

IEM®

Flow

Copyright

Copyright

Flow

Flow software is used to configure and visualize measurements taken with the Mobil-O-Graph® and the HeartX recorder.



IEM GmbH

Gewerbepark Brand 42
52078 Aachen
Germany

Email:

info@iem.de

Internet:

<https://www.iem.de>

The contents of this technical manual must not be duplicated or published without the written authorization of IEM GmbH.

All product and company names mentioned in this document are trademarks or registered trademarks of their respective owners.

The Flow software is protected by copyright and is the property of the manufacturer. All rights are reserved. Flow may not be read out, copied, decompiled, reverse-engineered, disassembled, or converted into a human-readable format. All rights of use and ownership of the software remain with IEM GmbH.

© IEM GmbH 2026 All rights reserved.

Table of Contents

1	Installation of the Software.....	4
1.1	IT Security Requirements.....	4
1.2	System Requirements.....	6
1.3	Install Software.....	6
1.3.1	Notification Icon.....	7
1.3.2	Note on using malware protection.....	7
2	Settings.....	8
2.1	Storage Location.....	8
2.2	Update.....	9
2.3	Cable List.....	9
2.4	Interfaces and Communication Paths.....	9
2.4.1	Setting up the Holter interface.....	12
2.4.2	GDT.....	12
2.4.3	HL7.....	13

1 Installation of the Software

New Installation

Before installing Flow, make sure that all system requirements are met, see [1.2 System Requirements, p. 6](#).

Download the latest version of Flow from the following URL: <https://www.iem.de/flow/download>

To install the software, follow the instructions in chapter [1.3 Install Software, p. 6](#).

Online-Update-Service for the existing installation

Flow regularly checks this service for updates and offers the user the option to upgrade to the latest version if necessary.

1.1 IT Security Requirements

The controls listed below have been incorporated into the cybersecurity risk assessment and form the basis for the secure operation of the software and the protection of the data required by the software. Partial implementation of these controls results in an increased security risk with regard to confidentiality, integrity, and availability.

Encrypted File System

- Use of a storage location that supports strong encryption (e.g., LUKS, BitLocker, VeraCrypt).
- Secure management of encryption keys.
- Access to unencrypted data during operation must be restricted exclusively to authorized processes.

Encrypted Data Communication

- If data is accessed over a network (e.g., network drive, remote access), communication must be secured using current cryptographic protocols (e.g., TLS 1.3, IPsec, SSH).
- Unencrypted (plaintext) transmissions (e.g., via FTP or SMBv1) are strictly prohibited.

TLS Connections and SSL/TLS Inspection

FLOW establishes TLS connections with strict server certificate validation. These connections must not be intercepted, terminated, decrypted, or re-encrypted by any proxy, firewall, SSL/TLS inspection appliance, antivirus solution, or other network security component. This is a mandatory technical requirement for correct FLOW operation. The affected connections and the details are given in the fact sheets in section [2.4 Interfaces and Communication Paths, p. 9](#) under note 2.

Strict Access Restrictions

- Access rights must be regularly reviewed and documented.
- Access may only be granted to individuals with a legitimate need-to-know.

Backup Strategy

The backup strategy reduces the likelihood of data loss and enables the operator to restore resources within the expected timeframe. The backup strategy also includes a security policy (including modern data encryption) as well as an access policy to prevent unauthorized third-party access.

Monitoring & Logging

Monitoring enables the early detection of system malfunctions. Intelligent log file analysis also enables the operator to detect intruders or malware.

Network and Firewall

Firewalls and packet filters prevent harmful network traffic and communication. Intelligent network segmentation increases reliability and availability in case resources are compromised.

Protection Against Malware

Malware protection on servers and desktop computers enhances the security of the infrastructure.

Strict Access Control and Secure Password Policies

Strict Access Control

- Principle of least privilege
- Multi-factor authentication (MFA)
- Role-based access control
- Just-in-time admin / break-glass accounts

Secure Password Policy

- Minimum password lengths
- Use of password managers
- Lockout mechanisms for failed login attempts

Emergency Plan

An emergency plan following the BSI guideline (100-4: Emergency Management) increases the likelihood of restoring the system infrastructure after a security-related incident.

DNS Configuration

The application uses the system-provided settings for name resolution of the online update service. Correct configuration of these settings, as well as verification of the DNS service's authenticity, reduces the risk of malicious attacks. Additional security measures have been implemented to ensure the integrity of the update package.

No Security-Critical Applications on the Computer

The computer system running the application is not intended for safety-critical or business-critical functions.

SBoM and VEX

The Software Bill of Materials (SBoM) is located in the installation directory under the SBOM subfolder. It is provided as a CycloneDX document in JSON format. It is recommended to include the third-party libraries listed in the SBoM into the internal monitoring system.

For each released FLOW version, IEM also publishes the SBoM at <https://www.cd.iem.zone/security/flow/> together with a Vulnerability Exploitability eXchange (VEX) document and a Cosign signature. The VEX document states whether each known CVE is exploitable in FLOW and the justification. See <https://www.cd.iem.zone/security/README.md> for URL conventions, signature verification and information on integrating the data into your monitoring system.

You can reach IEM's security team at security@iem.de.

1.2 System Requirements

Supported Medical Devices

- Mobil-O-Graph® with firmware 200007 (GTIN: 04041346100104) with 4-Pin cable (GTIN: 04041346101934)
- Mobil-O-Graph® with firmware 200212 (GTIN: 04041346100784, 04041346102269) with 4-pin cable (GTIN: 04041346101934)
- Mobil-O-Graph® with firmware 200212 (GTIN: 04041346102269) with USB-C cable
- HeartX Recorder (GTIN: 04250903203176), for AI service
- HeartX Recorder (GTIN: 04250903203398)

Operating System

Please note: Administrator rights are required to install the software.

Microsoft®	Windows 10, Windows 11®
Apple®	macOS 26 (Tahoe)

Minimum System Requirements

Screen Size (diagonal)	14 inches
Screen Resolution (in pixels)	1280 x 720
Hard Disk Space (in GB)	1 GB of permanently available free space (required for the software log files)
Device Interface	USB Type A (for connecting the Mobil-O-Graph®)
Optional	Network adapter with internet connection • For future software updates via the integrated online update service

Operating system-dependent system requirements

	Microsoft Windows® 10, 11	macOS® 15, Sequoia
Main memory (RAM), Minimum	4 GB	8 GB
Processor	x86 Intel Core i5 or equivalent AMD counterpart	x86 Intel Core i5 Apple Silicon

1.3 Install Software

Preparations

- Ensure that the system requirements are met, see [1.2 System Requirements, p. 6](#)
- Download the latest version of Flow from the following URL: <https://www.iem.de/flow/download>

Execution

1. Start the installation file for your operating system:

Microsoft Windows®	macOS®
flow-<version>-windows-amd64.exe	flow-<version>-macos-amd64.dmg (x86 Intel processor) flow-<version>-macos-aarch64.dmg (Apple Silicon processor)

2. Follow the instructions of the Flow setup assistant. At the end of the installation, you have the option to enable autostart for Flow.
3. If the software is already installed on the computer and you start the installation again, the Flow setup assistant will automatically detect the existing installation along with its installation directory. During reinstallation, all data and previously made settings will be retained.

1.3.1 Notification Icon

After successfully installing and launching the software, you will find the notification icon

- on Windows® in the lower right part of the taskbar. If you don't see the icon, you may need to expand the menu using the arrow to view all active applications.
- on macOS® in the upper right part of the menu bar.

Exiting the software via the notification icon

Windows®:

Right-click the software icon to exit the application.

macOS®:

Click the software icon with the primary mouse button to exit the application.

1.3.2 Note on using malware protection

FLOW extracts platform-specific native libraries from its installation packages into a temporary directory on startup. This directory is located at: <user home>/.flow/tmp/. This directory is created only after FLOW is launched for the first time.

The extracted files are signed components of the FLOW application and are required for device communication. They are recreated on each application start if missing.

Some antivirus or endpoint protection software may flag these extracted files as suspicious and quarantine or delete them. When this happens, FLOW may fail to start, crash during startup, or fail to detect connected devices. Log files may contain errors such as "UnsatisfiedLinkError" or "Library not found".

To resolve this, add the directory /.flow/tmp/ to the antivirus exclusion list or whitelist. After applying the exclusion, restart FLOW. The application will re-extract the required files and operate normally.

The exclusion applies only to the specified temporary directory and does not affect the overall security posture of the system.

Installation

The installer unpacks temporary files while installing. If an antivirus or endpoint protection program classifies these as suspicious, the installation may fail or remain incomplete.

In that case, allow the installer to run in your antivirus or endpoint protection program and start the installation again.

2 Settings

You can access the Settings menu by clicking the gear icon  in the upper-left corner of the user interface

2.1 Storage Location

Storage Location for Job List

Select the storage location where the software saves all job data. This setting must be defined when the software is started for the first time and can be changed later. Ensure that the software has read and write permissions for the selected folder.

Storage Location for Reports

Select the storage location where the software saves all reports. This setting must be defined when the software is started for the first time and can be changed later. Ensure that the software has read and write permissions for the selected folder.

If no report path has been selected, the reports can only be viewed in FLOW.

Note

Separate Storage Locations

The storage location for the job list and reports must not be the same folder used for the job list; likewise, no subfolders of that folder may be used.

Note

Multi room

The “Multi room” function allows multiple software instances to access the same job data.

Select a storage location for which all software instances have read and write access.

For the shared storage location in Multi room operation, a directly accessible network drive on the local network is recommended. Cloud storage with a synchronization client (e.g., Microsoft OneDrive, Google Drive, Dropbox, Nextcloud, Infomaniak kDrive) is not suitable for this purpose and is not supported, as synchronization delays, increased latency or inconsistent data states can result in delayed display or incorrect behavior. This applies regardless of whether the files are kept locally or downloaded on access.

A NAS is suitable when mounted as a network drive via an SMB share, but not through its synchronization client (e.g., Synology Drive).

Note

Network Connection Requirements

FLOW requires fast access to the storage location for the job list. All workstations access this storage location continuously. Delays of several seconds when accessing the storage location are not suitable for operating FLOW.

Use a network drive on the local, wired network. If noticeable delays occur, have your IT service provider check the network connection before you continue using FLOW.

2.2 Update

A prerequisite for using the Online Update Service is an internet connection and administrator rights for installation.

The software includes an integrated Online Update Service. FLOW regularly checks this service to determine whether a new program version is available. As soon as an update is available, the software downloads it and notifies the user that a new version can be installed. The user can start the update at any time.

During the update, the software closes and restarts automatically after the update is completed.

Data and settings are transferred to the new program version during the update.

Note

Security-critical updates

Critical updates fix security-related issues. They must be installed to ensure that FLOW continues to function properly.

2.3 Cable List

The software prompts users to register all 4-pin cables used with this software or to specify that they are not used with this software.

This prevents unwanted interactions with other devices and cables connected to the computer.

The "Cable List" feature allows you to delete all stored information about 4-pin cables. This function should be used if a 4-pin cable has been incorrectly categorized.

2.4 Interfaces and Communication Paths

General

Microsoft Azure / Online update	
Target-ID	A2916
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	cd.iem.zone/flow
Transferred data	Version check every 6 hours, download of the installer package
Security measures	TLS 1.2+
Notes for operator	1, 2

sentry.io, EU region	
Target-ID	A4941
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	o4510141214621696.ingest.de.sentry.io/

sentry.io, EU region	
Transferred data	Error messages with stack trace, preceding log lines, installation ID, application version, operating system, locale, IP address
Security measures	TLS 1.2+
Notes for operator	1, 2

IEM Website	
Target-ID	A3589
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	iem.de
Transferred data	FLOW Application, Release Notes, Device firmware, Data protection regulations
Security measures	TLS 1.2+
Notes for operator	1, 3

ABPM

IEM Mobil-O-Graph	
Target-ID	A2926
Direction	Locale I/O
Protocol / Port	USB / UART
Endpoint / Description	External recorder device
Transferred data	To the device when preparing: job reference (job ID). No patient names, no patient ID.
Security measures	-
Notes for operator	4

Holter

IEM HeartX Holter	
Target-ID	A4585
Direction	Locale I/O
Protocol / Port	USB
Endpoint / Description	External recorder device
Transferred data	To the device when preparing: job reference (job ID), date of birth rounded to the month, sex, pacemaker flag, recording duration. No patient names, no patient ID.
Security measures	-
Notes for operator	4

Azure Storage / Holter measurement upload	
Target-ID	A5078
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	gtmhxhcustomers05.blob.core.windows.net
Transferred data	ECG signal, job reference (job ID), date of birth rounded to the month, sex, pacemaker flag; plus the recorder log file. No patient names, no patient ID.
Security measures	TLS 1.2+
Notes for operator	1, 2

ECG AI backend	
Target-ID	A4588
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	hxxh-api.prod.heartxholter.com
Security measures	TLS 1.2+
Notes for operator	1, 2

Webviewer	
Target-ID	A5072
Direction	outgoing
Protocol / Port	HTTPS / TCP 443
Endpoint / Description	heartxholter.com
Security measures	TLS 1.2+
Notes for operator	1, 3

1. Internet connection with port 443 required.
2. Connection is established by FLOW itself. Any MITM-style TLS interception that substitutes the original server certificate will cause FLOW to reject the connection. The resulting error is typically a Java PKIX certificate path validation failure. In the FLOW error message and in the log file it reads, for example, "PKIX path building failed". These connections must be explicitly excluded from SSL/TLS inspection and passed through unchanged, preserving the original end-to-end TLS session and certificate chain. FLOW validates server certificates against the certificate list shipped with the application, not against the operating system's certificate store; custom certificates, such as a proxy CA, cannot be added. FLOW has no proxy setting; the targets marked this way must be reachable from the workstation directly or through a transparent proxy without TLS decryption.
3. Opened in the workstation's system browser. The browser's certificate validation and proxy settings apply; no exemption from SSL/TLS inspection is required.
4. Secure physical USB port.

2.4.1 Setting up the Holter interface

Precondition: HeartX Recorder (GTIN: 04250903203176) and account for Webviewer

To set up the interface to the AI evaluation service for the HeartX Recorder, proceed as follows:

- Log in to Webviewer with your account.
- Open the settings (gear icon).
- Click on the "IEM Integration"
- Create a token by clicking on Create Token. A .token file will be downloaded automatically.
- Save the file in the HeartX settings.

2.4.2 GDT

FLOW allows operators to configure a data interface to a practice management system (PVS) or hospital information system (HIS) using the GDT 2.1 standard (device data transfer).

For FLOW to accept and process a job from the desired system, the following codes must be included in the file sent to FLOW:

- 3000 – Patient identifier
- 8000 – Expected value "6302"
- 8402 – Expected value:
 - for ABPM "BDM01"
 - for Holter "EKG04"

Character Set

The configured character set must match the one the PVS/HIS uses when writing the GDT file. If the file contains code 9206 (character set), FLOW follows it. If the code is missing or does not match any of the values in the table below, the character set configured in the settings is used.

Code 9206	Setting	Character set
1	ASCII	7-bit ASCII – contains no umlauts
2	IBM437	DOS character set
3	ISO-8859-1	Latin-1, common in Windows environments

An incorrect setting has different effects:

- With "ASCII", all umlauts and special characters are replaced with "?", because this character set does not contain them – "Schröder" becomes "Schr?der". Only select ASCII if your PVS/HIS actually writes the files that way.
- If "IBM437" and "ISO-8859-1" are confused, no "?" appears. Umlauts are displayed as wrong characters instead – "Schröder" then becomes e.g. "Schr÷der".

If characters are displayed incorrectly in the report or "?" appears, take the character set to be used from the manual of your PVS/HIS.

The GDT specification defines only the file structure and semantics; it does not include security mechanisms such as encryption, authentication, or integrity protection. Data exchange is performed through shared directories ("GDT exchange folders"). The operation and protection of these directories is the responsibility of the operator (e.g., the medical practice or IT service provider). The application strictly supports data exchange within the GDT specification. End-to-end security mechanisms (such as encryption or digital signatures) are not part of the standard and therefore not implemented.

To ensure secure and compliant operation, the operator must implement the following measures:

- Implement access control measures. Only authorized entities may access the HIS-GDT interface.
- Ensure the integrity and confidentiality of GDT file transfers.
- Protect information at rest through encryption and technical safeguards.
- Maintain logging and monitoring of GDT exchanges for accountability.
- Provide adequate backup and recovery mechanisms to guarantee availability of exchanged GDT files.

Notes on configuring the PVS

After processing or importing the GDT file, the HIS/PVS must delete the GDT file and any reports imported along with it.

Important: Deleting further files present in that directory can lead to data loss and malfunctions.

Note

Multi room

The “Multi room” function allows multiple software instances to access the same job data.

Ensure that the following settings match across all instances that are to be connected via Multi room:

- GDT mode enabled
 - Character set encoding
 - Import and export directories
The same directories must be configured that are also used as exchange folders for the PVS/HIS at the respective workstation.
-

2.4.3 HL7

FLOW allows operators to configure a data interface to a practice management system (PVS) or hospital information system (HIS) based on HL7 v2. The exchange is file-based: the sending system places orders as message files in an import directory, and FLOW writes the result message of a completed order into an export directory. A network connection (e.g. MLLP) is not part of this version.

GDT and HL7 can be switched on at the same time. An order is always exported through the interface it came in through.

Settings

The HL7 page under **Interfaces** contains the following controls. All other values of the interface are predefined and cannot be configured through the user interface; they are listed in the next section.

Setting	Meaning
HL7 mode	Switches the interface on and off. Existing jobs keep the mode they were created with until they are completed.
Import Directory	Directory the sending system writes orders into
Export Directory	Directory FLOW writes result messages into
Quarantine Directory	Directory in which FLOW preserves messages it cannot process
Document Directory	Directory FLOW copies the report PDF into – only in the “File Reference” document mode

Setting	Meaning
Document Mode	“Embedded”: the report is embedded in the message. “File Reference”: the message carries only the path to the PDF file.

With HL7 mode switched on, the import, export, and quarantine directories must be set; in the “File Reference” document mode the document directory is required as well. FLOW needs read and write permissions for all directories.

The “File Reference” document mode requires sender and receiver to see the same file system. Choose a separate directory as the document directory, not the export directory: the receiving system collects the messages from the export directory and may treat other files there as foreign files that it moves or deletes. A PDF file in the export directory could thus disappear before the receiving system opens the path given in the message.

Note

Separate directories

The four directories must not overlap with each other or with the GDT exchange folders.

FLOW processes **every** regular file that appears in the import directory and deletes it after successful processing. Do not place any other files there.

Predefined values

The following values are fixed and cannot be changed in the user interface.

Parameter	Value
Channel	File drop
Accepted message type (inbound)	ORM^O01
Supported HL7 versions (inbound)	2.3, 2.3.1, 2.4, 2.5, 2.5.1
Message type (outbound)	ORU^R01
Encoding	ER7 (pipe-delimited)
Character set (inbound)	From MSH-18, UTF-8 as the fallback
Character set (outbound)	UTF-8, declared in MSH-18 as UNICODE UTF-8
HL7 version (outbound)	The version of the order being answered, 2.4 as the fallback
Sending application / facility	MSH-3 = FLOW, MSH-4 = IEM
Receiving application / facility	MSH-5 and MSH-6 from MSH-3 and MSH-4 of the incoming order, HIS and HOSPITAL as the fallback
Examination codes ABPM (OBR-4)	ABPM, 24h-RR, 24h Blutdruckmessung
Examination codes Holter (OBR-4)	HOLTER, LZ-EKG, 24h Langzeit-EKG
Strict validation	Off
File name (outbound)	The message control ID MSH-10 with the extension .hl7

The receiving application is therefore not a fixed value: FLOW answers the application that sent the order. The fallback values are used only when the incoming order says nothing.

Requirements for an incoming order

For FLOW to accept and process an order, the message must meet the following conditions. If one of them is violated, the message is refused and moved to the quarantine directory.

- The message type in MSH-9 is ORM^O01.
- The HL7 version stated in MSH-12 is one of the supported versions.
- The message carries exactly one order. Messages with more than one order are refused.
- The order control code in ORC-1 is NW (new order). Cancellations (CA) and changes (XO) are refused.
- The placer order number in ORC-2 or OBR-2 is present. The result message echoes it back; without it, the receiving system cannot match the result to its order.
- The examination code in OBR-4 matches one of the codes listed above. FLOW compares the code and the display text, ignoring upper and lower case.

FLOW reads the following fields from the message:

Field	Source
Patient identifier	PID-2, PID-3 as the fallback
Last name, first name	PID-5.1, PID-5.2
Date of birth	PID-7
Sex	PID-8
Examination	OBR-4 (code and display text)
Appointment	OBR-36, TQ1-7 as the fallback
Order number	ORC-2, OBR-2 as the fallback
Case number	PV1-19
Requesting physician	ORC-12.2, OBR-16.2 as the fallback
Sender	MSH-3, MSH-4

FLOW writes the appointment into the job's **Scheduled for** field when it creates the job. Where the message names no appointment, the field stays empty and can be set in FLOW. OBR-6 (requested date) and ORC-15 (order effective date) are not read as the appointment: neither states an agreed time, and many senders fill ORC-15 with the moment the order was entered.

A timestamp may state its UTC offset (20260728093000+0200). Without one, FLOW reads the value as local time on the machine it runs on.

Character set

The character set of an incoming order follows the MSH-18 field. That field carries the identifiers of HL7 table 0211, not the common names of the character sets. FLOW supports the values ASCII, 8859/1, 8859/15, UNICODE, and UNICODE UTF-8.

- If MSH-18 is empty, FLOW uses UTF-8.
- If MSH-18 names a character set FLOW does not know, the message is refused and moved to quarantine. A substitute character set would corrupt umlauts and special characters without anyone noticing. This includes UTF-8: the identifier for UTF-8 is UNICODE UTF-8.

FLOW writes the result message in UTF-8 and declares this in MSH-18 as UNICODE UTF-8.

Strict validation

Strict validation against the HL7 specification is switched off. Instead, FLOW checks the specific fields it needs for the order – see “Requirements for an incoming order”.

The result message

Once a job is completed and a report exists, FLOW writes an ORU^R01 message into the export directory. It carries the order number from the original order (OBR-2), the patient data, the case number (PV1-19), and the report:

- In the “Embedded” document mode, the PDF is base64-encoded in OBX-5.
- In the “File Reference” document mode, FLOW copies the PDF into the document directory, and OBX-5 contains only the path to it.

Every message receives its own control ID (MSH-10) and is filed under that name with the extension .hl7. FLOW writes the file with a .tmp extension first and renames it afterwards, so the receiver never sees a half-written message. No acknowledgement (ACK) is expected.

If FLOW cannot write the message – because the export directory is unreachable, for instance – the job stays queued for transmission and is retried every 20 seconds. If it has been waiting for more than five minutes, FLOW reports it in the job list as a failed transmission.

If a job is exported again, another file with its own control ID is created. A message written earlier is not overwritten.

Quarantine

Messages FLOW cannot process are not deleted but moved to the quarantine directory. This keeps the interface open for the orders that follow, and no order disappears unnoticed. FLOW records the reason in the application log.

FLOW never cleans up the quarantine directory by itself. Review it regularly, and have orders that were refused because of a misconfiguration sent again by the sending system once it has been fixed.

Security and operator responsibilities

The HL7 v2 specification defines only the structure and semantics of the messages; it does not include security mechanisms such as encryption, authentication, or integrity protection. Data exchange is performed through shared directories (import, export, quarantine, and document directory). The operation and protection of these directories is the responsibility of the operator (e.g., the medical practice or IT service provider). The application strictly supports data exchange within the HL7 v2 specification. End-to-end security mechanisms (such as encryption or digital signatures) are not part of the standard and therefore not implemented.

To ensure secure and compliant operation, the operator must implement the following measures:

- Implement access control measures. Only authorized entities may access the HL7 interface and the directories used for it.
- Ensure the integrity and confidentiality of the transferred HL7 messages.
- Protect information at rest through encryption and technical safeguards. This also applies to the quarantine directory and – in the “File Reference” document mode – to the document directory: both contain patient data or complete reports.
- Maintain logging and monitoring of HL7 exchanges for accountability.
- Provide adequate backup and recovery mechanisms to guarantee availability of the exchanged messages.
- Review the quarantine directory regularly and empty it in a controlled manner. FLOW preserves every message it could not process there and never deletes any of them by itself.
- Set up directories used exclusively by the HL7 interface. FLOW processes every regular file that appears in the import directory; the four directories must therefore not overlap with each other or with the GDT exchange folders.

Notes on configuring the receiving system

After processing or importing the result message, the receiving system must delete it from the export directory. FLOW deletes nothing there.

In the “File Reference” document mode this applies to the reports in the document directory as well. The receiving system has to collect the PDF file through the path given in OBX-5 while it is still there.

The sending system should write orders into the import directory atomically, that is, create them under a temporary name and rename them afterwards. FLOW skips files with the extensions .tmp and .part; an incomplete file under its final name, however, ends up in quarantine.