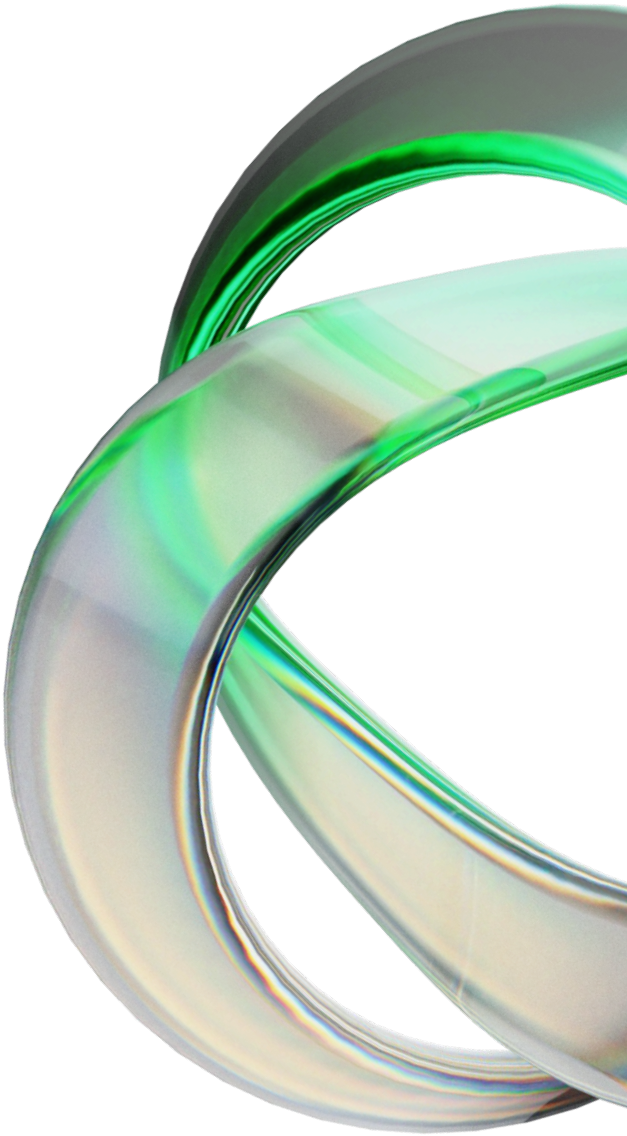
Data protection at Superchat

Use messaging in compliance with EU data protection regulations



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

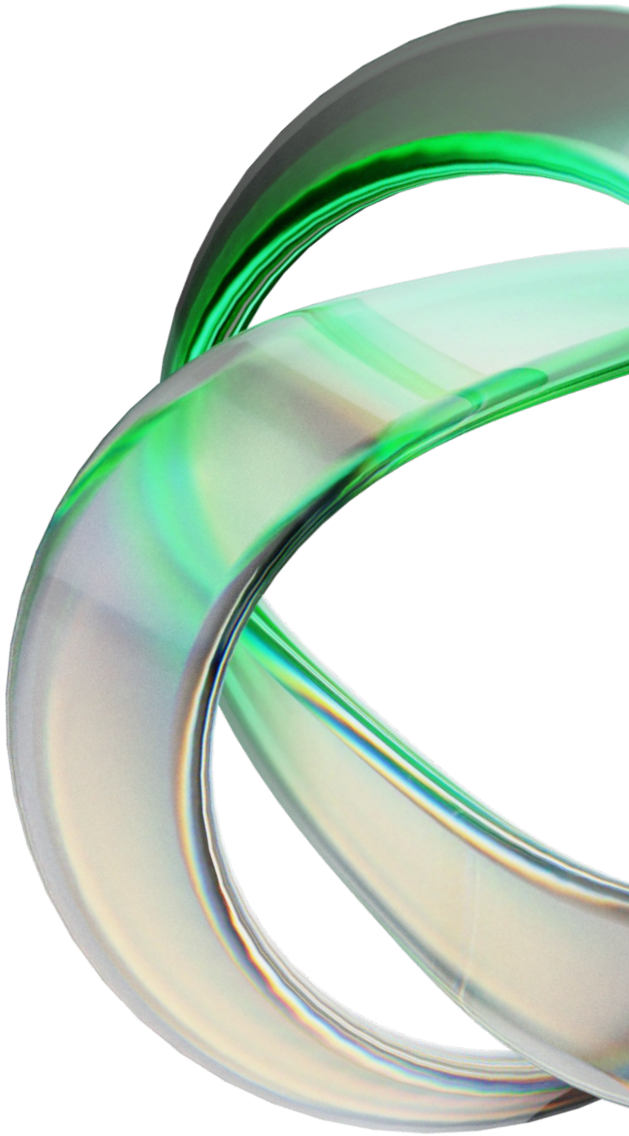
Table of Contents

At Superchat, we take data privacy seriously and are committed to transparency. We have made most of our data privacy information publicly available. For frequently asked questions about data privacy, please visit www.superchat.com/privacy-faqs.

Additionally, you can find your Data Processing Agreement (DPA) and sample texts on our website. We strive to ensure that you have all the information you need to feel confident about how your data is handled.

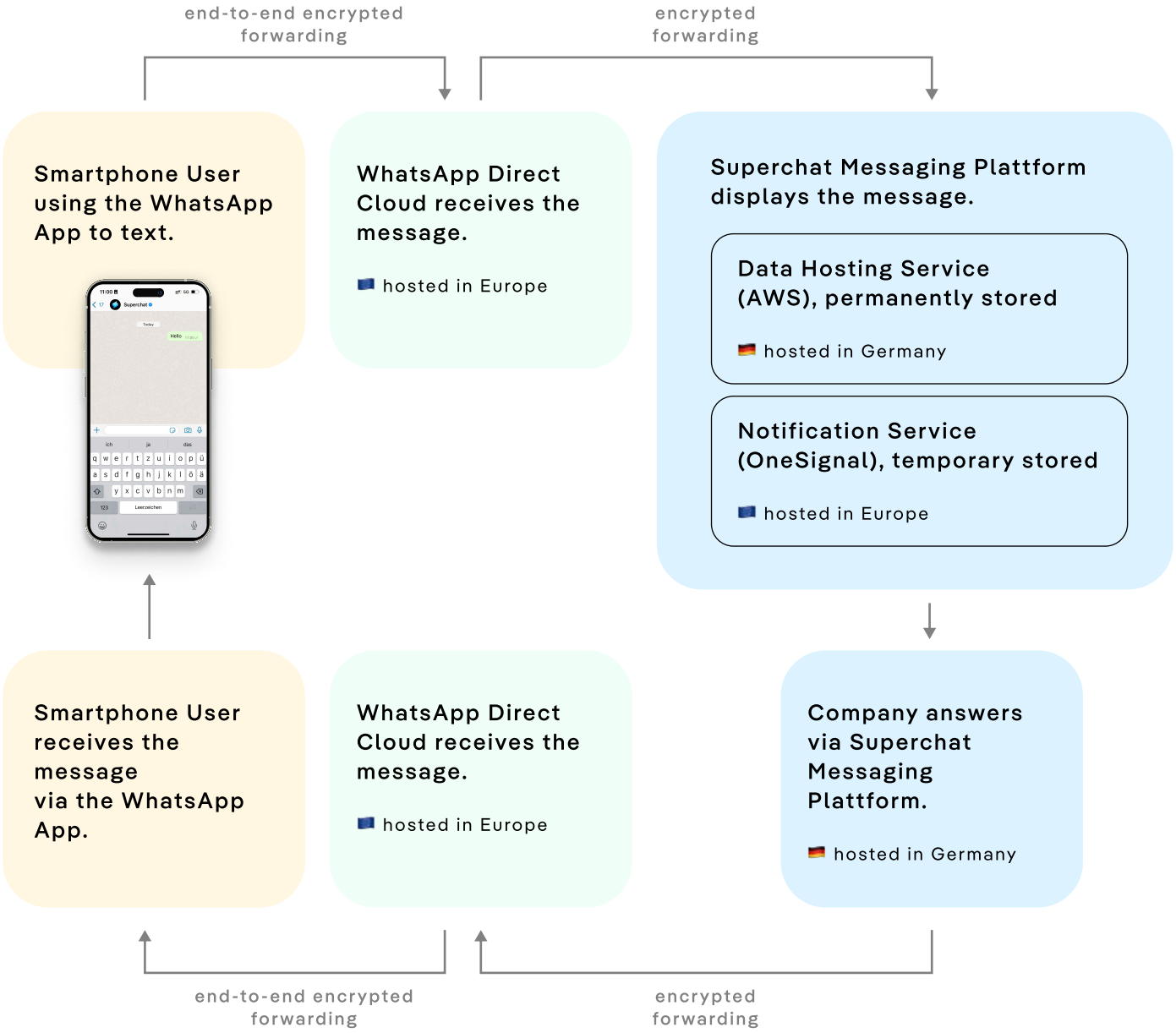
Using the WhatsApp API GDPR compliant

Data flow diagram



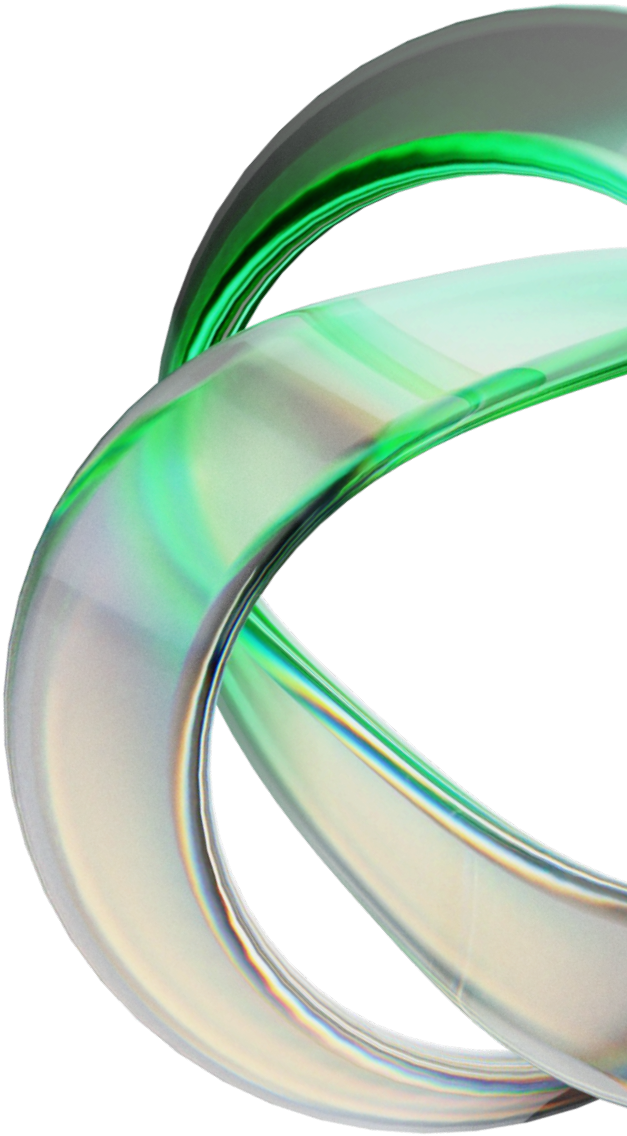
SuperX GmbH
Prenzlauer Allee 242 / Haus 7
Berlin, Germany
www.superchat.com
gdpr@superchat.de

An end customer sends a message to the WhatsApp number of a Superchat account. The message is transmitted end-to-end encrypted from the end customer's device to WhatsApp Direct Cloud. Meta has no access to the content of the message. The message is then transferred from WhatsApp Direct Cloud to Superchat. The message is only temporarily stored at WhatsApp Direct Cloud until it has been successfully forwarded to Superchat. The data is stored in your country's location. If there is no META server available, then your data will be stored in Germany. Once in Superchat, the message is saved and can be seen and answered by the Superchat account. Access to data is secured with regular internal audits to guarantee maximum security.



DPA

Data Processing Agreement with sub-processors



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

Contract on order processing (Art. 28 para. 3 GDPR)

This contract applies between the customer (hereinafter referred to as the "Client") 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 user agreement for the messaging software "Superchat". In addition to the user agreement, the parties hereby agree the following:

1. Subject matter of this contract and processing, scope of authority to issue instructions

1.1 The subject of this contract is the cooperation between the parties within the framework of the contract of use. The execution of the contract of use includes the data processing activities of the Contractor for the Client as specified in **Annex 1.**

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

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

1.4 The agreed processing activity shall take place exclusively within the European Union and the European Economic Area. The Contractor shall only be permitted to relocate the processing activity or transfer the data concerned to a third country if the Client has expressly given its consent in text form in advance and the conditions prescribed for the transfer of personal data to third countries or international organizations pursuant to Art. 44 et seq. GDPR are complied with. In such a case, the parties shall jointly examine the principles prior to the relocation or transfer and define them in suitable documentation, according to which the level of protection guaranteed by the General Data Protection Regulation guaranteed level of protection is maintained is (z. e.g. adequacy decision of the EU Commission pursuant to Art. 45 GDPR or other suitable guarantees pursuant to Art. 46 GDPR).

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

- The Contractor allows its employees to work from home. For this purpose, the Contractor has data protection regulations in place, which the employees have undertaken to comply with.
- For the subcontractors at the sites, all of which are listed in Annex 2.

2. Nature and purpose of processing

2.1 Access to personal data is necessary for the execution of the contract of use with the client.

2.2 The purposes of the order processing are specified in **Annex 1. The commissioned processing shall** only be carried out for the purposes of implementing the contract of use with the client; 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 fulfillment of the respective task. The Contractor has no authority of its own to decide how to handle the data and shall store it as determined by the Client.

3. Type of personal data and categories of data subjects

3.1 The types of personal data affected by data processing by the Contractor are listed in **Annex 1.**

3.2 The groups of persons affected by the processing are listed in **Annex 1.**

4. Rights and obligations of the client

4.1 The client is always responsible for checking the permissibility of data processing and safeguarding the rights of the data subjects. The client assumes the reporting obligations incumbent on it under the data protection provisions on its own responsibility (Art. 33, 34 GDPR).

4.2 The Client shall always confirm verbal 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 between the Client and the Contractor in advance; the parties shall make a corresponding agreement in text form.

4.3 The persons named in **Annex 1** are authorized to issue order-related instructions to the Contractor on behalf of the Client.

4.4 The Client shall inform the Contractor in an appropriate manner of any change of one of the persons named in Section 4.3 of this contract.

4.5 The Client is entitled to check the Contractor's compliance with the data protection provisions, the contractual agreements made here and the instructions issued at any time.

check. The inspection must always be carried out by prior notification. As part of the inspection, the company data protection officer and the auditor commissioned by the Client shall also be granted access to the Contractor's premises where the agreed processing takes place for the Client, in particular to the corresponding software applications, server rooms, operating software and other IT systems used for processing on behalf of the Client. The Contractor may satisfy this right of control of the Client 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 Client shall reimburse the Contractor in the amount of the usual remuneration agreed for the provision of services for the expenses incurred by the Contractor as a result of the inspection of the Client in accordance with Section 4.5 of this Agreement.

4.7 The Client shall only be entitled to surrender the data processed in the order or the databases created in the order upon termination of the contract of use or this order agreement. The Client shall pay the costs incurred for the release separately in accordance with the Contractor's applicable remuneration rates. The Contractor shall be entitled at any time right of retention (§§ 273, 320 BGB) to the data processed in the order or data stocks created in the order.

5. Further rights and obligations of the Contractor

5.1 The persons named in **Annex 1** are authorized to accept the instructions of the Client on behalf of the Contractor.

5.2 The Contractor shall only process, correct, delete or block the personal data specified in Section 3 or **Annex 1** of this contract in accordance with documented instructions from the Client. Where possible, it shall support the Client in fulfilling 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 Client without delay.

5.3 The Contractor shall keep its own record of processing activities. It shall participate in the preparation of records of processing activities and data protection impact assessments of the client and provide the client with the information required for this - insofar as possible and available to the contractor. In addition

In addition, the Contractor shall also support the Client to the extent of the information available to the Contractor in complying with the obligations incumbent on the Client under Art.
32 to Art. 36 GDPR. 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 the data protection impact assessments.

5.4 The Contractor shall store all documents and/or data carriers and/or databases containing personal data of the Client 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 unauthorized persons. As far as possible, the Contractor shall document the incoming and outgoing data.

5.5 The Contractor has duly appointed the person named in **Annex 1** as the company data protection officer (Art. 37 GDPR). Should this data protection officer change, the Contractor shall inform the Client immediately. informed without delay. The company data protection officer is responsible for compliance with data protection in the Contractor's company.

5.6 The Contractor shall inform the Client immediately of any order-related disruptions in the course of operations, violations of data protection provisions (including by instructions of the Client), inspections and measures of the supervisory authorities and other irregularities. The Contractor shall support the Client in fulfilling the reporting obligations incumbent on the Client 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 Client in connection with this order processing, the Contractor shall support the Client 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 Client has confirmed or amended them.

5.9 The Contractor shall enable the Client to carry out and exercise the data protection control rights to which the Client is entitled under Section 4.5 of this Agreement.

5.10 The Contractor shall only permit its employees to carry out activities for the Client from the home office with the prior express consent of the Client.

to be completed. Consent to this shall be deemed to have been given 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 Contractor shall be entitled to payment of the customary remuneration agreed for the provision of services for those expenses incurred by the Contractor 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.

6. Technical and organizational measures

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

6.2 The contractor will take the following criteria into account when selecting the specific TOM:

- the state of the art;
- the implementation costs;
- the nature, scope, circumstances and purposes of the processing in question;
- the likelihood and severity of the risk to the rights and freedoms of 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.
- 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 In the course of technical progress and further development, the Contractor shall be permitted to replace the specific TOMs once agreed with more modern TOMs that meet the criteria agreed in Clauses 6.2 and 6.3 of this contract and that are always ensure an appropriate level of protection. Should the review or an audit by the client or another accredited body reveal such a need for adjustment, the parties shall implement this by mutual agreement to a suitable and appropriate extent. All changes must be documented.

7. Secrecy

7.1 During the term of this agreement and for a period of 1 (one) year after termination of this agreement, the contracting 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 execution of this agreement.

7.2 The documents made available to the other party shall remain the property of the party concerned and must be treated as strictly confidential. They may not be reproduced, published or made accessible to third parties in any other way 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 unauthorized 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 was already known to a contracting party in advance or is publicly known or in the public domain or becomes known through no fault of the contracting party.

8. Obligation of confidentiality (data secrecy)

8.1 The contracting parties shall only collect, process and use personal data 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 automatically or non-automatically (manually).

8.2 Each party shall obligate its own employees used for data processing to maintain data secrecy before carrying out the work. The party's own employees must be informed of the relevant data protection provisions and familiarized with the resulting special requirements for data security and data protection, in particular the data protection provisions applicable under this agreement. applicable duties of care and confidentiality obligations applicable under this agreement.

8.3 The disclosure of personal data and/or other information from the area of

The Contractor is prohibited from disclosing data to third parties. This shall also apply if and insofar as a change or addition is made to the data.

9. Use of further processors (subcontractors)

9.1 The Contractor shall not subcontract other processors (subcontractors) to fulfill the contract of use without the prior separate or general written consent of the Client.

9.2 The Client hereby grants its general written approval for the further processors (subcontractors) named in **Annex 2** to this Agreement, which the Contractor uses. Appendix **2** hereby becomes part of the contract. The Contractor is authorized to use the additional processors (subcontractors) listed in Annex **2.** The service contributions to be provided by the other processors (subcontractors) are also specified in Annex **2.**

9.3 The Contractor has carefully selected the other processors (subcontractors) listed in **Annex 2.** It shall cooperate with the further processors (subcontractors) listed in Annex 2 regarding 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 Annex **2.** The other processors named in Annex 2 have assured the Contractor that they offer sufficient guarantees, in particular, that they will implement the appropriate technical and organizational measures to comply with the data protection provisions. The Contractor shall have the other processors (subcontractors) named in **Annex 2 grant the Contractor the** rights of control and review corresponding to this contract.

9.4 The Contractor shall inform the Client immediately of any intended change to another processor (subcontractor) listed in Annex **2.** If a new additional processor (subcontractor) is to be added or a previous one replaced, the Contractor shall amend the list contained in Annex **2** and send the amended **Annex 2 to** the Client at least ten (10) working days before the planned addition or replacement. The Client shall have the right to object to the amendment within a period of five (5) working days. If the objection is not raised within this period, the right of objection shall lapse. If the Client effectively raises an objection and the Contractor can proceed without the change or the use of the proposed

If the Contractor fails to perform the services of another processor (subcontractor), the Contractor shall be entitled to extraordinary termination of this contract and the contract of use without notice.

9.5 The other processors (subcontractors) listed in **Annex 2 shall provide** their respective services within the EU or the EEA. If one of the other processors (subcontractors) named in **Annex 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.

9.6 If third parties merely provide ancillary services for the Contractor to support the execution of the order vis-à-vis the Client, these third parties shall not be considered additional processors. This includes all services unrelated to the Client's order, e.g. anonymous statistical analysis services, mail, telecommunications services, transportation, 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 notice periods

10.1 This agreement shall commence upon conclusion of the user agreement and shall have the same term as the latter. The parties shall document any deviating term in **Annex 1**. In addition, the termination provisions set out in the user agreement shall apply. This agreement shall also end upon termination of the user agreement.

10.2 The right to extraordinary termination of this agreement remains unaffected by the parties.

11. Obligations upon termination of this contract

11.1 No copies of the client's data or databases shall be made without the client'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 contract of use, the Contractor shall also hand over to the Client all documents, processing and usage results and databases that have come into its possession as part of the contractual relationship or, with the prior consent of the Client, 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 shall apply

for documents or data carriers with personal data and/or other information from the client's area that are no longer required.

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

11.4 The Contractor shall also be entitled to payment of the usual remuneration agreed for the provision of services for those expenses incurred by the Contractor in connection with the termination of the contract of use.

12. Final provisions

12.1 There are no ancillary agreements to this contract. Amendments or additions to the agreement must be made in writing or in electronic form (at least by 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 April 11, 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 shall be the Contractor's registered office.

Annex 1: Details of the order processing

Name of the main contract	Authorized representatives and DPO AG	Instruction recipient and DPO AN	Object of the order processing	Categories of personal data	Categories of affected persons	Purpose of the data processing	Duration of the contract
Contract of use	You are obliged to provide us with your authorized representative (m/f/d) and - if applicable - your data protection officer (m/f/d) (e.g. by e-mail)	WB: Mika Hally DSB: Kathrin Siegmund datenschutz@superchat.de	– Setting up the User accounts for the client's employees Provision of the "Superchat" messaging platform – Processing the personal data in the context of the use of the messaging platform "Superchat"	The personal data processed via the Services is processed by the client at its own at its own discretion and controlled and can the following categories of personal data: - Inventory, Contact and communication data of the client's interested parties and customers - Name of the Employees and communication	– Customers of the Commissioned by, – Interested party of the client, – Employees the client	– Memory ng, use and disclosure for the purpose of providing the services – Support	Like contract of use

				nhalte mit dem Interessenten und Kunden der Auftraggeberin			

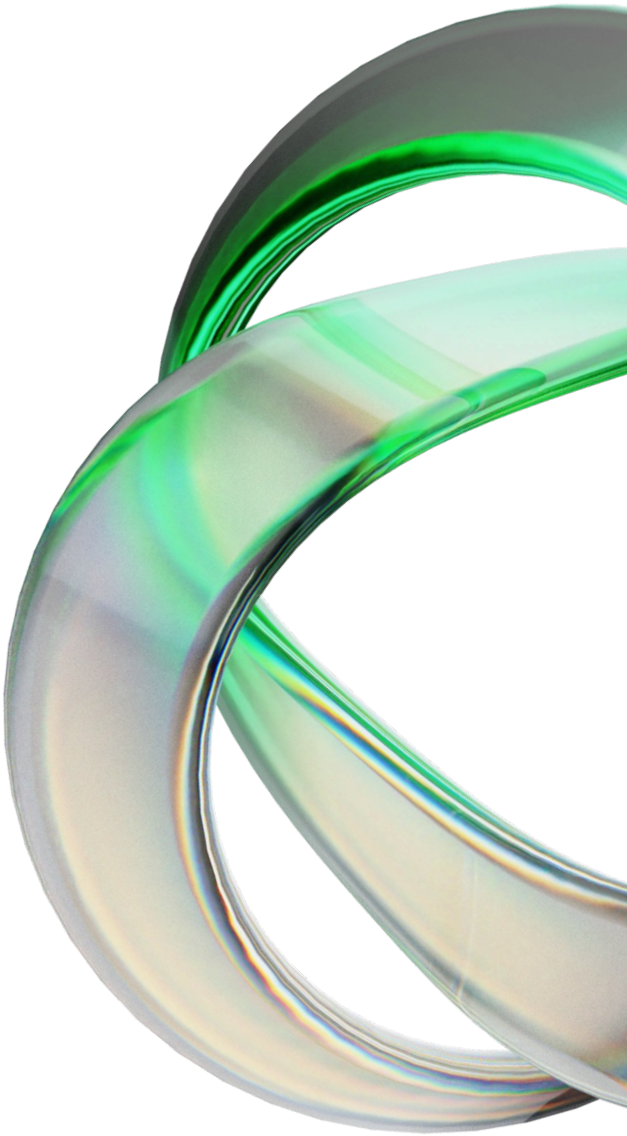
Annex 2: List of other processors (subcontractors)

Company, address	**Nature and purpose of processing**	**Type of data**	**Categories of data subjects**
Twilio Inc, 375 Beale Street, Suite 300, San Francisco, CA	Storage and use for the purpose of providing the SMS services	– Inventory, contact and communication data of the client's contacts and customers – Name of the Employee of the client and SMS communication with the contact and customer of the client	Contacts, customers and employees of the client
Nylas, Inc, 944 Market St, San Francisco, CA	Storage and use for the purpose of providing the E-mail services	– Inventory, contact and communication data of the client's contacts and customers – Name of the employee of the client and E-mail communication with the client's contact and customers	Contacts, customers and employees of the client
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg	Hosting	– Inventory, contact and Communication dates of the client's contacts and customers – Name of the Employee and communication with the client's contacts and customers	Contacts, customers and employees of the client

360dialog GmbH, Torstraße 61, 10119 Berlin, Germany	Storage and use for the purpose of providing WhatsApp Messenger services	– Inventory, contact and Communication dates of the client's contacts and customers – Name of the Employee of the client and WhatsApp communication with the contact and customer of the client	Contacts, customers and employees of the client
OneSignal, 201 South B Street, San Mateo, California 94401	Storage and use for the purpose of providing notification/notification services	– Inventory, contact and communication data of the client's contacts and customers – Name of the Employee of the client and communication with the contact and customer of the client	Contacts, customers and employees of the client
Meta Platforms Ireland Ltd. Merrion Road Dublin 4 D04 X2K5 Ireland	Storage and use for the purpose of providing WhatsApp Messenger services	– Inventory, contact and Communication dates of the client's contacts and customers – Name of the Employee of the client and WhatsApp communication with the contact and customer of the client	Contacts, customers and employees of the client

TOM

Technical and organizational measures



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

Description of the technical and organizational measures of SuperX GmbH

1. Summary of the measures taken

1.	Pseudonymization / encryption:
✗	Measures for encrypting file attachments in e-mails, e-mail transport and websites (see section 3 ff. below).
2.	Permanent assurance of: Confidentiality, integrity, availability, resilience of systems and services:
✗	Confidentiality is guaranteed by access and access control (see section 3 ff. below).
✗	Integrity is guaranteed by securing the entire company network with a firewall and mobile device management (MDM).
✗	Availability is ensured by the back-ups (see section 3 ff. below).
✗	The load capacity is guaranteed 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:
✗	A quick recovery is possible via the backup tapes.
✗	An emergency power supply for the server room ensures reliability. (AWS)
4.	Review, assessment and evaluation of the effectiveness of the technical and organizational measures:
✗	Automated, permanent monitoring of all systems takes place.
✗	An annual audit is carried out by the data protection officer.
✗	There are annual reports of technical failures.
✗	The hardware is regularly replaced and maintained.

2. General organizational 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:

Organizational measures	
✘	The employment contract obliges employees to comply with the prohibition on disclosing business secrets.
✘	Obligation of employees to handle personal data confidentially (Art. 28 para. 3 GDPR).
✘	A company data protection officer (DPO) has been appointed.
✘	There is a documented system configuration.
✘	The technical and organizational measures are reviewed at regular intervals.
✘	The DPO is involved in security incidents.
✘	Security incidents are documented.

3. Access control

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

The following measures are used at SuperX GmbH as part of the multi-level security zone concept, depending on the level of protection required.

SuperX GmbH has implemented the following measures:

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

4. Access control

Measures to prevent unauthorized persons from using data processing systems. SuperX GmbH has implemented the following measures:

Technical measures		Organizational measures	
✓	Authentication with user name / password	✓	Password regulation (minimum length, complexity, validity period, blocking/deletion, etc.)
✓	Authentication with biometric procedures (not yet widespread)	✓	Secure storage of data carriers (backup tapes, hard disks, etc.)
✓	Use of anti-virus software	✓	Creation of personal user profiles
✓	Use of a software firewall	✓	Guideline for a "clean desk"
✓	Encryption of data carriers in PC / notebooks		
✓	Use of lockable disposal containers for paper, files and data carriers		
✓	Encryption of the e-mail transport		
✓	Encryption of all websites		
✓	Encryption of e-mail attachments		
✓	Use of VPN technology (engineering, production database)		
✓	Use of a document shredder		

5. Access control

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

SuperX GmbH has implemented the following measures:

Technical measures		Organizational measures	
✓	Administrators have different areas of responsibility	✓	Procedure for revoking access authorizations
✓	Number of administrators limited to a minimum according to area of responsibility		

6. Transfer control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or during its 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	
✗	Use of VPN, firewall (see above).
✗	Encryption of the e-mail transport
✗	Encryption of e-mail attachments

7. Input control

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

SuperX GmbH has implemented the following measures:

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

8. Order 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 as the client.

SuperX GmbH has implemented the following measures:

✗	Careful selection of contractors and subcontractors (especially with regard to data security).
✗	The client checks the documentation and security measures at the contractor's premises before the start of 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		Organizational measures	
✘	Storage of data backups in a secure, off-site location. (AWS)	✘	Agreements (SLA) on availability
✘	Air conditioning of the server rooms.	✘	Concept for backing up and restoring data (backup, restore, recovery) by the contractor.
✘	Fire extinguishers in server rooms.		
✘	Smoke detectors in server rooms.		
✘	Protective socket strips in server rooms.		
✘	Devices for monitoring the temperature and humidity in server rooms.		
✘	Overvoltage protection.		
✘	Uninterruptible power supply (UPS)		
✘	Backups		
✘	Virus protection		
✘	Hard disk mirroring		

10. Separation control

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

Data processing takes place on the systems of SuperX GmbH logically and physically separated according to the respective customer databases or clients.

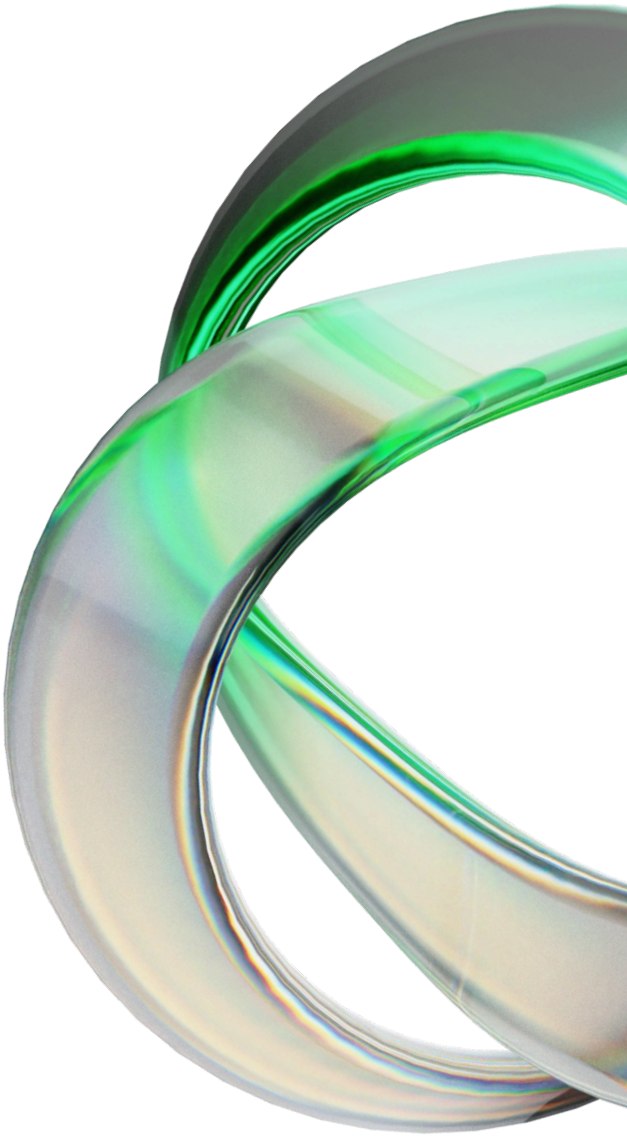
SuperX GmbH has implemented the following measures:

Technical measures		Organizational measures	
✘	Definition of database rights.	✘	Separation of production and test system.
		✘	Control via authorization concept

Data Privacy Review

By Lubberger Lehment Rechtsanwälte Partnerschaft mbB

Lubberger Lehment



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

Lubberger Lehment

Brief expert opinion

By: Dr David Weller, Lubberger Lehment, Hamburg

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

Date: 5 September 2024

SuperX GmbH ("Superchat") has asked us to evaluate 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.

I. Summary

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

II. Facts of the case

- Superchat offers a communication platform that bundles various communication channels in one web interface. These communication channels include WhatsApp Messenger.
- 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. The standard and business versions of WhatsApp Messenger can only be used if the sender and recipient have installed the WhatsApp application on their end device. The contact information stored locally on the respective end devices is automatically transmitted to WhatsApp servers in the USA in order to synchronise which of the stored contacts also use WhatsApp. This synchronisation affects all contacts, i.e. even those who do not use WhatsApp.
- If the 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 of data subjects in accordance with Art. 13 and 14 GDPR is not ensured. For this reason, data protection authorities (particularly in the states of Rhineland-Palatinate, North Rhine-Westphalia and Bavaria) have criticised the use of Whats App for business communication in the past.

- WhatsApp collects so-called metadata during communication. According to the WhatsApp privacy policy (available at https://www.whats- app.com/legal/privacy-policy-eea#privacy-policy-information-you-and-we-share), this includes in particular the time, frequency and duration of use, device information (hardware model and operating system, battery level, signal strength, app version, information on the browser and mobile network as well as on the connection, the mobile or internet provider, language and time zone, IP address, information on device operation) and general location information (IP and telephone dialling code). The privacy policy states that metadata is shared with other companies in the Meta Group and used to improve and develop the services. WhatsApp bases this data processing on Art. 6 (1) lit. b) GDPR (fulfilment of contract) and Art. 6 (1) lit. f) GDPR (legitimate interest). WhatsApp users - including business users - do not have access to metadata; WhatsApp does not provide users with analyses based on this data.

- The communication content is encrypted end-to-end. WhatsApp describes the specific technical implementation of this encryption in publicly available documentation ("WhatsApp Encryption Overview - Technical white paper", last updated in August 2024). The State Commissioner for Data Protection and Freedom of Information of the State of Saarland has reviewed the encryption described there and has come to the conclusion that it corresponds to the state of the art and ensures that WhatsApp cannot gain knowledge of the communication content (Activity Report of the State Commissioner for Data Protection and Freedom of Information of 11 March 2020, page 75 ff., available at https://www.da-tenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb28_2019.pdf).

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

  The Cloud API is provided as an independent service by Meta Ireland Ltd.

- According to Meta, messages are sent and received as follows: Messages to a company using WhatsApp Business via the Cloud API are transmitted end-to-end encrypted (using the Signal protocol) from the user to the Cloud API. The message is then decrypted.

encrypted and transmitted to the recipient company. The Cloud API only stores data temporarily (i.e. for as long as is necessary to provide the API functions). Conversely, when companies send messages to customers via Whats App Business, the message flow is such that the message is first sent from the company to the Cloud API and temporarily stored there. It is then forwarded end-to-end encrypted to the WhatsApp platform. WhatsApp acts as a transport service and cannot access message content at any time.

Sent or received messages are only accessed by the Cloud API and stored for a maximum of 30 days, for example to enable retransmission. The data is also encrypted at rest. Meta has a SOC 2 Type II report.

- The local storage of data at rest in the Cloud API can be realised with the so-called "Local Storage Solution" can be controlled. Storage then takes place in the selected country or, if no data centre is available there, in Germany. This local storage function covers both outgoing and incoming messages, as well as the message types of text messages, service messages and template messages. During dispatch, messages can also be transported via a Cloud API server in the USA, where all message content in transit (cache, queues) is automatically deleted after 60 minutes.
- According to Meta, the Cloud API does not use any information about the users with whom the company communicates other than the telephone number. The phone number is only used to send the message and is then deleted together with the message. Other parts of the Meta Group do not have access to the phone number.
- The Cloud API and Superchat as a business solution provider act as an intermediary between WhatsApp and the customer. The customer is the controller under data protection law. Superchat is the company's processor and Meta is in turn a (sub)processor within the meaning of Art. 28 GDPR. Superchat has concluded an order processing agreement with Meta (available here, "Exhibit A").

III. Assessment

1. No synchronisation of contact data

When using WhatsApp Business via the Cloud API, there is no need to use a WhatsApp application on the customer's end device. This means that there is no synchronisation of contact data. The central criticism of the German data protection authorities has thus been addressed.

2. Local storage of communication content on servers in Germany

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

In view of the certification of Meta Meta Platforms, Inc. under the EU-US Data Privacy Framework, we consider the fact that messages may be transported via a meta-server in the USA to be justified (Art. 45 para. 1 GDPR).

3. Metadata

In our opinion, WhatsApp is solely responsible for the processing of metadata. According to Art. 4 No. 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 Section 3 No. 61 TKG and is therefore itself the data controller in the sense of data protection law for the data processing to carry out the communication (see also EDPB, Guidelines 07/2020 on the terms "controller" and "processor" in the GDPR, Version 2.0, adopted on 7 July 2021, page 14).

The mere use of WhatsApp by companies does not constitute (joint) responsibility under data protection law. According to the principles developed by the ECJ in the decisions "Wirtschaftsakademie Schleswig-Holstein" (C-210/16 of 5 June 2018) and "Fashion ID" (C-40/17 of 29 July 2019), joint responsibility can only be assumed if the user actively influences the data processing operation (C-210/16, para. 39) and, together with the service provider, pursues common overriding purposes in that the economic advantage pursued by one party constitutes "the consideration for" the "advantage offered" by the other party (C-40/17, para. 80).

Neither is the case when using WhatsApp (see BeckOK DatenschutzR, 41st ed. 2022, Art. 26, para. 75 with further references). Unlike, for example, the operation of a Facebook fan page (through parameterisation), companies that use WhatsApp do not have any influence on data processing. The purposes pursued in each case (processing of metadata to improve the service on the one hand, implementation of communication on the other) also differ. With this justification, the

the State Commissioner for Data Protection and Freedom of Information of the State of Saarland authorises the municipalities of Saarland to use the WhatsApp Business API (this can be seen from the press release linked in Section II.)

Insofar as metadata is forwarded by WhatsApp Ireland Ltd. to WhatsApp LLC or Meta Platforms, Inc., this third country transfer is permitted in accordance with Art. 45 para. 1 GDPR. As of 3 September 2024, both recipients are certified under the EU-US Data Privacy Framework.