"How to…" Data Protection: Data protection during email dispatch

MAX PLANCK GESELLSCHAFT

WHAT REQUIREMENTS MUST BE MET WHEN SENDING PERSONAL DATA BY EMAIL?

The requirements for the procedures applicable to sending personal data by email are based on the provisions of Art. 5 (1) (f), 25 and 32 (1) GDPR.

Besides technical measures that must be implemented or provided by the IT service, there are also organizational measures that must be implemented by the responsible processor or the user before sending personal data by email.

In particular, the recommended measures serve to ensure confidentiality and integrity.

TECHNICAL MEASURES

- Use of end-to-end encryption for emails
  - Provision of email certificates for digital signature and encryption via S/MIME, e.g. via the DFN
  - Supplementary alternative for communication with external parties: PGP
- State-of-the-art configuration of the email server
  - Use of transport encryption (SMTPS or STARTTLS)
  - Verification of the authenticity of digital signatures
  - Use/activation of SPF and other methods
- Configuration of the email client to use digital signing of emails by default
- Further information/technical specifications can be found in the "Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" (Working Group "Technische und organisatorische Datenschutzfragen" of the Konferenz der Datenschutzbeauftragten).

ORGANIZATIONAL MEASURES

- Issuing of email certificates for each new user; if applicable, to be included in the on-boarding process
  - Regular reminder for renewal of certificates, if applicable
- Training of users on the practical application of email signatures and encryption (at least in the form of instructions for users)
- Classification of personal data according to the MPG's concept of data protection levels, documentation in the Processing Record, if applicable
- Contractual agreement with external service providers and cooperation partners on the use of email signatures/encryption, if applicable
- Selection of appropriate measures for email security depending on the protection level required and the (technical) possibilities on the recipient's side

Protection level - measures

Protection objective	Measure	Protection level		
		1 – normal	2 – high	3 – very high
Confidentiality	Email encryption			x
	Password protection for attachment file		x	x
	Cryptshare		x	x
	Transport encryption (on the server side)		x	x
Integrity	Email with digital signature	x	x	x
	Attachment file with digital signature		x	x

*https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Daten-per-E-Mail.pdf;jsessionid=A0EBA99FC059EB129105F971CCFB3DF7.2_cid319?__blob=publicationFile&v=1

“How to…” Data Protection: Data protection during email dispatch

MAX PLANCK GESELLSCHAFT

Frequently asked questions and answers

- **Why is it mandatory to encrypt emails with sensitive / confidential content even if they are only sent internally (within the same email server)?**
    - *Confidential data must be encrypted not only when being sent but also while being stored. Within the same infrastructure, unencrypted emails would thus still be available in plain text, which is not sufficient according to the supervisory authorities.*
- **What if an internal or external recipient is not able to use encryption?**
    - *Does the protection level pertaining to the data to be sent require encryption?*
        - *No: Email can be sent unencrypted.*
        - *Yes: Consideration of possible alternatives*
    - *An adequate alternative, especially for sending (multiple) documents, is Cryptshare or encryption of an attachment file with a secure password*
- **I would like to send an email to multiple recipients, what do I need to bear in mind?**
    - *Empfängerkreis und Thema prüfen:*
        - *A defined number of people who all know each other and are working on the same topic/project or who need to know who the recipients of a particular message are.*
            - *Variant 1: All addressees in the To field*
            - *Variant 2: Your own email address in the To field, the addressees in the Cc field*
        - *A larger or perhaps unknown number of recipients who need to be informed about a certain topic and who may not know each other*
            - *Variant 1: Your own email address in the To field, the addressees in the Bcc field*
            - *Variant 2: For periodic information or exchange: Setup of an email distribution list or use of a newsletter tool*

Note on the use of fax services

(from the “Orientierungshilfe der Landesbeauftragten für Datenschutz in Bremen”)*

Whereas some years ago a fax was considered a relatively secure method for the transmission of sensitive personal data, the situation has changed fundamentally: Both the terminals and the transport routes have undergone far-reaching changes. Previously, pure end-to-end telephone lines were used for sending faxes.

These days, technical changes in the telephone networks mean that pure telephone lines are no longer used, but that data is transported in packets through networks running on internet technology.

Furthermore, it is no longer safe to assume that there is an actual fax machine at the receiving end of the fax transmission. In most cases, systems are used that automatically convert incoming faxes into an email and then forward them to specific email inboxes.

Due to these circumstances, a fax has the same level of security with regard to confidentiality as an unencrypted email (which is often compared to the openly visible postcard).

Fax services are not equipped with any security measures to ensure the confidentiality of data. They are therefore not generally suitable for the transmission of personal data.

The use of fax services is not permitted for the transmission of special categories of personal data as defined under Article 9(1) of the General Data Protection Regulation.

Alternative, secure and thus suitable methods, such as end-to-end encrypted email or - if in doubt - conventional mail, must therefore be used for sending personal data.

*https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen_und_handlungshilfen/telefax_ist_nicht_datenschutz_konform-16111