Vertrag über die Auftragsverarbeitung (Art. 28 Abs. 3 DSGVO)

Dieser Vertrag gilt zwischen dem Kunden (nachfolgend bezeichnet als „Auftraggeberin“) und der SuperX GmbH, vertreten durch den Geschäftsführer Yilmaz Köknar und Mika Hally, Prenzlauer Allee 242-247, 10405 Berlin (nachfolgend bezeichnet als „Auftragnehmerin“). Die Parteien haben einen Nutzungsvertrag über die Messaging-Software „Superchat“ abgeschlossen. In Ergänzung zum Nutzungsvertrag vereinbaren die Parteien hiermit Folgendes:

1. Gegenstand dieses Vertrages und der Verarbeitung, Umfang der Weisungsbefugnisse

1.1 Gegenstand dieses Vertrages ist die Zusammenarbeit der Parteien im Rahmen des Nutzungsvertrages. Die Durchführung des Nutzungsvertrages beinhaltet die im **Anhang 1** benannten datenverarbeitenden Tätigkeiten der Auftragnehmerin für die Auftraggeberin.

1.2 Die Auftragnehmerin verarbeitet die ihr im Rahmen des Nutzungsvertrages zugänglichen personenbezogenen Daten im Auftrag der Auftraggeberin (Art. 28 DSGVO). Die Auftragnehmerin wird die Daten ausschließlich und streng nach den auftragsbezogenen Weisungen der Auftraggeberin erheben, verarbeiten und nutzen; die Ziele und Modalitäten der Auftragsverarbeitung kann allein die Auftraggeberin bestimmen.

1.3 Die Verantwortung für das Erstellen und Umsetzen des Löschungskonzepts, die Durchführung des Rechts auf Vergessenwerden, auf Berichtigung, Datenportabilität und Auskunft sind nicht Gegenstand dieses Vertrages. Diese wird allein die Auftraggeberin sicherstellen.

1.4 Die vereinbarte Verarbeitungstätigkeit durch die Auftragnehmerin findet grundsätzlich innerhalb der Europäischen Union und des Europäischen Wirtschaftsraums statt. Sofern Verarbeitungstätigkeiten durch Unterauftragnehmer in Drittländern erbracht werden, ist dies in **Anhang 2** entsprechend aufgeführt und es liegt für das betreffende Drittland entweder ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO vor oder es sind Standarddatenschutzklauseln mit sonstigen geeigneten Garantien nach Art. 46 DSGVO abgeschlossen.

1.5 Außerhalb der Betriebsstätte der Auftragnehmerin findet folgende Datenverarbeitung statt an folgenden Orten statt:

- Die Auftragnehmerin erlaubt ihren Mitarbeitern die Arbeit aus dem Home-Office. Hierfür gelten bei der Auftragnehmerin Regelungen zum Datenschutz, auf deren Einhaltung sich die Mitarbeiter verpflichtet haben.
- Bei den Unterauftragnehmern an den Standorten, die alle in Anhang 2 benannt sind.

2. Art und Zweck der Verarbeitung

2.1 Für die Durchführung des Nutzungsvertrages mit der Auftraggeberin ist der Zugriff auf personenbezogene Daten notwendig.

2.2 Die Zwecke der Auftragsverarbeitung sind in **Anhang 1** benannt. Die Auftragsverarbeitung erfolgt nur für die Zwecke der Durchführung des Nutzungsvertrages mit der Auftraggeberin; eine Verwendung für andere Zwecke erfolgt nicht. Den Mitarbeitern der Auftragnehmerin ist es untersagt, geschützte personenbezogene Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu erheben, zu verarbeiten oder zu nutzen. Die Auftragnehmerin hat keine eigene Entscheidungsbefugnis über den Umgang mit den Daten und bewahrt diese so auf, wie von der Auftraggeberin bestimmt.

3. Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1 Die Arten der personenbezogenen Daten, die von der Datenverarbeitung durch die Auftragnehmerin betroffen sind, sind in **Anhang 1** aufgelistet.

3.2 Die Personengruppen, die zum Kreis der durch die Verarbeitung betroffenen Personen gehören, sind in **Anhang 1** aufgelistet.

4. Rechte und Pflichten der Auftraggeberin

4.1 Die Prüfung der Zulässigkeit der Datenverarbeitung und die Wahrung der Rechte der Betroffenen obliegen stets der Auftraggeberin. Die Auftraggeberin übernimmt die ihr nach den Datenschutzbestimmungen obliegenden Meldepflichten in eigener Verantwortung (Art. 33, 34 DSGVO).

4.2 Die Auftraggeberin bestätigt mündlich erteilte Weisungen stets in Textform oder in einer zwischen den Parteien vereinbarten sonstigen elektronischen Form (z. B. Ticketing). Änderungen des Verarbeitungsgegenstandes oder Verfahrensänderungen stimmt die Auftraggeberin vorab gemeinsam mit der Auftragnehmerin ab; die Parteien treffen hierzu eine entsprechende Festlegung in Textform.

4.3 Für die Auftraggeberin sind in **Anhang 1** genannten Personen gegenüber der Auftragnehmerin berechtigt, auftragsbezogene Weisungen zu erteilen.

4.4 Die Auftraggeberin wird die Auftragnehmerin über den Wechsel einer der nach Ziffer 4.3 dieses Vertrages benannten Personen in geeigneter Form informieren.

4.5 Die Auftraggeberin ist berechtigt, bei der Auftragnehmerin jederzeit die Einhaltung der Datenschutzbestimmungen, der hier getroffenen vertraglichen Vereinbarungen und erteilter Weisungen zu überprüfen. Der betriebliche Datenschutzbeauftragte und der von der Auftraggeberin beauftragte Prüfer erhalten im Rahmen der Überprüfung auch Zutritt zu den Räumlichkeiten der Auftragnehmerin, in denen die vereinbarte Verarbeitung für die Auftraggeberin stattfindet, insbesondere zu den entsprechenden Softwareapplikationen, Serverräumen, zur Betriebssoftware und den sonstigen für die Verarbeitung

im Auftrag genutzten IT-Systemen. Die Auftragnehmerin kann diesem Kontrollrecht der Auftraggeberin durch Übermittlung eines jährlichen Datenschutzberichts oder genehmigter Verhaltensregeln (Art. 40 DSGVO) oder eines genehmigten Zertifikats oder Datenschutzsiegels oder Datenschutzprüfzeichens im Sinne von Art. 42 DSGVO genügen. Das gleiche gilt für die Auswahl und Erstmalige Überprüfung der Auftragnehmerin vor Aufnahme der vorliegend vereinbarten Verarbeitungstätigkeit.

4.6 Die Auftraggeberin hat das Recht, jederzeit die Herausgabe der im Rahmen dieses Vertrages verarbeiteten und/oder neu entstehenden oder entstandenen Daten, Daten-ergebnisse oder Datenbestände zu verlangen. Alle Rechte und das Eigentum an diesen Daten, Datenergebnissen oder Datenbeständen stehen allein der Auftraggeberin als Inhaber und allein berechtigter Eigentümerin zu. Mit Daten, Datenergebnissen oder Datenbeständen sind die technisch in einer Systemumgebung (Datenträger) gespeicherten Abbildungen von Informationen gemeint. Die Rechte zur Nutzung der in diesen Daten, Datenergebnissen oder Datenbeständen enthaltenen Informationen stehen ausschließlich der Auftraggeberin zu. Die Auftragnehmerin hat diesbezüglich kein Zurückbehaltungsrecht (§§ 273, 320 BGB). Etwaige urheberrechtliche Nutzungs- oder Lizenzrechte (z. B. an der Software) bleiben davon unberührt.

5. Weitere Rechte und Pflichten der Auftragnehmerin

5.1 Die in **Anhang 1** genannten Personen sind für die Auftragnehmerin befugt, die Weisungen der Auftraggeberin entgegenzunehmen.

5.2 Die Auftragnehmerin wird die in Ziffer 3 bzw. **Anhang 1** dieses Vertrages genannten personenbezogenen Daten nur nach dokumentierter Weisung der Auftraggeberin verarbeiten, berichtigen, löschen oder sperren. Sie wird die Auftraggeberin nach Möglichkeit bei der Erfüllung der Pflichten zu den Rechten betroffener Personen (Art. 12 bis Art. 23 DSGVO) unterstützen. Soweit eine betroffene Person sich unmittelbar an die Auftragnehmerin zwecks Berichtigung oder Löschung der eigenen personenbezogenen Daten wenden sollte, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

5.3 Die Auftragnehmerin führt ein eigenes Verzeichnis über die Verarbeitungstätigkeit. Sie wird an der Erstellung von Verzeichnissen über die Verarbeitungstätigkeit und Datenschutz-Folgenabschätzungen der Auftraggeberin mitwirken und der Auftraggeberin die dafür benötigten Informationen – soweit möglich und bei der Auftragnehmerin vorhanden – bereitstellen. Darüber hinaus wird die Auftragnehmerin die Auftraggeberin im Umfang der der Auftragnehmerin zur Verfügung stehenden Informationen auch bei der Einhaltung der Pflichten unterstützen, die der Auftraggeberin nach Art. 32 bis Art. 36 DSGVO zukommen. Dies gilt insbesondere für die Meldungen an die Aufsichtsbehörde oder Benachrichtigungen der betroffenen Personen im Falle von Datenschutzverletzungen oder für die Konsultationen der Aufsichtsbehörde im Falle von hohen Verarbeitungsrisiken als Ergebnis der Datenschutz-Folgenabschätzungen.

5.4 Alle Unterlagen und/oder Datenträger und/oder Datenbestände mit personenbezogenen Daten der Auftraggeberin wird die Auftragnehmerin so verwahren, dass sie von denjenigen weiterer Kunden der Auftragnehmerin getrennt und vor der Kenntnis bzw. dem Zugriff Unbefugter geschützt sind. Soweit möglich, wird die Auftragnehmerin den Eingang und Ausgang dokumentieren.

5.5 Die Auftragnehmerin hat die im **Anhang 1** genannte Person als betrieblichen Beauftragten für den Datenschutz ordentlich bestellt (Art. 37 DSGVO). Sollte dieser Datenschutzbeauftragte wechseln, wird die Auftragnehmerin die Auftraggeberin unverzüglich darüber unterrichten. Der betriebliche Datenschutzbeauftragte ist im Unternehmen der Auftragnehmerin für die Einhaltung des Datenschutzes zuständig.

5.6 Die Auftragnehmerin wird die Auftraggeberin von auftragsbezogenen Störungen im Betriebsablauf, Verletzungen von Datenschutzbestimmungen (auch durch Weisungen der Auftraggeberin), Kontrollen und Maßnahmen der Aufsichtsbehörden und anderen Unregelmäßigkeiten unverzüglich unterrichten. Die Auftragnehmerin unterstützt die Auftraggeberin bei der Erfüllung der Meldepflichten, die der Auftraggeberin im Fall von Datenschutzverletzungen nach den Datenschutzbestimmungen (Art. 33, 34 DSGVO) obliegen.

5.7 Macht eine betroffene Person oder ein Dritter einen Anspruch im Zusammenhang mit der vorliegenden Auftragsverarbeitung gegen die Auftragnehmerin oder die Auftraggeberin geltend, wird die Auftragnehmerin die Auftraggeberin mit den zur Verfügung stehenden Informationen unterstützen.

5.8 Die Auftragnehmerin ist berechtigt, die Durchführung von Weisungen, die nach Ansicht der Auftragnehmerin Datenschutzbestimmungen verletzen, solange auszusetzen, bis die Auftraggeberin diese bestätigt oder geändert hat.

5.9 Die Auftragnehmerin wird es der Auftraggeberin ermöglichen, die der Auftraggeberin nach Ziffer 4.5 dieses Vertrages zustehenden datenschutzrechtlichen Kontrollrechte durchzuführen und wahrzunehmen.

5.10 Die Auftragnehmerin wird es ihren Mitarbeitern nur mit vorheriger ausdrücklicher Zustimmung der Auftraggeberin gestatten, Tätigkeiten für die Auftraggeberin aus dem häuslichen Büro (Home-Office) zu erledigen. Die Zustimmung dazu gilt mit Unterzeichnung dieses Vertrages als erteilt. Im Falle einer solchen Tätigkeit wird die Auftragnehmerin sicherstellen, dass die Mitarbeiter Regelungen zum Datenschutz bei der Arbeit aus dem häuslichen Büro einhalten.

5.11 Die Aufwände, die der Auftragnehmerin für die Durchführung dieses Vertrages und durch die Erbringung von Unterstützungs- oder Dokumentationsleistungen nach den vorstehenden

Ziffern 5.2, 5.3, 5.6, 5.8 und 5.9 dieses Vertrages entstehen, sind mit der Zahlung der zwischen den Parteien für die Leistungsvereinbarung festgelegten Vergütung abgegolten.

6. Technische und organisatorische Maßnahmen

6.1 Die Auftragnehmerin hat im Zeitpunkt des Abschlusses dieses Vertrages bereits nachweislich alle für den vorliegenden Auftrag nach Art. 32 DSGVO erforderlichen und angemessenen technischen und organisatorischen Maßnahmen (TOM) zur Datensicherheit getroffen, die die Auftraggeberin akzeptiert hat. Diese sind in **Anhang 3** zu diesem Vertrag im Einzelnen beschrieben und entsprechen dem nach Art. 32 Abs. 1 DSGVO geregelten Maßnahmenkatalog. **Anhang 3** zu diesem Vertrag wird hiermit Vertragsbestandteil.

6.2 Bei der Auswahl der konkreten TOM wird die Auftragnehmerin folgende Kriterien berücksichtigen:

- den Stand der Technik;
- die Implementierungskosten;
- die Art, den Umfang, die Umstände und die Zwecke der vorliegenden Verarbeitung;
- die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen natürlichen Personen.

6.3 Die Auftragnehmerin verpflichtet sich, stets ein angemessenes Schutzniveau der getroffenen TOM zu gewährleisten. Bei der Auswahl der konkreten TOM nach Ziffer 6.2 dieses Vertrages gewährleistet die Auftragnehmerin ein dem Risiko angemessenes Schutzniveau u. a. durch:

- Pseudonymisierung und Verschlüsselung der personenbezogenen Daten.
- Dauerhafte Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung.
- Wiederherstellung der Verfügbarkeit der personenbezogenen Daten und des Zugangs zu ihnen bei einem physischen oder technischen Zwischenfall.
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM.

6.4 Der Auftragnehmerin ist es gestattet, die einmal getroffenen konkreten TOM im Zuge des technischen Fortschritts und der Weiterentwicklung durch modernere TOM zu ersetzen, die den in Ziffern 6.2 und 6.3 dieses Vertrages vereinbarten Kriterien entsprechen und stets ein angemessenes Schutzniveau gewährleisten. Sollten die Prüfung oder ein Audit durch die Auftraggeberin oder eine andere akkreditierte Stelle einen solchen Anpassungsbedarf ergeben, werden die Parteien diesen einvernehmlich im geeigneten und angemessenen Umfang umsetzen. Alle Änderungen sind zu dokumentieren.

7. Geheimhaltung

7.1 Die Vertragsparteien verpflichtet sich gegenseitig, während der Laufzeit dieses Vertrages und für die Dauer von 1 (einem) Jahr nach Beendigung dieses Vertrages alle ihnen im Rahmen der Durchführung dieser Vereinbarung bekannt gewordenen Informationen und Kenntnisse über die jeweils andere Partei, die Beschäftigten- und Kundendaten sowie Entwürfe, Konzepte, Methoden und/oder sonstige Geschäfts- und Betriebsgeheimnisse vertraulich zu behandeln.

7.2 Die der jeweils anderen Partei zugänglich gemachten Unterlagen bleiben Eigentum der betreffenden Partei und sind streng vertraulich zu behandeln. Sie dürfen ohne schriftliche Einwilligung der betreffenden Vertragspartei weder vervielfältigt, veröffentlicht, noch auf sonstige Weise Dritten zugänglich gemacht werden und dürfen nicht für einen anderen, als für den vereinbarten Zweck verwendet werden. Vertrauliche Unterlagen und/oder Daten sind nach Maßgabe dieses Vertrages und der Datenschutzbestimmungen gegen die Kenntnisnahme durch Unbefugte zu sichern.

7.3 Ausgenommen von der Geheimhaltungspflicht sind nicht geschützte Ideen, Konzeptionen, Erfahrungen sowie Informationen, die einer Vertragspartei bereits vorab bekannt waren oder öffentlich bekannt oder offenkundig sind oder ohne Verschulden der Vertragspartei bekannt werden.

8. Verpflichtung zur Vertraulichkeit (Datengeheimnis)

8.1 Die Vertragsparteien werden personenbezogene Daten nur nach Maßgabe der jeweils geltenden datenschutzrechtlichen Bestimmungen erheben, verarbeiten und nutzen. Die Vertragsparteien verpflichten sich gegenseitig zur Wahrung des Datengeheimnisses. Diese Verpflichtung bezieht sich auf alle Informationen bzw. Angaben zu einer identifizierten oder identifizierbaren natürlichen Person (Art. 4 Nr. 1 DSGVO). Sie gilt ohne Rücksicht darauf, ob die Parteien personenbezogene Daten automatisiert oder nicht automatisiert (manuell) verarbeiten.

8.2 Jede Partei wird die eigenen, zur Datenverarbeitung eingesetzten Mitarbeiter vor Durchführung der Arbeiten auf das Datengeheimnis verpflichten. Die eigenen Mitarbeiter sind über die einschlägigen Datenschutzbestimmungen in Kenntnis zu setzen und mit den sich daraus ergebenden besonderen Anforderungen an die Datensicherheit und den Datenschutz, insbesondere den nach dieser Vereinbarung geltenden Sorgfalts- und Geheimhaltungspflichten, vertraut zu machen.

8.3 Die Weitergabe personenbezogener Daten und/oder von sonstigen Informationen aus dem Bereich der Auftraggeberin an Dritte ist der Auftragnehmerin verboten. Dies gilt auch, wenn und soweit eine Änderung oder Ergänzung der Daten erfolgt.

9. Inanspruchnahme weiterer Auftragsverarbeiter (Nachunternehmer)

9.1 Die Auftragnehmerin wird zur Erfüllung des Nutzungsvertrages weitere Auftragsverarbeiter (Nachunternehmer) nicht ohne die vorherige gesonderte

oder allgemeine schriftliche Zustimmung der Auftraggeberin unterbeauftragen.

9.2 Die Auftraggeberin erteilt hiermit ihre allgemeine schriftliche Genehmigung für die in **Anhang 2** zu diesem Vertrag genannten weiteren Auftragsverarbeiter (Nachunternehmer), die die Auftragnehmerin in Anspruch nimmt. **Anhang 2** wird hiermit Vertragsbestandteil. Die Auftragnehmerin ist berechtigt, die im **Anhang 2** genannten weiteren Auftragsverarbeiters (Nachunternehmers) einzusetzen. Die von den weiteren Auftragsverarbeitern (Nachunternehmern) jeweils zu erbringenden Leistungsbeiträge sind im **Anhang 2** ebenfalls benannt.

9.3 Die Auftragnehmerin hat die im **Anhang 2** genannten weiteren Auftragsverarbeiter (Nachunternehmern) sorgfältig ausgewählt. Sie wird mit den im **Anhang 2** genannten weiteren Auftragsverarbeitern (Nachunternehmern) einen Vertrag über die bestimmten Verarbeitungstätigkeiten abschließen, die diese für die und im Namen der Auftraggeberin durchführen sollen. Die Auftragnehmerin wird diese Verträge so gestalten, dass den im **Anhang 2** genannten weiteren Auftragsverarbeitern die Verpflichtungen nach diesem Vertrag auferlegt werden. Die im **Anhang 2** genannten weiteren Auftragsverarbeiter haben der Auftragnehmerin versichert, insbesondere hinreichende Garantien dafür zu bieten, dass sie die zur Einhaltung der Datenschutzbestimmungen geeigneten technischen und organisatorischen Maßnahmen durchführen. Die Auftragnehmerin wird sich dem vorliegenden Vertrag entsprechende Kontroll- und Überprüfungsrechte von den im **Anhang 2** genannten weiteren Auftragsverarbeitern (Nachunternehmern) einräumen lassen.

9.4 Die Auftragnehmerin informiert die Auftraggeberin unverzüglich über jede beabsichtigte Änderung eines im **Anhang 2** genannten weiteren Auftragsverarbeiters (Nachunternehmers). Soll ein neuer weiterer Auftragsverarbeiter (Nachunternehmer) hinzugezogen oder ein bisheriger ersetzt werden, wird die Auftragnehmerin, die in **Anhang 2** enthaltene Liste anpassen und der Auftraggeberin den geänderten **Anhang 2** mindestens zwanzig (20) Werktage vor der geplanten Hinzuziehung bzw. Ersetzung zukommen lassen. Die Auftraggeberin hat das Recht, gegen die Änderung innerhalb einer Frist von vierzehn (14) Werktagen Einspruch zu erheben. Wird der Einspruch nicht innerhalb der Frist geltend gemacht, verfällt das Recht auf Einspruch. Erhebt die Auftraggeberin wirksam Einspruch und kann die Auftragnehmerin ohne die Änderung bzw. den Einsatz des vorgeschlagenen weiteren Auftragsverarbeiters (Nachunternehmers) ihre Leistungen nicht erbringen, steht der Auftragnehmerin ein Recht zur fristlosen außerordentlichen Kündigung dieses Vertrages und des Nutzungsvertrages zu.

9.5 Die im Anhang 2 genannten weiteren Auftragsverarbeiter (Nachunternehmers) erbringen ihre jeweiligen Leistungen gemäß der aus Anhang 2 hervorgehenden Informationen.

- Für Nachunternehmen, die ihre Leistung Innerhalb der EU bzw. des EWR erbringen, gilt:

  Sofern einer der im Anhang 2 genannten weiteren Auftragsverarbeiter (Nachunternehmers) seine Leistungserbringung in ein Drittland außerhalb der EU bzw. des EWR verlagert, sorgt die Auftragnehmerin durch die nach den Datenschutzbestimmungen erforderlichen Maßnahmen für die datenschutzrechtliche Zulässigkeit der Verarbeitung im Drittland.

- Für Nachunternehmer, die ihre Leistung innerhalb eines Drittlands außerhalb der EU bzw. des EWR erbringen, gilt:

  Es liegt ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO für das betreffende Drittland vor oder es sind Standarddatenschutzklauseln mit sonstigen geeigneten Garantien nach Art. 46 DSGVO abgeschlossen.

9.6 Sofern Dritte für die Auftragnehmerin lediglich Nebenleistungen zur Unterstützung der Auftragsdurchführung gegenüber der Auftraggeberin erbringen, gelten diese Dritten nicht als weitere Auftragsverarbeiter. Dazu zählen alle Leistungen ohne Bezug zum Auftrag der Auftraggeberin, z. B. anonyme statistische Analyseleistungen, Post, Telekommunikationsleistungen, Transport, Logistik, Reinigungsleistungen etc. Die Auftragnehmerin wird jedoch auch bei solchen Nebenleistungen die datenschutzrechtlichen Vorgaben beachten und entsprechende vertragliche Vereinbarungen nebst Kontrollmaßnahmen treffen.

10. Dauer der Vereinbarung und Kündigungsfristen

10.1 Dieser Vertrag beginnt mit Abschluss des Nutzungsvertrages und hat die gleiche Laufzeit wie dieser. Eine davon abweichende Dauer dokumentieren die Parteien im **Anhang 1**. Zudem gelten die im Nutzungsvertrag getroffenen Kündigungsregelungen. Mit Beendigung des Nutzungsvertrages endet auch dieser Vertrag.

10.2 Das Recht zur außerordentlichen Kündigung dieser Vereinbarung bleibt den Parteien unbenommen.

11. Pflichten bei Beendigung dieses Vertrages

11.1 Ohne Wissen der Auftraggeberin werden keine Vervielfältigungen ihrer Daten oder Datenbestände erzeugt. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind. Ausgenommen sind des Weiteren Daten oder Datenbestände, deren Archivierung zum Zwecke der Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich ist.

11.2 Mit Beendigung des Nutzungsvertrages wir die Auftragnehmerin der Auftraggeberin auch alle im Rahmen des Auftragsverhältnisses in ihren Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse und Datenbestände aushändigen oder nach vorheriger Zustimmung der Auftraggeberin datenschutzgerecht dauerhaft löschen bzw. vernichten. Gleiches gilt für Test- und Ausschussmaterial sowie Datensicherungskopien. Das Protokoll über die

dauerhafte Löschung bzw. Vernichtung wird die Auftragnehmerin unaufgefordert vorlegen. Dasselbe gilt für nicht mehr benötigte Unterlagen bzw. Datenträger mit personenbezogenen Daten und/oder sonstigen Informationen aus dem Bereich der Auftraggeberin.

11.3 Auftragsbezogene Dokumentationen kann die Auftragnehmerin für die Auftraggeber gegen entsprechende Vergütung für die Dauer der geltenden gesetzlichen Aufbewahrungsfristen aufbewahren. Anderenfalls wird die Auftragnehmerin diese zu ihrer Entlastung bei Beendigung des Nutzungsvertrages übergeben.

11.4 Die Aufwände der Auftragnehmerin im Zusammenhang mit der Beendigung der Leistungsvereinbarung sind durch die vereinbarte übliche Vergütung abgegolten.

12. Schlussbestimmungen

12.1 Nebenabreden zu diesem Vertrag bestehen nicht. Änderungen oder Ergänzungen der Vereinbarung bedürfen zu ihrer Wirksamkeit der Schriftform oder der elektronischen Form (mindestens E-Mail).

12.2 Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder nichtig sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Parteien verpflichten sich, statt einer unwirksamen oder nichtigen Bestimmung solche zu vereinbaren, die dem wirtschaftlich Gewollten am nächsten kommen. Das gleiche gilt, falls der Vertrag eine ergänzungsbedürftige Lücke enthalten sollte.

12.3 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Das UN-Übereinkommen über Verträge über den internationalen Warenkauf (CISG – Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf vom 11. April 1980) ist ausgeschlossen.

12.4 Leistungsort für alle Leistungen und Gerichtsstand für alle Rechtsstreitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz der Auftragnehmerin.

Anhang 1: Einzelheiten der Auftragsverarbeitung*

Bezeichnung d. Hauptvertrages	Weisungsbefugte und DSB AG	Weisungsempfänger und DSB AN	Gegenstand der Auftragsverarbeitung	Kategorien personenbezogener Daten	Kategorien betroffener Personen	Zweck der Datenverarbeitung	Dauer des Vertrages
Nutzungsvertrag	Sie sind verpflichtet uns Ihren Weisungsbefugten (m/w/d) und - falls zutreffend - Ihren Datenschutzbeauftragten (m/w/d) mitzuteilen (z. B. per E-Mail)	WB: Mika Hally DSB: Kathrin Siegmund (extern), datenschutz@superchat.de	– Einrichten des Nutzeraccounts für die Mitarbeiter der Auftraggeberin Bereitstellung der Messaging-Plattform „Superchat“ – Verarbeitung der personenbezogenen Daten im Rahmen der Nutzung der Messaging-Plattform „Superchat“	Die persönlichen Daten, die über die Dienste verarbeitet werden, werden von der Auftraggeberin nach eigenem Ermessen bestimmt und kontrolliert und können die folgenden Kategorien von persönlichen Daten umfassen: – Bestands-, Kontakt- und Kommunikationsdaten der Interessenten und Kunden der Auftraggeberin – Name des Mitarbeiters und Kommunikationsinhalte mit dem Interessenten und Kunden der Auftraggeberin	– Kunden der Auftraggeberin, – Interessenten der Auftraggeberin, – Mitarbeiter der Auftraggeberin	– Speicherung, Nutzung und Weitergabe zum Zweck der Erbringung der Dienste – Support	Wie Nutzungsvertrag

*Ausschließlich im Falle der zusätzlichen Buchung der Consulting-Dienstleistungen zur CRM-Integration von Superchat, erhält SuperX GmbH zusätzlich Zugriff auf das CRM-System der Auftraggeberin und somit ggf. Einsicht in die dort gespeicherten Kundendaten der Auftraggeberin. Zweck dieser Verarbeitung ist die Unterstützung der Auftraggeberin bei der Einbindung von Superchat in ihre CRM-Lösung, sowie die Prozessoptimierung des Zusammenspiels zwischen der CRM-Lösung und Superchat.

Anhang 2: Liste der weiteren Auftragsverarbeiter (Nachunternehmer)

Verarbeitungen im Rahmen Ihrer Nutzung von Superchat:

Firma, Anschrift	**Art und Zweck der Verarbeitung**	**Art der Daten**	**Kategorien der betroffenen Personen**	**Zulässigkeit Verarbeitung außerhalb der EU**
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxemburg	Hosting	- Bestands-, Kontakt- und Kommunikationsdaten der Kontakte und Kunden der Auftraggeberin - Name des Mitarbeiters der Auftraggeberin und Kommunikation mit dem Kontakt und Kunden der Auftraggeberin	Kontakte, Kunden und Mitarbeiter der Auftraggeberin	Verarbeitung in EU. Sofern in Ausnahmefällen eine Übermittlung an die Amazon Web Services, Inc. in den USA stattfindet: Angemessenheitsbeschluss, SCC, DPF-Teilnahme Zusätzliche Maßnahmen: clientseitige Verschlüsselung; AWS TOM (Annex I: Link)
Auth0, Okta Inc., 100 1st St Suite 150, San Francisco	Login	- Benutzername, E-Mail, Passwort	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme Informationssicherheits-Dokumentation (Link)
Cloudconvert, Lunaweb GmbH	Konvertierung/Komprimierung von Dateiuploads (Einsatz dieses Dienstleisters nur, sofern Dateiuploads in Superchat erfolgen)	- Inhalte hochgeladener Dateien - User-ID des Mitarbeiters der Auftraggeberin	Mitarbeiter der Auftraggeberin	EU Cloudconvert ist ISO 27001 zertifiziert

Nördliche Münchner Straße 14a DE-82031 Grünwald Germany				
Intercom, 55 2nd Street, 4th Floor, San Francisco, CA, United States	Livechat für Supportanfragen	- IP-Adresse, Name, E-Mailadresse, Standortdaten, Geräteinformationen, Browser-Typ, Betriebssystem der Mitarbeiter der Auftraggeberin	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme TOM: Annex II (Link) Data Region: EU
LangChain, Inc., 42 Decatur St., San Francisco, CA 94103, USA	Bereitstellung KI-Infrastruktur	- Endkunden Daten: Nachrichten / potentielle Kontakt Attribute	Kunden der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC Data Region: Deutschland / AWS self hosted LangChain Inc. ist SOC Type II zertifiziert. Zusätzliche Maßnahmen: verschlüsselte Übermittlung, MFA, restriktives Berechtigungskonzept (nur Administratoren haben Zugriff)
Meta Platforms Ireland Limited,	Speicherung und Nutzung zum Zweck der Erbringung der	- Bestands-, Kontakt- und Kommunikationsdaten der	Kontakte, Kunden und Mitarbeiter der Auftraggeberin	Verarbeitung grundsätzlich in Europa. Während des Versands können

Merrion Road, Dublin 4, D04 X2K5, Ireland	WhatsApp-Dienste über die WhatsApp Cloud API (Einsatz dieses Dienstleisters nur, sofern dieser Kommunikationskanal in Superchat verbunden ist.)	Kontakte und Kunden der Auftraggeberin - Name des Mitarbeiters der Auftraggeberin und Kommunikation mit den Kontakten und Kunden der Auftraggeberin		Nachrichten allerdings auch über einen Cloud API-Server in den USA transportiert werden, wobei alle Nachrichteninhalte im Transit (cache, queues) nach 60 Minuten automatisch gelöscht werden. Diese Übermittlung ist abgesichert über: Angemessenheitsbeschluss, SCC, DPF-Teilnahme Zusätzliche Maßnahmen: verschlüsselte Übermittlung Data Region: EU (via Local Storage Solution) Meta ist SOC Type II zertifiziert TOM: Link Datenschutz und Sicherheit bei Meta
Nylas, Inc., 944 Market St, San Francisco, CA	Speicherung und Nutzung zum Zweck der Erbringung der E-Mail-Dienste (Einsatz dieses Dienstleisters nur, sofern dieser Kommunikationskanal in Superchat verbunden ist.)	- Bestands-, Kontakt- und Kommunikationsdaten der Kontakte und Kunden der Auftraggeberin - Name des Mitarbeiters der Auftraggeberin und Kommunikation mit dem Kontakt und Kunden der Auftraggeberin	Kontakte, Kunden und Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme Nylas ist ISO 27001 zertifiziert. Security Whitepaper Data Region: EU

OneSignal, 201 South B Street, San Mateo, California 94401	Speicherung und Nutzung zum Zweck der Erbringung von Benachrichtigungs-/Notifications-Diensten	- Bestands-, Kontakt- und Kommunikationsdaten der Kontakte und Kunden der Auftraggeberin - Name des Mitarbeiters der Auftraggeberin und Kommunikation mit dem Kontakt und Kunden der Auftraggeberin	Kontakte, Kunden und Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme. OneSignal ist ISO 27001 und SOC 2 Type II zertifiziert. Data Region: EU
OpenAI, OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	OpenAI API	- SuperX GmbH übermittelt eine Client ID an OpenAI, die der Abgrenzung zu anderen SuperX GmbH Kunden dient. Für OpenAI bleibt diese Client ID anonym. Ausschließlich SuperX GmbH kann einen Bezug zu einem SuperX GmbH Kunden und ggf. dessen Mitarbeitern herstellen. - Es werden bei OpenAI keine personenbezogenen Daten verarbeitet, außer, die Auftraggeberin entscheidet sich dazu personenbezogene Daten in Prompts zu integrieren und/oder entscheidet sich dazu den Namen des Endkunden mit zu übergeben.	keine	− Verarbeitung vertraglich auf Server in Deutschland begrenzt. − Die KI lernt ausschließlich im Rahmen der jeweiligen, eigenen Client ID der Auftraggeberin. − Sofern in Ausnahmefällen eine Übermittlung an die OpenAI, L.L.C. in den USA stattfindet: Angemessenheitsbeschluss, SCC Zusätzliche Maßnahmen: verschlüsselte Übermittlung TOM (Exhibit B: Link) OpenAI ist SOC Type II zertifiziert.

Pusher Ltd., MessageBird UK Limited, 3 More London Riverside, 4th Floor, London, United Kingdom, SE1 2AQ	Bereitstellung der Funktionalität der Web- und Mobile-App	- Vor-/Nachname, Email, Telefonnummer, Nachrichten-Inhalt, IP des Nutzers	Mitarbeiter, Kontakte und Kunden der Auftraggeberin	UK Angemessenheitsbeschluss Data Region: EU (Irland) Pusher Ltd. ist ISO 27001 zertifiziert.
Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA	Speicherung und Nutzung zum Zweck der Erbringung der SMS-Dienste (Einsatz dieses Dienstleisters nur, sofern dieser Kommunikationskanal vor 2025 in Superchat verbunden war.) Kunden, die ab 2025 Superchat nutzen, betreiben ihren eigenen Twilio Account und Superchat bindet diesen Account lediglich über die API an.	- Bestands-, Kontakt- und Kommunikationsdaten der Kontakte und Kunden der Auftraggeberin - Name des Mitarbeiters der Auftraggeberin und Kommunikation mit den Kontakten und Kunden der Auftraggeberin	Kontakte, Kunden und Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, Binding Corporate Rules (BCR), SCC, DPF-Teilnahme TOM (Schedule 2: Link) Twilio ist ISO 27001 zertifiziert.

Verarbeitungen im Rahmen der Verwaltung und Betreuung Ihres Kundenaccounts bei SuperX GmbH:

Firma, Anschrift	**Art und Zweck der Verarbeitung**	**Art der Daten**	**Kategorien der betroffenen Personen**	**Zulässigkeit Verarbeitung außerhalb der EU**
Amplitude, 201 3rd Street, Suite 200, San Francisco, CA 94103	Analytics / Issue UX	- IP-Address, Client User Agent, Browser ID, Name und E-Mail von Mitarbeitern der Auftraggeberin - User-Statistics	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme.
Chargebee Inc., 909 Rose Avenue, Suite 950, North Bethesda, MD 20852	Rechnungserstellung über Chargebee's "core billing"	- Name und E-Mail-Adresse von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme
DataDog, 620 8th Avenue, Floor 45, New York, NY 10018, USA	Application Performance Monitoring	- Application-Logs, IP-Addresse, Client User Agent, Browser ID, Name und E-Mail von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme.
DocuSign, San Francisco, 221 Main St	Abschluss des AVV mit SuperX GmbH (Einsatz dieses Dienstleisters nur sofern nicht der	- Name und E-Mail-Adresse von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, BCR Zusätzliche Maßnahmen: verschlüsselte Übermittlung

#800, United States	Standard AVV abgeschlossen wird)			Data Region: EU Docusign ist ISO 27001, ISO 27017, and ISO 27018 zertifiziert. TOM (Annex II: Link)
Google Ireland Limited Gordon House, Barrow Street Dublin 4., Irland	Verwaltung der Kundenverträge, E-Mail-Verkehr	- Name, E-Mail-Adresse von Mitarbeitern der Auftraggeberin - E-Mail-Inhalte	Mitarbeiter der Auftraggeberin	Verarbeitung in EU. Sofern in Ausnahmefällen eine Übermittlung an die Google LLC in den USA stattfindet: Angemessenheitsbeschluss, SCC, DPF-Teilnahme
Hubspot, 2 Canal Park, Cambridge, MA, United States	CRM, Kundenverwaltung	- State/Region, Postal Code, Country Code, IP-Addresse, Client User Agent, Browser ID, Name und E-Mail von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme. Hubspot ist SOC Type II zertifiziert. TOM (Annex 2: Link) Data Region: EU
Make.com, Voctářova 2449, Hlavní město Praha, Czech Republic	Automation im Rahmen der Kundenverwaltung und -betreuung	- Name und Kontaktdaten von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	EU Make.com ist ISO-27001 zertifiziert.

Satellite, sipgate GmbH, Gladbacher Straße 74, 40219 Düsseldorf	Telefonie (DACH) im Rahmen der Kundenverwaltung und -betreuung	- Name und Telefonnummer von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	EU Sipgate setzt ausschließlich ISO 27001 zertifizierte Rechenzentren ein. TOM (Appendix 3: Link)
Sentry.io, Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Application Performance Monitoring	- Application-Logs, IP-Address, Client User Agent, Browser ID, Name und E-Mail von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme. Sentry.io ist SOC Type II und ISO 27001 zertifiziert.
Typeform, 163 Carrer De Bac De Roda Sant Martí, Barcelona, Spain	Abschluss des AVV mit SuperX GmbH (sofern nicht der Standard AVV abgeschlossen wird)	- Name und E-Mail-Adresse von Mitarbeitern der Auftraggeberin	Mitarbeiter der Auftraggeberin	EU Typeform ist ISO 27001 zertifiziert. TOM (Annex II: Link)

Anhang 3: Technische und organisatorische Maßnahmen der Auftragnehmerin

Beschreibung der technischen und organisatorischen Maßnahmen der SuperX GmbH

Inhaltsübersicht:

1. Zusammenfassung der getroffenen Maßnahmen

1.	Pseudonymisierung / Verschlüsselung:
✘	Maßnahmen zu Verschlüsselungen von Dateianhängen in E-Mails, des E-Mail-Transports, von Webseiten (s. nachfolgend Ziff. 3 ff.).
2.	Dauerhaftes Sicherstellen von: Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit bei Systemen und Diensten:
✘	Die Vertraulichkeit ist durch die Zutritts-, Zugangs- und Zugriffskontrolle gewährleistet (s. nachfolgend Ziff. 3 ff.).
✘	Die Integrität ist gewährleistet durch eine Absicherung des gesamten Unternehmensnetzwerks mit Firewall, Mobile Device Management (MDM).
✘	Die Verfügbarkeit ist durch Back-Ups gesichert (s. nachfolgend Ziff. 3 ff.).
✘	Die Belastbarkeit ist durch ausreichende Speicherkapazität auf den eingesetzten Servern gewährleistet.
3.	Fähigkeit zur Wiederherstellung der Verfügbarkeit der und des Zugangs zu personenbezogenen Daten bei einem Zwischenfall:
✘	Eine rasche Wiederherstellung ist über Backups möglich.
✘	Eine Notstromversorgung in den genutzten Rechenzentren sorgt für Ausfallsicherheit. (AWS)
4.	Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen u. organisatorischen Maßnahmen:
✘	Es findet ein automatisiertes, dauerhaftes Monitoring aller Systeme statt.

✘	Es findet eine jährliche Prüfung durch den/die Datenschutzbeauftragte/n statt.
✘	Es gibt jährliche Berichte über technische Ausfälle.
✘	Die Hardware wird regelmäßig ausgetauscht und gewartet.

2. Allgemeine organisatorische Maßnahmen

Maßnahmen, die die Unterweisung der Beschäftigten bei der SuperX GmbH im Umgang mit und Schutz von personenbezogenen Daten beschreiben.

Die SuperX GmbH hat die eingesetzten Beschäftigten zur Vertraulichkeit verpflichtet und über die rechtlichen Konsequenzen bei Zuwiderhandlung belehrt.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Organisatorische Maßnahmen	
✘	Über den Arbeitsvertrag sind Beschäftigte auf das Verbot des Verrats von Geschäftsgeheimnissen verpflichtet.
✘	Verpflichtung der Beschäftigten auf den vertraulichen Umgang mit personenbezogenen Daten (Art. 28 Abs. 3 DSGVO).
✘	Es wurde ein/eine betriebliche/r Datenschutzbeauftragte/r (DSB) bestellt.
✘	Es gibt eine dokumentierte Systemkonfiguration.
✘	Eine Überprüfung der technischen und organisatorischen Maßnahmen findet in regelmäßigen Abständen statt.
✘	Die/der DSB wird bei Sicherheitsvorfällen eingebunden.
✘	Sicherheitsvorfälle werden dokumentiert.

3. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen die personenbezogenen Daten verarbeitet und genutzt werden.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Technische Maßnahmen		Organisatorische Maßnahmen	
✘	Fenster-Vergitterung	✘	Schlüsselregelung (Schlüsselliste, Schlüsselausgabe)
✘	Manuelles Schließsystem	✘	Funktions- und rollenbasierte Zutrittsberechtigungen für Serverraum

		✘	Sorgfältige Auswahl von Reinigungspersonal

4. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Unbefugte Datenverarbeitungssysteme nutzen können.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Technische Maßnahmen		Organisatorische Maßnahmen	
✘	Authentifikation mit Benutzername / Passwort	✘	Passwortregelung (Mindestlänge, Komplexität, Gültigkeitsdauer, Sperrung/Löschung u.a.)
✘	Authentifikation mit biometrischen Verfahren (noch nicht flächendeckend)	✘	Sichere Aufbewahrung von Datenträgern (Sicherungsbänder, Festplatten etc.)
✘	Einsatz von Anti-Viren-Software	✘	Erstellen von personenbezogenen Benutzerprofilen
✘	Einsatz einer Software-Firewall	✘	„Clean Desk“ Richtlinie
✘	Verschlüsselung von Datenträgern in PC / Notebooks		
✘	Einsatz verschließbarer Entsorgungs-Behälter für Papier, Akten und Datenträger		
✘	Verschlüsselung des Transports der E-Mail		
✘	Verschlüsselung aller Webseiten		
✘	Verschlüsselung von E-Mail-Anhängen		
✘	Einsatz von VPN-Technologie (Engineering, Production Database)		
✘	Einsatz eines Aktenvernichters		
✘	Multi-Faktor-Authentifizierung		

5. Zugriffskontrolle

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

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Technische Maßnahmen		Organisatorische Maßnahmen	
✘	Administratoren haben unterschiedliche Aufgabengebiete	✘	Verfahren zum Entzug von Zugriffsberechtigungen
✘	Anzahl der Administratoren nach Aufgabengebiet auf ein Minimum begrenzt		
✘	Multi-Faktor-Authentifizierung		

6. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es soll zudem überprüfbar und feststellbar sein, an wen (welche Stellen) personenbezogene Daten übermittelt werden sollen oder wurden.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Technische Maßnahmen	
✘	Einsatz von VPN, Firewall (s. o).
✘	Verschlüsselung des Transports der E-Mail
✘	Verschlüsselung von E-Mail-Anhängen
✘	Multi-Faktor-Authentifizierung bei Zugriff auf externe Systeme, sofern MFA verfügbar.

7. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Technische Maßnahmen	
✘	Die eingesetzten IT-Systeme verfügen über eine Protokollierungsfunktion.

8. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen von SuperX GmbH als Auftraggeber verarbeitet werden können.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

✘	Verträge zur Auftragsverarbeitung werden mit allen Dienstleistern abgeschlossen (Art. 28 Abs. 3 DSGVO).
✘	Sorgfältige Auswahl von Auftragnehmern und Unterauftragnehmern (insbesondere im Hinblick auf Datensicherheit).
✘	Auftraggeber prüft Dokumentation und Sicherheitsmaßnahmen des Auftragnehmers vor Beginn der Datenverarbeitung.

9. Verfügbarkeitskontrolle

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

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Technische Maßnahmen		Organisatorische Maßnahmen	
✘	Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort. (AWS, Google)	✘	Vereinbarungen (SLA) zur Verfügbarkeit
✘	Klimatisierung der Serverräume.	✘	Konzept zur Sicherung und Wiederherstellung von Daten (Backup, Restore, Recovery) durch den Auftragnehmer.
✘	Feuerlöschgeräte in Serverräumen.		
✘	Rauchmelder in Serverräumen.		
✘	Schutzsteckdosenleisten in Serverräumen.		
✘	Geräte zur Überwachung der Temperatur und Feuchtigkeit in Serverräumen.		
✘	Überspannungsschutz.		
✘	Unterbrechungsfreie Stromversorgung (USV)		

✘	Backups		
✘	Virenschutz		
✘	Spiegelung von Festplatten		

10. Trennungskontrolle

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

Die Datenverarbeitung erfolgt auf den Systemen der SuperX GmbH logisch und physikalisch getrennt nach den jeweiligen Datenbeständen der Kunden bzw. nach Mandanten.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

Technische Maßnahmen		Organisatorische Maßnahmen	
✘	Festlegung von Datenbankrechten.	✘	Trennung von Produktiv- und Testsystem.
		✘	Steuerung über Berechtigungskonzept