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

Data Processing Agreement (Art. 28 para. 3 GDPR)

This contract applies between the customer (hereinafter referred to as the "Principal") and SuperX GmbH, represented by the managing directors Yilmaz Köknar and Mika Hally, Prenzlauer Allee 242-247, 10405 Berlin (hereinafter referred to as the "Contractor"). The parties have concluded a service agreement for the messaging software "Superchat". In addition to the service agreement, the parties hereby agree the following:

1. Subject of Contract and Processing, Scope of Authority

1.1 The subject matter of this agreement is the cooperation between the parties within the framework of the service agreement. The performance of the service agreement includes the data processing activities of the Contractor for the Principal as specified in Appendix 1.

1.2 The Contractor shall process the personal data made available to it under the service agreement on behalf of the Principal (Art. 28 GDPR). The Contractor shall collect, process and use the data exclusively and strictly in accordance with the Principal's order-related instructions; the objectives and modalities of the data processing may be determined solely by the Principal.

1.3 The responsibility for the creation and implementation of the erasure concept, the implementation of the right to be forgotten, to rectification, data portability and access are not the subject of this contract. These will be ensured solely by the Principal.

1.4 The agreed processing activities by the Contractor shall generally take place within the European Union and the European Economic Area. If processing activities are carried out by subcontractors in third countries, this is listed accordingly in Appendix 2 and there is either an adequacy decision by the EU Commission for the third country in question in accordance with Art. 45 GDPR or standard contractual clauses with other suitable guarantees in accordance with Art. 46 GDPR have been concluded.

1.5 The following data processing takes place at the following locations outside the Contractor's premises:

mit sonstigen geeigneten Garantien nach Art. 46 DSGVO abgeschlossen.	
1.5 Außerhalb der Betriebsstätte der Auftragnehmerin findet folgende Datenverarbeitung 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.	● The Contractor allows its employees to work from their home office. The Contractor's data protection regulations apply to this, and the employees have undertaken to comply with them. ● At the subcontractors' locations, all of which are listed in Appendix 2.
2. Art und Zweck der Verarbeitung	**2. Type and purpose of processing**
2.1 Für die Durchführung des Nutzungsvertrages mit der Auftraggeberin ist der Zugriff auf personenbezogene Daten notwendig.	2.1 Access to personal data is necessary for the performance of the service agreement with the Principal.
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.	2.2 The purposes of the data processing are specified in Appendix 1. The data processing shall only be carried out for the purposes of implementing the service agreement with the Principal; it shall not be used for any other purposes. The Contractor's employees are prohibited from collecting, processing or using protected personal data for any purpose other than the legitimate fulfilment of the respective task. The Contractor shall have no authority of its own to decide on the handling of the data and shall store it as determined by the Principal.
3. Art der personenbezogenen Daten und Kategorien betroffener Personen	**3. Type of personal data and categories of data subjects**
3.1 Die Arten der personenbezogenen Daten, die von der Datenverarbeitung durch die Auftragnehmerin betroffen sind, sind in **Anhang 1** aufgelistet.	3.1 The types of personal data affected by the Contractor's data processing are listed in **Appendix 1**.
3.2 Die Personengruppen, die zum Kreis der durch die Verarbeitung betroffenen Personen gehören, sind in **Anhang 1** aufgelistet.	3.2 The categories of data subjects affected by the processing are listed in **Appendix 1**.
4. Rechte und Pflichten der Auftraggeberin	**4. Rights and obligations of the Principal**
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).	4.1 The Principal is always responsible for checking the permissibility of data processing and safeguarding the rights of the data subjects. The Principal assumes the reporting obligations incumbent on it under the data protection provisions on its own responsibility (Art. 33, 34 GDPR).
4.2 Die Auftraggeberin bestätigt mündlich erteilte Weisungen stets in Textform oder in einer zwischen den Parteien vereinbarten sonstigen elektronischen Form (z. B.	4.2 The Principal shall always confirm verbally issued instructions in text form or in another electronic form agreed between the parties (e.g. ticketing). Changes to the object of processing or procedural changes shall be agreed in advance between the Principal and the Contractor; the parties shall make a corresponding agreement in text form.
	4.3 The persons named in Appendix 1 are authorised to issue order-related instructions to the Contractor on behalf of the Principal.
	4.4 The Principal shall inform the Contractor in an appropriate form if one of the persons named in Section 4.3 of this Agreement changes.

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.	4.5 The Principal shall be entitled to check the Contractor's compliance with the data protection provisions, the contractual agreements made here and the instructions issued at any time. As part of the inspection, the company data protection officer and the auditor appointed by the Principal shall also be granted access to the Contractor's premises in which the agreed processing takes place for the Principal, in particular to the corresponding software applications, server rooms, operating software and other IT systems used for processing on behalf of the Principal. The Contractor may satisfy this right of control of the Principal by submitting an annual data protection report or approved rules of conduct (Art. 40 GDPR) or an approved certificate or data protection seal or data protection test mark within the meaning of Art. 42 GDPR. The same applies to the selection and initial review of the contractor before commencing the processing activity agreed here.
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	4.6 The Principal shall have the right to demand the surrender of the data, data results or data sets processed and/or newly created or generated within the scope of this contract at any time. All rights and ownership of such data, data results or data sets shall be vested solely in the Principal as the holder and sole authorised owner. Data, data results or datasets refer to the technical images of information stored in a system environment (data carrier). The rights to utilise the information contained in these data, data results or data sets shall belong exclusively to the Principal. The Contractor has no right of retention in this respect (Sections 273, 320 BGB). Any rights of use or licence under copyright law (e.g. to the software) shall remain unaffected.
	5. Further rights and obligations of the Contractor
	5.1 The persons named in **Appendix 1** are authorised to accept the instructions of the Principal on behalf of the Contractor.
	5.2 The Contractor shall only process, correct, delete or block the personal data specified in Section 3 or **Appendix 1** of this contract in accordance with documented instructions from the Principal. It shall support the Principal as far as possible in the fulfilment of the obligations relating to the rights of data subjects (Art. 12 to Art. 23 GDPR). If a data subject contacts the Contractor directly for the correction or deletion of their own personal data, the Contractor shall forward this request to the Principal without delay.
	5.3 The Contractor shall keep its own register of

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.	processing activities. It shall participate in the preparation of records of processing activities and data protection impact assessments of the Principal and provide the Principal with the information required for this - insofar as possible and available to the Contractor. In addition, the Contractor shall also support the Principal in complying with the obligations incumbent on the Principal pursuant to Art. 32 to Art. 36 GDPR to the extent of the information available to the Contractor. This applies in particular to notifications to the supervisory authority or notifications to data subjects in the event of data breaches or consultations with the supervisory authority in the event of high processing risks as a result of data protection impact assessments.
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.	5.4 The Contractor shall store all documents and/or data carriers and/or data files containing personal data of the Principal in such a way that they are separate from those of other customers of the Contractor and protected from the knowledge of or access by unauthorised persons. As far as possible, the Contractor shall document incoming and outgoing data.
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.	5.5 The Contractor has duly appointed the person named in **Appendix 1** as the company data protection officer (Art. 37 GDPR). Should this data protection officer change, the Contractor shall inform the Principal immediately. The company data protection officer is responsible for compliance with data protection in the Contractor's company.
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.	5.6 The Contractor shall inform the Principal immediately of any order-related disruptions in the operational process, violations of data protection provisions (including by instructions from the Principal), inspections and measures by the supervisory authorities and other irregularities. The Contractor shall support the Principal in the fulfilment of the reporting obligations incumbent on the Principal in the event of data protection violations in accordance with the data protection provisions (Art. 33, 34 GDPR).
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	5.7 If a data subject or a third party asserts a claim against the Contractor or the Principal in connection with the present data processing, the Contractor shall support the Principal with the information available.
	5.8 The Contractor shall be entitled to suspend the implementation of instructions which, in the Contractor's opinion, violate data protection provisions until the Principal has confirmed or amended them.
	5.9 The Contractor shall enable the Principal to carry out and exercise the data protection

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.

control rights to which the Principal is entitled under Section 4.5 of this Agreement.

5.10 The Contractor shall only allow its employees to carry out activities for the Principal from the home office with the prior express consent of the Principal. This consent shall be deemed to have been granted upon signing this contract. In the event of such work, the Contractor shall ensure that the employees comply with data protection regulations when working from the home office.

5.11 The expenses incurred by the Contractor for the performance of this contract and through the provision of support or documentation services in accordance with the above Sections 5.2, 5.3, 5.6, 5.8 and 5.9 of this contract shall be compensated with the payment of the remuneration agreed between the parties for the service agreement.

6. Technical and organisational measures

6.1 At the time of conclusion of this contract, the Contractor has already demonstrably taken all necessary and appropriate technical and organisational measures (TOM) for data security for the present order in accordance with Art. 32 GDPR, which the Principal has accepted. These are described in detail in Appendix 3 to this contract and correspond to the catalogue of measures regulated under Art. 32 para. 1 GDPR. Appendix 3 to this contract hereby becomes an integral part of the contract.

6.2 When selecting the specific TOM, the Contractor shall take the following criteria into account

- the state of the art;
- the implementation costs;
- the nature, scope, circumstances and purposes of the processing in question
- the probability of occurrence and the severity of the risk to the rights and freedoms of the natural persons affected by the data processing.

6.3 The Contractor undertakes to always ensure an appropriate level of protection of the TOM taken. When selecting the specific TOM in accordance with Section 6.2 of this contract, the Contractor shall ensure a level of protection appropriate to the risk by, among other things

- Pseudonymization and encryption of personal data.

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

- Permanent assurance of confidentiality, integrity, availability and resilience of the systems and services in connection with the processing.
- Restoring the availability of and access to personal data in the event of a physical or technical incident.
- A process for regularly reviewing, assessing and evaluating the effectiveness of the TOM.

6.4 The Contractor shall be permitted to replace the specific TOMs once implemented with more modern TOMs in the course of technical progress and further development, which comply with the criteria agreed in sections 6.2 and 6.3 of this contract and always guarantee an appropriate level of protection. Should the review or an audit by the Principal or another accredited body reveal such a need for adaptation, the parties shall implement this by mutual agreement to a suitable and appropriate extent. All changes must be documented.

7. Nondisclosure

7.1 During the term of this Agreement and for a period of 1 (one) year after termination of this Agreement, the Parties mutually undertake to treat as confidential all information and knowledge about the other Party, employee and customer data as well as drafts, concepts, methods and/or other business and trade secrets that become known to them in the course of the performance of this Agreement.

7.2 The documents made available to the other party shall remain the property of the party concerned and shall be treated as strictly confidential. They may not be reproduced, published or otherwise made accessible to third parties without the written consent of the party concerned and may not be used for any purpose other than the agreed purpose. Confidential documents and/or data must be secured against unauthorised access in accordance with this contract and the data protection provisions.

7.3 Excluded from the confidentiality obligation are unprotected ideas, concepts, experience and information that were already known to a contracting party in advance or are publicly known or in the public domain or become known through no fault of the contracting party.

8. Obligation of confidentiality (data secrecy)

8.1 The contracting parties shall collect, process and use personal data only in accordance with the applicable data protection

physischen oder technischen Zwischenfall. ● Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM.	regulations. The contracting parties mutually undertake to maintain data secrecy. This obligation applies to all information or details relating to an identified or identifiable natural person (Art. 4 No. 1 GDPR). It applies regardless of whether the parties process personal data in an automated or non-automated (manual) manner.
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.	8.2 Each party shall oblige its own employees used for data processing to maintain data secrecy before carrying out the work. Its own employees shall be informed of the relevant data protection provisions and familiarised with the resulting special requirements for data security and data protection, in particular the duties of care and confidentiality applicable under this Agreement.
7. Geheimhaltung	8.3 The Contractor is prohibited from passing on personal data and/or other information pertaining to the Principal to third parties. This also applies if and to the extent that the data is changed or supplemented.
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.	**9. Utilisation of other Processors (Subcontractors)** 9.1 The Contractor shall not subcontract further processors (subcontractors) for the fulfilment of the contract of use without the prior separate or general written consent of the Principal.
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.	9.2 The Principal hereby grants its general written authorisation for the further processors (subcontractors) named in Appendix 2 to this contract, which the Contractor uses. Appendix 2 hereby becomes part of the contract. The Contractor is authorised to use the additional processors (subcontractors) listed in Appendix 2. The service contributions to be provided by the other processors (subcontractors) are also specified in Appendix 2.
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.	9.3 The Contractor has carefully selected the other processors (subcontractors) listed in Appendix 2. It shall conclude a contract with the additional processors (subcontractors) named in Appendix 2 for the specific processing activities that they are to carry out for and on behalf of the Principal. The Contractor shall draft these contracts in such a way that the obligations under this contract are imposed on the additional processors named in Appendix 2. The other processors named in Appendix 2 have assured the Contractor that they offer sufficient guarantees, in particular, that they will implement the appropriate technical and organisational measures to comply with the data protection provisions. The Contractor shall have the other processors

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.

(subcontractors) named in Appendix 2 grant the Contractor corresponding control and inspection rights under this contract.

9.4 The Contractor shall inform the Principal immediately of any intended change to another processor (subcontractor) named in Appendix 2. If a new additional processor (subcontractor) is to be added or a previous one replaced, the Contractor shall amend the list contained in Appendix 2 and send the amended Appendix 2 to the Principal at least twenty (20) working days before the planned addition or replacement. The Principal shall have the right to object to the amendment within a period of fourteen (14) working days. If the objection is not raised within this period, the right of objection shall lapse. If the Principal effectively raises an objection and the Contractor is unable to provide its services without the change or the use of the proposed additional processor (subcontractor), the Contractor shall be entitled to extraordinary termination of this contract and the service agreement without notice.

9.5 The other processors (subcontractors) listed in Appendix 2 shall provide their respective services in accordance with the information contained in Appendix 2.

- The following applies to subcontractors that provide their services within the EU or the EEA:

  If one of the other processors (subcontractors) named in Appendix 2 relocates its service provision to a third country outside the EU or the EEA, the Contractor shall ensure that the processing in the third country is permissible under data protection law by taking the measures required under data protection regulations.

- The following applies to subcontractors who provide their services in a third country outside the EU or the EEA:

  There is an adequacy decision by the EU Commission in accordance with Art. 45 GDPR for the third country in question or standard contractual clauses with other suitable guarantees in accordance with Art. 46 GDPR have been concluded.

9.6 If third parties merely provide the Contractor with ancillary services to support the fulfilment of the order vis-à-vis the Principal, these third parties shall not be considered additional processors. This includes all services unrelated to the Principal's order,

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:

e.g. anonymous statistical analysis services, post, telecommunications services, transport, logistics, cleaning services, etc. However, the Contractor shall also comply with the data protection regulations for such ancillary services and shall enter into corresponding contractual agreements together with control measures.

10. Duration of the agreement and periods of notice

10.1 This agreement shall commence upon conclusion of the service agreement and shall have the same term as the latter. The parties shall document any deviating duration in Appendix 1. In addition, the cancellation provisions set out in the service agreement shall apply. Upon termination of the service agreement, this agreement shall also end.

10.2 The parties retain the right to extraordinary cancellation of this agreement.

11. Obligations upon termination of this agreement

11.1 No copies of the Principal's data or data sets shall be made without the Principal's knowledge. Excluded from this are backup copies, insofar as these are necessary to ensure proper data processing. Also excluded are data or data sets whose archiving is necessary for the purpose of complying with statutory retention obligations.

11.2 Upon termination of the service agreement, the Contractor shall also hand over to the Principal all documents, processing and utilisation results and data sets that have come into its possession within the scope of the contractual relationship or, with the prior consent of the Principal, permanently delete or destroy them in accordance with data protection regulations. The same applies to test and scrap material and data backup copies. The Contractor shall submit the record of the permanent deletion or destruction without being requested to do so. The same applies to documents or data carriers no longer required containing personal data and/or other information related to the Principal.

11.3 The Contractor may retain order-related documentation for the Principal for the duration of the applicable statutory retention periods in return for appropriate remuneration. Otherwise, the Contractor shall hand them over to the Principal at the end of the service agreement.

11.4 The Contractor's expenses in connection with the termination of the service agreement

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,

shall be covered by the agreed customary remuneration.

12. Final provisions

12.1 There are no collateral agreements to this contract. Amendments or additions to the agreement must be made in writing or in electronic form (at least e-mail) to be effective.

12.2 Should individual provisions of this contract be or become invalid or void in whole or in part, this shall not affect the validity of the remaining provisions. The parties undertake to replace an invalid or void provision with a provision that comes as close as possible to the economic intent of the invalid or void provision. The same applies if the contract contains a gap that needs to be filled.

12.3 This contract is subject to the law of the Federal Republic of Germany. The UN Convention on Contracts for the International Sale of Goods (CISG - United Nations Convention on Contracts for the International Sale of Goods of 11 April 1980) is excluded.

12.4 The place of performance for all services and the place of jurisdiction for all legal disputes arising from or in connection with this contract is the registered office of the Contractor.

12.5 This contract (including all appendices) is entered into in German and English. In the event of any discrepancies between the language versions, the German version shall prevail.

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 wird 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 Auftraggeberin 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.	
12.5	Dieser Vertrag (einschließlich aller Anhänge) wird in deutscher und englischer Sprache geschlossen. Bei Abweichungen zwischen den Sprachfassungen ist die deutsche Fassung maßgeblich.	

Anhänge / Appendices:

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
Nutzungs-vertrag	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 Nutzungs-vertrag

*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)

Allgemeine Unterauftragnehmer (Core-Produkt „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, Standarddatenschutzklauseln der EU (im Folgenden „SCC“), Teilnahme am Datenschutzrahmen EU-USA (im Folgenden „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)

DataDog, 620 8th Avenue, Floor 45, New York, NY 10018, USA	Application Performance Monitoring zur Überwachung der Systemstabilität, Performance und Verfügbarkeit der Plattform sowie der frühzeitigen Erkennung technischer Störungen.	- 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. Data Region: EU
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
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
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.

Sentry.io, Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Fehler- und Ausnahmeüberwachung. Unterstützt bei der Identiizierung, Analyse und Behebung von Softwarefehlern, Abstürzen und unerwartete Systemzuständen.	- 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.

Unterauftragnehmer beim optionalen Einsatz des Kommunikationskanals „E-Mail“

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

Unterauftragnehmer beim optionalen Einsatz des Kommunikationskanals „SMS-Dienste“

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	- 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.

	diesen Account lediglich über die API an.			

Unterauftragnehmer beim optionalen Einsatz des Kommunikationskanals „WhatsApp“

Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland	Speicherung und Nutzung zum Zweck der Erbringung der WhatsApp-Dienste über die WhatsApp Cloud API (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 den Kontakten und Kunden der Auftraggeberin	Kontakte, Kunden und Mitarbeiter der Auftraggeberin	Verarbeitung grundsätzlich in Europa. Während des Versands können 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

Unterauftragnehmer beim optionalen Einsatz des Datei-Upload-Features

Cloudconvert, Lunaweb GmbH Nördliche Münchner Straße 14a, DE-82031,	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

Grünwald, Germany				

Unterauftragnehmer beim optionalen Einsatz des „KI-Chatbot“-Features

LangChain, Inc., 42 Decatur St., San Francisco, CA 94103, USA	Bereitstellung und Orchestrierung von KI-Funktionalitäten innerhalb der Plattform. Technische Infrastruktur zur Verarbeitung und Steuerung von KI-Workflows, insbesondere zur Anbindung und Nutzung von Sprachmodellen.	- Endkunden Daten: Nachrichten / potentielle Kontakt Attribute	Kunden der Auftraggeberin	USA: Angemessenheitsbeschluss, SCC Data Region: Deutschland / AWS self hosted Zusätzliche Maßnahmen: verschlüsselte Übermittlung, MFA, restriktives Berechtigungskonzept (nur Administratoren haben Zugriff) LangChain Inc. ist SOC Type II zertifiziert.
OpenAI, OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	OpenAI API (Einsatz dieses Dienstleisters nur, sofern der KI-Chatbot genutzt wird.)	- 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	keine	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: SCC Zusätzliche Maßnahmen: verschlüsselte Übermittlung TOM (Exhibit B: Link) OpenAI ist SOC Type II zertifiziert.

		dazu den Namen des Endkunden mit zu übergeben.		

Unterauftragnehmer beim optionalen Einsatz des „KI-Anruf“-Features

Assembly.ai Inc., 169 Madison Ave STE 38365, New York, NY 10016, USA	Speech-to-Text-Engine zur Transkription von Audio	- Sprachinhalte mit ggf. personenbezogenen Daten, transkribierte Texte, Namen, Ort, E-Mailadressen, Telefonnummern, Beruf, Titel	Kunden, Kontakte der Auftraggeberin (Anrufende)	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme Zusätzliche technische Maßnahmen: Data Retention 11 Tage
Cartesia AI, Inc., 1766 18th Street, San Francisco, California 94017, USA	Text-to-Speech-Engine zur Transkription von Audio	- Text-Prompts mit ggf. personenbezogenen Inhalten (z.B. Namen, Telefonnummern), generierte Audio-Dateien mit ggf. personenbezogenen Daten	Kunden, Kontakte der Auftraggeberin (Anrufende)	USA: Angemessenheitsbeschluss, SCC Cartesia ist SOC 2 Type II zertifiziert
Eleven Labs Inc., 169 Madison Ave #2484, New York, NY 10016, USA	Text-to-Speech-Engine zur Transkription von Audio	- Text-Prompts mit ggf. personenbezogenen Inhalten (z.B. Namen, Telefonnummern), generierte Audio-Dateien mit ggf. personenbezogenen Daten	Kunden, Kontakte der Auftraggeberin (Anrufende)	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme. Zusätzliche technische Maßnahmen: Zero Retention bei der Sprachausgabe (verhindert, dass Audio- und Textdaten nach der Verarbeitung auf ElevenLabs-Servern gespeichert werden) Data Region: EU Eleven Labs Inc. ist SOC 2 Type II und ISO 27001 zertifiziert

LiveKit Inc., 4285 Payne Avenue Suite 9154, San Jose, California 95157, USA	Verbindet den Twilio Anruf mit der KI, so dass Elevenlabs in Echtzeit antworten kann	- Sprachdaten - Transkriptdaten - technische Verbindungsdaten - Kommunikationsmetadaten	Kunden, Kontakte der Auftraggeberin (Anrufende)	USA: Angemessenheitsbeschluss, SCC, DPF-Teilnahme Data Region: EU Livekit Inc. ist SOC 2 Type II zertifiziert
OpenAI, OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	Speech-to-Text-Engine zur Transkription von Audio	- Sprachinhalte mit ggf. personenbezogenen Daten, transkribierte Texte.	Kunden, Kontakte der Auftraggeberin (Anrufende)	– Verarbeitung vertraglich auf Server in der EU 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: SCC Zusätzliche Maßnahmen: verschlüsselte Übermittlung, Zero Retention bei der Transkription (Audiodaten werden nach Transkription serverseitig nicht gespeichert) TOM (Exhibit B: Link) OpenAI ist SOC Type II zertifiziert.
Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA	Anruf-Annahme, Verbindung einer IP-Telefonieinfrastruktur mit dem öffentlichen Telefonnetz (PSTN)	- Anrufdaten (z. B. Telefonnummer, Zeitstempel) - Metadaten (z. B. IP-Adressen, SIP-Metadaten)	Kontakte, Kunden und Mitarbeiter der Auftraggeberin	USA: Angemessenheitsbeschluss, Binding Corporate Rules (BCR), SCC, DPF-Teilnahme TOM (Schedule 2: Link) Twilio ist ISO 27001 zertifiziert.

Anhang 3: Technische und organisatorische Maßnahmen der Auftragnehmerin

Version 1.3

Diese Beschreibung der technischen und organisatorischen Maßnahmen („TOM“) konkretisiert die von SuperX GmbH implementierten Maßnahmen zum Schutz personenbezogener Daten im Zusammenhang mit den von SuperX GmbH erbrachten Leistungen. Sie dient dem Nachweis eines dem Risiko angemessenen Schutzniveaus unter Berücksichtigung von Art. 24, Art. 25, Art. 28 und Art. 32 DSGVO sowie unter Beachtung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen. SuperX GmbH überprüft die nachfolgend beschriebenen Maßnahmen regelmäßig und entwickelt sie entsprechend der technischen, organisatorischen und rechtlichen Rahmenbedingungen fort. Die in diesem Dokument beschriebenen Maßnahmen gelten für alle Systeme, Prozesse und organisatorischen Einheiten, soweit diese für die Erbringung der vertragsgegenständlichen Leistungen personenbezogene Daten verarbeiten. Soweit SuperX GmbH Unterauftragnehmer einsetzt, werden diese auf Grundlage vertraglicher Regelungen und risikobasierter Auswahl- und Kontrollprozesse in das Schutzkonzept einbezogen.

Diese TOM sind Bestandteil des Vertrags zur Auftragsverarbeitung und beschreiben die zum Zeitpunkt der jeweils aktuellen Fassung dieser TOM umgesetzten Maßnahmen.

1. Allgemeine Maßnahmen

Referenz zu ISO 27001 Annex A: A.6.3 Information security awareness, education and training; A.5.1 Policies for information security; A.5.37 Documented operating procedures

Folgende konkrete allgemeine Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Über den Arbeitsvertrag sind Beschäftigte auf das Verbot des Verrats von Geschäftsgeheimnissen verpflichtet.	☒	Es wurde ein/eine betriebliche/r Datenschutzbeauftragte/r (DSB) bestellt.
☒	Es gibt regelmäßige datenschutzrechtliche Unterweisungen/Schulungen der Beschäftigten.	☒	Die/der DSB wird bei Sicherheitsvorfällen eingebunden.
☒	Ein Datenschutzmanagementsystem ist etabliert.	☒	Ein Information Security Management System (ISMS, engl. Für „Managementsystem für Informationssicherheit“) ist etabliert.
☒	Es ist ein Prozess zur technischen und organisatorischen Abwicklung der Geltendmachung von Betroffenenrechten (Auskunfts-, Löschbegehren) etabliert, der die fristgerechte Bearbeitung sicherstellt.	☒	Bei der Software-Entwicklung werden die Grundsätze „Privacy by Design“ und „Privacy by Default“ (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) berücksichtigt und eingehalten.
☒	Sofern Verarbeitungsprozesse identifiziert werden, die unter Art. 35 DSGVO fallen und SuperX GmbH als Verantwortlicher fungieren, erstellt SuperX GmbH die erforderliche Datenschutz-Folgenabschätzung. Soweit SuperX GmbH als Auftragsverarbeiter für den betreffenden Verarbeitungsprozess agiert, unterstützt SuperX GmbH den Auftraggeber bei der Erstellung der Datenschutz-Folgenabschätzung.	☒	Verpflichtung der Beschäftigten auf den vertraulichen Umgang mit personenbezogenen Daten (Art. 28 Abs. 3 DSGVO).
☒	Es gibt eine dokumentierte Systemkonfiguration.	☒	Eine Überprüfung der technischen und organisatorischen Maßnahmen findet in regelmäßigen Abständen statt.
☒	Sicherheitsvorfälle werden dokumentiert.	☒	Data Privacy (IM1.4.1): SuperX GmbH regelt Rollen und Verantwortlichkeiten im Umgang mit Personendaten (Datenschutz) in der gesamten Organisation. Weiter verfügt SuperX GmbH über einen Datenschutzbeauftragten.

☒	Security Agreements (PM1.2.1): SuperX GmbH regelt verbindlich die Rollen und Verantwortlichkeiten bezüglich Datensicherheit in ihrer Organisation. Sie kommuniziert diese gegenüber den internen und externen Beschäftigten und stellt deren Einhaltung sicher.	☒	Information Lifecycle (IM1.2.1): SuperX GmbH garantiert, dass kritische und sensible Personendaten in jeder Phase des Informationslebenszyklus geschützt werden. Dies umfasst die Erstellung, Verarbeitung, Übertragung, Speicherung und Löschung von Informationen, unabhängig davon, ob sie in digitaler oder physischer vorliegen.
☒	Information Classification and Handling (IM1.3.1): SuperX GmbH verfügt über ein Schema für die einheitliche und durchgängige Bestimmung des Schutzbedarfs. Dieses Schema dient auch der Klassifizierung von Geschäfts- und Personendaten sowie Systemen, Anwendungen und Infrastruktur.	☒	Information Classification and Handling (IM1.3.3): SuperX GmbH garantiert ein konsistentes und strukturiertes Vorgehen, das Personendaten entsprechend ihrer Klassifizierung vor unbefugter Änderung, unautorisiertem Zugriff/Offenlegung sowie vor Verlust schützt.

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

2.1. Zutrittskontrolle

Referenz zu ISO 27001 Annex A: A.7.1 Physical security perimeters; A.7.2 Physical entry; A.7.3 Securing offices, rooms and facilities; A.7.4 Physical security monitoring.

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

Die nachfolgend genannten Maßnahmen kommen in Abhängigkeit zum Schutzbedarf bei SuperX GmbH zum Einsatz.

☒	Fenster-Vergitterung	☒	Funktions- und rollenbasierte Zutrittsberechtigungen für Serverraum
☒	Manuelles Schließsystem	☒	Schlüsselregelung (Schlüsselliste, Schlüsselausgabe)
☒	Sorgfältige Auswahl von Reinigungspersonal		

2.2. Zugangskontrolle

Referenz zu ISO 27001 Annex A: A.5.15 Access control; A.5.16 Identity management; A.5.17 Authentication information; A.5.18 Access rights; A.8.5 Secure authentication.

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

Folgende konkrete Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Authentifikation mit Benutzername / Passwort	☒	Verschlüsselung aller Webseiten (SSL, HTTPS)
☒	Sichere Aufbewahrung von Datenträgern (Sicherungsbänder, Festplatten etc.)	☒	Verschlüsselung von E-Mail-Anhängen
☒	Einsatz von Anti-Viren-Software / Malware Protection Software (TP1.2.1): SuperX GmbH stellt sicher, dass Anwendungen, Systeme sowie Infrastruktur, die gegen Schadsoftware und Cyberangriffe ausgesetzt sind, eine aktuelle Malware-Schutzsoftware installiert haben.	☒	Einsatz von VPN-Technologie (Engineering, Production Database)
☒	Multi-Faktor-Authentifizierung	☒	Mobile Device Management
☒	Einsatz einer Software-Firewall	☒	Einsatz eines Aktenvernichters
☒	Verschlüsselung von Datenträgern in PC / Notebooks (z. B. Bitlocker)	☒	Schlüsselregelungen (Richtlinie/Anweisung zur Ausgabe von Schlüsseln)
☒	Passwortregelung (Mindestlänge, Komplexität, Gültigkeitsdauer, Sperrung/Löschung u.a.)	☒	Richtlinie für einen „Clean Desk“
☒	Einsatz verschließbarer Entsorgungs-Behälter für Papier, Akten und Datenträger	☒	Erstellen von personenbezogenen Benutzerprofilen
☒	Verschlüsselung des Transports der E-Mail (TLS 1.2, TLS 1.3)	☒	Multi-Faktor-Authentifizierung
☒	Access Control Arrangements (AC1.2.1): SuperX GmbH stellt sicher, dass der Zugang zu Anwendungen, Systemen, Infrastruktur sowie Personendaten nur autorisierten Personen oder Services gewährt wird. Diese müssen entsprechende Aufgaben oder Tätigkeiten haben. Der Zugriff erfolgt nach dem Need-to-know-Prinzip.	☒	Verschlüsselung at rest: • Für Datenbanken: (AWS RDS) -> SYMMETRIC_DEFAULT • Für Dateien (AWS S3) Verwaltung der Schlüssel -> AWS KMS (AWS managed keys), jährliche Schlüsselerneuerung

2.3. Zugriffskontrolle

Referenz zu ISO 27001 Annex A: A.5.15 Access control; A.5.18 Access rights; A.8.15 Logging; A.8.16 Monitoring activities; A.8.2 Privileged access right; A.8.24 Use of cryptography; A.8.25 Key management.

Zugriffskontrolle umfasst 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. Insbesondere kryptografische Maßnahmen (Verschlüsselung), so dass Daten – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Administratoren haben unterschiedliche Aufgabengebiete	☒	Access Control Arrangements (AC1.2.1): SuperX GmbH stellt sicher, dass der Zugriff auf Anwendungen, Systeme, Infrastruktur nach dem Need-to-know-Prinzip erfolgt.
☒	Anzahl der Administratoren nach Aufgabengebiet auf ein Minimum begrenzt	☒	Cryptographic Solutions (CP1.1.1): Zur Sicherstellung der Vertraulichkeit, Integrität, Authentizität und Nichtabstreitbarkeit setzt SuperX GmbH anerkannte kryptografische Verfahren und Lösungen ein. Diese entsprechen mindestens dem aktuellen Standard. Verschlüsselung **at rest**: • Für Datenbanken: (AWS RDS) -> SYMMETRIC_DEFAULT (LINK) • Für Dateien (AWS S3) (LINK) Verwaltung der Schlüssel -> AWS KMS (AWS managed keys), jährliche Schlüsselerneuerung Verschlüsselung **in transit**: AWS ELBSecurityPolicy-TLS13-1-2-2021-06 (LINK)
☒	Funktions- und rollenbasiertes Berechtigungskonzept	☒	Offboarding: Beim Ausscheiden von Mitarbeitern oder bei Änderungen von Zuständigkeiten werden Berechtigungen entfernt.

☒	Clean Desk Policy	☒	Verfahren zum Entzug von Zugriffsberechtigungen (z. B. bei Ausscheiden eines Beschäftigten aus dem Unternehmen)

2.4. Trennungskontrolle

Referenz zu ISO 27001 Annex A: A.8.31 Separation of development, test and production environments; A.8.22 Segregation of networks; A.8.12 Data leakage prevention;.5.15 Access control.

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

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Festlegung von Datenbankrechten.	☒	Trennung der Daten verschiedener Auftraggeber.
☒	Trennung von Produktiv- und Testsystem.	☒	Steuerung über Berechtigungskonzept

2.5. Pseudonymisierung

Referenz zu ISO 27001 Annex A: A.8.11 Data masking; A.8.24 Use of cryptography.

Soweit der Verarbeitungszweck dies zulässt, werden personenbezogene Daten pseudonymisiert verarbeitet. Der Identifizierungsschlüssel oder sonstige Zusatzinformationen werden getrennt gespeichert, gesondert geschützt und nur einem eng begrenzten Personenkreis zugänglich gemacht. Die Auswahl der Pseudonymisierungsmethoden erfolgt zweck- und risikobasiert unter Berücksichtigung des Standes der Technik.

3. Integrität (Art. 32 Abs. 1 Buchstabe b DSGVO)

3.1. Weitergabekontrolle

Referenz zu ISO 27001 Annex A: A.8.24 Use of cryptography; A.5.14 Information transfer; A.8.21 Security of network services.

Weitergabekontrolle umfasst 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:

☒	Einsatz von VPN, Firewall (s. o).	☒	Verschlüsselung von E-Mail-Anhängen

☒	Verschlüsselung des Transports der E-Mail (TLS 1.2, TLS 1.3)	☒	Multi-Faktor-Authentifizierung bei Zugriff auf externe Systeme.
☒	Verschlüsselung **in transit**: AWS ELBSecurityPolicy-TLS13-1-2-2021-06 (LINK)		

3.2. Eingabekontrolle

Referenz zu ISO 27001 Annex A: A.8.15 Logging; A.8.16 Monitoring activities; A.5.37 Documented operating procedures.

Eingabekontrolle umfasst 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:

☒	Die eingesetzten IT-Systeme verfügen über eine Protokollierungsfunktion.	☒	Customer Connections (BA2.3.2): SuperX GmbH stellt die Vertraulichkeit und Integrität von Personendaten bei der Bearbeitung (insbesondere bei der Eingabe, dem Zugriff, der Speicherung, der Verarbeitung und der Ausgabe) in Anwendungen durch integrierte Massnahmen und Kontrollen jederzeit angemessen sicher.

3.3. Dokumentationskontrolle

Referenz zu ISO 27001 Annex A: A.5.37 Documented operating procedures; A.5.1 Policies for information security; A.5.9 Inventory of information and other associated assets.

Dokumentationskontrolle umfasst Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Führung eines Verzeichnisses von Verarbeitungstätigkeiten	☒	Es gibt eine Dokumentation zum Sicherheitskonzept.
☒	Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration	☒	Sicherheitsvorfälle werden dokumentiert.

☒	Es existiert ein Löschkonzept, in dem alle Aufbewahrungsfristen und Löschzeitpunkte dokumentiert sind. Wo technisch möglich, sind automatisierte Löschroutinen in den Datenbanken implementiert, die Daten nach Ablauf der definierten Aufbewahrungsfristen ohne manuellen Eingriff zur Löschung markieren oder physisch entfernen. Als Alternative zur Löschung werden Daten nach Zweckfortfall so anonymisiert, dass kein Personenbezug mehr hergestellt werden kann (statistische Aufbereitung). Sofern physische Datenträger genutzt werden, werden diese gemäß DIN 66399 (Schutzklasse 2/3) durch zertifizierte Entsorgungsfachbetriebe vernichtet.		

3.4. Auftragskontrolle

Referenz zu ISO 27001 Annex A: A.5.19 Information security in supplier relationships; A.5.20 Addressing information security within supplier agreements; A.5.21 Managing information security in the ICT supply chain; A.5.22 Monitoring, review and change management of supplier services.

Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen seitens des Auftraggebers verarbeitet werden können.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Verträge zur Auftragsverarbeitung werden mit allen Dienstleistern abgeschlossen (Art. 28 Abs. 3 DSGVO). Supplier Contracts (SC1.3.1) : SuperX GmbH regelt verbindlich die Cyber- und Datensicherheitsanforderungen bei externen Lieferanten und Dienstleistungserbringern. Sie holt entsprechende Zusicherungen ein und überprüft diese regelmässig.	☒	Drittlandübermittlung: Sofern Verarbeitungstätigkeiten durch Unterauftragnehmer in Drittländern erbracht werden, liegt für das betreffende Drittland entweder ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO vor (bei US-Übermittlungen liegt zusätzlich eine Data Privacy Zertifizierung des Dienstleisters vor) oder es sind Standarddatenschutzklauseln mit sonstigen geeigneten Garantien nach Art. 46 DSGVO abgeschlossen.
☒	Sorgfältige Auswahl von Auftragnehmern und Unterauftragnehmern (insbesondere im Hinblick auf Datensicherheit).	☒	Gegenüber allen Auftragnehmern bestehen vertragliche Kontrollrechte bezogen auf Einhaltung des Datenschutzes.

☒	Auftraggeber prüft Dokumentation und Sicherheitsmaßnahmen bei dem Auftragnehmer vor Beginn der Datenverarbeitung.	☒	Die datenschutzgerechte Vernichtung/Löschung von Daten nach Beendigung des Auftrags ist geregelt.

4. Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit (Art. 32 Abs. 1 Buchstabe b, c DSGVO)

Referenz zu ISO 27001 Annex A: A.8.13 Information backup; A.5.30 ICT readiness for business continuity; A.8.14 Redundancy of information processing facilities.

Verfügbarkeitskontrolle, Belastbarkeit & Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort. (Amazon Web Services, Google)	☒	Schutzsteckdosenleisten in Serverräumen.
☒	Klimatisierung der Serverräume.	☒	Geräte zur Überwachung der Temperatur und Feuchtigkeit in Serverräumen.
☒	Feuerlöschgeräte in Serverräumen.	☒	Überspannungsschutz.
☒	Rauchmelder in Serverräumen.	☒	Unterbrechungsfreie Stromversorgung (USV)
☒	Backups / Backup and Restore (SR1.5.1): SuperX GmbH garantiert, dass Anwendungen (inkl. deren Daten) und Systeme regelmässig mittels Backup gesichert werden. Zudem bestehen regelmässig getestete Verfahren für die Wiederherstellung (Recovery).	☒	Spiegelung von Festplatten

☒	Virenschutz	☒	Business Continuity Management (BC1.1.1) : SuperX GmbH verfügt über eine unternehmensweite, aktuelle Business ContinuityStrategie und Prozesse. Diese werden durch eine widerstandsfähige technische Infrastruktur und ein effektives Krisenmanagement unterstützt.
☒	Backup and Restore (SR1.5.2) : SuperX GmbH stellt sicher, dass Backups bzw. Sicherungsmassnahmen vor Verlust, Beschädigung und unbefugtem Zugriff geschützt sind.	☒	Notfallplan
☒	kontinuierliches Monitoring der IT-Ressourcen (CPU, Arbeitsspeicher, Speicherplatz, Netzwerkbandbreite) auf Schwellwert-Alarme und regelmässige Evaluierung der Kapazitätsplanung.	☒	Vereinbarungen (SLA) zur Verfügbarkeit
☒	Hazard Protection (PE1.5.1): Die Einrichtungen zur Datenbearbeitung (Räumlichkeiten und Infrastruktur) werden von der Beauftragten angemessen gegen Beschädigung, Stromausfall, Feuer und andere Umwelt- und Naturgefahren, etc. geschützt.	☒	Business Continuity Management (BC2.3.1) : SuperX GmbH stellt sicher, dass Pläne und Vorkehrungen zur Aufrechterhaltung des Geschäftsbetriebs regelmässig getestet werden. Dies gilt für kritische Geschäftsprozesse sowie# Anwendungen, Systeme und Infrastruktur.
☒	Konzept zur Sicherung und Wiederherstellung von Daten (Backup, Restore, Recovery) durch den Auftragnehmer.	☒	EDR (Endpoint Detection and Response)
☒	Access Control Arrangements (SY.2): SuperX GmbH stellt sicher, dass der Betrieb von Systemen, Anwendungen und Infrastruktur durch durchgängige und nachvollziehbare Backups und Recovery Prozesse, Change-Management, Kapazitätsmanagement sowie Monitoring der Leistung und Verfügbarkeit sichergestellt wird.	☒	Business Continuity Management (BC1.1.1): SuperX GmbH verfügt über eine unternehmensweite, aktuelle Business Continuity Strategie und Prozesse. Diese werden durch eine widerstandsfähige technische Infrastruktur und ein effektives Krisenmanagement unterstützt.

☒	AWS RDS - verschlüsselte Backups, die in verschiedenen Datenzentren in der jeweiligen AWS Region gespeichert werden.		

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchstabe d DSGVO; Art. 25 Abs. 1 DSGVO)

Referenz zu ISO 27001 Annex A: A.5.36 Compliance with policies, rules and standards for information security; A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.15 Logging; A.8.16 Monitoring activities; A.5.24 Information security incident management planning and preparation; A.5.25 Assessment and decision on information security events.

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig überprüft, bewertet und bei Bedarf angepasst. Dies erfolgt insbesondere durch interne Kontrollen, Audits, Management-Reviews, Schwachstellenanalysen, Patch- und Änderungsmanagement, Auswertung von Sicherheitsereignissen sowie die Überprüfung von Berechtigungen, Richtlinien und technischen Baselines. Erkenntnisse aus Vorfällen, Tests oder externen Anforderungen fließen in die Weiterentwicklung der Maßnahmen ein.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	☒	Information Risk Assessment (IR1.3.1): SuperX GmbH bewertet Datensicherheitsrisiken regelmässig mittels systematischer Assessments und überwacht deren Entwicklung.
☒	Es sind Verfahren zur regelmäßigen Bewertung/Überprüfung etabliert, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management).	☒	Security Assurance Programme (AS1.1.1): SuperX GmbH gewährleistet, dass die Effizienz der Cyber- und Informationssicherheitsmassnahmen regelmässig durch nachvollziehbare Verfahren validiert und geprüft werden (z.B. durch Audits, Penetrationstests sowie Sicherheits- und Risikoüberwachung).

☒	Technical Vulnerability Management (TP2.1.1): SuperX GmbH stellt sicher, dass sie Cyber- und Informationssicherheitsgefahren und Schwachstellen in Anwendungen, Systemen und Infrastruktur durch strukturierte Prozesse zeitnah erkennt und behebt.	☒	Security Incident Management Framework (SE2.1.1): SuperX GmbH garantiert das Vorhandensein eines Frameworks für das Management von Datensicherheitsverletzungen. Sie stellt sicher, dass Prozesse für die Identifikation, Meldung, Reaktion, Wiederherstellung und nachträgliche Überprüfung von Verletzungen oder Ereignissen bestehen.
☒	Es ist ein Incident-Response-Management etabliert, so dass auf Datenschutzvorfälle zeitnah, fristgerecht (72-Stunden-Frist) und effizient reagiert werden kann. Der DSB ist in den Prozess integriert und berät die Geschäftsführung zur Entscheidung, ob der Vorfall meldepflichtig ist.	☒	Patch- und Änderungsmanagement
☒	EDR (Endpoint Detection and Response)		

6. Systemverwaltung

Referenz zu ISO 27001 Annex A: A.8.9 Configuration management; A.8.2 Privileged access rights.

Systeme, Endpunkte und sicherheitsrelevante Infrastrukturen werden zentral oder nach einheitlichen Vorgaben administriert. Administrative Konten sind besonders geschützt, werden getrennt von Standardkonten geführt und nur einem begrenzten Personenkreis zugewiesen. Änderungen an Systemkonfigurationen, sicherheitsrelevanten Parametern und produktionsnahen Umgebungen unterliegen einem dokumentierten Freigabe- und Änderungsprozess.

Folgende konkrete Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Hard- und Software werden von einer zentralen Stelle nach einheitlichen Vorgaben konfiguriert.	☒	Network (NC2.1.1): SuperX GmbH stellt sicher, dass externe Netzwerkverbindungen zu Anwendungen, Systemen und Infrastruktur eingeschränkt sind. Diese Verbindungen werden zudem protokolliert.

☒	Eine Inventarisierung der Hardware findet statt.	☒	Asset Ownership (AM1.2.2): SuperX GmbH schützt physische Anwendungen, Systeme und Infrastruktur, die einen Bezug zu den vertraglich bearbeiteten Personendaten aufweisen. Dies geschieht während ihres gesamten Lebenszyklus unter Einhaltung der Anforderungen an die Datensicherheit.
☒	System Development (SD1.1.2): SuperX GmbH stellt sicher, dass die (Weiter-)Entwicklung von Anwendungen und Systemen entlang von strukturierten und nachvollziehbaren Verfahren ablaufen, die mitunter sicherstellen, dass Cyber- und Informationssicherheits-anforderungen angemessen implementiert werden.	☒	Machine Learning Systems (UA3.2.2): SuperX GmbH stellt sicher, dass die eingesetzten ML- und KI-Modelle hinsichtlich Leistung, Sicherheit, Transparenz und ethischen Richtlinien überprüft werden. Zur kontinuierlichen Gewährleistung werden sie überwacht und/oder regelmässig aktualisiert
☒	Network (NC1.1.1): SuperX GmbH garantiert, dass die Netzwerk- und Kommunikationsinfrastruktur gemäss aktuell anerkannten Sicherheitsstandards konfiguriert sind.		

7. Mobiles Arbeiten / Mobile Datenträger

Referenz zu ISO 27001 Annex A: A.6.7 Remote working; A.8.1 User endpoint devices; A.8.24 Use of cryptography.

Für mobiles Arbeiten bestehen verbindliche Sicherheitsvorgaben, die insbesondere Geräteschutz, verschlüsselte Speicherung, gesicherte Fernzugriffe, Verlustmeldungen, Bildschirm- und Zugriffssperren sowie den Umgang mit lokalen Datenbeständen regeln. Mobile Endgeräte werden soweit möglich zentral verwaltet; sicherheitsrelevante Einstellungen, Softwarestände und Schutzmaßnahmen können zentral durchgesetzt werden. Die Nutzung externer Datenträger ist auf freigegebene Fälle beschränkt und technisch sowie organisatorisch abgesichert.

Folgende Maßnahmen hat die SuperX GmbH umgesetzt:

☒	Richtlinie für mobiles Arbeiten	☒	Es existiert eine Notfall- und Handlungsanweisung im Verlustfall von Hardware.

☒	Mobile Device Management	☒	Beschäftigte werden über eine Vereinbarung zum mobilen Arbeiten zum Datenschutz, zur Datensicherheit und zur Verschwiegenheit verpflichtet.
☒	Endpoint Device Configuration (HE2.1.5): SuperX GmbH stellt sicher, dass sensible Informationen, die auf Endgeräten bearbeitet werden, gegen Verlust, Diebstahl und unautorisierte Offenlegung geschützt sind (z.B. durch Verschlüsselung, physische Anwendungskontrollen etc.).		

8. Abschlussklausel

Die beschriebenen technischen und organisatorischen Maßnahmen werden von SuperX GmbH regelmäßig sowie anlassbezogen überprüft, bewertet und bei Bedarf angepasst. Anlassbezogene Anpassungen erfolgen insbesondere bei wesentlichen Änderungen der verarbeiteten Daten, der eingesetzten Systeme und Prozesse, der Bedrohungslage, der eingesetzten Unterauftragnehmer, der rechtlichen Anforderungen oder der angebotenen Leistungen. SuperX GmbH ist berechtigt, diese Maßnahmen weiterzuentwickeln, zu ersetzen oder zu ändern, sofern hierdurch das vertraglich geschuldete und datenschutzrechtlich erforderliche Schutzniveau nicht unterschritten wird. Maßgeblich ist jeweils die aktuelle Fassung der TOM, die den Vertragsparteien auf Anforderung zur Verfügung gestellt wird. Diese Beschreibung begründet keine Beschränkung auf die ausdrücklich genannten Einzelmaßnahmen; maßgeblich ist vielmehr das insgesamt gewährleistete Schutzniveau.

Aus Sicherheitsgründen enthält diese Beschreibung nicht zwingend sämtliche technischen Implementierungsdetails, sondern eine dem Zweck der Nachweisführung angemessene Darstellung der wesentlichen Schutzmaßnahmen.

9. Status der jährlichen Überprüfung der TOM

Status der jährlichen Überprüfung der TOM					
Datum	**Prüfgegenstand**	**Prüfergebnis**	**Stand Anpassungen** (soweit erforderlich)	**Externer Prüfer**	**Bearbeitung intern / Abstimmung mit Prüfer**
22.01.2024	„Verpflichtung der Beschäftigten auf den vertraulichen Umgang mit personenbezogenen Daten (Art. 28 Abs. 3 DSGVO).“	Die Verpflichtung liegt aktuell nur für deutschsprachige Mitarbeiter vor. Es ist zusätzlich eine Version in englischer Sprache zu erstellen.	erledigt, 09.02.2024	DSB	Madeline Rennen
25.01.2024	TOM in Gänze (jährliche Gesamtprüfung)	Alle Maßnahmen sind weiterhin umgesetzt wie beschrieben und gewährleisten ein angemessenes Schutzniveau.	n/a	DSB	Maurice Pomsel
03.02.2025	TOM in Gänze (jährliche Gesamtprüfung)	Alle Maßnahmen sind weiterhin umgesetzt wie beschrieben und gewährleisten ein angemessenes Schutzniveau.	n/a	DSB	Maurice Pomsel
22.05.2026	TOM in Gänze (jährliche Gesamtprüfung)	Alle Maßnahmen sind weiterhin umgesetzt wie beschrieben und gewährleisten ein angemessenes Schutzniveau. Es sind umfangreiche weitere Maßnahmen umgesetzt worden, die in den TOM noch entsprechend zu dokumentieren sind.	erledigt, 09.07.2026	DSB	Fabian Wernecke, Maurice Pomsel

Appendix 1: Details of the data processing*

Name of the main contract	Authorised recipient and DPO Principal	Instruction recipient and DPO Contractor	Subject of the data processing	Categories of personal data	Categories of data subjects	Purpose of the data processing	Duration of the contract
Service Agreement	You are obliged to inform us of your authorised representative (m/f/d) and - if applicable - your data protection officer (m/f/d) (e.g. by e-mail)	WB: Mika Hally DPO: Kathrin Siegmund (external), datenschutz@superchat.de	Setting up the user account for the Principal's employees Provision of the "Superchat" messaging platform Processing of personal data in the context of the use of the "Superchat" messaging platform	The personal data processed via the services is determined and controlled by the Principal at its own discretion and may include the following categories of personal data: – Inventory, contact and communication data of the Principal's prospects and customers – Name of the employee and communication content with the Principal's prospects and customers	Customers of the Principal, Interested parties of the Principal, Employees of the Principal	Storage, use and disclosure for the purpose of providing the services Support	Corresponds with the service agreement

*Only in the case of the additional booking of consulting services for the CRM integration of Superchat, SuperX GmbH also receives access to the Principal's CRM system and thus, if necessary, access to the Principal's customer data stored there. The purpose of this processing is to support the Principal in integrating Superchat into its CRM solution and to optimise the interaction between the CRM solution and Superchat

Appendix 2: List of other processors (subcontractors)

General subcontractors (core product ‘Superchat’)

Company, address	**Type and purpose of processing**	**Type of data**	**Categories of data subjects**	**Permissibility of processing outside the EU**
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg	Hosting	- Inventory, contact and communication data of the Principal's contacts and customers - Name of the employee of the Principal and communication with the contact and customer of the Principal	Contacts, customers and employees of the Principal	Processing in the EU. If, in exceptional cases, data is transferred to Amazon Web Services, Inc. in the USA: Adequacy decision, EU Standard Contractual Clauses (hereinafter ‘SCCs’), participation in the EU-US Data Privacy Framework (DPF participation’) Additional measures: client-side encryption; AWS TOM (Annex I: Link)
Auth0, Okta Inc, 100 1st St Suite 150, San Francisco	login	- User name, Email address, Password	Employees of the Principal	USA: Adequacy decision, SCC, DPF participation Information security documentation (link)

DataDog, 620 8th Avenue, Floor 45, New York, NY 10018, USA	Application Performance Monitoring to monitor the system stability, performance, and availability of the platform, as well as detecting technical issues early on.	- Application logs, IP address, client user agent, browser ID, name and email address of the Principal's employees	Employees of the Principal	USA: Adequacy decision, SCC, DPF participation.
Intercom, 55 2nd Street, 4th Floor, San Francisco, CA, United States	Live chat for support requests	- IP address, name, email address, location data, device information, browser type, operating system of the Principal's employees	Employees of the Principal	USA: Adequacy decision, SCC, DPF participation TOM: Annex II (link) Data Region: EU
OneSignal, 201 South B Street, San Mateo, California 94401	Storage and use for the purpose of providing notification services	- Inventory, contact and communication data of the Principal's contacts and customers - Name of the employee of the Principal and communication with the contact and customer of the Principal	Contacts, customers and employees of the Principal	USA: Adequacy decision, SCC, DPF participation. OneSignal is ISO 27001 and SOC 2 Type II certified. Data Region: EU
Pusher Ltd., MessageBird UK Limited, 3 More London Riverside, 4th Floor, London, United Kingdom, SE1 2AQ	Provision of web and mobile app functionality	- First name/surname, Email, telephone number, Message content, IP of user	Contacts, customers and employees of the Principal	UK Adequacy decision Data Region: EU (Ireland) Pusher Ltd. is ISO 27001 certified.

Sentry.io, Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Error and exception monitoring. Helps identify, analyze, and resolve software errors, crashes, and unexpected system conditions.	- Application logs, IP address, client user agent, browser ID, name and email address of the Principal's employees	Employees of the Principal	USA: Adequacy decision, SCC, DPF participation. Sentry.io is SOC Type II and ISO 27001 certified.

Subcontractors for the optional use of „E-Mail“ as a communication channel

Nylas, Inc, 944 Market St, San Francisco, CA	Storage and use for the purpose of providing e-mail services (use of this service provider only if this communication channel is connected in Superchat)	- Inventory, contact and communication data of the Principal's contacts and customers - Name of the Principal's employee and communication with the Principal's contact and customer	Contacts, customers and employees of the Principal	USA: Adequacy decision, SCC, DPF participation Nylas is ISO 27001 certified. Security Whitepaper Data Region: EU

Subcontractors for the optional use of „SMS“ as a communication channel

Twilio Inc, 375 Beale Street, Suite 300, San Francisco, CA	Storage and use for the purpose of providing the SMS services (use of this service provider only if this communication channel is connected in Superchat before 2025). Customers who have been using Superchat from 2025 onwards	- Inventory, contact and communication data of the Principal's contacts and customers - Name of the Principal's employee and communication with the Principal's contacts and customers	Contacts, customers and employees of the Principal	USA: Adequacy decision, Binding Corporate Rules (BCR), SCC, DPF participation TOM (Schedule 2: Link) Twilio is ISO 27001 certified.

	operate their own Twilio account and Superchat only connects to this account via the API.			

Subcontractors for the optional use of „WhatsApp“ as a communication channel

Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland	Storage and use for the purpose of providing WhatsApp services via the WhatsApp Cloud API (use of this service provider only if this communication channel is connected in Superchat)	- Inventory, contact and communication data of the Principal's contacts and customers - Name of the Principal's employee and communication with the Principal's contacts and customers	Contacts, customers and employees of the Principal	Processing generally takes place in Europe. However, during transmission, messages may also be transported via a Cloud API server in the USA, whereby all message content in transit (cache, queues) is automatically deleted after 60 minutes. This transmission is secured via: Adequacy decision, SCC, DPF participation Additional measures: encrypted transmission Data Region: EU (via Local Storage Solution) Meta is SOC Type II certified TOM: Link Data Privacy and Security at Meta

Subcontractors for the optional File-Upload-Feature

Cloudconvert, Lunaweb GmbH Nördliche Münchner Straße 14a, DE-82031 Grünwald, Germany	Conversion/compression of file uploads (use of this service provider only if file uploads are made in Superchat)	- Contents of uploaded files - User ID of the Principal's employee	Employees of the Principal	EU Cloudconvert is ISO 27001 certified

Subcontractors for the optional „KI-Chatbot"-Feature

LangChain, Inc., 42, Decatur St., San Francisco, CA 94103, USA	Provision and orchestration of AI functionalities within the platform. Technical infrastructure for processing and managing AI workflows, particularly for connecting to and using language models.	- End customer data: Messages / potential contact attributes	Customers of the Principal	USA: Adequacy decision, SCC Data Region: Germany / AWS self hosted Additional measures: encrypted transmission, MFA, restrictive authorisation concept (only administrators have access) LangChain Inc. is SOC II certified.
OpenAI, OpenAI Ireland Ltd, 1st Floor, The Liffey, Trust Centre, 117-126 Sheriff Street Upper,	OpenAI API	- - SuperX GmbH transmits a Client ID to OpenAI, which serves to distinguish it from other SuperX GmbH - customers. This client ID remains anonymous to	None	The AI learns exclusively within the scope of the Principal's own client ID. If, in exceptional cases, a transfer to OpenAI, L.L.C. in the USA takes place the transfer is secured through:

Dublin 1, D01 YC43, Ireland		OpenAI. Only SuperX GmbH can establish a reference to a SuperX GmbH customer and, if applicable, its employees. - No personal data is processed by OpenAI unless the Principal decides to integrate personal data into prompts and/or decides to disclose the name of the end customer.		Adequacy decision, SCC Additional measures: encrypted transmission TOM (Exhibit B: Link) OpenAI is SOC Type II certified.

Subcontractors for the optional “AI Call” feature

Assembly.ai Inc., 169 Madison Ave STE 38365, New York, NY 10016, USA	Speech-to-text engine for audio transcription	- Audio content that may contain personal data, transcribed texts, names, locations, email addresses, phone numbers, occupations, and titles	Customers, contacts of the client (caller)	USA: Adequacy decision, SCC, DPF participation Additional technical measures: Data Retention 11 days
Cartesia AI, Inc., 1766 18th Street, San Francisco, California 94017, USA	Text-to-speech engine for audio transcription	- Text prompts that may contain personally identifiable information (e.g., names, phone numbers), and generated audio files that may contain personally identifiable information	Customers, contacts of the client (caller)	USA: Adequacy Decision, SCC Cartesia is SOC 2 Type II certified
Eleven Labs Inc., 169 Madison Ave #2484, Ne	Text-to-speech engine for audio transcription	- Text prompts that may contain personally identifiable information (e.g., names, phone numbers), and generated	Customers, contacts of the client (caller)	USA: Adequacy Decision, SCC, DPF participation.

w York, NY 10016, USA		audio files that may contain personally identifiable information		Additional technical measures: Zero retention for voice output (prevents audio and text data from being stored on ElevenLabs servers after processing) Data Region: EU Eleven Labs Inc. is SOC 2 Type II and ISO 27001 certified
LiveKit Inc., 4285 Payne Avenue Suite 9154, San Jose, California 95157, USA	Connects the Twilio call to the AI so that Elevenlabs can respond in real time	- Voice data - Transcript data - Technical connection data - Communication metadata	Customers, contacts of the client (caller)	USA: Adequacy Decision, SCC, DPF Participation Data Region: EU Livekit Inc. is SOC 2 Type II certified
OpenAI, OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	Speech-to-text engine for audio transcription	- Audio content that may contain personal data, transcribed texts.	Customers, contacts of the client (caller)	– Data processing is contractually limited to servers in the European Union. – The AI learns exclusively within the scope of the client's own unique client ID. In exceptional cases where data is transferred to OpenAI, L.L.C. in the United States: SCC Additional measures: encrypted transmission, zero retention for transcriptions (audio data is not stored on the server after transcription)

				TOM (Exhibit B: Link) OpenAI is SOC Type II certified.
Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA	Call Handling, Connecting an IP Telephony Infrastructure to the Public Switched Telephone Network (PSTN)	- Call data (e.g., phone number, timestamp) - Metadata (e.g., IP addresses, SIP metadata)	Customers, contacts of the client (caller)	USA: Adequacy Decision, Binding Corporate Rules (BCR), SCC, DPF Participation TOM (Schedule 2: Link) Twilio is ISO 27001 certified.

Appendix 3: Technical and organisational measures of the contractor

Version 1.3

This description of the technical and organisational measures ('TOM') sets out in detail the measures implemented by SuperX GmbH to protect personal data in connection with the services provided by SuperX GmbH. It serves as evidence of a level of protection appropriate to the risk, taking into account Articles 24, 25, Articles 28 and 32 of the GDPR, whilst taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons. SuperX GmbH regularly reviews the measures described below and develops them further in line with the technical, organisational and legal framework. The measures described in this document apply to all systems, processes and organisational units insofar as they process personal data for the provision of the contractual services. Where SuperX GmbH engages sub-processors, these are incorporated into the data protection framework on the basis of contractual provisions and risk-based selection and control processes.

These TOM form an integral part of the data processing agreement and describe the measures implemented at the time of the current version of these TOM.

1. General measures

Reference to ISO 27001 Annex A: A.6.3 Information security awareness, education and training; A.5.1 Policies for information security; A.5.37 Documented operating procedures

SuperX GmbH has implemented the following specific general measures:

☒	Employees are bound by their employment contracts to refrain from disclosing trade secrets.	☒	A company Data Protection Officer (DPO) has been appointed.
☒	Regular data protection briefings and training sessions are provided for employees.	☒	The DPO is involved in the event of security incidents.
☒	A data protection management system is in place.	☒	An Information Security Management System (ISMS) has been established.
☒	A process has been established for the technical and organisational handling of data subjects' rights (requests for access and erasure), which ensures that these are processed within the prescribed time limits.	☒	In software development, the principles of 'Privacy by Design' and 'Privacy by Default' (data protection through technical design and privacy-friendly default settings) are taken into account and adhered to.

☒	Where processing operations are identified that fall under Article 35 of the GDPR and SuperX GmbH acts as the data controller, SuperX GmbH carries out the necessary data protection impact assessment. Where SuperX GmbH acts as a data processor for the relevant processing operation, SuperX GmbH assists the client in carrying out the data protection impact assessment.	☒	Obligation of employees to treat personal data confidentially (Article 28(3) of the GDPR).
☒	There is a documented system configuration.	☒	Technical and organisational measures are reviewed at regular intervals.
☒	Security incidents are documented.	☒	Data Privacy (IM1.4.1): SuperX GmbH defines roles and responsibilities regarding the handling of personal data (data protection) throughout the organisation. Furthermore, SuperX GmbH has a Data Protection Officer.
☒	Security Agreements (PM1.2.1): SuperX GmbH sets out binding roles and responsibilities regarding data security within its organisation. It communicates these to internal and external staff and ensures compliance.	☒	Information Lifecycle (IM1.2.1): SuperX GmbH guarantees that critical and sensitive personal data is protected at every stage of the information lifecycle. This covers the creation, processing, transmission, storage and deletion of information, regardless of whether it is in digital or physical form.

☒	Information Classification and Handling (IM1.3.1): SuperX GmbH has a framework in place for the consistent and comprehensive determination of protection requirements. This framework is also used to classify business and personal data, as well as systems, applications and infrastructure.	☒	Information Classification and Handling (IM1.3.3): SuperX GmbH guarantees a consistent and structured approach that protects personal data, in accordance with its classification, against unauthorised alteration, unauthorised access or disclosure, and loss.

2. Confidentiality (Article 32(1)(b) of the GDPR)

2.1. Admission control

Reference to ISO 27001 Annex A: A.7.1 Physical security perimeters; A.7.2 Physical entry; A.7.3 Securing offices, rooms and facilities; A.7.4 Physical security monitoring.

Admission control comprises measures designed to prevent unauthorised persons from gaining access to data processing facilities used to process and utilise personal data.

The measures listed below are implemented at SuperX GmbH depending on the level of protection required.

☒	Window grilles	☒	Function- and role-based access authorisations for the server room
☒	Manual locking system	☒	Key management (key list, key issue)
☒	Careful selection of cleaning staff		

2.2. Equipment access control

Reference to ISO 27001 Annex A: A.5.15 Access control; A.5.16 Identity management; A.5.17 Authentication information; A.5.18 Access rights; A.8.5 Secure authentication.

Equipment access control comprises measures to prevent unauthorised persons from using data processing systems.

SuperX GmbH has implemented the following specific measures:

☒	Authentication using username and password	☒	Encryption of all web pages (SSL, HTTPS)
☒	Secure storage of data media (backup tapes, hard drives, etc.)	☒	Encryption of email attachments
☒	Use of anti-virus software / malware protection software (TP1.2.1): SuperX GmbH ensures that applications, systems and infrastructure exposed to malware and cyber-attacks have up-to-date malware protection software installed.	☒	Use of VPN technology (Engineering, Production Database)
☒	Multi-factor authentication	☒	Mobile Device Management
☒	Use of a software firewall	☒	Use of a document shredder
☒	Encryption of data storage media in PCs and laptops (e.g. BitLocker)	☒	Key management policies (guidelines/instructions on the issue of keys)
☒	Password policy (minimum length, complexity, validity period, locking/deletion, etc.)	☒	‘Clean Desk’ policy

☒	Use of lockable waste bins for paper, files and data storage media	☒	Creation of personal user profiles
☒	Encryption of email transmission (TLS 1.2, TLS 1.3)	☒	Multi-factor authentication
☒	Access Control Arrangements (AC1.2.1): SuperX GmbH ensures that access to applications, systems, infrastructure and personal data is granted only to authorised persons or services. These must have relevant duties or responsibilities. Access is granted in accordance with the need-to-know principle.	☒	Encryption at rest: ● For databases: (AWS RDS) -> SYMMETRIC_DEFAULT ● For files (AWS S3): Key management -> AWS KMS (AWS-managed keys), annual key renewal

2.3. Data access control

Reference to ISO 27001 Annex A: A.5.15 Access control; A.5.18 Access rights; A.8.15 Logging; A.8.16 Monitoring activities; A.8.2 Privileged access rights; A.8.24 Use of cryptography; A.8.25 Key management.

Data access control comprises measures which ensure that those authorised to use a data-processing system can access only the data covered by their access authorisation, and that personal data cannot be read, copied, altered or deleted without authorisation during processing, use and after storage. In particular, cryptographic measures (encryption), ensure that data – particularly during transmission – can no longer be read without the key, thereby preventing unauthorised access by third parties.

SuperX GmbH has implemented the following measures:

☒	Administrators have different areas of responsibility	☒	Access Control Arrangements (AC1.2.1): SuperX GmbH ensures that access to applications, systems and infrastructure is granted in accordance with the need-to-know principle.

☒	The number of administrators is kept to a minimum according to their area of responsibility	☒	Cryptographic Solutions (CP1.1.1): To ensure confidentiality, integrity, authenticity and non-repudiation, SuperX GmbH uses recognised cryptographic methods and solutions. These comply with at least the current standard. Encryption **at rest**: ● For databases: (AWS RDS) -> SYMMETRIC_DEFAULT (LINK) ● For files (AWS S3) (LINK) Key management -> AWS KMS (AWS-managed keys), annual key renewal Encryption **in transit**: AWS ELB Security Policy TLS13-1-2-2021-06 (LINK)
☒	Function- and role-based authorisation model	☒	Offboarding: Permissions are revoked when employees leave the organisation or when responsibilities change.
☒	Clean Desk Policy	☒	Procedure for revoking access authorisations (e.g. when an employee leaves the company)

2.4. Separation control

Reference to ISO 27001 Annex A: A.8.31 Separation of development, test and production environments; A.8.22 Segregation of networks; A.8.12 Data leakage prevention; A.5.15 Access control.

Separation control comprises measures that ensure that data collected for different purposes can be processed separately.

SuperX GmbH has implemented the following measures:

☒	Definition of database access rights.	☒	Separation of data from different clients.
☒	Separation of production and test systems.	☒	Control via an authorisation scheme

2.5. Pseudonymisation

Reference to ISO 27001 Annex A: A.8.11 Data masking; A.8.24 Use of cryptography.

Where the purpose of processing permits, personal data is processed in a pseudonymised form. The identification key or other supplementary information is stored separately, protected independently and made accessible only to a strictly limited group of individuals. The selection of pseudonymisation methods is based on the purpose and risk, taking into account the state of the art.

3. Integrity (Article 32(1)(b) of the GDPR)

3.1. Control of disclosure

Reference to ISO 27001 Annex A: A.8.24 Use of cryptography; A.5.14 Information transfer; A.8.21 Security of network services.

Control of disclosure comprises measures that ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission, whilst in transit or whilst stored on data media. It must also be possible to verify and determine to whom (which bodies) personal data is to be or has been transferred.

SuperX GmbH has implemented the following measures:

☒	Use of a VPN and firewall (see above).	☒	Encryption of email attachments
☒	Encryption of email transmission (TLS 1.2, TLS 1.3)	☒	Multi-factor authentication when accessing external systems.
☒	Encryption **in transit**: AWS ELB Security Policy TLS13-1-2-2021-06 (LINK)		

3.2. Input control

Reference to ISO 27001 Annex A: A.8.15 Logging; A.8.16 Monitoring activities; A.5.37 Documented operating procedures.

Input control comprises measures that ensure it is possible to subsequently verify and determine whether, and by whom, personal data has been entered into, modified or removed from data processing systems.

SuperX GmbH has implemented the following measures:

☒	The IT systems in use have a logging function.	☒	Customer Connections (BA2.3.2): SuperX GmbH ensures the confidentiality and integrity of personal data at all times during processing (in particular during input, access, storage, processing and output) in applications through integrated measures and controls.

3.3. Documentation control

Reference to ISO 27001 Annex A: A.5.37 Documented operating procedures; A.5.1 Policies for information security; A.5.9 Inventory of information and other associated assets.

Documentation control comprises measures that ensure that the procedures for processing personal data are documented in such a way that they can be reasonably traced.

SuperX GmbH has implemented the following measures:

☒	Maintaining a record of processing activities	☒	Documentation of the security policy is in place.
☒	Documentation of the IT systems used and their system configuration	☒	Security incidents are documented.
☒	A data deletion policy is in place, setting out all retention periods and deletion dates. Where technically feasible, automated deletion routines are implemented in the databases to flag data for deletion or physically remove it once the defined retention		

	periods have expired, without the need for manual intervention. As an alternative to deletion, data is anonymised once it is no longer required for its intended purpose in such a way that it can no longer be linked to any individual (statistical processing). Where physical data carriers are used, these are destroyed in accordance with DIN 66399 (Protection Class 2/3) by certified specialist disposal companies.		

3.4. Contract management

Reference to ISO 27001 Annex A: A.5.19 Information security in supplier relationships; A.5.20 Addressing information security within supplier agreements; A.5.21 Managing information security in the ICT supply chain; A.5.22 Monitoring, review and change management of supplier services.

Control of processing on behalf of others comprises measures that ensure that personal data processed on behalf of others can only be processed in accordance with the instructions provided by the client.

SuperX GmbH has implemented the following measures:

☒	Data processing agreements are concluded with all service providers (Art. 28(3) GDPR). Supplier Contracts (SC1.3.1): SuperX GmbH sets out binding cyber and data security requirements for external suppliers and service providers. It obtains appropriate assurances and reviews them regularly.	☒	Transfers to third countries: Where processing activities are carried out by sub-processors in third countries, either an adequacy decision by the European Commission pursuant to Article 45 of the GDPR is in place for the third country in question (for transfers to the US, the service provider also holds a data privacy certification), or standard data protection clauses with other appropriate safeguards pursuant to Article 46 of the GDPR have been concluded.

☒	Careful selection of contractors and sub-processors (particularly with regard to data security).	☒	Contractual rights of supervision relating to compliance with data protection apply to all contractors.
☒	The client checks the contractor's documentation and security measures before data processing begins.	☒	The destruction or erasure of data in accordance with data protection regulations upon completion of the contract is regulated.

4. Availability, resilience, recoverability (Art. 32(1)(b), (c) GDPR)

Reference to ISO 27001 Annex A: A.8.13 Information backup; A.5.30 ICT readiness for business continuity; A.8.14 Redundancy of information processing facilities.

Availability control, resilience and recoverability comprise measures that ensure that personal data is protected against accidental destruction or loss.

SuperX GmbH has implemented the following measures:

☒	Storage of data backups at a secure, off-site location. (Amazon Web Services, Google)	☒	Security power strips in server rooms.
☒	Air conditioning in the server rooms.	☒	Equipment for monitoring temperature and humidity in server rooms.
☒	Fire extinguishers in server rooms.	☒	Surge protection.

☒	Smoke detectors in server rooms.	☒	Uninterruptible power supply (UPS)
☒	Backups / Backup and Restore (SR1.5.1): SuperX GmbH guarantees that applications (including their data) and systems are regularly backed up. In addition, regularly tested procedures are in place for recovery.	☒	Hard disk mirroring
☒	Virus protection	☒	Business Continuity Management (BC1.1.1): SuperX GmbH has a company-wide, up-to-date business continuity strategy and processes. These are supported by a resilient technical infrastructure and effective crisis management.
☒	Backup and Restore (SR1.5.2): SuperX GmbH ensures that backups and security measures are protected against loss, damage and unauthorised access.	☒	Contingency Plan
☒	Continuous monitoring of IT resources (CPU, RAM, storage space, network bandwidth) for threshold alerts and regular evaluation of capacity planning.	☒	Service Level Agreements (SLAs) for availability
☒	Hazard Protection (PE1.5.1): The data processing facilities (premises and infrastructure) are adequately protected by the data controller against damage, power failure, fire and other environmental and natural hazards, etc.	☒	Business Continuity Management (BC2.3.1): SuperX GmbH ensures that plans and measures to maintain business operations are tested regularly. This applies to critical business processes as well as applications, systems and infrastructure.

☒	Concept for the backup, restoration and recovery of data by the contractor.	☒	EDR (Endpoint Detection and Response)
☒	Access Control Arrangements (SY.2): SuperX GmbH ensures that the operation of systems, applications and infrastructure is safeguarded through consistent and traceable backup and recovery processes, change management, capacity management and monitoring of performance and availability.	☒	Business Continuity Management (BC1.1.1): SuperX GmbH has a company-wide, up-to-date business continuity strategy and processes. These are supported by a resilient technical infrastructure and effective crisis management.
☒	AWS RDS – encrypted backups stored in various data centres within the respective AWS region.		

5. Procedures for regular review, assessment and evaluation (Article 32(1)(d) of the GDPR; Article 25(1) of the GDPR)

Reference to ISO 27001 Annex A: A.5.36 Compliance with policies, rules and standards for information security; A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.15 Logging; A.8.16 Monitoring activities; A.5.24 Information security incident management planning and preparation; A.5.25 Assessment and decision on information security events.

The effectiveness of the technical and organisational measures is regularly reviewed, assessed and, where necessary, adjusted. This is carried out in particular through internal controls, audits, management reviews, vulnerability analyses, patch and change management, the evaluation of security events, and the review of authorisations, policies and technical baselines. Findings from incidents, tests or external requirements are incorporated into the further development of the measures.

SuperX GmbH has implemented the following measures:

☒	Privacy-friendly default settings (Art. 25(2) GDPR)	☒	Information Risk Assessment (IR1.3.1): SuperX GmbH regularly assesses data security risks through systematic assessments and monitors their development.

☒	Procedures for regular evaluation and review have been established to ensure the security of data processing (data protection management).	☒	Security Assurance Programme (AS1.1.1): SuperX GmbH ensures that the effectiveness of cyber and information security measures is regularly validated and tested using transparent procedures (e.g. through audits, penetration tests and security and risk monitoring).
☒	Technical Vulnerability Management (TP2.1.1): SuperX GmbH ensures that it promptly identifies and rectifies cyber and information security threats and vulnerabilities in applications, systems and infrastructure through structured processes.	☒	Security Incident Management Framework (SE2.1.1): SuperX GmbH guarantees the existence of a framework for managing data security breaches. It ensures that processes are in place for the identification, reporting, response, recovery and subsequent review of breaches or incidents.
☒	An incident response management system has been established to ensure that data protection incidents can be responded to promptly, within the required timeframe (72-hour deadline) and efficiently. The Data Protection Officer (DPO) is integrated into the process and advises the management on whether the incident is subject to mandatory reporting.	☒	Patch and change management
☒	EDR (Endpoint Detection and Response)		

6. System administration

Reference to ISO 27001 Annex A: A.8.9 Configuration management; A.8.2 Privileged access rights.

Systems, endpoints and security-relevant infrastructure are administered centrally or in accordance with standardised guidelines. Administrative accounts are subject to special protection, are managed separately from standard accounts and are assigned only to a limited group of

individuals. Changes to system configurations, security-relevant parameters and production-related environments are subject to a documented approval and change process.

SuperX GmbH has implemented the following specific measures:

☒	Hardware and software are configured by a central unit in accordance with standardised guidelines.	☒	Network (NC2.1.1): SuperX GmbH ensures that external network connections to applications, systems and infrastructure are restricted. These connections are also logged.
☒	An inventory of the hardware is carried out.	☒	Asset Ownership (AM1.2.2): SuperX GmbH protects physical applications, systems and infrastructure that are related to the personal data processed under contract. This is done throughout their entire lifecycle in compliance with data security requirements.
☒	System Development (SD1.1.2): SuperX GmbH ensures that the (further) development of applications and systems follows structured and traceable procedures, which, amongst other things, ensure that cyber and information security requirements are implemented appropriately.	☒	Machine Learning Systems (UA3.2.2): SuperX GmbH ensures that the ML and AI models used are reviewed in terms of performance, security, transparency and ethical guidelines. To ensure this on an ongoing basis, they are monitored and/or regularly updated
☒	Network (NC1.1.1): SuperX GmbH guarantees that the network and communication infrastructure are configured in accordance with currently recognised security standards.		

7. Mobile working / Mobile data storage devices

Reference to ISO 27001 Annex A: A.6.7 Remote working; A.8.1 User endpoint devices; A.8.24 Use of cryptography.

There are binding security requirements for mobile working, which specifically govern device protection, encrypted storage, secure remote access, loss reporting, screen and access locks, and the handling of local data sets. Mobile end devices are managed centrally wherever possible; security-related settings, software versions and protective measures can be enforced centrally. The use of external data storage media is restricted to authorised cases and is secured both technically and organisationally.

SuperX GmbH has implemented the following measures:

☒	Policy on mobile working	☒	There are emergency and action procedures in place in the event of hardware loss.
☒	Mobile Device Management	☒	Employees are bound by an agreement on mobile working to comply with data protection, data security and confidentiality requirements.
☒	Endpoint Device Configuration (HE2.1.5): SuperX GmbH ensures that sensitive information processed on end devices is protected against loss, theft and unauthorised disclosure (e.g. through encryption, physical application controls, etc.).		

8. Final clause

The technical and organisational measures described are reviewed, assessed and, where necessary, adapted by SuperX GmbH on a regular basis and as and when required. Adaptations made as and when required occur in particular in the event of significant changes to the data processed, the systems and processes used, the threat landscape, the subcontractors engaged, the legal requirements or the services offered. SuperX GmbH is entitled to further develop, replace or amend these measures, provided that this does not result in a level of protection falling below that contractually owed and required under data protection law. The current version of the TOM, which is made available to the contracting parties on request, shall prevail in each case. This description does not constitute a limitation to the specific measures expressly mentioned; rather, the overall level of protection guaranteed is decisive.

For security reasons, this description does not necessarily contain all technical implementation details, but rather a presentation of the essential protective measures appropriate to the purpose of providing evidence.

9. Status of the annual review of the TOM

Status of the annual review of the TOM					
Date	**Subject of the audit**	**Test result**	**Status of adjustments** (where necessary)	**External Auditor**	**Internal processing / Coordination with auditor**
22.01.2024	“Employees’ obligation to treat personal data confidentially (Article 28(3) of the GDPR).”	This obligation currently applies only to German-speaking staff. An English-language version must also be produced.	Completed, 9 February 2024	DPO	Madeline Rennen

25.01.2024	TOM in full (annual comprehensive audit)	All measures continue to be implemented as described and ensure an adequate level of protection.	n/a	DPO	Maurice Pomsel
03.02.2025	TOM in full (annual comprehensive audit)	All measures continue to be implemented as described and ensure an adequate level of protection.	n/a	DPO	Maurice Pomsel
22.05.2026	TOM in full (annual comprehensive review)	All measures continue to be implemented as described and ensure an appropriate level of protection. Extensive further measures have been implemented, which still need to be documented accordingly in the TOM.	Completed, 9.07.2026	DPO	Fabian Wernecke, Maurice Pomsel