ENCRYPTION

Emails in business.

Sending secure emails in conformity to GDPR.

digicert®

InterNetX

Table of contents.

EXECUTIVE SUMMARY 03

EMAILS IN BUSINESS 04

SECTION 01
LEGAL REQUIREMENTS FOR MAILINGS 06

SECTION 02
ENCRYPTION – ONLY FOR IT COMPANIES? 08

SECTION 03
BEST PRACTICE: EMAIL ENCRYPTION FOR COMPANIES 16

CONCLUSION 21

REFERENCES & PHOTO CREDITS 22

ABOUT 23

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

Executive Summary.

All companies have felt the effects of the EU Data Protection Regulation (GDPR) to a greater or lesser degree. It has led to changes in many areas and remains one of the driving forces in digitization processes.

Nevertheless, sending emails, and the technical and legal requirements that go hand in hand with this, still frequently remain uncertain terrain. For a start, companies frequently do not know enough about the norms, especially as they allow some margin for interpretation with regard to technical protective measures. Moreover, they are also often unaware of the urgency of content and transport encryption for emails. But one thing remains certain. Apart from enormous damage to the company's reputation, fines amounting to millions can be incurred for violations regarding email communication.

For the transmission of emails in conformity to the GDPR, the following is required:

- internal compliance guidelines
- strategic decisions about security dimensions
- implementation measures

This e-paper clarifies which measures are required for GDPR conformity when sending emails and offers possible technical solutions. It ends by presenting a best-practice scenario to help companies be prepared.

However, we would like to draw your explicit attention to the fact that this e-paper is intended for informative purposes only. It does not constitute legal advice and cannot replace legal counseling in individual cases.

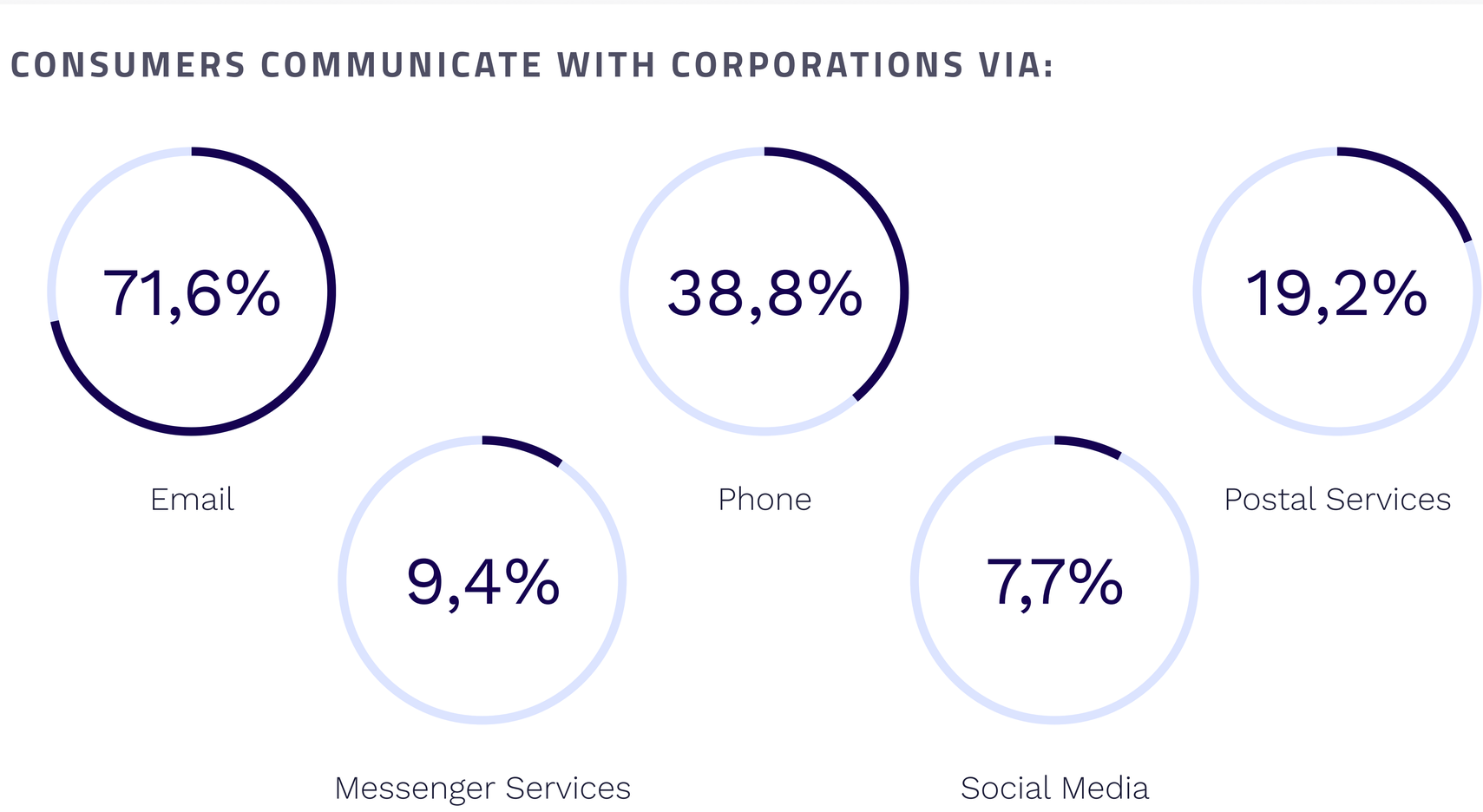
INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

Emails in business.

Phishing attacks are booming and cases of (online) identity theft and email fraud are on the rise. After a number of data scandals in recent years, it should be thoroughly clear that information is systematically monitored and intercepted online. This includes data in companies. And data protection advocates are demanding higher standards, particularly with regard to email communication.

It’s not without reason that emails are often likened to digital postcards. Anyone who can transport them, can also read them, as long as no further protective measures have been taken. Without additional protection, data is easy to access online for other parties. Unauthorized access to customer or employee data, the latest project in development or the internal security system could hit companies hard, regardless of their size.

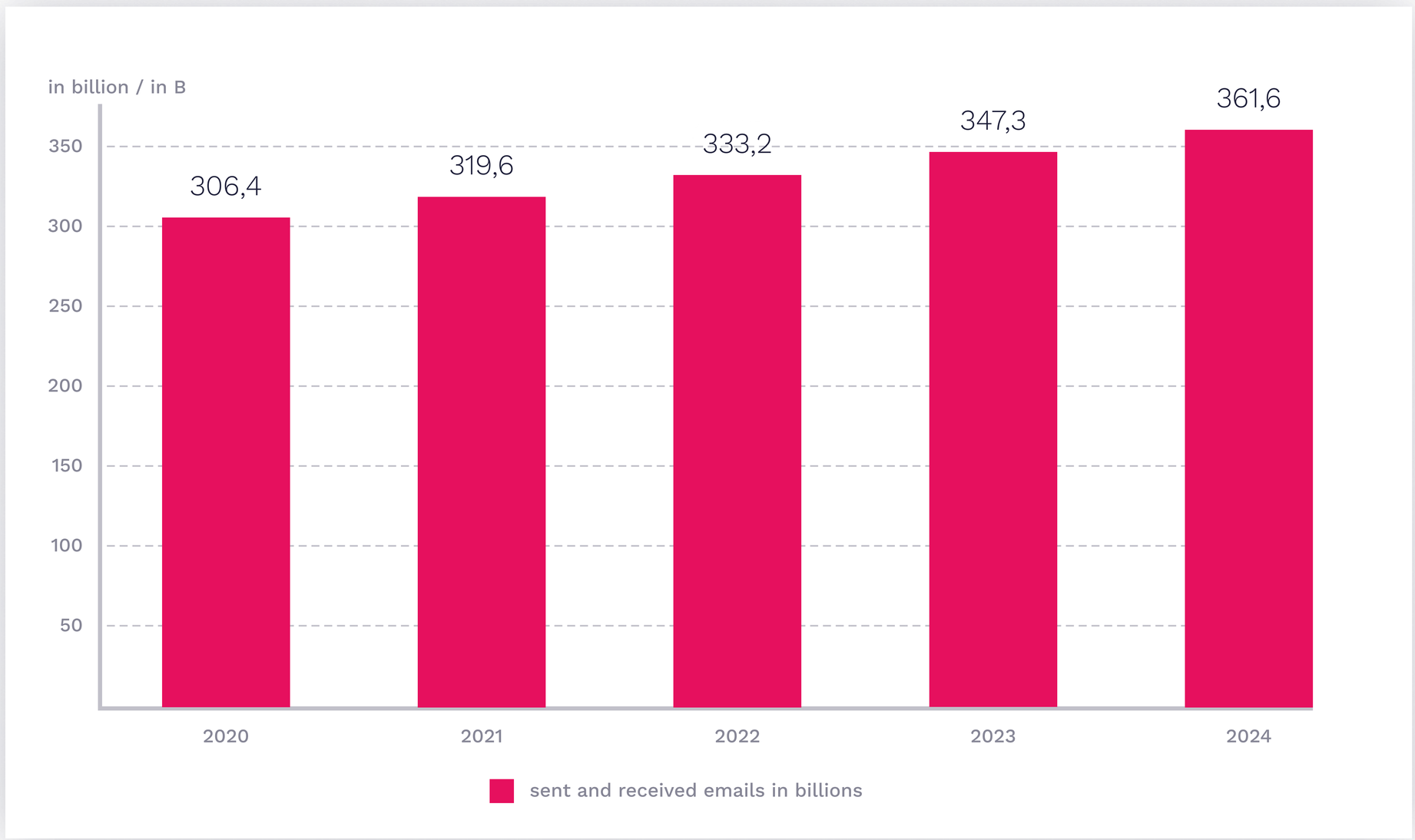
According to a study undertaken by Convios Consulting for GMX and WEB.de, email remains the most popular means of communication for consumers to contact companies, leading with a formidable 71.6%. Telephone follows with 38.8%, postal services with 19.2%, messenger services with 9.4% and Social Media with 7.7%.



Digital Germany 2020 commissioned by WEB.DE and GMX
(Representative study by Convios Consulting GmbH (in German)

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

This is also demonstrated by the prognosis that email communication will increase by 18% worldwide by 2024:



Source (in German): Prognosis of daily number of emails sent and received worldwide from 2020 to 2024 (in billions)© Statista 2021

Companies distribute all kinds of information in emails, starting from simple notes through to personal data and sensitive internal company information. For this reason, this communication channel has proven to be of central importance and therefore also requires protection.

And this is particularly important with regard to the GDPR. As digitization accelerates, companies frequently feel uncertain, not least of all due to the related legal requirements. The predominant questions are whether the measures they have implemented are sufficient and whether they have all the necessary information about requirements and risks.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

Legal requirements for mailings.

All companies are therefore well advised to protect their own data, as well as that of their customers and partners. And lawmakers hold the same opinion, even if from a slightly different perspective. With the introduction of the GDPR, the EU has strengthened the rights of residents with regard to their own data, which may no longer be stored or processed without having a clear legal basis for doing so. The principle of data minimization applies. So, information about an individual may no longer be collected without taking careful precautions.

> **Article 32 of the regulation** explicitly stipulates that those responsible must implement appropriate technical measures to protect personal data, such as pseudonymization and encryption. Violations of the GDPR may result in rather hefty fines and, depending on the scope, certainly result in unpleasant headlines.

The German Federal Data Protection Act **(BDSG)** complements and gives concrete form to the requirements of the GDPR for Germany and lays a stringently regulated framework for how to handle personal data.

In addition, the **Law on Control and Transparency in Business (KonTraG)** has also applied for German companies since 1998. Amongst others, it prescribes the use of the following measures for risk identification:

- **Firewalls** as a barrier between networks
- **Signatures** for checking identity
- **Encryption** to ensure confidentiality of content

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

DSGVO or GDPR

The term DSGVO occasionally pops up in relation to the GDPR. It stands for Datenschutzgrundverordnung and is the German term for the General Data Protection Regulation (GDPR).

Compliant email communication is therefore not just a necessity to avoid penalties. Rather, it can be used as a decisive competitive factor:

Customers and partners are increasingly considering what happens to their data and how companies handle it. When in doubt, they are more likely to choose a provider that offers more security with encrypted communication.

Encryption (also called cryptography)

Data, also called “plaintext” is coded using a key. This unreadable sequence can only be turned back into plaintext using the key.

The GDPR is not only valid for all companies located in the EU, but also for those outside of Europe who are active on the European market or process the personal data of EU residents.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

Encryption – only for IT companies?

In this regard, the answer is very clear. Absolutely not. All companies that maintain digital correspondence are facing ever more threats online as well as new legal and technical requirements. It is a mistake to think that this only counts for highly-specialized providers in the IT industry. Encryption makes sense for one-man businesses and multinational corporations alike, regardless of the sector.

ENCRYPTING EMAILS SECURELY

In order to protect information using encryption, the information itself can be ciphered. In this case, one speaks of **content encryption**. A well-known example of this is S/MIME for emails.

On the contrary, **transport encryption** is aimed at the channel transmitting the information. This does not always necessarily relate to the transmission of emails, but also to websites, for which e.g. **TLS/SSL** is utilized.

The options available for encryption are as diverse as the types of data that are transmitted on the internet. For example, using Code Signing, software providers can add a digital signature to the program code they make available. So, users can rest assured that the software is from the provider and they are not downloading third-party malware.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

TRANSPORT ENCRYPTION WITH SSL

SSL stands for Secure Socket Layer. In this context, layer refers to the transport layer between two computers, loosely speaking, between the two communication channels. During a secure connection, the computers involved exclusively communicate via the mechanism provided by SSL, so the **transport route** is encrypted. The content itself remains in plaintext.

The digital key pair, i.e. the public and private key of the server, is at the heart of the way SSL functions. In addition, the digital certificates are used to authenticate the keys.

An encrypted SSL connection always originates from the client, which contacts the server and starts a kind of digital "greeting", referred to as the handshake. The server sends its SSL certificate back to the client, where its validity is checked. It also sends a request to the certification authority (short CA) to verify the signature.

Once the check has been completed successfully, the client creates a symmetric key called **Premaster Secret (PMS)**, codes it with the server's public key and sends it back. On its side, the server uses its private key to decode the PMS. Using the PMS, both sides then generate a symmetric key, which also creates a symmetrically encrypted communication channel and the SSL connection is set up.

So, asymmetric encryption is initially used for the handshake. However, the transmission of data later follows with symmetric encryption.

TLS/SSL certificate

There are different types of SSL certificates, depending on the requirements of the applicant. They differ, for example, with regard to encryption strength, the type of validation and which browsers support them.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

TRANSPORT ENCRYPTION WITH TLS

TLS (Transport Layer Security) is, to put it briefly, the successor of SSL. Development of the protocol started in 1996 and it was initially named SSL 3.1. Since 1999, the official term is TLS. The current version 1.3 has been in existence since 2018.

The functional principle with the handshake is identical with both, but security against attacks was increased with the new protocol. It also supports more algorithms for encryption between server and client. For this reason, SSL should no longer be used these days. However, the abbreviation is much more widely-used than TLS, which is why people often speak about SSL even though they are actually referring to TLS.

If you want to play safe, use the term **TLS/SSL**.



Ministry recommendation

Due to COVID-19 and the resulting increase in working from home, The German Federal Office for Information Security has updated its guidelines on minimum standards for the utilization of Transport Layer Security (TLS). For secure transport encryption, exclusively TLS 1.3 or TLS 1.2 should be used, the latter only with a special procedure for key exchange (Diffie Hellman protocol). TLS 1.2 and TLS 1.3 are generally used as the standard.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

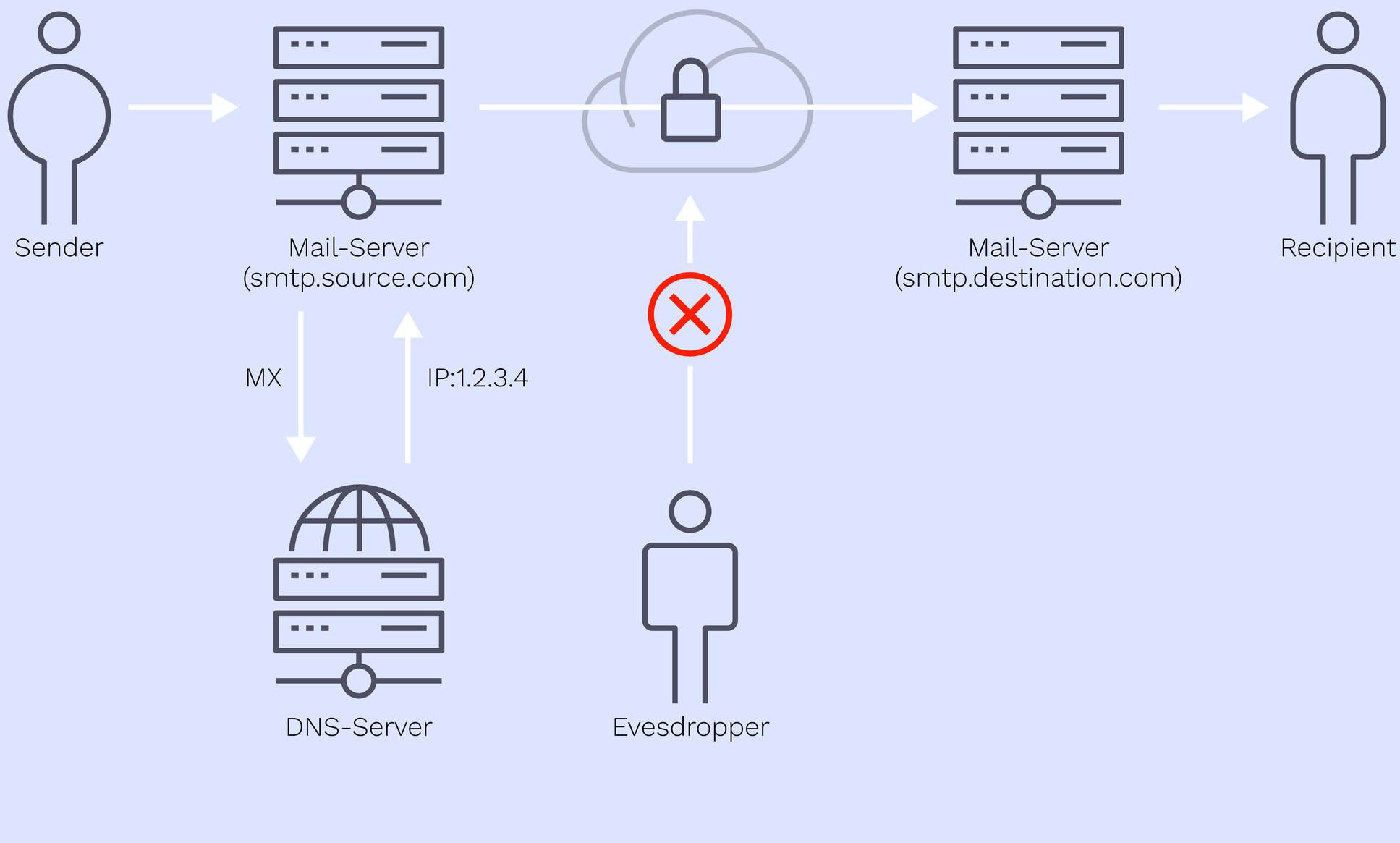
IS TRANSPORT ENCRYPTION SUFFICIENT FOR SECURE EMAIL COMMUNICATION THAT CONFORMS TO THE GDPR?

As previously mentioned, **SSL** and **TLS** encrypt the channel via which the message is transmitted, but not the actual message itself. At the beginning and end of the transport route, the message is unencrypted on the respective servers.

In theory, it can be intercepted or manipulated by a third party between the servers and end devices.

The Bavarian Agency for Data Protection Supervision (BayLDA) has therefore published the notice that the encryption of emails via TLS alone is not sufficient. Nevertheless, transport encryption should form a central building block of the implemented security measures.

For real end-to-end encryption, companies are advised to make sure they set up content encryption for their digital communication. The message itself is encrypted directly on the sender's device and decrypted only once it reaches the receiver's device. In this way, the highest degree of security for digital information exchange is achieved for everyone involved.



INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

EMAIL ENCRYPTION WITH S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) has been around since 1995. S/MIME enables encryption of various data forms, although emails are likely the most well-known application. It is based, as is PGP (Pretty Good Privacy), on hybrid encryption, which is a combination of symmetric and asymmetric encryption. Although the functional principle of both procedures are comparable, S/MIME and PGP are not compatible with each other. One is therefore forced to either convince all communication partners of your preferred standard or to implement both.

In addition to encryption, S/MIME also offers a signature function. When using it, the message remains accessible for everyone, but a cryptographic signature is added that the receiver can verify. If the signature is verified, it indicates that the content of the email has not been manipulated. Another point in favor of S/MIME is that it is compatible with a wide range of mail clients.

As so-called **client certificates**, S/MIME certificates are issued in personalized form and installed on individual computers. An S/MIME certificate authenticates each individual user that has access to a server during the SSL handshake as a result of the client certificate exchange.

The **public key procedure** (asymmetric encryption) applied for S/MIME uses a key pair (in the case of S/MIME the certificates): a **public** as well as a **private key**. Each key (certificate) is unique worldwide.

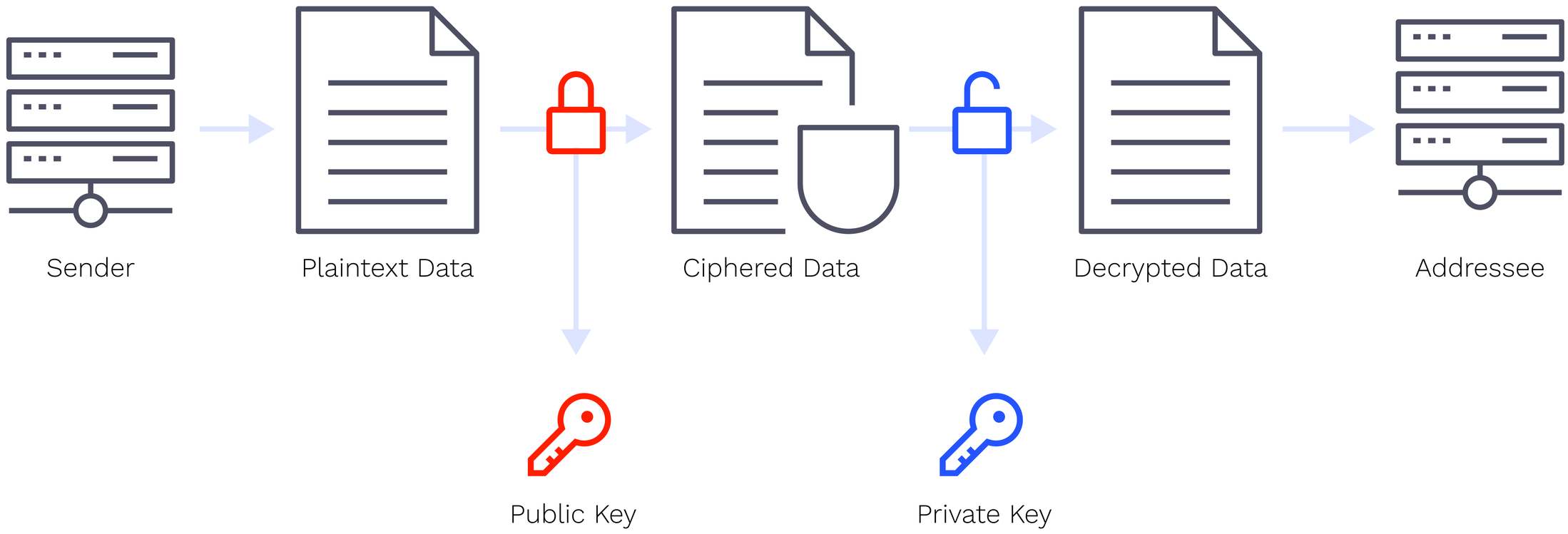
Very important is that the private key cannot be deduced from the public key. The public key serves to code the emails and is offered to the addressee for exchange so that the encryption process can function.

The exchange of the public key per email between sender and addressee is the fundamental requirement for the encryption process.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

THE S/MIME PROCEDURE SPECIFICALLY WORKS LIKE THIS:

- The sender and addressee both use an email certificate and must first exchange their public keys. This is done by sending an email and saving a signed email.
- The sender then uses the public key of the addressee to encrypt his/her email. However, only the private key of the addressee can be used to decrypt the message.
- The email signature using an S/MIME certificate (public key) verifies
  a) that the sender of the email has been validated by an independent authority (CA)
  b) that the email has not been manipulated during transmission.



S/MIME relies on **certificate authorities** (CAs like DigiCert). CAs generally issue certificates in three to four different classes.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

CLASS	DESCRIPTION
Class 1: DV (domain validation)	The certificate authority checks whether the domain and email address exists and also includes this information in the certificate. It is suitable for general use, but not necessarily for business use in conformity with the GDPR.
Class 2: IV (identity validation)	This also includes email validation. Over and above this, applicants also verify their identity by submitting a copy of their identity document (for individuals) or trade register excerpt (for companies). The name of the individual or company and corresponding email address are included in the certificate.
Class 3: OV (organization validation)	In addition to the data in class 2, the CA also verifies whether an individual really belongs to the specified organization. In order to do this, the CA contacts the human resources department using publicly available contact information. The CA also requires proof of the trade register entry.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

The different classes also represent different levels of trust. For a class 3 certificate, greater effort is undertaken to verify the participant. For a class 1 certificate, one can only be assured that the email address exists.

However, secure encryption is achieved with all classes, as they use identical algorithms, and, according to current regulations, GDPR conformity is also ensured.

IS CONTENT ENCRYPTION SUFFICIENT?

Although content encryption makes the message text and any attachment unreadable for third parties, important metadata are not included. The email address of the sender as well as the addressee and the subject line of the message are still accessible.

Real end-to-end encryption of the entire message can only be attained when both content and transport encryption are combined. The sender first encrypts and signs the content of the email with S/MIME. To create a secure communication channel and protect the metadata, transport encryption comes into play with TLS. Once the message is received by the addressee, the message is decrypted and the digital signature is verified. This ensures that the email is authentic, has not been manipulated and remains confidential.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

Best practice: email encryption for companies.

There is no way of avoiding encryption if you want to fulfill legal requirements and protect sensitive data. Protecting confidentiality and maintaining integrity of personal data when sending emails requires senders and addressees to work together and adhere to security standards.

> Article **32 GDPR** mentions possible security measures that should be implemented under consideration of
>
> - the available technology,
> - the cost of implementation,
> - the type, scope, circumstances and reasons for processing
> - the differing probability of occurrence
> - the severity of risk for the rights and freedoms of individuals

The responsibility of each transmission process lies with the sender. However, anyone who specifically receives personal data via email is also obliged to create the appropriate environment for secure reception of email messages with an encrypted channel. And also for storing the information securely.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION



However, the following questions arise:

- Do all emails have to be encrypted?
- Which technical requirements must be established?
- Who can help with the implementation?

TAKING STOCK: WHAT KIND OF DATA DOES MY COMPANY SEND?

The GDPR recommends the encryption of emails. A direct obligation has not been introduced so far. However, if the guidelines are not followed and a data breach ensues, the affected individuals must be informed within 72 hours and can, under circumstances, assert legal claims.

Apart from this, if data ends up in the wrong hands, it can prove to be an economic threat, not to mention loss of trust in the company. If personal data is collected or processed by email, it should certainly be encrypted.

Personal data includes, for example:

- postal address
- phone number
- bank account details
- payment details
- customer number
- IP address

Sensitive data refers to personal information which is particularly sensitive and requires special protection:

- cultural origin
- biometric data
- political, religious and philosophical beliefs
- sexuality and health
- trade union membership

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

WHICH MEASURES DO COMPANIES NEED TO IMPLEMENT?

1 Start with an **audit** and an **analysis** of what requires protection, clarify the central questions: Who sends which data to what addressees and how often? Which standards does the current supporting IT infrastructure fulfill? Do these reduce the risk? And do they fulfill the legal requirements?

2 **Encryption only makes sense when everyone in the team regards it as a sensible measure and uses it correctly. Training and internal guidelines for using emails and coding help the team to implement the security measures in practice.**

3 Data protection specialists agree: Emails that contain information that is **personal or critical to the business** should always be encrypted.

4 **If teams or departments often send sensitive data (internally or externally), they can add additional protection by using passwords that they share via a separate communication channel.**

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

5 Both transport and content encryption on their own potentially leave the door open for data espionage. For the highest possible security, both should be combined and/or **S/MIME** should be considered.

6 If a complete end-to-end encryption cannot be achieved internally, then at least the content and transport channel of messages should be coded from the moment they leave the company's network.

7 If possible, **internal communication should also be encrypted**.

8 Depending on the **setup of data and email infrastructure**, the company should check whether S/MIME is necessary and/or suitable for the content encryption. Are all clients supported? Is the Web of Trust (PGP) sufficient as a basis of trust or would it be better to use a publicly trusted certificate with the highest possible trust level? For most companies considering this question, S/MIME proves to be the most sensible option to offer the highest level of protection and reduce the risks.

9 A **competent partner** can help you select the best certificate for encryption, ideally offering solutions for both content and transport encryption in line with your available budget.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

GETTING IT DONE: WHO CAN HELP ME WITH THE IMPLEMENTATION?

You have decided to set up transport and/or content encryption? This will put you on the safe side legally. The team at InterNetX will advise you on questions regarding TLS/SSL and S/MIME.

With products from leading providers like DigiCert, Thawte and GeoTrust, companies can find the perfect solution to fit their requirements and budget. The domain and TLS/SSL platform AutoDNS offers easy and efficient certificate management.

S/MIME certificates are available in different trust levels to protect personal and sensitive data shared internally in the company or to clients and partners.

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

Conclusion.

Phishing, the loss and misuse of data as well as the legal frameworks mean that email encryption is a must for companies.

Hybrid encryption methods and end-to-end solutions offer the highest possible level of security. These days, there are a number of cost-efficient and user-friendly solutions that companies can implement in order to minimize the risk of data theft in email communication.

Service providers like InterNetX can assist you with competent support and the most suitable products for encrypting your emails in conformance to the GDPR.

Further resources / links.

- Federal Data Protection Act (BDSG): Section 22 Processing of special categories of personal data
- Federal Data Protection Act (BDSG): Section 64 Requirements for the security of data processing
- How does the GDPR affect email?

INTRODUCTION
SECTION 01
SECTION 02
SECTION 03
CONCLUSION

References.

- gdpr-info.eu
- KonTraG - German Law on Control and Transparency in Business (in German)
- Statista Research Department: Prognosis on number of email sent and received daily up to 2024 worldwide (in German)
- Digital Germany 2020 commissioned by WEB.DE and GMX (in German) (Representative study by Convios Consulting GmbH)
- IHK Mittelfranken: FAQ to the BayLDA about implementation of GDPR in practice (in German)

Picture credits.

- Cover image: Joanna Kosinska on Unsplash

About.

With more than 4 million managed domains, InterNetX is one of the leading providers of white-label products for hosting and domains. As experts in website & email encryption and as DigiCert Platinum Elite Certified Partner, the company offers a wide range of high-quality certificates from global market leaders on its all-in-one domain and SSL management platform AutoDNS.

InterNetX GmbH
Johanna-Dachs-Str. 55
93055 Regensburg
Germany
Phone +49 941 59559-0
Fax +49 941 59559-55
email: info@internetx.com
www.internetx.com

Follow us:

Subscribe to our newsletter:
www.internetx.com/internetxpress

Our Premium Platform Partner

digicert®

InterNetX