

Content

1	Introduction.....	2
2	Files and directories	2
2.1	General information on files and directories	2
2.2	Filenames and file formats.....	2
2.3	Directories.....	2
3	Direct creation of PDF files versus Scan and OCR (optical character recognition).....	3
4	Scanning documents	3
4.1	General information on scanning documents	3
4.2	Settings for standard documents	3
4.3	Colour documents.....	3
5	Submission as a zip archive	3
6	Reporting of incidents (Procedures acc. to European Regulations/Directives).....	5
7	Using the mdc secure space (MSS) for upload	5
7.1	Introducing the mdc secure space	5
7.2	System Requirements.....	5
7.3	Transmission of the documentation	6

1 Introduction

Digital documents have replaced paper in various situations. The exchange of digital media promises a significant simplification and acceleration in the daily work. In order to achieve this goal, regulations must be made. This is the only way to ensure efficient processes and data security.

In order to ensure that your documents are submitted securely and reliably within the scope of the certification procedures at mdc, we ask you to comply with the rules described below. Furthermore, we would like to provide you with practical tips to make it easier for you to implement these rules.

We endeavour to interpret the following points in a practical manner in everyday life, but ask you to comply with them. This will help us to avoid delays in the assessment of your documents.

2 Files and directories

2.1 General information on files and directories

As an accredited certification body or notified body, we are also subject to strict requirements. Our activities are based on confidentiality and independence.

In the sensitive field of medical technology, safety for users, patients and third parties is also a top priority. As in hardly any other branch of industry, long-term and sustainable thinking and action are therefore required. This is reflected in particular in the documentation and its archiving.

When working with electronic documents, these aspects sometimes get out of sight. Well thought-out and consistently adhered to technical concepts for handling digital documents are therefore a basic prerequisite for responsible dealing in the sense of the aforementioned premises.

The following principles stand for

- Fault tolerance - ensuring that information is available when conditions change and become more difficult
- Interoperability - Ensuring the availability of documents using different systems or systems that may be used in the very future.
- Security - ensuring readability even after a very long time combined with protection against loss
- Practicability - ensuring quick and easy access to the information contained in the document

2.2 Filenames and file formats

We ask you to provide files in PDF format, full text searchable. For applications under European Regulations and Directives (surveillance only), this is a mandatory requirement for submission. In this context, please also note the considerations outlined below regarding the direct creation of PDF files versus OCR of PDF files.

In certain cases, in addition to searchable PDFs, files in the following formats are also accepted

- Microsoft Word, Excel, Works, Rich-Text, Power-Point as well as plain-Text (doc, docx, xls, xlsx, ppt, pptx, wks, rtf, txt) - but only without macros
- equivalent OpenOffice documents odt, ods, odp
- Images JPG, PNG (please contact your supporting project team in advance, e.g. certificates, diplomas, etc.)

if technically readable. Files in other formats and documents with macros are filtered out by the technical security systems for security reasons.

Choose a maximum length of 50 characters for your file names. The characters < > ? " : | \ / * are generally not allowed and are usually already avoided by your system. In general, however, you should also avoid characters such as ! ' = \$ % & and limit yourself to using Arabic numerals and Latin letters in the Microsoft Windows-1252 character set, which represents the standard in Microsoft Windows systems operated in western Europe. Please refrain from using file-names in the Unicode character set.

For technical reasons, it is also not permitted to choose file names with the single letter sequences (words) CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9.

Files that only have a file name but no content are not permitted and will not be accepted as submissions.

2.3 Directories

Choose directory/folder names with a maximum of 50 characters (path length) for the submission of the requested documentation. A structure consisting of several subdirectories must not exceed 150 characters at any time. The same restrictions on characters and words as for file names also apply.

3 Direct creation of PDF files versus Scan and OCR (optical character recognition)

Generally, we recommend creating the pdf documents directly from the underlying electronic document (e.g. Word file). In some cases, in accordance with your document control, it may make sense to submit an electronically signed version or to attach the scanned signature page to the directly created pdf.

If you have a complete paper based document control, please describe the release of the documents and submit a confirmation that the electronically created documents correspond to the originals in paper form.

If you submit scanned documentation (e.g. manuals, technical documentation, technical drawings, reports etc.), we ask you to perform a text recognition (OCR) so that the documents are searchable for us.

4 Scanning documents

4.1 General information on scanning documents

From the technical point of view, scanning documents is at a disadvantage compared to electronically created documents and is therefore always a compromise solution. If submission as a scanned document is unavoidable, the following rules must be strictly observed.

Please provide scanned documents only as searchable PDF documents with a maximum file size of 0.5 MB per ISO 216 A4 page.

- Ensure sufficient contrast and prefer black and white scans to colour or greyscale scans.
- Only scan in colour if this is necessary for the correct readability of the document.

A slightly higher effort in the choice of scan settings results in significantly smaller, but still assessable files.

For a practical and safe handling of scanned documents it is important to create them in an appropriate size. Select the correct settings for the respective document when scanning. Please also ensure that the page orientation of all document pages is the same and can be read without any further turning.

4.2 Settings for standard documents

Standard documents containing only text or simple sketches and diagrams:

- Scan default colour depth: text / line drawing / line art / black and white.
- Resolution: 300 dpi

4.3 Colour documents

Documents containing text and images that absolutely must be reproduced in colour, as well as individual images, must be scanned in the following quality:

- Scan specification Colour depth: colour
- Resolution: 200 dpi

5 Submission as a zip archive

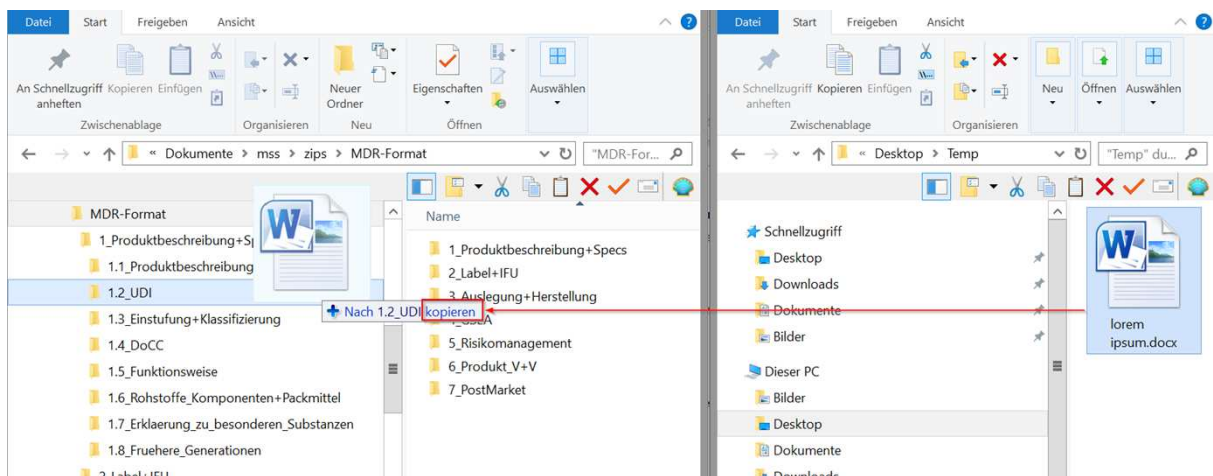
If a submission consists of several files, you have to submit them as a ZIP archive. Zip archives are accepted by mdc in the formats ZIP, ZIP 2.0 and 7zip.

The ZIP archive must not exceed a total size of 2.0 GB per submission. The contents must comply with the specifications as described above.

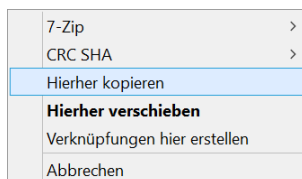
- Copy the documents from your documentation repository into an appropriate directory structure. (Illustration only exemplary for the possible structure of a technical documentation)

- ▼ 1_Description+Specs
 - > 1.01_Dev.Desc
 - 1.02_UDI
 - 1.03_Delineation+Classification
 - 1.04_DoC
 - 1.05_OperatingPrinciples
 - 1.06_SSCP
 - > 1.07_Materials
 - > 1.08_SpecialSubstances
 - > 1.09_Generations
 - 1.10_QM-System_(MDD_only)
 - > 2_Labelling+IFU
 - > 3_Design+manufacturing
 - > 4_GSPR
 - > 5_Risk_management
 - > 6_Product_V+V
 - > 7_PMS

- Please make sure that you don't accidentally move files so that you only submit a copy of your documentations.



- You may use the right mouse button instead of the left mouse button for dragging and clicking. The system will ask for the desired operation.



- After the structure has been completely filled, create a new archive by right-clicking the root directory and selecting 7-zip → Add to ...zip.



5. Use the MSS upload link you received to transfer the file.

For the submission of a technical documentation in procedures according to European Regulations and Directives, please adhere to the specifications of the following additional instructions:


- [Structure of Technical Documentation \(medical devices\)](#)
- [Structure of Technical Documentation \(in-vitro-diagnostics\)](#)


For structured and easy transmission of your technical documentation, please use the structure provided. The template is available for download on our [homepage](#) as a ZIP archive together with a description in English and German language.

6 Reporting of incidents (Procedures acc. to European Regulations/Directives)

When reporting incidents, please use the template 'Manufacturer Incident Report' (MIR). Always make sure to use the latest version of the form. The templates can be downloaded from the [EU website](#); furthermore, the German translation can be obtained from the BfArM under the heading [Report Incidents](#). When submitting the report, please proceed as follows:

- Create an XML from the report, e.g. from the e-mail functionality at the end of the report.
- Rename the XML according to the following scheme:
MIR certificate number your-reference
e.g. 'MIR D1234500001 abc 001.xml'.
- Rename the PDF file of the Manufacturer Incident Report according to the same scheme.
- Always send the two files as pair.

 MIR D1234500001 abc 001.pdf

 MIR D1234500001 abc 001.xml

Send this pair of files to vigilance@mdc-ce.de.

7 Using the mdc secure space (MSS) for upload

7.1 Introducing the mdc secure space

mss - mdc secure space is a tool for the exchange of sensitive data between mdc and you as our customer. The following instruction describes how you can transmit data (e.g. the documentation of a QM system or a technical documentation) to mdc via the system ('upload').

mdc secure space is a modern, secure transmission platform for the exchange of corporate data. The data is stored on secured and encrypted servers, ensuring the highest possible data security and availability. Only mdc employees and experts or auditors commissioned by mdc have access to the data. The data is always transmitted with end-to-end encryption and is therefore encrypted from the moment you start uploading it. The access rights are limited to individual folders and are only granted for the necessary period of time, so that - especially external experts - only have access to the data at the time and to the extent needed.

7.2 System Requirements

To be able to use mss (both with the link or login), an *up to date* browser must be used. Only in this way the encryption of the data can be guaranteed:

- Firefox 49 or higher
- Chrome 41 or higher
- Safari 8 or higher
- Microsoft Edge

7.3 Transmission of the documentation

You will receive an e-mail with a link for secure data transfer (upload link). Please note that the upload link is automatically terminated (and not functional) after the timeline communicated by the mdc project team. If you want to submit additional documents please contact the mdc project team.

We kindly ask you send the requested documentation (e.g. QM manual, technical documentation, etc.) in the form of **one** zip file. Incident reports shall be submitted as described in chapter 'Reporting of Incidents'.

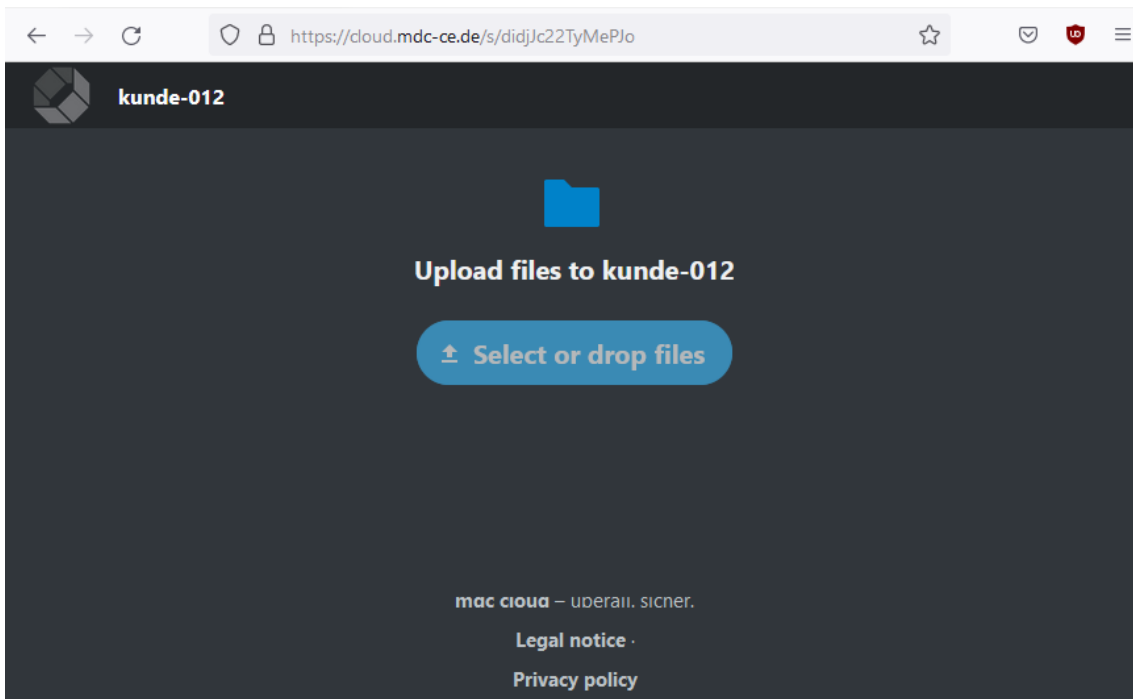
Concerning technical documentation:

A separate ZIP file must be submitted for each technical documentation.

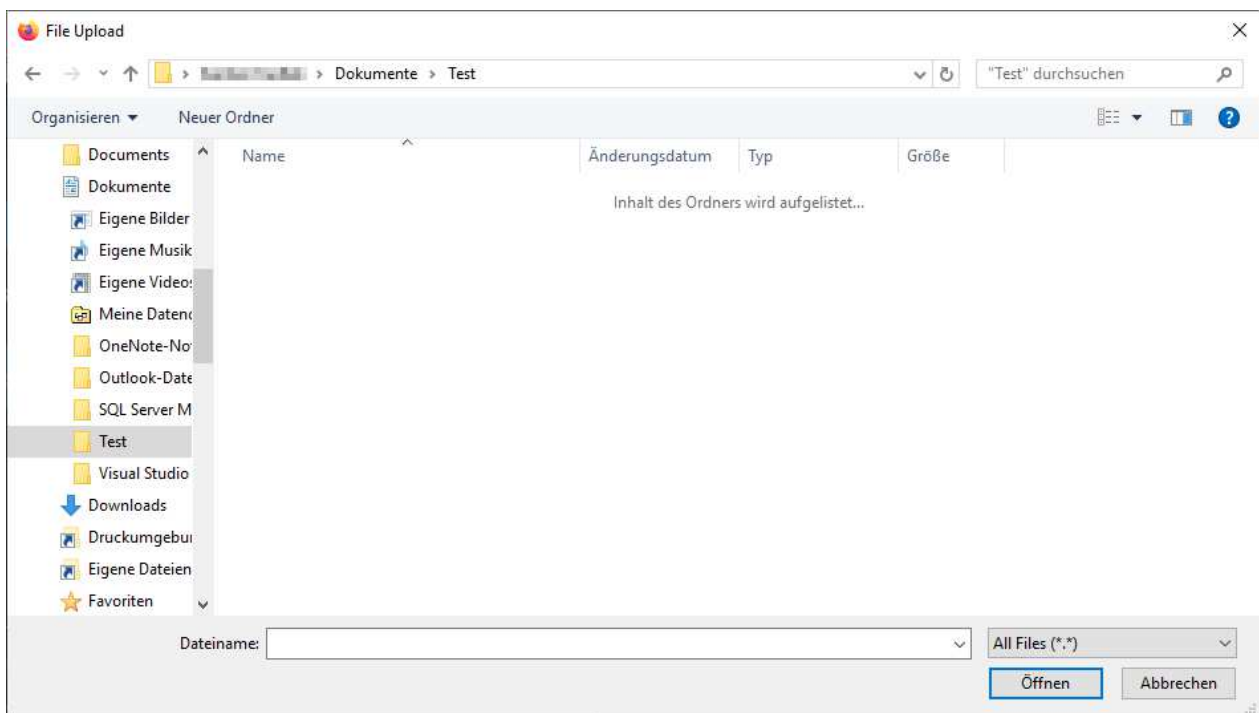
Concerning prequalification documents:

If you use an mss upload for the submission of the PQ documents, we kindly ask you to submit a separate ZIP file for each prequalifying location.

After opening the link, you can either drag the files to be uploaded from a file manager onto the open page or click "Select files....". (Upload files...).



When using the upload button, a file selection window opens for selecting the ZIP file(s). These can be safely transferred to mdc after selecting them and clicking on "Open". You can select several ZIP files at the same time by holding down the CTRL key while clicking.



A list of successfully transferred files is displayed as long as you keep the browser window with the upload link open. This view is reset after closing and reopening it for security reasons.

You can use the upload link several times until the end of the submission deadline and transfer files one after the other. However, please note that related documents, e.g. all documents of each technical documentation, should be transferred as one ZIP file. Please let the project team know as soon as the submission documents have been completely transferred.