Information on electronic communication procedures with MackSmaTec GmbH

These provisions apply exclusively to electronic communication with MackSmaTec GmbH and do not apply to links or references to third-party offers, over whose content and security standards MackSmaTec GmbH has no influence. The transmission of electronic documents to MackSmaTec GmbH is only permitted under the following conditions:
Please note that legally binding communication can only take place in compliance with these requirements.

1. Access in the sense of this access authorisation refers to the email addresses published on the website and on business documents of MackSmaTec GmbH.
2. MackSmaTec GmbH accepts documents in the following file formats for electronic communication:
   - Portable Document Format (.pdf)
   - Rich Text Format (.rtf)
   - Microsoft Word (.docx)
   - Microsoft Excel (.xlsx)
   - Text formats (.txt)
   - Graphic formats: .jpg / .jpeg / .gif / .bmp / .tiff
   - Compressed, non-self-extracting (!) files (.zip)
   - Other formats are permitted if their transmission has been agreed in advance with the relevant departments and the IT department
3. No automated processes or programming (so-called macros) may be used in any of the permitted formats.
4. The total size of an email, including all attachments, is limited to ten megabytes (MB).
5. In emails with executable files (e.g. *.exe, *.bat), these attachments will be deleted unread.
6. We also ask you not to send MackSmaTec GmbH any electronic messages without prior consultation whose contents must first be accessed or downloaded via a link from an external website. For security reasons, such emails will not be opened or processed.
7. By using electronic communication, you expressly agree that incoming emails will be automatically checked for viruses and spam. Emails identified as containing viruses will be deleted unread and will not be processed further for security reasons. Due to the fact that emails containing computer viruses often contain fake sender addresses, no electronic notification will be sent to the alleged sender in such cases.
8. It is strongly recommended that you run a virus scan with an up-to-date and reliable antivirus programme before sending emails. If such a scan is not performed, it is also advisable to confirm receipt of the email by telephone. It is the sender's responsibility to ensure that the email has been transmitted correctly and received by MackSmaTec GmbH. There is no automatic confirmation of receipt. Please note that the transmission of data via email/the internet is generally considered to be insecure. There is a risk that unauthorised third parties may gain access to or manipulate the transmitted information. It is therefore recommended that particularly sensitive or confidential data be sent exclusively by post or secure electronic means of communication (e.g. encrypted emails).
9. In addition, emails sent in HTML format and containing scripts are automatically rejected for security reasons, as such scripts can trigger unnoticed actions on the receiving system. MackSmaTec GmbH accepts no liability for any delays or loss of data caused by security measures.
10. To avoid unwanted emails (spam), MackSmaTec GmbH uses software to automatically detect and filter such messages. Please note that your emails may be rejected by this checking mechanism if they are identified as spam. No separate notification of such rejection will be given.
11. When entering into electronic communication, MackSmaTec GmbH generally assumes that further correspondence can also be conducted in this manner, unless legal regulations or legitimate interests prevent this.
12. For correspondence that requires the written form under applicable law, no electronic form of transmission is permitted until further notice. Please note that formal delivery requiring legally binding proof of delivery cannot currently be carried out electronically.
13. PGP is used for the transmission of encrypted emails. The key exchange (public key) takes place in advance between the communication partners. Alternatively, Microsoft Office 365 Message Encryption (OME) can also be used.