Data protection at Superchat

Use messaging in compliance with data protection regulations with Superchat

y,p Superchat

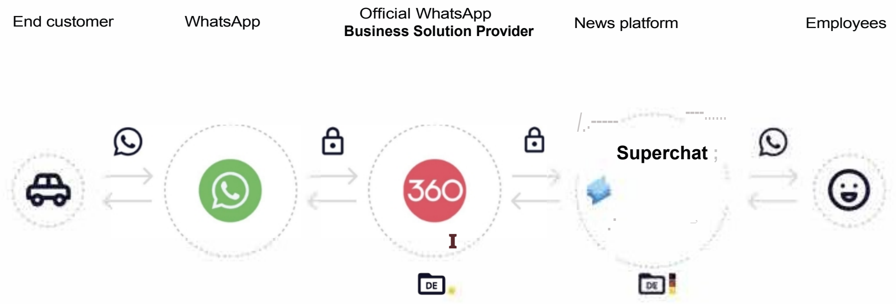
Table of contents

Superchat

Using the WhatsApp API in compliance with the GDPR

The most important facts in brief

Figure GDPR-compliant WhatsApp communication via the official WhatsApp. Business solution provider 360 Dialog and the Superchat messaging platform



- End customer sends message to the WhatsApp number of a Superchat account
- Message is transmitted end-to-end encrypted from the end customer's device to 360dialog
- Meta has no access to the content of the message
- Message is transferred from 360dialog to Superchat
- Message is only temporarily stored at 360dialog (until the message has been successfully forwarded to Superchat)
- Message is saved in Superchat and can be seen and answered by the Superchat account
- Data is stored on servers in Frankfurt
- Access to data is secured and regular internal audits guarantee maximum security

Superchat

Data protection declaration

Superchat

Information on data protection for our customers

Ladies and Gentlemen,

As our customers, we would like to inform you below within the framework of the General Data Protection Regulation (GDPR) about the handling of your personal data that we collect, store and use to initiate, execute and process an order with you.

is responsible for the processing of your data:

SuperX GmbH
represented by the managing directors Yilmaz Köknar and Mika Hally
House 7, Prenzlauer Allee 242-247,
10405 Berlin
hello@superchat.de

How to contact our company data protection officer:

E-mail: datenschutz@superchat.de

Description, purpose and legal basis of data processing:

You may provide us with the following information by handing over a business card or we may collect it as part of the initiation or execution of an order:

- For commercial customers (companies):

  Company name/name and address of the commercial customer, VAT identification number,

  - Details to the Contact person: Name, NaChname, AnsChrift,

    Communication data (telephone, mobile number, fax, e-mail address), function in the company, date of birth,
  - Contract master data (contractual relationship, product or contract interest,

    Order, purchase and delivery history including type of goods, warranties, any warranty rights asserted),
  - Payment data such as account number, IBAN,

    Swift, planning and control data,
  - Information from credit agencies or public directories.

  For end customers (consumers):

  - Salutation, name, surname and title,
  - Address,

    Communication data (telephone, mobile number, e-mail address),

- Contract master data (contractual relationship, product or contractual interest, order, purchase and delivery history including type of goods, warranties, any warranty rights asserted),
- If applicable, information from credit agencies or public directories.

Failure to provide the aforementioned data may mean that the contract with us cannot be concluded.

We collect, store and process your personal data exclusively in the context of contract initiation or in the course of the proper execution or termination of existing contractual relationships (supply or purchase contracts) for the following purposes:

- to be able to identify you as our contractual partner;
- for contract-related contact and correspondence with you;
- for invoicing, accounting;
- to manage and process the contractual relationship;
- if necessary for the assertion, exercise or defense of legal claims.

This procedure is justified by Art. 6 (1) sentence 1 letter b) GDPR. Without this type of use of your data, it is not possible to carry out the business relationship between you and us.

Any further processing of your personal data will only take place if this is required or permitted by law or if you have given us your express consent to do so. If you have given us your express consent for a specific processing operation, the legal basis for this processing is Art. 6 (1) (a) GDPR.

In certain cases, we process your aforementioned data to the extent permitted on the basis of a legitimate interest in accordance with Article 6(1)(f) GDPR, e.g. for the purpose of statistical evaluations and optimization of our services or to decide on the risk of payment defaults. This only applies if no conflicting interest is known and there is no objection.

Automated decision making/profiling:

There are no exclusively automated decisions. We do not use artificial intelligence or profiling to make decisions when processing your personal data.

Consent to newsletters, participation in competitions or special promotions:

As a customer, you also have the option of subscribing to a newsletter or taking part in a competition, prize draw or other special promotion. In this case, we ask you to provide us with your name, address and e-mail address so that we can notify you. Participation in such a promotion also requires your consent in accordance with Article 6(1)(a) GDPR. We will inform you in detail about the use of your data when you register. You are always free to decide whether you wish to give your consent for such a promotion.

Once you have given your consent, you can withdraw it at any time with effect for the future. To do so, please use the links provided in the relevant campaign or contact our data protection officer. However, this does not affect the lawfulness of the processing carried out until the revocation.

Credit check

If we make advance payments to you (e.g. with deliveries of goods when paying on account) or you conclude a loan or other credit agreement with us, we have a legitimate interest in checking your creditworthiness or credit standing. We use the credit check for the following purposes:

- Identity check to ensure that we only deliver our goods to contractual partners who are of legal age and correct.
- Decision by our employees as to whether an order should be placed on account or the conclusion of a credit agreement are possible.
- Assessment of the probability of fulfillment, namely whether existing payment obligations to us can be fulfilled in full and on time.
- Assessment of the default or credit risk.

For this purpose, we work together with so-called credit agencies, to which we transmit your above-mentioned data and from which we receive information. These are the following companies:

- Verband der Vereine Creditreform e.V., Hellersbergstraße 12, 41460 Neuss.
- IHD Gesellschaft für Kredit- und Forderungsmanagement mbH, Augustinusstr. 11 B, 50226 Frechen (only for commercial customers or companies).
- SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden (only for private customers) or consumer).

These credit agencies operate databases and use mathematical-statistical procedures to carry out credit checks (so-called scoring). Credit information is provided to us on this basis. You can find more detailed information in the data protection declarations on the websites of the aforementioned credit agencies. If the credit check is positive, an order on account or the conclusion of a credit agreement with us is possible. If the credit check is negative, it is not possible to place an order on account or conclude the desired credit agreement.

The legal basis for the credit check is Article 6 para. 1 letter f) GDPR.

Recipient of your data:

At our company, only the employees in the Sales and Controlling departments have access to your personal data as mentioned above. Your data will not be passed on to third parties unless you have given your express consent for such a transfer.

We use certain contractors to assist us in processing your personal data. These contractors work on our behalf and in accordance with our instructions. We have concluded an order processing contract with these contractors. All employees of the contractors are bound to confidentiality and data secrecy when handling personal data.

We may have to pass on your personal data to an authority (e.g. tax office, court, etc.) for the purpose of fulfilling legal obligations that apply to us. In such a case, the legal basis for the disclosure is Art. 6 (1) (c) GDPR.

Depending on the payment method you have selected, your payment data will be transmitted to the relevant payment service provider. This applies in particular to cashless payments,
z. e.g. with a credit or EC card. Here we work together with Stripe. These payment service providers are responsible for protecting your payment data.

Beyond this, your personal data will not be passed on. We do not transfer any data to third countries outside the EU or the EEA.

Storage duration:

We delete your personal data according to the following criteria:

- When the contract with us ends, we will immediately block your personal data for any further use.
- We will delete your personal data at the latest on expiry of the statutory retention period (Section 147 (3) of the German Fiscal Code), i.e. after 10 years have elapsed since the order in question.
- If you have given us your express consent for a specific processing operation without a time limit, we will store your data until you withdraw your consent or until you delete your corresponding customer account yourself or the contract with you ends.

You have the following rights:

The right to information

You have the right to request confirmation from us as to whether your personal data is being processed. If this is the case, you have the right to receive information about the personal data collected, stored or used about you, as well as the following information:

the purposes of processing;
the recipients or categories of recipients to whom we have disclosed or will disclose the personal
- data;
- the duration of storage or the criteria for determining this duration; the
existence of further rights (see below);
- if the personal data is not collected from you, all available information about its origin;
- the existence of automated decision-making, including profiling and, where applicable,
- further information on this.

You have the right to be informed of the appropriate safeguards pursuant to Art. 46 GDPR when your data is transferred to a third country or an international organization.

Right to rectification

You have the right to obtain from us without undue delay the rectification of inaccurate or incomplete personal data concerning you.

Right to erasure

You may request that we erase the personal data concerning you without undue delay. We are obliged to delete your personal data immediately if one of the following reasons applies:

- Your personal data are no longer necessary for the purposes for which we collected or otherwise processed them.
- You withdraw your consent and there i s no legal basis for the other processing.
- You object to the processing (see below). Your personal data has been processed unlawfully.
- The deletion of your personal data is necessary for us to fulfill a legal obligation under Union law or the law of the Member States.
- We have collected personal data on the basis of a child's consent.

Right to restriction of processing:

You have the right to obtain from us restriction of processing where one of the following applies:

- You dispute the accuracy of the personal data.
- The processing of the data is unlawful and you oppose the erasure of the personal data and request the restriction of the use of the personal data instead.
- We no longer need the personal data for the purposes of the processing, but you require the data for the establishment, exercise or defense of legal claims; or
- You have lodged an objection to the processing (see below) and it it is not yet clear whether our legitimate reasons outweigh yours.

Right to information

If you have asserted the right to rectification, erasure or restriction of processing against us, we are obliged to notify all recipients to whom the personal data concerning you have been disclosed of this rectification or erasure of the data or restriction of processing, unless this proves impossible or involves a disproportionate effort. You have the right vis-à-vis us to be informed about these recipients.

Right to data portability

You also have the right to receive the personal data concerning you in a structured, commonly used and machine-readable format. In exercising this right, you may request that the personal data concerning you be transferred directly by us to another controller, insofar as this is technically feasible. The freedoms and rights of other persons must not be impaired by this.

Right of objection

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on one of the following grounds:

- The processing of your personal data by us is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us; or
- processing is necessary for the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by your interests or fundamental freedoms which require protection of your personal data.

You also have the right to object to profiling based on this processing.

If we process your personal data for the purpose of direct marketing, you have the right to object at any time to the processing of your personal data for the purpose of such marketing. This also applies to profiling insofar as it is associated with such direct advertising.

You also have the right to object, on grounds relating to your particular situation, to the processing of your personal data which we carry out for scientific or historical research purposes or for statistical purposes, unless the processing is necessary for the performance of a task carried out in the public interest.

Right to withdraw consent under data protection law

You can revoke your consent to us at any time with effect for the future. The revocation is possible at any time informally, e.g. by e-mail to the sales department. However, this does not affect the legality of the processing carried out up to the point of revocation.

Right to lodge a complaint with the supervisory authority

You have the right to lodge a complaint with a supervisory authority, in particular in your country of residence or place of work or the place of the alleged infringement. If you have any doubts, you can contact the Berlin Commissioner for Data Protection and Freedom of Information (Friedrichstraße 219, 10969 Berlin, Tel.: 030 138890), who is responsible for us. In addition to exercising this right, any other administrative or judicial remedy remains unaffected.

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, Schönhauser Allee 180, 10119 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, Luxemburg	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

Appendix 3

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

Expert opinion WhatsApp Business API

Superchat

Brief expert opinion

By: Dr. David Wetter, Lubberger Lehment, Hamburg

Subject: Data protection assessment of the WhatsA pp Business API Date: October 12, 2022

SuperX GmbH ("Superchat") has asked us to evaluate the use of the WhatsApp Business API provided in cooperation with 360dialog GmbH ("360dialog") from a data protection perspective.

I. Summary

In our opinion, the use of the WhatsApp Business API offered by Superchat in cooperation with 360dialog GmbH 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 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 on the respective end devices is automatically transmitted to WhatsApp servers in the USA in order to synchronize which of the stored contacts also use WhatsApp. This synchronization 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 the data subjects pursuant to Art. 13 and 14 GDPR is not ensured. Data protection authorities (in particular of the federal states of Rhineland-Palatinate,

North Rhine-Westphalia and Bavaria) have therefore critically assessed the use of WhatsApp for business communication in the past.

- WhatsApp collects so-called metadata during communication. This includes, according to the WhatsApp privacy policy (available at https://www.whatsapp.com/leqal/privacv-policy-eea#privacv-policv-information-vou-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 prefix). 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 (performance of a 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 any 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 November 2021). 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 (press release dated 16.01.2020, available at https://www.datenschutz.saarland.de/fileadmin/user upload/uds/PM/2020/PM WhatsApp.pdf).

- In addition to the standard and business versions, WhatsApp offers companies the use of WhatsApp Messenger via the WhatsApp Business API. This is an interface that is provided by a WhatsApp-approved Business Solution Provider ("BSP"). 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 technical infrastructure of the BSP.

- Superchat uses the services of 360dialog GmbH, based in Berlin, to offer the WhatsApp Business API. 360dialog is an official BSP for the WhatsApp Business API.

  WhatsApp messages are transmitted encrypted to 360dialog and then transmitted end-to-end encrypted to the WhatsApp interface.

  360dialog offers hosting either in the customer's data center ("on-premise") or in certified data centers in the European Union. According to 360dialog, the communication content is deleted after delivery to the recipient, at the latest within seven days. 360dialog is a processor within the meaning of Art. 28 GDPR and provides a data processing agreement in accordance with Art. 28 (3) GDPR.

III. Assessment

1. No synchronization of contact data

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

2. Communication content hosted on servers in the EU

360dialog has made a commitment to Su- perchat as part of the order\/processing contract to store personal data exclusively on servers in the European Union or the European Economic Area. A justifiable third country transfer within the meaning of Art. 44 GDPR does not take place in this context.

No separate justification is required for data processing by 360dialog. The exchange of data with a processor is not a disclosure by transmission within the meaning of Art. 4 No. 2 GDPR (BeckOK DatenschutzR, 41st ed. 2022, Art. 28, para. 29 with further references).

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 processing of personal data".

decides jointly with others on the purposes and means of the processing of personal data".

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 June 5, 2018) and "Fashion ID" (C-40/17 of July 29, 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 parameterization), 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 the communication on the other) also differ. With this justification, the State Commissioner for Data Protection and Freedom of Information of the State of Saarland has also permitted the municipalities of Saarland to use the WhatsApp Business API (this can be seen in the press release linked in Section II.)

Life
Attorneys at Law Partnership mbB
Theodorstraße 41a
22761 Hamburg
Tel. 040 / 81 95 14 80
Fax 040 / 81 95 14 82 2

Any further questions?

Write to us at: legal@superchat.de

Superchat