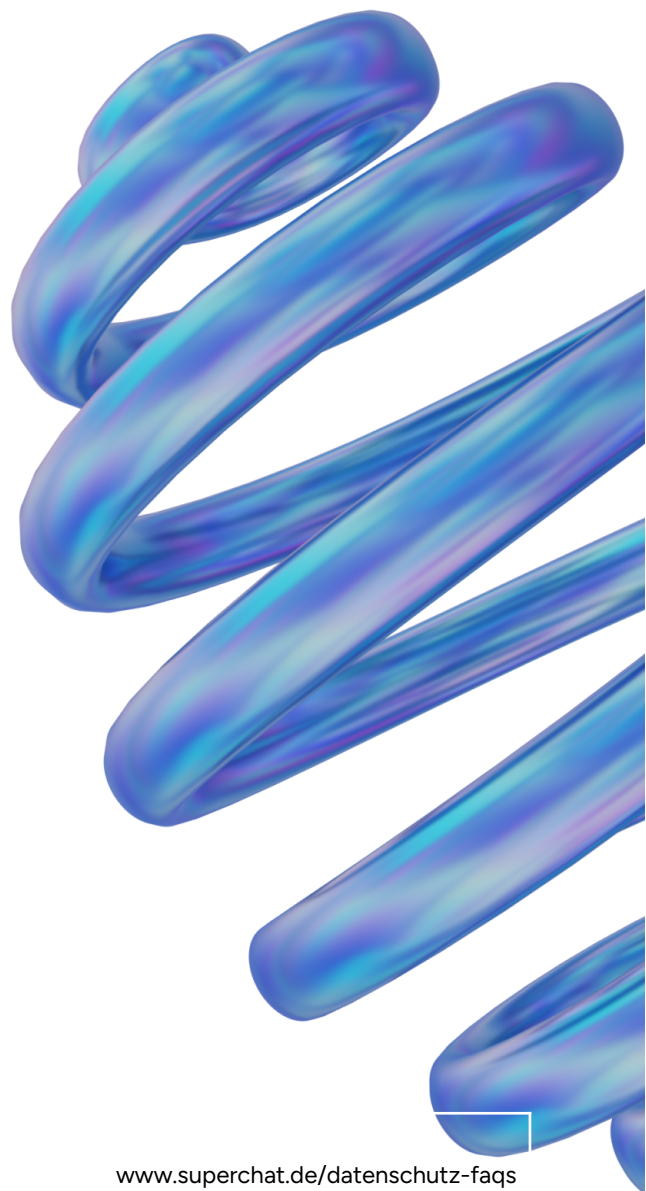


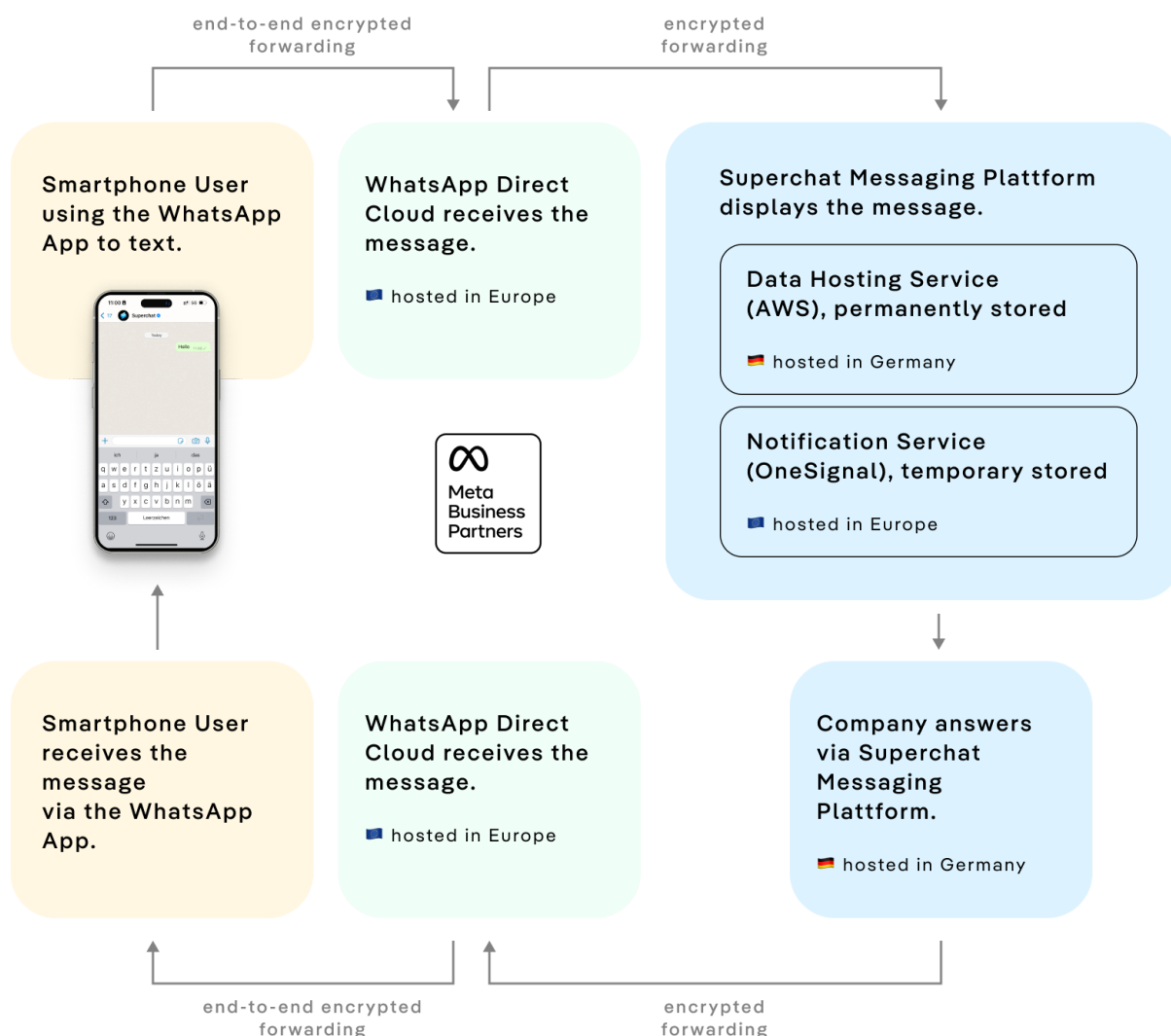
The Superchat Data Protection Folder

Messaging in compliance with EU data protection regulations.

SuperX GmbH
Prenzlauer Allee 242 / Haus 7
Berlin, Germany
www.superchat.com
datenschutz@superchat.de



An end customer sends a message to the WhatsApp number of a Superchat account. The message is end-to-end encrypted from their device to the WhatsApp Direct Cloud. Meta has no access to the content of the message. The message is then forwarded from the WhatsApp Direct Cloud to Superchat. In the WhatsApp Direct Cloud, the message is stored only temporarily until it has been successfully delivered to Superchat. The data is stored at the location within your country. If no META server is available there, your data will be stored in Germany. Once the message has arrived in Superchat, it is stored there and can be viewed and answered by the Superchat account. Access to the data is secured through regular internal audits to ensure maximum security.



Summary

Agreement on Data Processing (Art. 28 (3) GDPR)	4
Annex 1: Details of the Processing	3
Annex 2: List of Sub-processors	7
Processing activities in the context of your use of Superchat:	7
Processing in the context of administering and managing your customer account with SuperX GmbH:	12
Annex 3: Technical and Organisational Measures implemented by the Processor	15
Data Protection Brief Expert Opinion	22

At Superchat, we place great importance on data protection and transparency. Most of our data protection information is publicly available. For frequently asked questions about data protection, please visit: www.superchat.de/datenschutz-faqs

In addition, you will find your Data Processing Agreement (DPA) and template texts on our website. We want to ensure that you have all the information you need to trust the way your data is handled.

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 information 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:

- 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. Type and purpose of processing

- 2.1 Access to personal data is necessary for the performance of the service agreement with the Principal.
- 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. Type of personal data and categories of data subjects

- 3.1 The types of personal data affected by the Contractor's data processing are listed in **Appendix 1**.
- 3.2 The categories of data subjects affected by the processing are listed in **Appendix 1**.

4. Rights and obligations of the Principal

- 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 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.

- 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 The Principal shall have the right to demand the surrender of the data, data results or databases 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 databases 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 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.
- 5.4 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.
- 5.5 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.
- 5.6 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).
- 5.7 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 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

- Pseudonymisation and encryption of personal data.

- 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 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.

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.

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.

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.

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**.

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 (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, 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 user 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 databases 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 stocks 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 databases 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 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 loophole 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.

Appendix 2: List of subprocessors

Processing of data in the course of your use of Superchat:

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.

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, SCC, 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)
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

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
LangChain, Inc., 42 Decatur St., San Francisco, CA 94103, USA	Provision of AI infrastructure	- End customer data: Messages / potential contact attributes	Customers of the Principal	USA: Adequacy decision, SCC Data Region: Germany / AWS self hosted LangChain Inc. is SOC II certified. Additional measures: encrypted transmission, MFA, restrictive authorisation concept (only administrators have access)
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
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
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
OpenAI, OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland	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 OpenAI. Only SuperX GmbH can establish a reference to a SuperX GmbH customer and, if applicable, its employees.	None	- Processing contractually limited to servers in Germany. - 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:

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

Processing in the context of the administration and support of your customer account at SuperX GmbH:

Company, address	Type and purpose of processing	Type of data	Categories of data subjects	Permissibility of processing outside the EU
Amplitude, 201 3rd Street, Suite 200, San Francisco, CA 94103	Analytics / Issue UX	- IP address, client user agent, browser ID, name and email address of the client's employees - User statistics	Employees of the Principal	USA: Adequacy decision, SCC, DPF participation.
Chargebee Inc., 909 Rose Avenue, Suite 950, North Bethesda, MD 20852	Invoicing via Chargebee's 'core billing'	- Name and email address of the Principal's employees	Employees of the Principal	USA: Adequacy decision, SCC, DPF participation.
DataDog, 620 8th Avenue, Floor 45, New York, NY 10018, USA	Application Performance Monitoring	- 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.
DocuSign, San Francisco, 221 Main St #800, United States	Conclusion of the DPA with SuperX GmbH (use of this service provider only if the standard DPA is not concluded)	- Name and email address of the Principal's employees	Employees of the Principal	USA: Adequacy decision, SCC, BCR Additional measures: encrypted transmission Data Region: EU Docusign is ISO 27001, ISO 27017, and ISO 27018 certified. TOM (Annex II: Link)

Google Ireland Limited Gordon House, Barrow Street Dublin 4., Ireland	Management of customer contracts, email correspondence	- Name and email address of the Principal's employees - Email content	Employees of the Principal	Data Region: EU. If, in exceptional cases, a transfer to Google LLC in the USA takes place the transfer is secured through: Adequacy decision, SCC, DPF participation.
Hubspot, 2 Canal Park, Cambridge, MA, United States	CRM, customer management	- State/region, postal code, country code, IP address, Principal user agent, browser ID, name and email of Principal's employees	Employees of the Principal	USA: Adequacy decision, SCC, DPF participation. Hubspot is SOC Type II certified. TOM (Annex 2: Link) Data Region: EU
Make.com, Voctářova 2449, Hlavní město Praha, Czech Republic	Automation in the context of customer management and support	- Name and contact details of the Principal's employees	Employees of the Principal	EU Make.com is ISO-27001 certified.
Satellite, sipgate GmbH, Gladbacher Straße 74, 40219 Düsseldorf, Germany	Telephony (DACH) in the context of customer administration and support	- Name and telephone number of the Principal's employees	Employees of the Principal	EU Sipgate only uses ISO 27001 certified data centres. TOM (Appendix 3: Link)

Sentry.io, Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Application Performance Monitoring	- Application logs, IP address, client user agent, browser ID, name 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.
Typeform, 163 Carrer De Bac De Roda Sant Martí, Barcelona, Spain	Conclusion of the DPA with SuperX GmbH (unless the standard DPA is concluded)	- Name and e-mail address of the Principal's employees	Employees of the Principal	EU Typeform is ISO 27001 certified. TOM (Annex II: Link)

Appendix 3: Technical and organisational measures of the contractor

Description of the technical and organisational measures of SuperX GmbH

Table of contents:

1. Summary of the measures taken.
2. General organisational measures.
3. Admission control.
4. Equipment access control.
5. Data access control.
6. Transfer control.
7. Input control.
8. Processing control.
9. Availability control.
10. Separation control.
11. Appendix: Status of the annual review of the TOM

1. Summary of the measures taken

1.	Pseudonymisation / encryption:
x	Measures to encrypt file attachments in emails, email transport, websites (see section 3 ff. below).
2.	Permanent safeguarding of: Confidentiality, integrity, availability, resilience of systems and services:
x	Confidentiality is guaranteed by access, entry and access control (see section 3 ff. below).
x	Integrity is ensured by securing the entire company network with a firewall and mobile device management (MDM).
x	Availability is ensured by back-ups (see section 3 ff. below).
x	Resilience is ensured by sufficient storage capacity on the servers used.
3.	Ability to restore the availability of and access to personal data in the event of an incident:
x	Rapid recovery is possible via back-ups.
x	An emergency power supply for the server room ensures reliability. (AWS)
4.	Review, assessment and evaluation of the effectiveness of the technical and organisational measures:
x	Automated, permanent monitoring of all systems takes place.
x	An annual audit is carried out by the data protection officer.
x	There are annual reports on technical failures.
x	The hardware is regularly replaced and maintained.

2. General organisational measures

Measures that describe the instruction of employees at SuperX GmbH in the handling and protection of personal data.

SuperX GmbH has obliged its employees to maintain confidentiality and has instructed them about the legal consequences of non-compliance.

SuperX GmbH has implemented the following measures:

Organisational measures	
x	Employees are bound by their employment contract to observe the prohibition on disclosing business secrets.
x	Obligation of employees to handle personal data confidentially (Art. 28 para. 3 GDPR).
x	A company data protection officer (DPO) has been appointed.
x	There is a documented system configuration.
x	The technical and organisational measures are reviewed at regular intervals.
x	The DPO is involved in security incidents.
x	Security incidents are documented.

3. Admission Control

Measures to prevent unauthorised persons from gaining access to data processing systems with which personal data is processed and used.

SuperX GmbH has implemented the following measures:

Technical measures		Organisational measures	
x	Window bars	x	Key regulation (key list, key issue)
x	Manual locking system	x	Function and role-based access authorizations for server room
		x	Careful selection of cleaning staff

4. Equipment Access Control

Measures to prevent unauthorised persons from using data processing systems.

SuperX GmbH has implemented the following measures:

Technical measures		Organisational measures	
x	Authentication with user name / password	x	Password regulation (minimum length, complexity, validity period, blocking/deletion, etc.)
x	Authentication with biometric procedures (not yet comprehensive)	x	Secure storage of data carriers (backup tapes, hard drives, etc.)
x	Use of anti-virus software	x	Creation of personal user profiles
x	Use of a software firewall	x	"Clean desk" policy
x	Encryption of data carriers in PCs / notebooks		
x	Use of lockable disposal containers for paper, files and data carriers		
x	Encryption of e-mail transport		
x	Encryption of all websites		
x	Encryption of e-mail attachments		
x	Use of VPN technology (Engineering, Production Database)		
x	Use of a document shredder		
x	Multi-Factor-Authentication		

5. Data Access Control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

SuperX GmbH has implemented the following measures:

Technical measures		Organisational measures	
x	Administrators have different areas of responsibility	x	Procedure for withdrawing access authorisations
x	Number of administrators limited to a minimum according to area of responsibility		

x	Multi-Factor-Authentication		
---	-----------------------------	--	--

6. Transfer control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or during transport or storage on data carriers. It should also be possible to check and determine to whom (which bodies) personal data is to be or has been transmitted.

SuperX GmbH has implemented the following measures:

Technical measures	
x	Use of VPN, firewall (see above).
x	Encryption of the e-mail transport
x	Encryption of e-mail attachments
x	Multi-factor-authentication when accessing external systems, whenever MFA is available.

7. Input control

Measures to ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered into, changed or removed from data processing systems.

SuperX GmbH has implemented the following measures:

Technical measures	
x	The IT systems used have a logging function.

8. Processing control

Measures to ensure that personal data processed on behalf of SuperX GmbH can only be processed in accordance with the instructions of SuperX GmbH.

SuperX GmbH has implemented the following measures:

x	Data Processing Agreements are concluded with all service providers (Art. 28 (3) GDPR)
x	Careful selection of contractors and subcontractors (especially with regard to data security).
x	The Principal shall check the Contractor's documentation and security measures before commencing data processing.

9. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.

SuperX GmbH has implemented the following measures:

Technical measures		Organisational measures	
x	Storage of data backups in a secure, outsourced location. (AWS, Google)	x	Agreements (SLA) on availability
x	Air conditioning of the server rooms.	x	Concept for backing up and restoring data (backup, restore, recovery) by the contractor.
x	Fire extinguishers in server rooms.		
x	Smoke detectors in server rooms.		
x	Protective socket strips in server rooms.		
x	Devices for monitoring the temperature and humidity in server rooms.		
x	Overvoltage protection.		
x	Uninterruptible power supply (UPS)		
x	Backups		
x	Virus protection		
x	Hard drive mirroring		

10. Separation control

Measures that ensure that data collected for different purposes can be processed separately.

Data processing on the systems of SuperX GmbH is logically and physically separated according to the respective customer databases or customers.

SuperX GmbH has implemented the following measures:

Technical measures		Organisational measures	
x	Definition of database rights.	x	Separation of productive and test systems.
		x	Control via authorisation concept

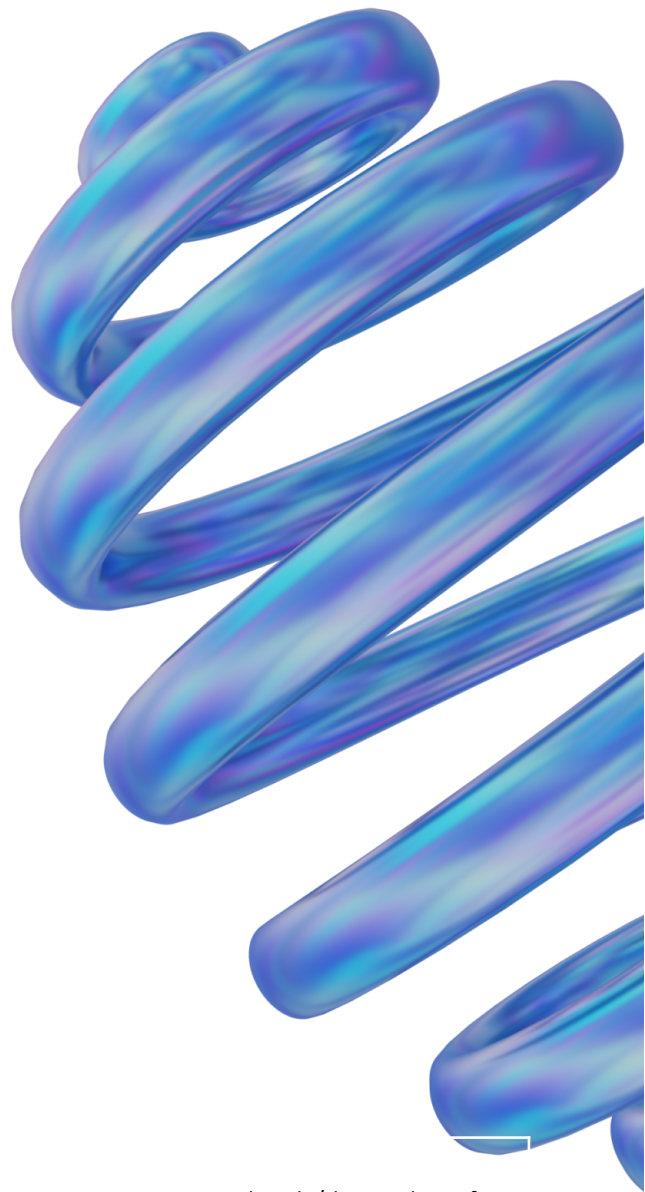
Data Protection

Brief Expert Opinion

Von Lubberger Lehment Rechtsanwälte Partnerschaft mbB

SuperX GmbH
Prenzlauer Allee 242 / Haus 7
Berlin, Deutschland
www.superchat.de
datenschutz@superchat.de

Lubberger Lehment
Rechtsanwälte Partnerschaft mbB
Meinekestraße 4, 10719 Berlin
Borselstraße 20, 22765
Hamburg Sternwartstraße 2, 81679 München
Tel. 030 8803350
Fax 030 88033533
office@lubbergerlehment.co



From: Dr. David Weller, Lubberger Lehment, Hamburg

Subject: Data protection assessment of the use of WhatsApp via Cloud API

Date: 8 August 2025

SuperX GmbH ("Superchat") has asked us to assess the use of the WhatsApp Business Platform provided by Superchat as a Business Solutions Provider ("BSP") via the Cloud API from a data protection perspective.

Summary

In our assessment, the use of the WhatsApp Business Platform via the Cloud API as offered by Superchat enables companies to use the WhatsApp messenger in compliance with data protection law.

Facts

Superchat offers a communications platform that consolidates various communication channels in a web interface. Among these communication channels is the WhatsApp messenger.

The WhatsApp messenger is operated in the European Union by WhatsApp Ireland Limited, based in Ireland ("WhatsApp"). WhatsApp Ireland Limited is part of the Meta group. Use of the WhatsApp messenger in both the standard and business versions requires that both sender and recipient have the WhatsApp application installed on their device. The locally stored contact information on the respective devices is automatically transmitted to WhatsApp servers in the United States in order to check which of the stored contacts also use WhatsApp. This synchronization affects all contacts, including those who do not use WhatsApp.

If communication is not exclusively for private purposes, it is subject to the requirements of the General Data Protection Regulation (GDPR). There is no legal basis under the GDPR for the automated transmission of contact information; moreover, the information obligations towards data subjects pursuant to Articles 13 and 14 GDPR are

not ensured. For this reason, data protection authorities (in particular those of Rhineland-Palatinate, North Rhine-Westphalia, and Bavaria) have in the past critically assessed the use of WhatsApp for business communication.

WhatsApp collects so-called metadata in the course of communication. According to WhatsApp's privacy policy (available at <https://www.whatsapp.com/legal/privacy-policy-eea#privacy-policy-information-you-and-we-share>), these include, in particular, the time, frequency and duration of use, device information (hardware model and operating system, battery level, signal strength, app version, browser and mobile network information as well as connection details, mobile or internet provider, language and time zone, IP address, information on device operation) as well as general location information (IP and phone area code). The privacy policy states that metadata is shared with other companies of the Meta group and used for the improvement and development of services. WhatsApp bases this data processing on Article 6(1)(b) GDPR (performance of a contract) as well as Article 6(1)(f) GDPR (legitimate interest). WhatsApp users – including business users – have no access to metadata; WhatsApp also does not provide users with any evaluations based on this data.

Communication content is end-to-end encrypted. WhatsApp describes the specific technical implementation of this encryption in publicly accessible documentation (last updated in August 2024). The Saarland Commissioner for Data Protection and Freedom of Information reviewed the encryption described therein and concluded that it corresponds to the state of the art and ensures that WhatsApp cannot gain knowledge of communication content (Annual Report of the Saarland Commissioner for Data Protection and Freedom of Information of 11.03.2020, p. 75 ff., available at https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/alle_Dateien_und_Ordnungen_bis_2025/tberichte/tb28_2019.pdf).

In addition to the standard and business versions, WhatsApp and Meta offer companies the use of the WhatsApp messenger via the WhatsApp Cloud API. In this case, WhatsApp communication with customers or users does not take place via an application installed on a device, but via the Cloud API on which the service is hosted.

SuperX uses only the Cloud API (not the Business API) for WhatsApp communication. The Cloud API is a service provided by Meta Platforms Ireland Ltd. SuperX has concluded both a service agreement and a data processing agreement with Meta. Thus, Meta provides the Cloud API on behalf and under the instructions of SuperX; SuperX, in turn, acts on behalf and under the instructions of its customers.

The sending and receiving of messages, according to Meta's description, proceeds as follows: messages to a company using WhatsApp Business via the Cloud API are transmitted (using the Signal protocol) end-to-end encrypted from the user to the Cloud API. The Cloud API uses industry-standard encryption methods. The message is then decrypted and forwarded to the recipient company. The Cloud API only stores data temporarily (as long as required for the provision of the API functions). Conversely, when companies send messages to customers via WhatsApp Business, the message is first sent to the Cloud API by the company and stored there temporarily. It is then forwarded end-to-end encrypted to the WhatsApp platform. WhatsApp functions here as a transport service and cannot access message content at any time.

Messages sent or received are only accessed by the Cloud API and retained for a maximum of 30 days, for example to enable retransmission. Data is also encrypted at rest. Meta provides an SOC 2 Type II report.

Local storage of data at rest in the Cloud API can be controlled using the so-called "Local Storage Solution." Storage then takes place in the chosen country or, if no data center is available there, in Germany. This local storage function covers both outgoing and incoming messages as well as the message types text messages, media messages, and template messages. During transmission, messages may also be routed via a Cloud API server in the United States, with all message content in transit (cache, queues) automatically deleted after 60 minutes.

According to Meta, the Cloud API does not use any information other than the phone number of the users with whom the company communicates. The phone number is used solely to transmit the message and then deleted together with the message. Other parts of the Meta group have no access to the phone number. Meta is

contractually strictly bound to instructions in this regard and is not authorized to access the communication.

The Cloud API and Superchat as Business Solution Provider function as intermediaries between WhatsApp and the customer. The customer is the controller within the meaning of data protection law. Superchat is the processor of the company and Meta, in turn, is the (sub-)processor within the meaning of Article 28 GDPR. Superchat has concluded a data processing agreement with Meta (available here, "Exhibit A"). The use of processors in the processing of even sensitive data is permissible under Article 28 GDPR, provided that appropriate contractual, organizational, and technical measures exist. This applies even if processors could theoretically access unencrypted content (cf. FAQ of the Data Protection Commissioner of Lower Saxony, January 2024). For the Cloud API, we consider the requirements of Article 32 GDPR to be met.

Assessment

No synchronization of contact data

When using WhatsApp Business via the Cloud API, the use of a WhatsApp application on a customer's device is eliminated. As a result, there is no synchronization of contact data. The central criticism of German data protection authorities is thus addressed.

Local storage of communication content on servers in Germany

Superchat activates local data storage in Germany for customers using WhatsApp via the Cloud API.

That messages may be routed via a Meta server in the United States is, in our view, justified in light of the certification of Meta Platforms, Inc. under the EU-U.S. Data Privacy Framework (Article 45(1) GDPR).

Encryption and role of the Cloud API

WhatsApp communication via the Cloud API is secured by encryption measures that correspond to the state of the art. If an (end) user sends a message via WhatsApp to a company using the Cloud API, the message is encrypted by WhatsApp and transmitted between the user and the Cloud API. Upon receipt of the message by the

Cloud API, it is decrypted there and forwarded to the company. The same process occurs in reverse when a company sends a message via the Cloud API to a user. Upon receipt of a message from a company, it is encrypted by the Cloud API using the Signal protocol and then transmitted to the user via WhatsApp. According to the Signal protocol, encryption codes are negotiated between the user and the Cloud API (on behalf of the company) to establish a secure communication channel. The Cloud API uses industry-standard encryption methods to secure data both in transit and at rest. Messages at rest are encrypted and automatically deleted after 30 days at the latest. WhatsApp does not describe the encryption as end-to-end encryption because the Cloud API technically decrypts and re-encrypts the messages for transport. However, Meta manages the keys exclusively on behalf and under the instructions of SuperX or its customers. Use of the encryption and decryption keys for purposes other than providing the service for message delivery is excluded by the service agreement and the data processing agreement between SuperX and Meta. Due to this contractual commitment and the technical safeguards, in our assessment, the use of the Cloud API meets the requirements for data processing and for security of processing pursuant to Article 32 GDPR.

Metadata

In our assessment, WhatsApp alone is responsible for the processing of metadata. Pursuant to Article 4(7) GDPR, the controller is “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.” We assume that WhatsApp is a telecommunications service within the meaning of § 3(61) TKG and therefore itself the controller in terms of data protection law for the processing of data for the conduct of communication (cf. also EDPB Guidelines 07/2020 on the concepts of “controller” and “processor” in the GDPR, version 2.0, adopted on 7 July 2021, p. 14).

Mere use of WhatsApp by companies does not create (joint) controllership under data protection law. According to the principles developed by the ECJ in the “Wirtschaftsakademie Schleswig-Holstein” decision (C-210/16 of 5 June 2018) and the “Fashion ID” decision (C-40/17 of 29 July 2019), joint controllership can only be assumed if the user actively influences the data processing operation (C-210/16, para.

39) and pursues overarching purposes together with the service provider, whereby the economic advantage pursued by one party essentially constitutes "the consideration for" the advantage offered by the other party (C-40/17, para. 80).

This is not the case when using WhatsApp (cf. BeckOK Data Protection Law, 41st ed. 2022, Art. 26, para. 75 with further references). Unlike, for example, in the operation of a Facebook fan page (through parameter settings), companies using WhatsApp do not influence the data processing. The respective purposes pursued (processing of metadata to improve the service on the one hand, conduct of communication on the other hand) also differ. For this reason, the Saarland Commissioner for Data Protection and Freedom of Information has permitted municipalities in Saarland to use the WhatsApp Business API (as follows from the press release linked under item II.).

If metadata is transferred by WhatsApp Ireland Ltd. to WhatsApp LLC or Meta Platforms, Inc., this third-country transfer is permissible pursuant to Article 45(1) GDPR. As of the effective date 3 September 2024, both recipients are certified under the EU-U.S. Data Privacy Framework.