White paper

WhatsApp Business API and GDPR – what companies need to know

link mobility

LINK Mobility GmbH
Am Sandtorkai 73
20457 Hamburg

Phone: +49 40 88 88 08 – 44
Web: www.linkmobility.de

Table of Contents

link mobility

[1] "Einführung von animierten Stickern, QR-Codes und mehr", WhatsApp Ireland Limited, https://blog.whatsapp.com/introducing-animated-stickers-qr-codes-and-more, as of 13.04.2021, own translation

[2] David Hein, "Verliert Facebook bei jungen Nutzern den Anschluss?", Horizont, 17.09.2020, https://www.horizont.net/medien/nachrichten/auswertung-von-audience-project-facebook-verliert-bei-jungen-nutzern-den-anschluss-185778?fbclid=IwAR0brzp0vNHD81gV_Re5KBtKm4YK8Z-V1fOeSk4p-zwzY5MpewQMRoCyRzwM, own translation

Two billion people worldwide use WhatsApp[1], in Germany it is 87% of the population.[2] This makes it the most popular messenger in this country. It is therefore obvious that more and more companies are using this channel to get in touch with their customers. In this white paper we will explain what companies need to pay attention to regarding the GDPR when using WhatsApp.

1. WhatsApp, WhatsApp Business, WhatsApp Business API - what is the difference here?

While **WhatsApp is intended for private use**, businesses can choose between **WhatsApp Business** and the WhatsApp Business API. The former is intended for **small businesses** such as small retail shops. The application is installed on the smartphone. However, these solutions are not GDPR compliant. When WhatsApp or WhatsApp Business is installed on the smartphone WhatsApp tries to access the phone's contacts. As a result, these apps do not comply with the data protection guidelines. Using the **WhatsApp Business API** there is no need to install an app. It can only be used via **WhatsApp Business Solution Providers** such as LINK Mobility, partner companies certified by WhatsApp.

The use of the WhatsApp API is the only way to enable companies to use WhatsApp in a GDPR compliant manner. It is also the only scalable solution because the WhatsApp Business API enables several employees to access the account using different devices.

2. May I reply to users who have contacted me via WhatsApp?

Yes. Choosing the WhatsApp channel to initiate communication with the company is **equivalent to consent**. Specialist solicitor for IT law Dr. Hauke Hansen explains in an interview with the Deutsche Handwerks Zeitung: "If the customer writes to the craftsman via WhatsApp, he consciously chooses this communication channel. Theoretically, both also know that

data will be transmitted to the USA. After all, they have agreed to the terms and conditions beforehand".[3] And what applies to crafts businesses also applies to all other companies.

WhatsApp itself allows two types of messages: customer-initiated "**session messages**" and company-initiated "**template messages**". A session message requires that you as a company are proactively contacted by the user. You then have 24 hours to respond with a session message. An opt-in from the customer is not required within this period. Nevertheless, companies should not forget the reference to data processing.

3. Can I proactively send WhatsApp messages to my clients and contacts?

Yes, if you have the **explicit consent** of the person. By the way, it is not enough to have the general consent to use the mobile number, it must be a **WhatsApp-specific consent**. WhatsApp writes in its guidelines: "The opt-in must (a) clearly state that the person is **opting in to receive messages from you over WhatsApp** and (b) clearly state your **business' name**".[4] Furthermore, WhatsApp points out that you are responsible for complying with **applicable laws** when obtaining the opt-in yourself. The structure formerly prescribed by WhatsApp, "Receive [type of information], [WhatsApp logo and name], on [number]" is no longer a mandatory requirement since mid-2020. Companies can only initiate a chat themselves if they use **template messages** approved by WhatsApp. However, these may only be used in the form of notifications about orders (confirmations, delivery updates, etc.). More on this here: https://www.whatsapp.com/legal/business-policy/?lang=en. An opt-in is indispensable for this.

Apart from the WhatsApp conditions there are also some legal framework conditions to consider:

- Consent must be **purpose-specific**, i.e. the recipient must be informed about the type of messages for which his or her data will be used (e.g. status updates).

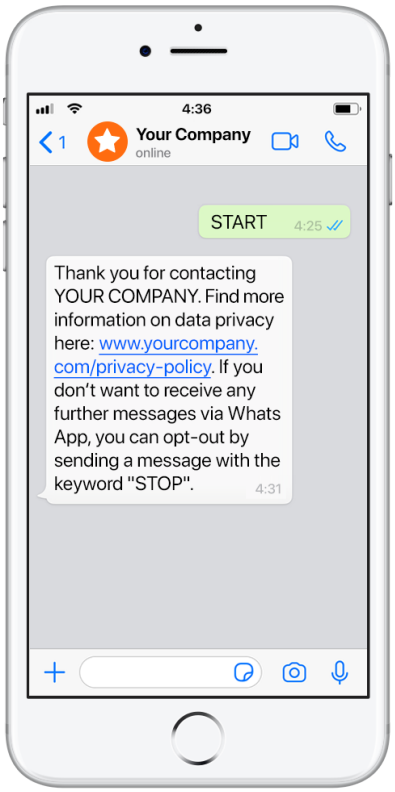
[3] Max Frehner, "WhatsApp und DSGVO: Das gilt rechtlich beim Datenschutz", Deutsche Handwerks Zeitung, 09.10.2018, https://www.deutsche-handwerks-zeitung.de/whatsapp-betrieblich-nutzen-was-beim-datenschutz-wirklich-gilt/150/3101/363865, own translation

[4] https://www.whatsapp.com/legal/business-policy?l=kk, last modified: Jan 2021

- The **type**, **purpose** and **scope** of data processing must be communicated in a comprehensible manner[5]
- Only **necessary** data may be collected. This means that anyone who collects a mobile phone number must also use it for the stated purpose. Otherwise the collection of the number is not appropriate. (cf. Article 5 sec. 1 GDPR)
- **Evidence** of consent must be available at any time (obligation to provide evidence).
- **Revocation** (opt-out) must be possible at any time and must be as simple as giving consent (Article 7 sec. 3 GDPR). For example, customers can opt out by sending a specific keyword (e.g. "STOP").

A **double opt-in** is **not mandatory** in principle, but is **recommended** by many legal experts. VFR Verlag für Rechtsjournalismus GmbH, for example, write on their website: "Although there is no binding legal position for the double opt-in, it is ordered more and more frequently if there is a dispute about the registration procedures".[6]

With regard to the use of WhatsApp, a double opt-in could look as follows: The user **agrees on the company website** to be contacted via WhatsApp and leaves his mobile number in an online form (1st opt-in). The user is then shown the company's mobile phone number to which he or she **should send a specific keyword** (e.g. "START") via WhatsApp. Only when the user has sent this keyword (2nd opt-in) may the company itself send a message. WhatsApp offers the option to send an automated reply. When sending the first company message, however, there are a few things to keep in mind. Lawyer David Oberbeck advises: "Since the data protection notices must be communicated immediately



[5] Thomas Schwenke, "DSGVO: So holst du Einwilligungen richtig ein (Teil 3)", t3n, 31.03.2018, https://t3n.de/news/dsgvo-einwilligungen-843918/, own translation

[6] VFR Verlag für Rechtsjournalismus GmbH, "Was ist Opt-In: Das Zustimmungsverfahren", 29.01.2021, https://www.datenschutz.org/opt-in/, own translation

after storage, the automatic message function can be used for these GDPR obligations to inform the clients. For reasons of clarity, it is also advisable to link to the data protection information (supplemented by WhatsApp) on your website".[7] The first message should therefore also contain information on **data protection**, **data processing** and the **opt-out**.

[7] David Oberbeck, "Ist WhatsApp in Unternehmen mit der DSGVO vereinbar?", 27.05.2020, https://www.datenschutzkanzlei.de/ist-whatsapp-in-unternehmen-mit-der-dsgvo-vereinbar/, own translation

4. Can any company use the WhatsApp Business API?

No. WhatsApp imposes restrictions on certain industries and products. The following businesses are not allowed to use WhatsApp or only to a **limited extent**:

- Drugs/medicines
- Tobacco products and accessories
- Alcohol
- Unsafe ingestible supplements
- Weapons, ammunition, explosives
- Animals
- Adult products and services
- Body parts and fluids
- Medical and healthcare products
- Items or products with overtly sexualized positioning
- Real money gambling services
- Dating services
- Products or items that facilitate or encourage unauthorized access to digital media
- Digital and subscription services, including links to or processing of any subscription sales, renewals, or upgrades
- Business models, goods, items, or services that we determine may be or are fraudulent, misleading, offensive, or deceptive, or may be or are exploitative, inappropriate, or exert undue pressure on targeted groups
- Real, virtual or fake currency
- Third-Party Infringement

Full details of the restrictions can be found here: https://www.whatsapp.com/legal/commerce-policy/

5. What else has to be considered when using the WhatsApp Business API?

a. Imprint obligation

When using WhatsApp, there is also an imprint obligation according to § 5 of the German Telemedia Act. With WhatsApp Business, an "imprint" can be added under "Company info" – which can then also be seen when the section is collapsed – to make it as easy as possible for the user to find the imprint.

b. Privacy policy

Every WhatsApp business profile must contain a privacy policy. If this does not fit in the business description due to lack of space, you can include a link to the privacy policy. However, make sure that it is a "speaking" link, i.e. it contains the term "privacy policy".

6. Is the WhatsApp Business API really GDPR compliant?

Yes. Even though the use of WhatsApp is controversial from a data protection perspective, companies **can use the WhatsApp Business API in compliance with the GDPR**. According to Article 49 sec. 1a GDPR personal data may be transferred to third countries with **explicit consent** after being informed about the existing potential risks.

Don't forget that all your contacts who have installed WhatsApp **have already agreed to the terms of use anyway**. Nevertheless, it can only be an advantage if you point this out. If an exchange of sensitive personal data in the context of customer service is necessary you can also offer your customers to switch to another channel for this purpose.

WhatsApp should not be the only option for customers to contact a company. If **other channels** are available in addition

to the messenger, such as email, telephone, web chat or contact form, the customer can choose freely and is not dependent on the use of WhatsApp.

7. Why is WhatsApp criticized by data protectionists?

In several respects, WhatsApp has some weak points in terms of data protection. Although **end-to-end encryption** of the chat content ensures that **no one can read the messages** – not even WhatsApp – the situation is different with the **meta data**. Meta data can include sender, recipient, location, times or message size. WhatsApp **still has access** to this and changed its terms and conditions at the beginning of 2021 to the effect that **user data may now also be shared with other Facebook companies**. Anyone who wants to continue using the service must agree to the new terms of use.

This is probably also the reason why **WhatsApp does not offer a genuine Order Processing Contract**. The GDPR requires the conclusion of a Order Processing Contract if personal data are processed on behalf of a company. This is the case with WhatsApp. But a Order Processing Contract prohibits the transfer of personal data to third parties (Facebook). WhatsApp currently only offers "data processing terms and conditions", in which the required information stated in Article 28 (3) GDPR is missing. Facebook has already provided a data processing agreement, so it can be assumed that WhatsApp will follow soon.

Another critical issue: since the European Court of Justice declared the **Privacy Shield Agreement**, which until then regulated the transfer of personal data to the USA, invalid on 16 July 2020, **NO software service of a US company is compliant with the GDPR**. Although the EU Standard Contractual Clauses (SCC) apply, which certify compliance with the GDPR and were also valid before the Privacy Shield agreement, data protectionists doubt that US companies can meet this standard at all. This is because the US authorities have permission to access personal data of all US companies. For this reason

authorities advise against the use of many software programs. The Data Protection Commissioner of Mecklenburg-Western Pomerania, Heinz Müller, for example, warns against the use of Microsoft programs and demands that public institutions and authorities switch to open source applications.[8] WhatsApp is thus only one of many software services affected by the invalidity of the Privacy Shield agreement. But to stop all use of US software with immediate effect is almost impossible for most companies.

[8] Pressemitteilung des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, "Land muss Schutz personenbezogener Daten sicherstellen", 17.03.2021, https://www.datenschutz-mv.de/presse/?id=168438, own translation

Nevertheless, as described under 6., those who have valid consent can continue to communicate via WhatsApp Business.

For companies using WhatsApp, comprehensive user education is the best precaution. Point out in your **privacy policy** that WhatsApp processes data independently and link to WhatsApp's terms of use.

Yvonne Bachmann lawyer at the Händlerbund advises: "Some APIs are connected to other service providers, such as support software. Here, the use and transfer of data must also be completely secured. It would also be important that the **hosting servers of the business solution provider are located in Germany or the EU**".[9] The customer chats are stored on the servers of the partners, not on those of WhatsApp. Therefore, LINK Mobility GmbH only uses certified servers located in the EU.

[9, 10] Yvonne Bachmann, lawyer at Händlerbund, personal correspondence, 09.04.2021, own translation

Conclusion

WhatsApp remains controversial in terms of data protection, but communication via WhatsApp Business API is possible with the express consent of the user in compliance with the GDPR. The Händlerbund points out that there is still no official statement or instruction for action from the German "Datenschutzkonferenz" on the use of the WhatsApp Business API.[10] However, more than 50 million companies worldwide are already using WhatsApp Business, including German law firms such as Legal Smart.[11] Anyone who does not offer their

[11] Dave Sebastian, "WhatsApp's Business-User Base Grew Tenfold From 2019", The Wall Street Journal, https://www.wsj.com/articles/whatsapps-business-user-base-grew-tenfold-from-2019-11594298961

customers flexible customer support in their favorite channels nowadays runs the risk of no longer meeting the customers‘ requirements and being overtaken by their competitors in terms of digitalization. Lawyer Jan Lennart Müller assumes “that, at least in the near future, fines or warnings are unlikely to be issued”.[12] So companies should weigh up which risk is higher.

[12] Jan Lennart Müller, “EuGH erklärt sog. Privacy-Shield für ungültig! Wie ist nun zu verfahren?”, 17.07.2020, https://www.it-recht-kanzlei.de/privacy-shield-ungueltig-handlungsoptionen.html, own translation