c DS-GVO i.V.m. Art. 32 DS-GVO und Art. 5 DS-GVO gewährleistet wird. 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 [Einzelheiten in Anlage 1: TOMs].

(4) 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 Personen gewährleistet wird.

(5) Der Auftragnehmer gewährleistet gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen nach § 8 dieses Vertrages.

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

(7) 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.

§ 7 Pflichten des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer verantwortlich, gemäß Art. 4 Nr. 7 DS-GVO.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich darüber zu informieren, soweit er in den Auftragsergebnissen Fehler oder sonstige Unregelmäßigkeiten hinsichtlich der datenschutzrechtlichen Bestimmungen feststellt.

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

§ 8 Kontrollrechte des Auftraggebers

(1) Sollten im Einzelfall Inspektionen (in Form von Stichprobenkontrollen) durch den Auftraggeber oder einen durch diesen beauftragten Personen (Prüfer) erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung bei dem Auftragnehmer unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Hierbei erhält der Auftraggeber die Gelegenheit, sich von der Einhaltung dieser Vereinbarung innerhalb des Geschäftsbetriebes des Auftragnehmers, zu überzeugen.

(2) Der Auftragnehmer ist dazu berechtigt, die Durchführung einer in § 8 Abs. 1 genannten Stichprobenkontrolle von einer vorherigen, ordnungsgemäßen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung bezüglich sämtlicher Daten sowie der eingerichteten technischen und organisatorischen Maßnahmen abhängig zu machen.

(3) 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.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann 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);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(5) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer, soweit dies vertraglich vereinbart wurde, einen Vergütungsanspruch geltend machen.

§ 9 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, so wird dieser die betroffene Person an den Auftraggeber verweisen, sofern dem Auftragnehmer eine Zuordnung nach den Angaben der betroffenen Person möglich ist. Der Auftragnehmer verpflichtet sich dazu, den Antrag der entsprechenden Person unverzüglich an den Auftraggeber weiterzuleiten.

(2) Eine Haftung des Auftragnehmers ist ausgeschlossen, soweit das Ersuchen der betroffenen Person durch den Auftraggeber nicht, nicht vollständig oder nicht fristgerecht bearbeitet werden kann.

§ 10 Subunternehmer

(1) Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter neben dem Auftragnehmer ist zulässig, soweit der Auftraggeber im Vorfeld eine Zustimmung abgegeben hat, welche ausschließlich in schriftlicher Form gemäß Art. 28 Abs. 2 S. 1 DS-GVO zu erfolgen hat.

(2) Die Zustimmung kann sowohl in allgemeiner Form als auch in konkreter Form (speziell für den jeweiligen Unterauftrag) durch den Auftraggeber abgegeben werden, gemäß Art. 28 Abs. 2 DS-GVO.

(3) Ein zustimmungsbedürftiges Subunternehmerverhältnis im Sinne des § 10 Abs. 1 dieser Vereinbarung liegt vor, soweit der Auftragnehmer weitere Auftragnehmer beauftragt, die vertraglich vereinbarte Leistung vollständig oder teilweise zu erbringen. Als Subunternehmerverhältnisse 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, Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(4) Bei Inanspruchnahme von Subunternehmern durch den Auftragnehmer, hat der Auftragnehmer sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau inklusive der technischen und organisatorischen Maßnahmen mindestens der Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer entspricht und alle gesetzlichen und vertraglichen Pflichten beachtet werden. Der Auftragnehmer ist 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.

(5) Soweit der Auftraggeber dem Auftragnehmer eine allgemeine Zustimmung in schriftlicher Form erteilt hat, welche sich auf die Hinzuziehung weiterer Auftragsverarbeiter (Subunternehmer) bezieht, ist der Auftragnehmer zur Beauftragung weiterer

Auftragnehmer bzw. zur Auswechslung bestehender Auftragnehmer berechtigt, soweit folgende Voraussetzungen kumulativ erfüllt sind:

a) Der Auftraggeber wird durch den Auftragnehmer bezüglich eines jeden Einzelfalles einer weiteren Beauftragung innerhalb eines angemessenen Zeitraums im Vorfeld in Kenntnis gesetzt,
b) der Auftraggeber gegen diese Beauftragung nicht innerhalb von 14 Tagen Widerspruch im Rahmen des Weisungsrechts gegenüber der durch den Auftragnehmer bezeichnete Stelle erhoben hat gem. Art. 28 Abs. 2 S. 2 DS-GVO sowie
c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Erfolgt kein Widerspruch durch den Auftraggeber innerhalb der vorgegebenen Frist, ist eine wirksame Zustimmung in Bezug auf die weitere Beauftragung gegeben.

(6) Der Auftragnehmer trifft die Auswahlentscheidung hinsichtlich der Hinzuziehung weiterer Subunternehmer, gemäß Art. 28 Abs. 4 DS-GVO. Der Auftragnehmer verpflichtet sich dazu, im Rahmen seiner Auswahlentscheidung die in Art. 28 Abs. 4 S. 1 DS-GVO genannten Grundsätze einzuhalten. Dem Subunternehmer sind hierbei in schriftlicher Form die gleichen Verpflichtungen aufzuerlegen, welche für den Auftragnehmer nach Art. 28 Abs. 3 DS-GVO bestehen.

(7) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen Aufnahme der Verarbeitungstätigkeit ist unzulässig, soweit nicht alle Voraussetzungen für eine Subunternehmerbeauftragung gemäß § 10 Abs. 1, 3 und 4 dieser Vereinbarung vorliegen.

(8) Der Auftragnehmer hat den jeweiligen Subunternehmer dazu zu verpflichten, die geeigneten technischen und organisatorischen Maßnahmen zu treffen, um eine der Datenschutz-Grundverordnung konforme Verarbeitung sicherzustellen.

(9) Erbringt der Subunternehmer die vereinbarte Leistung außerhalb der EU/des EWR, so ist der Auftragnehmer dazu verpflichtet die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicherzustellen.

(10) Die Auslagerung durch den Subunternehmer an einen weiteren Auftragnehmer (Sub-Subunternehmer) bedarf der ausdrücklichen Zustimmung in Schriftform sowohl durch den Auftraggeber als auch durch den Auftragnehmer. Die in dieser Vereinbarung niedergelegten Bestimmungen gelten in gleichem Umfang für den weiteren Unterauftragnehmer.

(11) Soweit der Auftragnehmer ein Auftragsverhältnis mit einem weiteren Subunternehmer eingeht, steht es dem Auftragnehmer frei, seine datenschutzrechtlichen Pflichten aus dem Hauptvertrag auf diesen zu übertragen.

§ 11 Informationspflichten / Mitteilung bei Verstößen des Auftragnehmers / Meldepflichten bei Datenpannen

(1) Der Auftragnehmer hat den Auftraggeber unverzüglich davon in Kenntnis zu setzen, soweit die mit dem Auftragsverhältnis in Zusammenhang stehenden Daten durch Pfändung oder Beschlagnahme, ein Insolvenz - oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden oder diesbezüglich eine Vermutung seitens des Auftragnehmers besteht. Der Auftragnehmer ist dazu verpflichtet, sämtliche in diesem Zusammenhang Zuständige unverzüglich darüber in Kenntnis zu setzen, dass die Hoheit an den jeweiligen Daten ausschließlich dem Auftraggeber angehören.

(2) 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 unter anderem:

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 und
e. die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(3) Die den Auftraggeber unterstützende Informationspflicht des Auftragnehmers bezieht sich zudem uneingeschränkt auf sämtliche Pflichten des Auftraggebers gemäß Art. 28 DS-GVO sowie auf Überprüfungen, welche durch den Auftragnehmer oder von diesem beauftragten Personen durchgeführt werden, gemäß Art. 28 Abs. 3 S. 2 lit. h DS-GVO.

(4) Der Auftragnehmer hat den Auftraggeber unverzüglich im Sinne des § 121 Abs. 1 S. 1 BGB zu informieren, soweit er seiner subjektiven Einschätzung zufolge der Meinung ist, eine durch den Auftraggeber erteilte Weisung verstoße gegen anwendbare Datenschutzvorschriften oder sonstiges Recht. Der Auftraggeber ist verpflichtet, auf die Information des Auftragnehmers hin unverzüglich tätig zu werden.

(5) Der Auftragnehmer ist zur Unterstützung des Auftraggebers nur insofern verpflichtet, soweit die Tätigkeit des Auftraggebers nicht dem rechtswidrigen Bereich unterliegt (besondere Treuepflicht des Auftragnehmers).

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

§ 12 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer ist zur Berichtigung oder Löschung der vertragsgegenständlichen Daten berechtigt und verpflichtet, soweit der Auftraggeber dies anweist. Die Anweisung durch den Auftraggeber hat ausschließlich in dokumentierter Form zu erfolgen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Ist es dem Auftragnehmer unmöglich, die vertragsgegenständlichen Daten zu löschen oder eine Einschränkung der Datenverarbeitung vorzunehmen, so ist der Auftragnehmer zu einer datenschutzkonformen Vernichtung der entsprechenden Daten oder Datenträger berechtigt soweit dies durch eine Einzelbeauftragung durch den Auftraggeber umfasst ist. Alternativ ist der Auftragnehmer dazu berechtigt, die Datenträger und sonstige Materialien an den Auftraggeber zurückzugeben.

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

§ 13 Löschung und Rückgabe von personenbezogenen Daten

(1) Zu einer Erstellung von Kopien oder Duplikaten der vertragsgegenständlichen Daten ist der Auftragnehmer berechtigt, soweit diesbezüglich eine Zustimmung durch den Auftraggeber vorliegt. 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) Der Auftragnehmer ist dazu verpflichtet, sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Daten, Datenträger oder sonstige Materialien, die in einem Zusammenhang mit der Auftragstätigkeit stehen, zu löschen, herauszugeben oder auf datenschutzkonforme Art und Weise zu vernichten, soweit dies durch den Auftraggeber verlangt wird. Gleiches gilt für Test- und Ausschussmaterial. Der Auftragnehmer hat das Protokoll der Löschung auf Anforderung des Auftraggebers diesem zur Verfügung zu stellen.

(3) Der Auftragnehmer ist spätestens zum Zeitpunkt der Beendigung des Auftragsverhältnisses zu einer vollständigen Löschung der in § 13 Abs. 1 dieser Vereinbarung genannten Materialien verpflichtet.

(4) 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.

(5) Der Auftragnehmer kann zu einer Speicherung der vertragsgegenständlichen Daten nach Beendigung des Auftragsverhältnisses verpflichtet sein, soweit nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine solche Verpflichtung zur Speicherung von personenbezogenen Daten besteht, gemäß Art. 28 Abs. 3 S. 2 lit. g DS-GVO.

§ 14 Haftung und Schadensersatz

Der Auftraggeber und der Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO genannten Regelungen.

§ 15 Schlussbestimmungen

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

(2) Soweit ein Vertragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer nicht zustande kommt, verliert die nachfolgend unterzeichnete Vereinbarung entsprechend ihre Wirkung und ist somit nichtig.

(3) Beim Auftreten etwaiger Widersprüche gehen die Regelungen dieses Vertrages den Regelungen der Customer Order vor.

(4) Sollten Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(5) Neben dem Recht der Europäischen Union findet das deutsche Recht Anwendung.

(6) Dieser Vertrag ist ohne Unterschrift gültig.

Anlage 1: Technisch organisatorische Maßnahmen (TOMs)

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

Rechenzentren

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Rechenzentren: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen, Vereinzelungsanlagen;

Büroräume der x-ion

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Büroräumen: Zutrittskarten, Schlüssel, Empfang, Videoanlagen mit Alarmierung;

Global

- Zugangskontrolle
  Keine unbefugte Systemnutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

Global

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

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

Rechenzentren

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Meldewege und Notfallpläne

Büroräume der x-ion

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie, unterbrechungsfreie Stromversorgung (USV), Meldewege und Notfallpläne

Global

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

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

Global

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
- Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.