100% on the safe side

The necessary security settings of an enterprise messaging app

VERSION 1.0

Table of contents

Foreword

There is hardly an industry or a sector of public life that has not fallen victim to critical circumstances in the past: environmental events such as fires or floods, sudden lockdowns, acute shortages of supply chains or targeted hacker attacks - organizations, whether companies, associations, ministries, authorities or public facilities, unexpectedly meet situations to the limits of what can be solved. An indispensable anchor for surviving even in uncertain times: reliable communication.

Secondary communication channels such as instant messaging solutions play an important role here. Detached from all other infrastructures, they enable smooth communication across different locations, departments and teams, even in the event of an emergency or crisis. Even mobile workers can be reached in no time at all and informed about the current situation. However, even when introducing and using such a communicative “safety net”, some essential aspects must be taken into account, because not every messaging tool is suitable for business use. In the worst case, organizations only bring in more problems.

So that this does not happen to you and you can still benefit from the advantages of business messaging, in this white paper you will learn:

- which security topics you need to be aware of,
- how these can be implemented technologically,
- which functionalities a communication tool must have,
- what legal requirements are placed on such a solution and
- how to convince your internal critics of a secure messaging app.

All organizational levels for which the topic of security is relevant - from management to IT management to the data protection officer - receive answers to urgent questions. Everything you need to know about secure messaging communication is available here in a clear format. We wish you an insightful read!

Tobias Stepan
Managing Director of
Teamwire GmbH

100%

operational reliability and ability to act

Security requirements that ensure the operation of a communication app

Not only in crisis and exceptional situations should communication be one hundred percent guaranteed - organizations should also always ensure smooth exchange between their members or employees in everyday life. Because only if information flows can take place uninterrupted, organizations remain able to act, no matter what happens. [1]

For a communication solution like a messaging app, availability and reliability must therefore be guaranteed. It also means designing the operation and the entire infrastructure in such a way that communication is secure at all times and possible in accordance with all specifications. For example, in emergency situations, it is important to set up targeted information flows only for members of the crisis management team or managers. In addition, from a technical point of view, a solid basis must be created.
This includes the following aspects:

- **High availability and failure safety**
  High availability can be achieved primarily through redundant server architectures. For this purpose, the communication solution should be operated on several servers and ideally mirrored at different locations. This means that three or more servers are used, although one would be sufficient for the operation. Even if a server fails, operational reliability remains unaffected.

What is operational reliability? [1]

Operational reliability is the trouble-free and application-safe operation of a plant, system or infrastructure. For software applications and communication solutions, this means in concrete terms that their operational readiness and availability must be guaranteed at all times.

100%

operational reliability and ability to act

Security requirements that ensure the operation of a communication app

A business messaging app should be scalable and work just as reliably in small organizations as in large corporations.

Performance and reliability

With the help of redundant cluster setups or servers, the reliability and performance of the communication solution can be guaranteed at all times, for organizations of all sizes. If, for example, there are peak loads due to very high usage, the load is automatically distributed to the servers. The delivery of messages, content and status updates remains fast and is constantly secured.

Scalability

A business messaging app should be scalable and work just as reliably in small organizations as in large corporations. To do this, the computing power must be adjustable as needed so that reliable communication is ensured for all users of the organization. With a scalable server architecture, this can be implemented easily and flexibly in a public or private cloud as well as on-premises.

Low infrastructure requirements

Even if the servers of a business messaging have to be highly available and scalable, it is still necessary that they work resource-efficiently and put little strain on the infrastructure. In this respect, the communication solution should place the fewest possible demands on the infrastructure and require little hardware.

Multi-tenant and multi-domain capability

Companies with different business areas and organizations need a software solution that is multi-tenant capable and enables these tenants to be managed individually. Companies that use different e-mail domains should rely on a communication solution that is multi-domain capable and automatically creates user directories for these domains.

100%

operational reliability and ability to act

Security requirements that ensure the operation of a communication app

Fully automated and secure roll-out

Being up and running quickly also means that the setup and registration process of the application on the end devices is possible automatically and without the need for user intervention. This guarantees a company-wide security setting and accelerates the roll-out.

Central administration of users

In order to centralize and automate user management as comprehensively as possible, you should make sure that the software solution allows the import or ideally synchronization of a Lightweight Directory Access Protocol (LDAP) or Active Directory (AD). Such a function ensures a uniform company directory and allows users to be easily blocked for all applications if necessary. Besides, such functions save the administrators a lot of time.

100%

operational reliability and ability to act

Security requirements that ensure the operation of a communication app

- **Usage Statistics**
  For organizations to be able to observe the use of a communication solution and to understand usage behavior. This makes it easier to understand and anticipate peak loads during use. For this purpose, the software should provide usage statistics.

In order to remain able to act now and in the future, not only an operationally safe and reliable communication solution is required. Rather, this must also guarantee the organization the greatest possible control and data sovereignty - and that usually starts with hosting. Therefore, US providers are usually out of the question. In the next chapter you will find out why this is the case and what organizations need to pay attention to when it comes to data sovereignty.

The organization has the greatest possible control and data sovereignty - and that usually starts with hosting. Therefore, US providers are usually out of the question.

100%

data sovereignty

Security requirements with which data sovereignty lies with the organization

Linked to the operational and future security of systems within organizations, the area of communication, collaboration and information exchange is also specifically about the handling of data. Here, the transparency and control on the part of the organization is to be regarded as a particularly valuable asset: it is about their data sovereignty. [2]

In the area of software and provider selection, it is therefore important to check what influence, access and control options the organization or its IT department has on the data when using a business messaging app. This affects both the technical basis and the hosting as well as the features and, above all, configuration options. [3]

Free choice of hosting

The software and its hosting should fit the organization's IT strategy and therefore allow the solution to be operated in a secure public cloud, private cloud or on- premises on company-owned servers. This should also have no restrictions on the range of features and available functionality.

Policies for data retention

It should be possible for the IT administrator to determine the data retention periods for all end devices and servers, so that messages that have exceeded a certain storage period are

What is data sovereignty ↓ actually? [2]

Data sovereignty describes the greatest possible sovereignty and control over (own) data. An organization should be able to handle its own data of members (e.g. employees) and external persons (e.g. applicants, customers or partners) as well as its own business, research and development and other data in a self-determined manner. This means that the collection, storage, processing and use of your own data should be free from access, restrictions or dependencies by third parties. Otherwise, there is a particular risk that the organization's data will also be used by software providers for their own purposes and that migration to alternative providers will not be possible. These risks can lead to monopoly formations on the market, closed systems or almost restrictive license agreements.

100%

data sovereignty

Security requirements with which data sovereignty lies with the organization

automatically deleted from the end devices or servers. In this way, data – especially on mobile devices – is not kept longer than necessary and access is reduced to what is necessary.

Exclusive server location in Germany

In order to avoid any legal exceptions in certain countries, European organizations should rely on a server location in Europe or even Germany – a very safe option. Local privacy and data security laws ensure that the organization is the sole legal owner of the data.

Remote deletion of data on mobile devices

Whether through theft or loss - if end devices are lost, it should be possible to block individual devices or users remotely and delete any data from the device. In this way, typical “Data Loss Prevention “ scenarios can be easily solved. PIN codes also make it more difficult for unauthorized persons to gain access to the application via a terminal device.

No hidden analysis of metadata

In order to exclude any influence of third parties, no analysis of metadata, user information or communication should take place by the software provider. If the provider needs data to operate the solution, he should clearly state and explain this. In principle, the data belongs exclusively to the organization itself.

Professional administration

A communication solution for organizations should offer an easy-to-use and professional administrator portal or dashboard in order to be able to control all users and data of an organization easily and centrally at any time. These include user management, access management, monitoring functions, company-wide guidelines and communication rules.

Reading tip 3

You can read all the background information on the dilemma with US providers on our blog!

OPEN LINK

100%

data sovereignty

Security requirements with which data sovereignty lies with the organization

Secure and controllable app container

A business messaging app should have its own secure container where all messages and data are stored in encrypted form. The app container should be able to be centrally configured and controlled by the IT administration using numerous guidelines. This provides the best possible protection for company data on end devices and prevents uncontrolled data leakage.

White listing of users

If the communication solution allows selected users, teams and business areas to be activated for use (white listed), the organization then controls the company-wide use of the tool and can ensure that only authorized employees have access.

User pooling

If users can be assigned to closed areas (e.g. research and development, accounting, investment banking), this enables the organization to restrict the exchange of confidential content and prevent data leakage.

Secure integration of third-party systems

In the case of connections, integrations and APIs to third-party providers, it is particularly important to ensure that data access and exchange is authorized. It must be possible to configure the data access of each third-party system individually and to block

100%

data sovereignty

Security requirements with which data sovereignty lies with the organization

it at any time if necessary. In this way, data can be exchanged in a controlled manner – without uncontrolled data leakage.

Anyone who has sovereignty over their data must also bear responsibility for its protection and security - across the entire organization and along the entire infrastructure and supply chain. Unfortunately, companies whose industry, competitors or even themselves have been victims of cyber attacks still haven't internalized what they need to do in terms of cyber security. The following chapter explains.

It must be possible to configure the data access of each third-party system individually and to block it at any time if necessary. In this way, data can be exchanged in a controlled manner – without uncontrolled data leakage.

100%
cyber security

Security requirements to prevent cyber attacks

The most powerful argument for building security into any software solution is the potential threat posed by cybercriminals. The report on the **IT security situation in Germany in 2022** by the Federal Office for Information Security (BSI) confirms it: The number of hacker attacks and security incidents in the field of cyber security is increasing rapidly, and very few organizations are aware of the risks their IT decisions really pose recover [4]

Examples of potential cyber threats for specific industries:

Police
e.g. hacker attacks to steal data or paralyze the system

Healthcare
e.g. ransomware attacks that render critical systems inoperable

Authorities & Ministries
e.g. cyber attacks to view data or to influence critical infrastructures

Banks & insurance companies
e.g. cyber attacks that steal sensitive customer and account data

Military & Defense
e.g. cyber espionage and sabotage

Logistics & Transportation
e.g. attacks on the fleet management system when transporting dangerous goods, delays in supply chains

Utilities
e.g. attacks on supply networks and control units that interrupt the supply

Production
e.g. industrial espionage attacks

Retail & Trade
e.g. cyber attacks on online shops to access customer and payment data

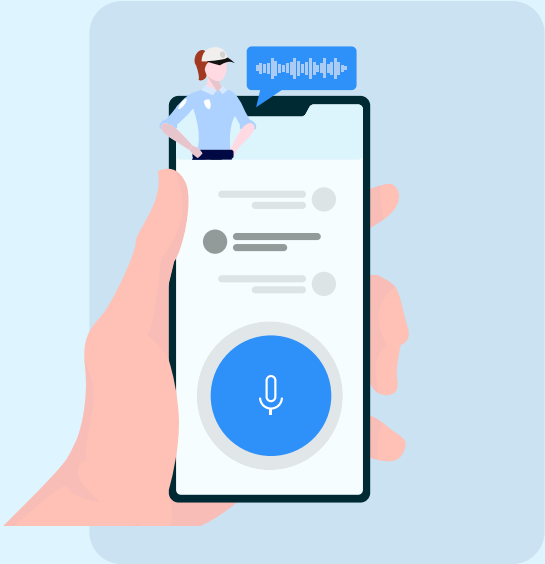
Why is cyber security so important? [4]

Cyber security describes the protection of systems, networks and applications against digital attacks. These cyber attacks are mostly aimed at accessing, changing or destroying data, extorting money or disrupting processes. Cyber security is therefore the most important requirement for protecting information, people and other assets of an organization and itself.

100%

cyber security

Security requirements to prevent cyber attacks



From a technological point of view, fundamental requirements must therefore be met in order to ensure cyber security. These include the following aspects:

- **Zero trust approach**
  Organizations are well-advised to follow the zero trust approach – that is, to treat every internal and external access as a potential threat and breach and to play it safe when it comes to authentication. Therefore, the communication solution should comprehensively control identities and rights as well as protect against unauthorized access to apps, devices and servers by users, bots or third-party systems. [5]

- **ISO 27001 certification**
  If the decision is made to leave the hosting to the provider, it is important to ensure the greatest possible security. The use of ISO 27001-certified data centers is a best practise, which, in addition to standardized security processes, should also offer a reliable infrastructure, network connection, 24/7 security, strict access controls, emergency protection and the like.

Reading tip [5]

Read more online about how zero trust and messenger communication interact!

OPEN LINK

100%

cyber security

Security requirements to prevent cyber attacks

Protection of infrastructure and networks

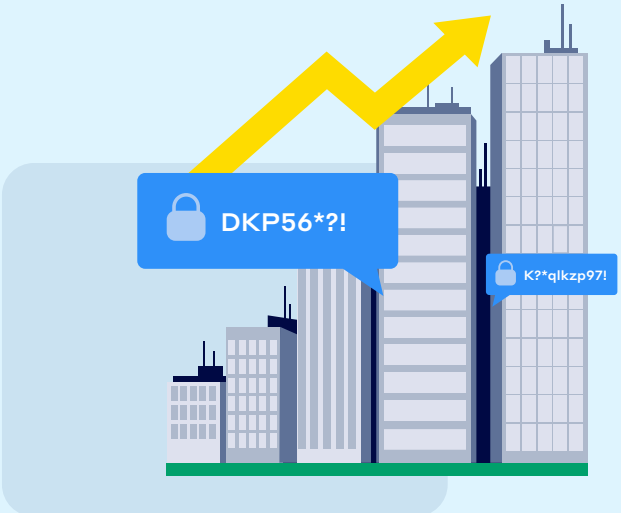
Data centers and servers should have modern protection mechanisms (e.g. firewalls, fire protection and modern security software) and - strictly guarded – should only allow selected persons access. The provider's security guidelines should ensure that the protective measures are maintained.

Regular security audits

Internal and external audits with penetration tests and vulnerability analyses, which, among other things, simulate typical attacks, should take place at the provider's premises at regular intervals. This is the only way to guarantee the long-term functionality of the protective measures and sustainable security of data and systems.

Transmission encryption

In order to protect the connection between the application and the servers of a communication solution, the data exchange should be https-encrypted. Random temporary keys and pinned certificates should be used. As a result, a potential attacker cannot subsequently decrypt the data transmission in the network. For enterprises and public authorities, in addition VPN tunnels are recommended for the transport channel, which secure access to their own infrastructure.



100%

cyber security

Security requirements to prevent cyber attacks

All data should also be stored in encrypted form – whether on a smartphone, tablet or desktop, on a server in the cloud or on-premises. The respective keys for this should be under the control of the organization.

Metadata encryption

In order to prevent eavesdropping attacks or “man-in- the -middle “ attacks, in which attackers often try to compromise the https channel in order to get in between the sender and recipient and access information, the metadata must also be encrypted before transmission. The validation and decryption of these communication packets can then only be carried out by the application itself and legitimate recipients. This means that the metadata is also well protected.

Message and content encryption

In addition, the sender should encrypt all messages and digital content and the recipient should only be able to decrypt them after transmission. While in some cases a complete end-to-end encryption is necessary, there are often situations in the business world in which the organization - for example for compliance reasons - needs access to the communication of its users. It is important to have an end-to-end encryption in place, in which the provider has no access to the messages and content.

Encrypted data storage

All data should also be stored in encrypted form – whether on a smartphone, tablet or desktop, on a server in the cloud or on-premises. The respective keys for this should be under the control of the organization.

Two-factor authentication for administrators

Access to the administration portal should be secured by two-factor authentication. Administrators must enter a password and an app-based second factor to access the administration portal and confidential company data.

100%
cyber security

Security requirements to prevent cyber attacks

Authorization of end devices through MDM/EMM

Through enrollment tokens and secure app tunnels from MDM (Mobile Device Management) and EMM (Enterprise Mobility Management) solutions, organizations can ensure that only authorized devices have access to the application and infrastructure. In addition, integration into the organization's EMM allows for advanced configuration of the application - for example, when defining rules that allow or prevent the sharing or copying of messages with other applications. [6]

When protecting against cyber attacks and loss of data, the focus is primarily on information that is of great value to the company. This often includes personal data, which must also be protected from a legal point of view. The following chapter tells you which data protection requirements apply to messenger communication and how they can be met.

Reading tip [6]

Find out how enterprise mobility management complements secure messaging on our blog!

OPEN LINK

100%
data protection

Security requirements to protect personal data

Data protection is one of the greatest goods of our time. The right to informational self-determination, which is enshrined in fundamental rights, guarantees every natural person the right to decide for themselves how personal data is processed and used. This is accompanied by specific legal requirements that serve to protect this right. Anchored in the European General Data Protection Regulation (GDPR) and the German Data Protection Act (BDSG), they contain specific requirements for all organizations that collect, process, store or use personal data. [7]

GDPR as a basis

The provider should process data in accordance with the European data protection requirements of the GDPR. Likewise, data should only be processed with express consent.

Data reduction and data economy

In general, a provider should only access data if it is necessary for the provision of the service. In this respect, the provider should only access personal data if it is absolutely necessary for security or administration reasons. In addition, data that is no longer required should be automatically deleted. In this way, the GDPR principles of data economy and data reduction can be satisfied in the best way.

Data protection vs. data security - what is the difference? [7]

Data protection includes all legal aspects with regard to the collection, processing and use of personal data. Personal data is any information that identifies a person or makes them identifiable. Data security, on the other hand, deals with the general protection of data - also, but not exclusively, with personal data.

100%

data protection

Security requirements to protect personal data

GDPR compliant contracts

It is necessary to conclude an data processing agreement for the solution with the provider that meets all the requirements of the GDPR. In addition, the provider should have a privacy policy that is easy to understand and creates transparency about all data processing and activities. [8]

Anonymization and encryption of user data

The communication solution should ensure the protection of personal data (e.g. IDs, phone numbers, email addresses and passwords) through anonymization and encryption.

Multiple authentication

The users of the solution should be authenticated at multiple stages. In addition to the telephone number and e-mail address, these can also be IDs or PINs as a second factor, which are continuously checked and thus reliably authenticate the users. [9]

No complicated settings

Ideally, the communication solution should be developed for secure and confidential communication in the team and avoid complicated data protection settings. Data exchange and communication should always be compliant with data protection and secure per se.

Data storage on end devices

It is recommended that the address book with all contact data is not stored on the provider's servers, but only on the user's end device. User data and messages should also be stored encrypted on the end device so that the organization's data is protected as best as possible and separated from other applications.

Reading tip [8] ↓

In our blog, we will tell you why and how you (should) not make any compromises when it comes to data protection!

OPEN LINK

Privacy by design and privacy by default – what does that mean? [9] ↓

Privacy by design describes compliance with data protection through technology design. This means that every software solution should be designed in such a way that it complies with legal requirements. Privacy by default means that strong data protection settings, which protect the rights of data subjects in the best possible way, are set as a standard.

100%
data protection

Security requirements to protect personal data

Backup and deletion of data

All data must be backed up regularly and automatically. The backup should be carried out redundantly at several locations in order to be prepared against data loss. In addition, data should not be stored longer than the organization wishes. Ideally, content and messages should be deleted after a defined period of time.

In addition to the general requirements for an organization to position itself securely in terms of data sovereignty and data protection and to ensure operational reliability and cyber security, legal and compliance requirements must also be taken into account. The following chapter shows what this means in concrete terms for certain sectors.

It is recommended that the address book with all contact data is not stored on the provider's servers, but only on the user's end device.

100%

compliance and audit proof

Security requirements to be met from a legal point of view

Certain industries are faced with various legal requirements - such as a duty of confidentiality, necessary risk assessments or the required archiving of data. Cross-industry laws such as a supply chain acts or the General Data Protection Regulation can also play a role here. This is usually accompanied by internal demands on the behavior of organizational members and employees. This also applies in particular to communication relating to work processes and thus the use of communication solutions such as a business messaging app. [10]

Examples of specific laws and regulations for compliance:

Police
e.g. mission documentation

Healthcare
e.g. medical confidentiality, documentation of patient cases

Authorities & Ministries
e.g. duty of documentation, electoral law

Banks & insurance companies
e.g. securities trading act, MiFID-II, DORA

Military & Defense
e.g. obligation of confidentiality, protection against sabotage

Logistics & Transportation
e.g. transport of dangerous goods, export control

Utilities
e.g. security act, KRITIS law

Produktion
e.g. environmental protection, workers safety

Retail & Trade
e.g. principles of the honest merchant

What does compliance mean? [10]

Compliance means conforming to a rule and obeying an order. What is meant here is the fulfillment of ethical, legal and legal requirements within an organization by the organization itself and its employees. These are measures that serve to fulfill the organizational purpose in a legally compliant manner and to minimize risks (e.g. criminal and civil law).

100%

compliance and audit proof

Security requirements to be met from a legal point of view

The requirement to document communication via a business messaging app and to archive it in an audit-proof manner affects the majority of all organizations. These usually result from tax and accounting obligations, legal requirements, ethical guidelines or internal compliance. It is also a fact that organizations that do not archive their business communication should expect legal problems. This also applies to the question of access rights for individual organization members and groups. Therefore, the following points must be taken into account.

- **Implementation of permissions & security policies**
  Organization-wide secure messaging requires roles and permissions to be implemented as part of a dedicated access management. This should cover granular security, privacy, and compliance policies that protect corporate data and comply with legal requirements.

- **Archiving options**
  It should be possible to archive messages and data of the organization members easily and encrypted. An audit-proof archive should be available according to specific time periods and user groups or clients, and it should be searchable. In addition, only authorized persons (e.g. data protection officers, internal auditors) should be able to access and search the audit-proof archive. [11]

- **Audit logging**
  Audit logs, which create a chronological log, are helpful for reliably documenting all activities. This allows all administration and compliance related processes to be recorded and replicated if necessary. For this purpose, the audit logs should be searchable: Past activities can be easily found and assessments can be carried out just as easily.

Reading tip [11]

We have summarized which specifications for an audit-proof archive may have to be relevant!

OPEN LINK

100%

compliance and audit proof

Security requirements to be met from a legal point of view

Auditor access

Frequently, the fulfillment of compliance and legal requirements must be assessed by auditors or external auditors. Therefore, access to the relevant documented data - and only to this - is important and it should be possible to set up a special access with limited rights for examiners, auditors or revisers. This supports audit-proof work and compliance without having to unnecessarily distribute data.

From compliance and audit proof to data sovereignty and cyber security to data protection - for management, IT and data protection officers, there are sometimes different but also overlapping requirements with regard to secure communication within the organization. In order to find the right messaging solution or to check your own tools, the final checklist sums up all the relevant aspects.

Audit logs, which create a chronological log, are helpful for reliably documenting all activities. This allows all administration and compliance related processes to be recorded and replicated if necessary.

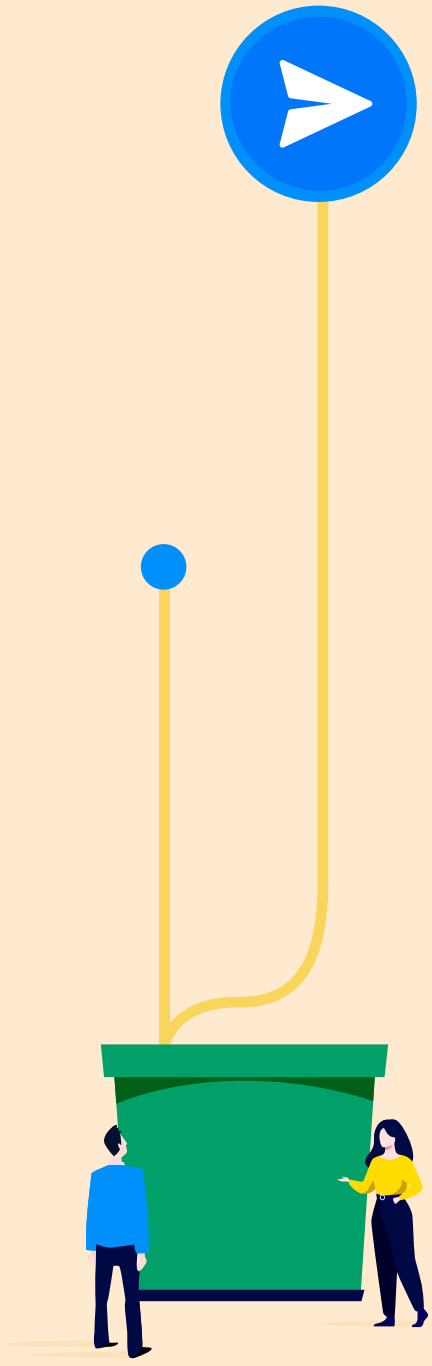
Checklist : Safe with your business messaging?

The following overview shows which security requirements a messenger should meet for reliable and secure communication within the organization:

- Implementation of permissions & security policies
- Anonymization and encryption of user data
- Archiving options
- Exclusive server location in Germany
- Authorization of end devices through MDM/EMM
- Data economy and data reduction
- Data storage on end devices
- GDPR as a basis
- GDPR compliant contracts
- Remote deletion of data on mobile devices
- Free choice of hosting
- Low infrastructure requirements
- High availability and failure safety
- ISO 27001 certification
- No complicated settings
- No hidden analysis of metadata
- Performance and reliability
- Multiple authentication
- Multi-tenant and multi-domain capability
- User pooling
- Usage Statistics
- Professional administration
- Audit logging
- Regular security audits
- Rules for data retention periods
- Auditor access
- Protection of infrastructure and networks
- Secure integration of third-party systems
- Secure and controllable app container
- Backup and deletion of data
- Scalability
- Transmission encryption
- Encrypted data storage
- Message and content encryption
- Metadata encryption
- Fully automated and secure roll-out
- White listing of users
- Central administration of users
- Zero trust approach
- Two-factor authentication for administrators

Do the check · now with your planned or already installed business messaging app!

Conclusion



Like any other software, a communication solution must be seamlessly integrated into an organization's IT landscape. Security requirements for compliance, operational reliability, data sovereignty, cyber security and data protection are essential aspects that ensure smooth functioning and secure communication via this solution. In particular, a business messaging app, whose particular benefit is in the connection of all employees - whether in the office, remotely or mobile - must offer 100% security across all end devices.

In this way, organizations protect themselves from potential cyber threats, meet all legal requirements for their communication and ensure the protection of all data - whether business-critical or personal. This strengthens the future viability of an organization today, but also in the long term.

About Teamwire

With the business messaging app of the same name, Teamwire GmbH has specialized in secure, simple and fast communication via text and voice messages as well as video calls. Founded in 2015 and headquartered in Munich, the company helps companies, public authorities, blue light organizations and the healthcare sector to improve the productivity and results of mobile collaboration. The business messaging app offers innovative functions that are tailored to the use cases of companies with a large number of mobile workers, while guaranteeing professional administration and the highest security requirements. The company complies with all European data protection requirements and the GDPR. Numerous customers rely on Teamwire, including the police, the Federal Ministry of Labor and Social Affairs, the clinic of Chemnitz, Dataport and Vodafone.

teamwire.eu

Imprint

Editor
Teamwire GmbH
Tittmoninger Strasse 11
81679 Munich

teamwire.eu
E-mail: **info@teamwire.eu**

Management
Tobias Stepan
Registration court: District Court of Munich
HRB 187102

Conception
Tobias Stepan, Teamwire GmbH, teamwire.eu
Katja Dreißig and Jennifer Köhler, Möller Horcher Kommunikation GmbH, www.moeller-horcher.de

Text
Jennifer Köhler, Möller Horcher Kommunikation GmbH, moeller-horcher.de

Layout & Graphics
Salva González, Pilar Sabogal, Teamwire GmbH, teamwire.eu

Version 1.0
The contents of the white paper were created with the greatest care. However, we cannot assume any liability for the correctness, completeness and topicality.