BRANDI
RECHTSANWÄLTE

MESSENGER SERVICES WITHIN THE COMPANY

Information on data protection I May 2024

Introduction

The use of messenger services has become an integral part of everyday business life. This applies to internal company communication on the one hand and communication with customers on the other. From the company's point of view, the main advantages are easier accessibility for employees without a fixed PC workstation, more personal communication with customers and target group-oriented accessibility. On the contrary, it is often problematic that messenger services have extensive access to and analyze the data and metadata stored on users' mobile devices.

If WhatsApp & Co. are used in the company, it is therefore important to comply with the relevant data protection requirements.

WhatsApp (for Business)

When using WhatsApp, there is the particular problem that the user regularly authorizes the app to read out the contact data on the mobile device and to transfer the personal data stored in the address book, above all names and telephone numbers, to a WhatsApp (Meta) server at regular intervals. By using the messenger service, the user initiates a recurring transfer of personal data to the USA. If business contact data is also stored in the user's address book, the company is generally responsible for the processing of this personal contact data and the transfer to third countries that takes place in the course of WhatsApp use.

At least the transfer of data to the USA can be justified to some extent at the present time, as both WhatsApp and the Meta Group are certified under the EU-US Data Privacy Framework and therefore the transfer of data to third countries in the USA associated with the use of the messenger service can be based on the European Commission's adequacy decision applicable to certified companies.

However, certification under the Data Privacy Framework does not justify the reading and transmission of contact data. There is likely to be no legal basis for the data processing in question. However, it is possible to use WhatsApp on a voluntary basis after prior agreement between the communication partners. If all contacts stored in the address book have consented to the use, the data processing procedures carried out in connection with the use of the messenger service can be based on the legal basis of consent pursuant to Article 6 (1) (1) (a) GDPR. However, if the consent of all contacts cannot be ensured, the use of the address book on the mobile device used should always be prevented or the synchronization of the address book on the mobile device should be deactivated in order to prevent unlawful data processing. Care must be taken to ensure that the setting is made from the outset and permanently for WhatsApp. Alternatively, it is also possible to deny WhatsApp access to the address book by separating the address book into an isolated area of the mobile device, a so-called "sandbox". However, this does not prevent WhatsApp from collecting and analyzing metadata in the course of using the service.

If WhatsApp is to be used as a communication channel with customers, it must be ensured that the customer has consented to its use in advance. In this respect, WhatsApp should only be used after consultation in individual cases, ideally when the initiative comes from the customer or communication partner. Companies must also comply with their data protection information obligations and inform customers transparently about the use of the messenger and the associated data processing procedures. The same ultimately applies to internal company communication via WhatsApp. In addition, despite end-to-end encryption, care should always be taken to ensure that personal data or sensitive content is not exchanged and disclosed without due diligence when using WhatsApp.

The statements apply accordingly to other messenger services, insofar as their use also involves the transfer of data to external companies and similar data protection issues arise in this respect.

A special case: Microsoft Teams Chat

The chat function of Microsoft Teams is still predominantly used in the desktop application, but the mobile Teams version for smartphones becomes more and more popular. It is mainly used for internal company communication and occasionally also for communication with external parties. Microsoft Teams Chat is not a classic messenger service, but it is often used for communication, which is why a number of special data protection features must also be taken into account here.

Both the content of the chats and the data about the users, such as the user name, email address or profile picture, are stored by Microsoft Teams on servers in the USA. The problem of third-country transfers raised above must therefore be considered again. However, Microsoft has also certified itself under the EU-US Data Privacy

Framework. This means that data can be transferred lawfully on the basis of the adequacy decision.

If Microsoft Teams and the chat function are used to establish or execute contracts, Article 6 (1) (1) (b) GDPR is the relevant legal basis. In the majority of cases, however, communication will take place within the company and is then to be based on Article 6 (1) (1) (f) GDPR. The company's interest lies in the simple integration of the other, frequently used Microsoft products and communication between employees both in dialog form and in the group.

In the run-up to using the service, employees must be made aware of the conditions of use and the transfer to the USA.

Threema

The Threema service, for example, is preferable from a data protection perspective. The first positive aspect is that the service can be used without providing a telephone number or e-mail address and even without providing your own name, as individual users are identified by a randomly generated ID.

The users' contact lists are managed directly on the users' devices. As part of the contact matching process, the address book entries are only transmitted to the servers of the messenger service in Switzerland in anonymized form and only if the user expressly requests this, and are deleted from the servers again after the matching process. Messages and media, such as images, videos or files, are also not stored permanently on the company's servers. They are deleted by them as soon as they have been sent to the recipient. The keys are generated decentrally on the user devices during registration, so that the private keys are not known to the messenger service and messages cannot be decrypted. Threema also promises not to analyze personal data or store metadata or log files about who communicated with whom and when.

In view of its less widespread use, the service is probably best suited for internal company communication. The business version Threema Work ("SaaS" solution) also offers various configuration options, for example in the areas of administration and user management. For example, access to the app can be centrally revoked for employees who have left the company. Threema also offers companies the option of concluding a data processing agreement. Threema also provides companies with an "on-premise" solution with an independent chat environment and self-hosted administration portal. Corresponding solutions are also suitable for external communication.

The main disadvantage of Threema is the comparatively low level of connectivity, as the various messenger services are incompatible with each other.

Conclusion

If messenger services are to be used in the company, care must be taken to ensure that they are implemented in compliance with data protection regulations. In particular, the data processing that takes place in this context requires a robust legal basis. Depending on the respective provider, attention must also be paid to the legality of data transfer to third countries in some cases. The specific requirements that arise beyond this in the context of use depend on the specific design - the communication partners, devices used and content to be transmitted. In this respect, it is advisable to consider the respective circumstances on a case-by-case basis.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net