Guideline for EMVO and NMVO stakeholders: recommendations for alert handling and prevention process

January 2019

The following document has been developed by experts representing the main stakeholder associations member of EMVO (research-based manufacturers, generic manufacturers, parallel distributors, full-line wholesalers, community pharmacists and hospital pharmacists) as well as technical experts from EMVO and NMVOs. The draft recommendations listed below are still being discussed and refined by the stakeholders and technical experts.

As the medicines verification system is not, today, systematically used by all supply chain actors the recommendations below have been developed with a theoretical and normative view of how alerts should be prevented and managed. However, at this point in time, stakeholders recognize that real-world situations might require a pragmatic approach in managing alerts to avoid disruptions in forwards logistics.

The following guidelines reflect the best effort and thinking of stakeholder experts with the information available to them, on 4 February 2019.

Above and beyond their best efforts to comply with the requirements, all supply chain stakeholders maintain the goal to ensure access to safe medicines for patients in Europe. They are expressing, once again, their willingness to work closely together with national authorities to receive guidance and insights, on a case by case basis, on how to overcome the initial 'growing pains' of using the new system. It is their utmost desire to ensure availability of medicines to patients while working together to prevent the entry of falsified medicines in the supply chain

© EMVO 2019

Uncontrolled when printed

Contents

I. Scope

The purpose of this document is to provide guidance for stakeholders of the European and National Medicines Verification Organisations including EMVO and NMVOs, to enable a harmonized approach on managing all level 5 alerts, as set out in article 36(b) and 37(b) of Commission Delegated Regulation (EU) 2016/161 of the 2 October 2015 and related Q&A version 12, topic 7.17.[1] These recommendations aim to ensure a closing of the loop between a suspect falsified pack and reporting the incident to the relevant authorities.

The objective is to define the touchpoints with existing alert processes, where possible. If new processes are required, these should be aligned and standardized to build transparent and effective practices.

Note:

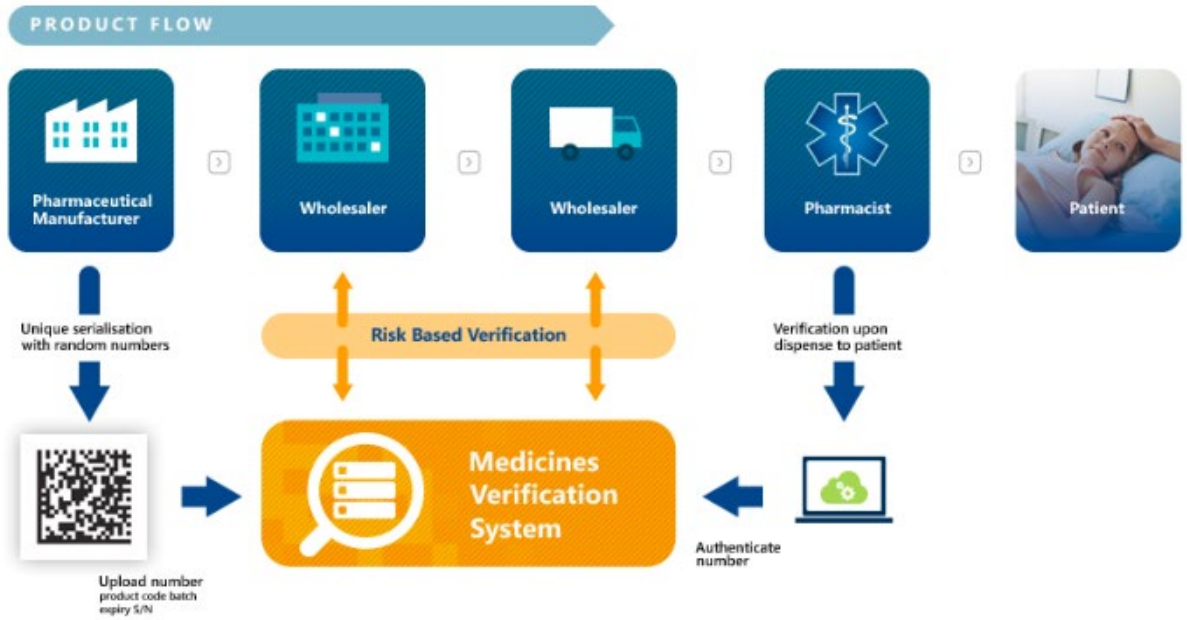
A Level 5 alert is generated when the NMVS detects a potential suspect falsified pack within the European Medicines Verification System (EMVS), which are escalated to end-users as well as NMVO's, National Competent Authorities (NCAs) and OBP / MAHs.

[1] European Commission Directorate-General for Health and Food Safety: Health systems and products: Medical products – quality, safety and innovation. Safety Features for Medicinal Products for Human Use, Questions and Answers, version 13, January 2019

© EMVO 2019

II. Introduction

In preparation of the Delegated Regulation implementation by Feb 9th, 2019 and in the interest of guaranteeing the continuity of supply of medicines, it is important to define and harmonize where possible the Alert Handling process of 'Level 5 alerts', amongst the involved stakeholders.



Source 1:https://emvo-medicines.eu/mission/emvs/

Clarification of concepts used in the paper:

On-boarding Partner

The concept of On-boarding Partner (OBP) has been defined in order to facilitate the on-boarding process for pharmaceutical corporations to the EMVO (legal onboarding) and the EU Hub (technical onboarding and connection). The OBP represents/groups the companies holding marketing authorizations and/or parallel import authorizations/parallel distribution notices among its corporation (same economic undertaking).

From a legal perspective, each Marketing Authorization Holder (MAH), or parallel distributor, is ultimately responsible for complying with the requirements set out in the Delegated Regulation. However, an MAH may choose to delegate certain tasks to the OBP. For the purposes of this document, it is understood that MAHs delegate to their respective OBP the task of connecting to the EU Hub and uploading serialization data. The same delegation applies to the task of handling alerts. Typically, this delegation is done in writing. It is up to each respective OBP to ensure that proper documentation and processes are put in place amongst its MAHs to ensure that these tasks are dutifully carried and that ultimate responsibility rests with the respective MAHs.

3PL (3rd Party Logistics provider)

© EMVO 2019

A 3PL represents a (typically independent) logistics company which provides the outsourced activity of distribution, warehousing, and fulfillment services on behalf of a Marketing Authorization Holder.

A Marketing Authorization Holder can delegate the task of distribution, warehousing, and fulfillment of its products to a 3PL while retaining final responsibility for these activities. A 3PL will always operate under specific contact and quality standards as imposed by the MAH. A 3PL holds a wholesale distribution license, however, as opposed to a traditional full-line wholesaler, will not own the products as it will be distributing them merely 'on behalf of the MAH'.

From a system perspective 3PLs may connect via 2 options:

- Directly to the National Medicines Verification System – using their wholesale distribution license they can request and obtain a direct connection in order to verify/decommission products
- Use the connection/system credentials of his contracting OBP – under specific contract/quality agreement, an OBP may choose to extend the outreach of its Hub connection and integrate it with the 3PL IT system so that the 3PL may verify/decommission products via the Hub, under the credentials of the OBP. In this instance, responsibility remains solely with the OBP.

No matter the circumstances, no 3PL (nor any purely wholesale distribution authorization holder) can connect to the EU Hub directly, nor can a 3PL upload any data into the system. Both connections mentioned above are available only for verification/decommissioning activities.

Investigative roles of NMVOs and MAHs

The Commission Delegated Regulation foresees that the National Medicines Verification Organisations (NMVOs) 'should provide for the immediate investigation of all potential incidents of falsification' (Art 37 (d)). At the same time, European Commission Q&A document version 13, explains, in question 7.17 that NMVOs may 'fulfil this obligation either directly or by ensuring the task is performed by someone else'. Moreover, the Q&A document refers to the fact that 'NMVOs should ensure authorities are informed as soon as it is clear that the alert…cannot be explained by technical issues…'. In order to rule out such root causes, an interaction between the actors involved (end-user, NMVO and OBP) is necessary.

While national level flexibility is possible to provide for more precise agreements between the NMVOs and the NCAs, the following guidelines assume that NMVOs have discharged of their Art 37 (d) obligations by implementing a system design, based on the EMVO URS, which automatically (and instantly) escalates/communicates level 5 alerts to the NMVO, relevant OBP as well as the NCA.

We assume that Art 38 (b) provides sufficient grounds for NMVOs to access the data in the system for the purpose of investigating potential incidence of falsification.

As such, the following document aims to provide guidelines for how the supply chain stakeholders may interact/communicate in order to 'close the loop' and identify the root cause of the alerts such communicated (via the IT systems connection).

Sytem security:

© EMVO 2019

The EMVS was designed from the outset to be a secure system. Security not only in terms of protection from external malicious access but also in terms of data partitioning to ensure that data access is limited to only those with a 'right'. Data ownership requirements and data access restrictions within the system were fundamental design constraints. To further enhance system security, many data items held within the system are encrypted.

The system has been designed with security and data integrity as fundamental principles, and, as such, there is not a 'data warehouse' capability implemented. This prevents free-form data mining and protects both stakeholder interest as well as individual client data integrity. With the sole exception of data required to perform medicine verification operations, data can only be accessed by means of pre- defined reports and each report type is further restricted by user permissions.

To this end, free and unfettered access to any aspect of stored data within the system is, by design, simply not possible and these design decisions help make the system data secure.

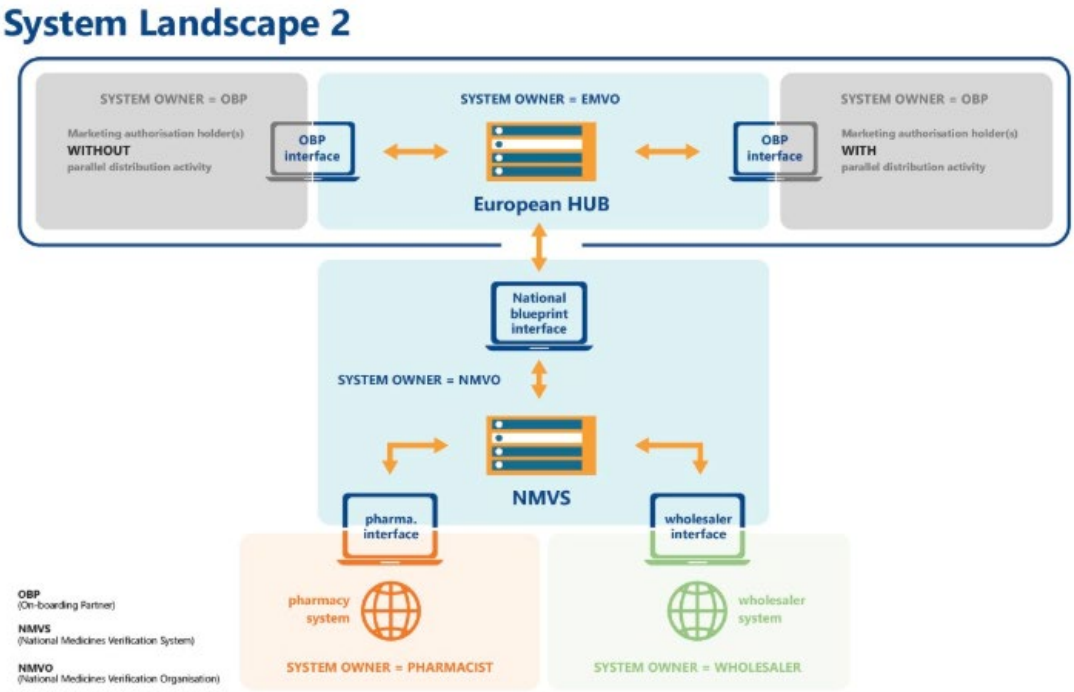
Pack Disclosure Report:

One such report is the Pack Disclosure Report which allows the entire visibility of the transactions related to a specific pack from initial upload to last scan. It is to be provided in the event of a suspect pack but only when the unique ID generated at the point where the scan raising the alert occurs. Recognising the need to investigate the alerts, stakeholders have commonly agreed to include such a Report in the system specifications. It is understood that an alert is a public safety issue which supersedes the Article 38 and stakeholders have commonly understood their joint responsibility (and ability) to investigate alerts.

In practical terms this means that a Pack Disclosure Report is created only when an alert is generated (and an alert ID is created). All mentions provided in this document to stakeholder interactions to manage alerts should be understood in this paradigm: 1 product - 1 alert - 1 alert ID - 1 Pack Disclosure Report.

© EMVO 2019
Uncontrolled when printed

The generation (and sharing) of a Pack Disclosure Report does not allow the posiblity for any supply chain actor to access any other data generated by any other supply chain actor regarding any other product.



Source 2https://emvo-medicines.eu/mission/emvs/

The intent of the requirements for reporting of falsified medicines set out in the Falsified Medicines Directive is to protect patient safety. Therefore, it is in the interest of all stakeholders involved that any reporting system in the EU territory is pragmatic, effective, efficient and focused on the EU market and risk based to avoid overloading authorities with false signals and implemented in a harmonised manner across Europe.[2]

This guideline is based on defined recommendations by a broad representation of stakeholders across the supply chain.

Procedures

During the starting phase many level 5 alerts will not be due to falsified products but might be triggered by procedural or technical errors. It is therefore important to minimize these kinds of errors so that the availability of medicines to patients is not impacted.

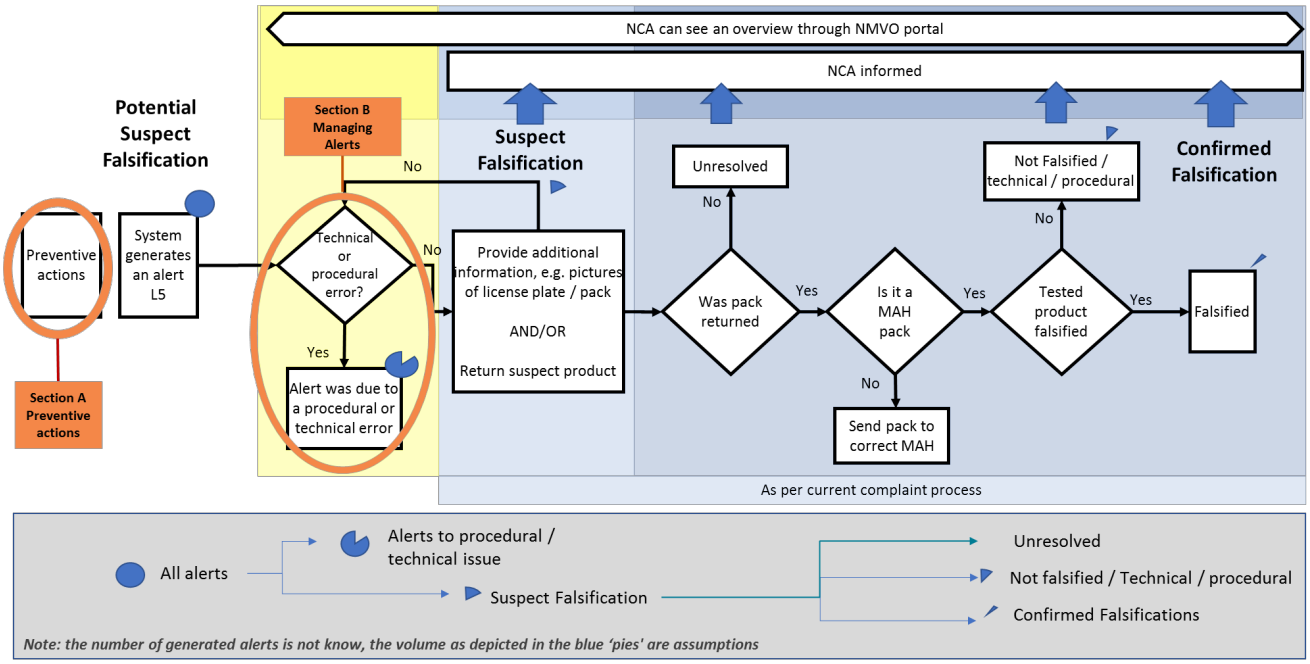
Therefore, this document encourages a joint effort from EMVO stakeholders in the implementation of preventive actions, to avoid/minimize system alerts caused due to a procedural or technical issue,

[2] EFPIA Position Paper for EU Reporting Requirements concerning Falsified Medical Products, 25/10/2016

© EMVO 2019

which will interrupt the process of dispensing a pack to a patient at a pharmacy level with non-value added to protecting patient safety. The EU Delegated Act regulation requires investigation efforts to focus on "potential and/or confirmed falsified medicines" that reach the legal supply chain putting patient safety at risk.

Figure 1 Alert Handling process



As such, implementation of preventive actions is encouraged to all stakeholders to avoid distraction from managing 'level 5 alerts' of "potential and/or confirmed falsified medicines" which are the real threat to patient safety.

Clarification on process steps and reporting requirements:

	Process steps	**Reporting requirements**
Potential Suspect Falsification	• Distinguish alerts generated by technical and / or procedural issues • Communication between end-user, NMVO and OBP / MAH	• No report to NCA, as all alerts are visible in the NMVS
Suspect Falsification	• End-user will provide additional information on pack • End-user will return pack to MAH or act according to the returns process specified on national level	• "**regular reporting**" for non-confirmed falsified medicines to NCA, as all alerts are visible in the NMVS

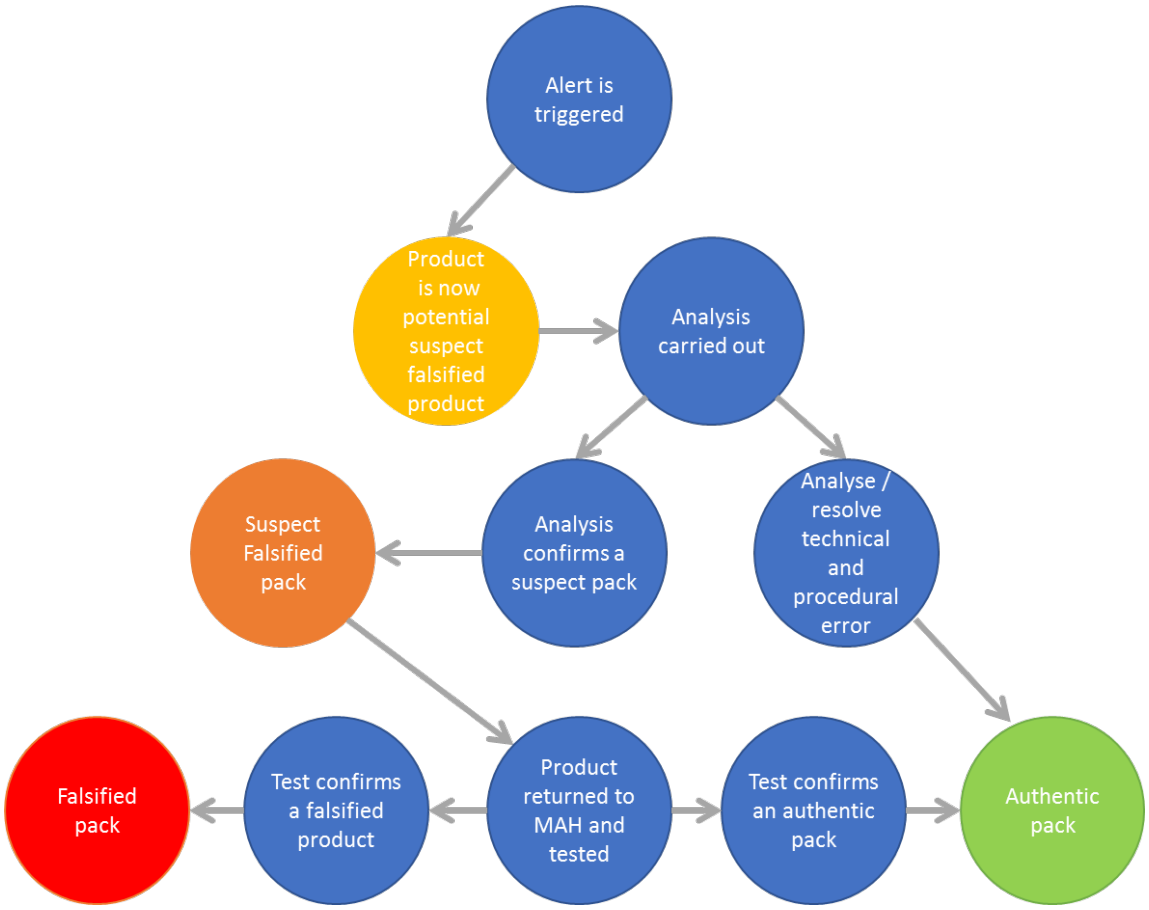
© EMVO 2019

Confirmed Falsification	• Continue analysis by MAH following existing complaint process	• "**immediate reporting**" for confirmed falsified medicines (understanding time is needed for confirmation) to NCA (EMA and EC) by MAH as soon as falsification has been confirmed.

Reporting requirements by individual stakeholders

The system aims to streamline the reporting of alerts by all individual stakeholders. The IT system connection of all stakeholders to the NMVO and its connection to the IT system of the National Competent Authorities provides for this facility. However, these guidelines do not prevent nor do they absolve each individual stakeholder from their reporting requirements as outlined in Articles 18, 24 and 30 of the Delegated Regulation. It should be noted that the system can only channel alerts generated by the information (or lack thereof) contained in the Unique Identifier. Verification of the integrity of the Anti-Tampering Device remains the responsibility of each stakeholder in the supply chain.

As the system becomes systematically used by all stakeholder (including the National Competent Authorities) national level discussions may be undertaken to see how these 2 lines of reporting: via the system IT connection, and via each individual stakeholder reporting may be streamline, adjusted, perfected etc.



© EMVO 2019

According to the EMVO URS - '0017_EMVS Req Spec Part IV Exceptions - Exception Handling – Alerts', different exception types have been described causing a level 5 exception with raising a unique alert identifier.

By understanding the root cause of each of these scenarios, the associated exception types can be grouped into two basic scenarios:

1. **Scenario: Data error**

Scenario type	Scenario description	Root causes
Pack (UI) unknown	End-user receives an alert when the scanned or manual entered identifiers do not match with the information available in the NMVS.	1) OBP did not upload (correct) pack data
Mismatch batch and/or expiry date		2) End-user has typed the wrong data
		3) Suspect falsification

Scenario: Pack (UI) status error

Scenario type	Scenario description	Root causes
Pack (UI) status error	End-user receives an alert related to the scanned or manually entered identifiers already been given a decommissioned status in the NMVS.	1) Multiple decommissioning attempts (above predefined threshold) [3]
		2) Pack on hand is already dispensed at same location for other reason
		3) The pack on hand is already dispensed at other location for same or different reason
		4) Suspect falsification

Product code unkown – one additional scenario, which is not covered by this document, is 'product code unknown' which means the system has no information regarding the existence of this code (i.e. there is no master data uploaded in the system which corresponds to this code). A number of root causes for this alert can be identified:

- 'Indian pack' – packs manufactured in India (prior to 9 February 2019) and serialized according to the Indian Track and Trace system for export of pharmaceuticals (coded using GS1 standards)
- Master data error – Master data has been erroneously uploaded in the EU Hub (e.g. due to human error in encoding the digits) thus no longer corresponding to the data coded on the packs
- 'Lost 3rd country packs' – packs coded according to 3rd country standards (e.g. Turkey) which accidentally found their way on the EU market (without repackaging)
- Etc.

[3] 'Double dispense' functionality threshold is managed at NMVS level

At the moment, this scenario is not treated as a level 5 alert, rather as a 'system exception'. Nonetheless all information is recorded in the National Medicines Verification System. NMVOs and NCAs may discuss at national level the ways and instances when such 'system exceptions' may be escalated directly to the NCA.

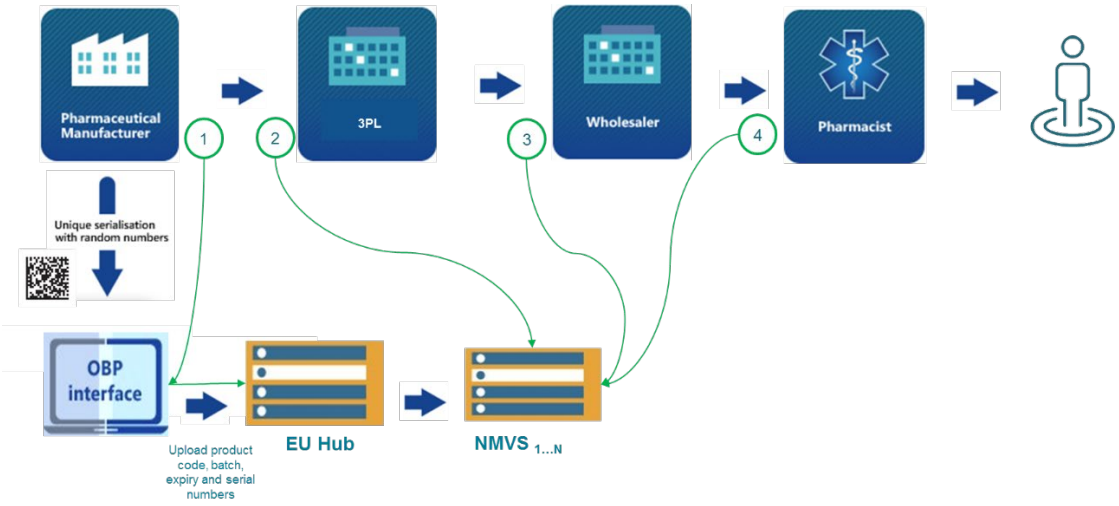
A. Preventive actions

Actions to be considered by all stakeholders within their own responsibility to avoid the system generating avoidable technical and / or procedural 'level 5 alerts' raising unique alert identifiers. Recommending preventive actions to be done by each stakeholder aims to enhance the compounded effect on the supply chain. While they may be perceived as redundant, they are important during a 'ramp-up phase'.

Each stakeholder has the responsibility to ensure users of the system(s) receives proper guidance, e.g. training, documentation.

1. Scenario: Data error

The defined preventive actions below are not exhaustive. Other preventive actions can be defined based on stakeholder discretion.



Possible root cause level	Serial number missing in system Batch or expiry data mismatch	Incorrect manual entry of serial number
1 **OBP Mfg / OBP PD**	Verify batch upload before shipping to the market Ensure data is correctly uploaded (example QP to scan samples of packs before batch release) Check receipt of confirmation message from EU Hub on distributed pack data to NMVS	Additional check by second person prior to submitting the action in the system
2 **3PL**	Recommend verifying during ramp-up phase – one pack per batch at receiving	Additional check by second person prior to submitting the action in the system

3 **End-user: wholesaler/distributor**	Recommend verifying during ramp-up phase – one pack per batch at receiving	Additional check by second person prior to submitting the action in the system
4 **End-user: pharmacist**	Advising verification each pack at point of entry during ramp-up phase. In hospitals this might happen at different points at receiving	Additional check by second person prior to submitting the action in the system

A verification will check the existence of the data in the systems and if not present an alert will be raised. This verification check will also provide information on the status of the pack. If the status is not as expected the operator can carry out appropriate actions.

© EMVO 2019
Uncontrolled when printed

A. Preventive actions

2. Scenario: Pack (UI) status error

<table>
<tr><th>Root cause</th><th>OBP Mfg / OBP PD</th><th>3PL</th><th>End-user: wholesaler/distributor</th><th>End-user: pharmacist</th><th>NMVO</th><th>EMVO</th></tr>
<tr><td>Pack already decommissioned for same reason (in same location – e.g. double dispense)</td><td colspan="4" rowspan="4">Perform a verify before decommissioning on risk base.</td><td>Managing country configure ‘double dispense’ setting</td><td rowspan="4">N/A</td></tr>
<tr><td>Pack already decommissioned for other reason (in same location)</td><td rowspan="3">N/A</td></tr>
<tr><td>Pack already decommissioned for other reason – different location e.g. pack for export, ending up in the pharmacy for dispensing</td></tr>
<tr><td>Pack already decommissioned for same reason (in different location)</td></tr>
<tr><td>Undo-decommission</td><td colspan="4">Perform a verify before undo-decommission on risk base.</td><td colspan="2"></td></tr>
</table>

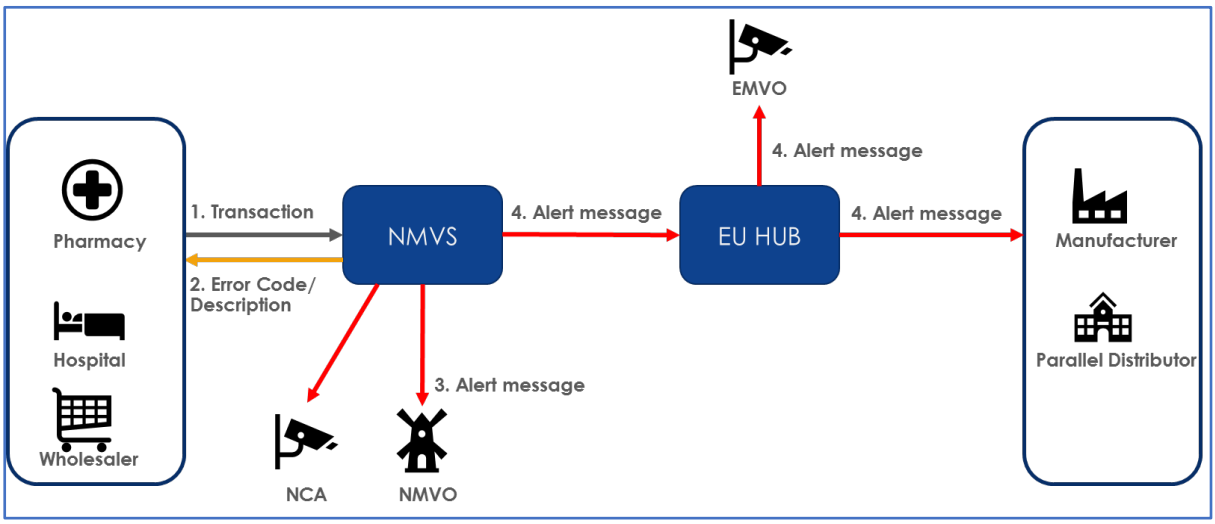
© EMVO 2019

Uncontrolled when printed

B. Managing alerts

In case all preventive actions have been done, and an alert has been generated by the system, the process to analyses, communicate and taken actions is a process involving different stakeholders.

See below the system process of an alert.



Reflects system-to-system connections. Does not show nor does it aim to explain the reporting routes which each supply chain stakeholder needs to ensure in order to comply with Art 18, 24 and 30.

1) End user scans a pack.
2) Error is returned to the End-user by the National System
3) The National System raises an alert to the NMVO and the NCA
    a. Automatic transaction to NCA is configurable in the National System
4) EU HUB processes the alert and raises its own alert to the OBP and the EMVO

The generated alert is sent to the NMVO, NCA (once configured), EMVO and the OBP. Based on the UniqueAlertID / UPRC (Unique Pack Return Code), a Pack Disclosure Report (PDR) [4] can be requested by each of these stakeholders (see explanation in Introduction).

This PDR is based on the audit trail of the pack and "*contains all data associated with one individual product pack, starting with the creation of the pack in the national system across the entire 'life' of the pack…*".[5]

The history of the pack will be disclosed, but in the current version of the PDR the exact location of where the alert has been generated is not available, only the client ID and the country. This does drive the interactions between different stakeholders in performing the root cause analysis of an alert.

[4] See EMVO_0016_EMVS Req Spec Part III Use Case Process Step Descriptions, §6.3.2 Pack Data Disclosure Report.
[5] See EMVO_0016_EMVS Req Spec Part III Use Case Process Step Descriptions, §6.1.2 Product Pack Audit Trail.

© EMVO 2019

Based on existing capability of the systems three options of communication (e.g. either direct or via implemented information exchange platform) have been identified.
Sequence in preference:

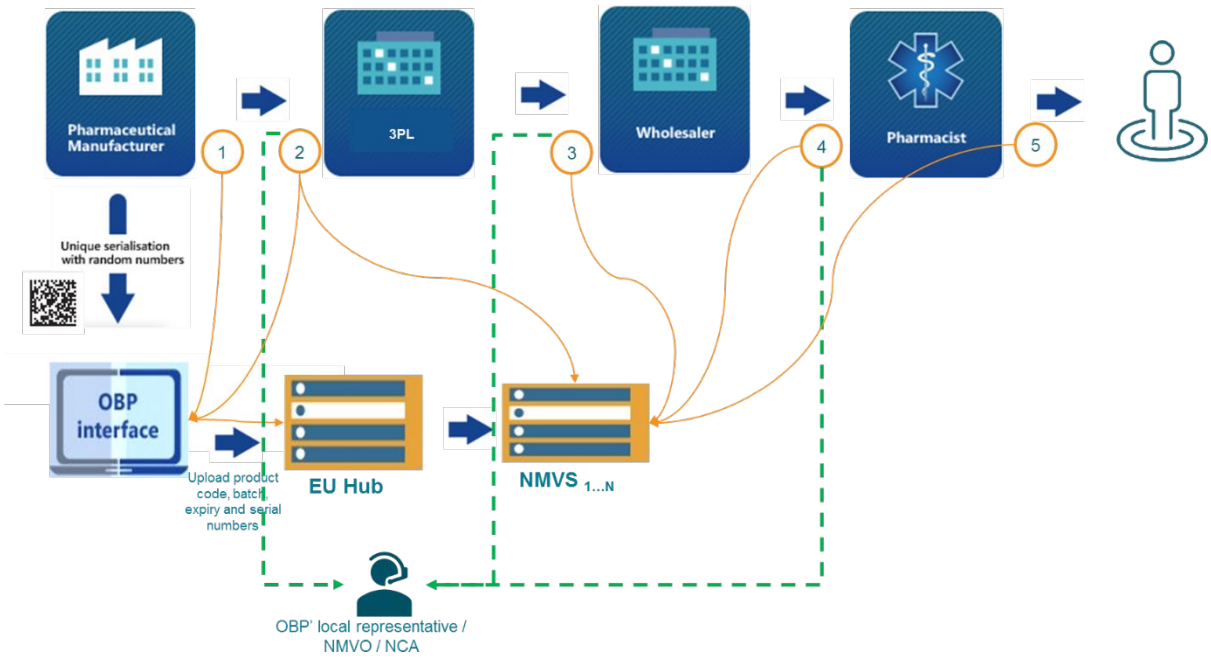
1) End-user contacts OBP local representative; besides this, the end-user may also contact the NMVO / NCA as per country defined process.
2) OBP local representative contacts NMVO / NCA to disclose end-user results in 2 options:
    a) OBP local representative contacts end-user;
    b) NMVO / NCA facilitated communication between end-user and OBPs local representative.

These communication flows might change due to ongoing improvement of the systems capabilities.

B. Managing alerts

1. Scenario: Data error

In case an alert has been triggered under scenario: Data error, 3 root causes have been identified (see section Procedures):



© EMVO 2019

	End-user **has not caused** the alert	End-user **has caused** the alert
Possible root cause level	**Pack (UI) unknown / Mismatch batch / expiry date**	**End-user entered wrong data in system**
4 5 **End-user: pharmacist**	Put pack in quarantine for max 2 business days and attach the uniqueAlertID / UPRC. Within 2 business days retry to scan, In case the OBP has caused the error and solved the RC and end-user is known, OBP will inform end-user about successful data upload. Communication with OBPs local representatives as per agreed process on national level. In case the OBP has not caused the alert, the OBPs affiliate will advise the end-user on the next steps.	Document investigation, correct action and include uniqueAlertID / UPRC in communication with OBPs local representatives within 1 business day, as per agreed process on national level.
3 **End-user: wholesaler/ distributor**	Put batch in quarantine for max 2 business days and attach the uniqueAlertID / UPRC WH contacts OBPs local representatives as per agreed process on national/company level. *Scan a 2nd pack of the same batch, on request.* In case the OBP has caused the error and solved the RC and is able to inform the end-user about successful data upload, the OBP will inform the end-user. The stock level is driving the criticality. In case the OBP has not caused the alert, the OBPs affiliate will advise the end-user on the next steps.	Document investigation, correct action and include uniqueAlertID / UPRC in communication with OBPs local representatives within 1 business day as per agreed process on national level.
2 **3PL connected via NMVS**	3PL will follow agreed process between 3PL and OBP/MAH OR Put batch in quarantine for max 2 business days and attach the uniqueAlertID / UPRC	3PL will follow agreed process between 3PL and OBP/MAH OR Document investigation, correct action and include uniqueAlertID / UPRC in communication with OBPs local

© EMVO 2019

	3PL contacts OBPs local representatives as per agreed process on national/company level. *Scan a 2nd pack of the same batch, on request* In case the OBP has caused the error and solved the RC and end-user is known, OBP will inform end-user about successful data upload. In case the OBP has not caused the alert, the OBPs affiliate will advise the 3PL on the next steps.	representatives within 1 business day as per agreed process on national level.
2 **3PL connected via OBP system**	3PL will follow agreed process between 3PL and OBP/MAH	3PL will follow agreed process between 3PL and OBP/MAH
1 **OBP Mfg / OBP PD - Outbound**	Performs internal analyses. If data are wrongly or not uploaded, correctly upload data. Inform end-user / NMVO as per national level agreed In case OBP uploaded data correctly, OBP will inform end-user / NMVO because of suspect falsification to request additional information of the pack or return pack.	OBP internal analysis is not needed if end-user error is confirmed by end-user. .
1 **OBP PD - Inbound**	Put pack in quarantine for max 2 business days and attach the uniqueAlertID / UPRC. Within 2 business days retry to scan, In case the OBP has caused the error and solved the RC and end-user is known, OBP will inform end-user about successful data upload. Communication with OBPs local representatives as per agreed process on national level. In case the OBP has not caused the alert, the OBPs affiliate will advise the PD on the next steps.	Document investigation, correct action and include uniqueAlertID / UPRC in communication with OBPs local representatives within 1 business day, as per agreed process on national level.
NMVO	The NMVO will facilitate with communication from the OBP local representative to the end user in case the end user contact details are	The NMVO will facilitate with communication from the OBP local representative to the end user in case the end user contact details are

	unknown to the OBP local representative	unknown to the OBP local representative.
NCA	Will be informed in case alert has not been caused by technical and / or procedural error by the OBP. This alert becomes a 'suspected falsification'. Report to NCA by OBPs local representative.	As root cause of alert was because of technical or procedural error, NCA will not be informed directly, but on request results of analysis can be given.
EMVO	N/A	**N/A**

B. Managing alerts

2. Scenario: Pack (UI) status error

Regardless the different root causes, e.g. dispense for same / different reason, or in same / different location, the result of the analyses can be classified as end-user did or did not caused the alert:

	End-user **has not caused** the alert	End-user **has caused** the alert
Possible root cause level	**Status change not allowed**	**Status change not allowed**
End-user: pharmacist	Put pack in quarantine and attach the uniqueAlertID / UPRC. End-user contacts OBPs local representative as per agreed process on national level to provide additional information on pack causing alert or to send the pack back as per national agreement.	Document investigation, correct action and include uniqueAlertID / UPRC in communication with OBPs local representatives within 1 business day as per agreed process on national level.
End-user: wholesaler/ distributor	Put pack in quarantine and attach the uniqueAlertID / UPRC. End-user contacts OBPs local representative as per agreed process on national level to provide additional information on pack causing alert or to send the pack back as per national agreement.	Document investigation, correct action and include uniqueAlertID / UPRC in communication with OBPs local representatives within 1 business day as per agreed process on national level.
3PL connected via NMVS	3PL will follow agreed process between 3PL and OBP/MAH OR Put pack in quarantine and attach the uniqueAlertID / UPRC. End-user contacts OBPs local representative as per agreed process on	3PL will follow agreed process between 3PL and OBP/MAH OR Document investigation, correct action undo-decommission and include uniqueAlertID / UPRC in communication with OBPs local representatives within

	national level to provide additional information on pack causing alert or to send the pack back as per agreement.	1 business day as per agreed process on national level.
3PL connected via OBP system	3PL will follow agreed process between 3PL and OBP/MAH	3PL will follow agreed process between 3PL and OBP/MAH
OBP Mfg	OBP performs (internal) analyses. OBPs local representative will request end-user to provide additional information or return pack.	OBP performs (internal) analyses. OBP will request NMVO to investigate further in case same pack causing multiple alerts.
OBP PD - inbound	Put pack in quarantine and attach the uniqueAlertID / UPRC. PD contacts OBPs local representative as per agreed process on national level to provide additional information on pack causing alert or to send the pack back as per national agreement.	Document investigation, correct action undo-decommission and include uniqueAlertID / UPRC in communication with OBPs local representatives within 1 business day as per agreed process on national level.
OBP PD - outbound	OBP performs (internal) analyses. OBPs local representative will request end-user to provide additional information or return pack.	OBP performs (internal) analyses. OBP will request NMVO to investigate further in case same pack causing multiple alerts.
NMVO	The NMVO will facilitate with communication from the OBP local representative to the end user in case the end user contact details are unknown to the OBP local representative.	The NMVO will facilitate with communication from the OBP local representative to the end user in case the end user contact details are unknown to the OBP local representative.
NCA	Will be informed in case alert can't be ruled out by technical and / or procedural root cause and turned into 'suspected falsification' by OBP local representative and / or NMVO.	As root cause of alert was because of technical or procedural error, NCA will not be informed directly, but on request results of analysis can be given.
EMVO	In case the alert has been generated because of pack status is 'checked-out, the EMVO act as connection point between both types of OBP.	In case the alert has been generated because of pack status is 'checked-out, the EMVO act as connection point between both types of OBP.

© EMVO 2019

C. Monitoring and process improvements

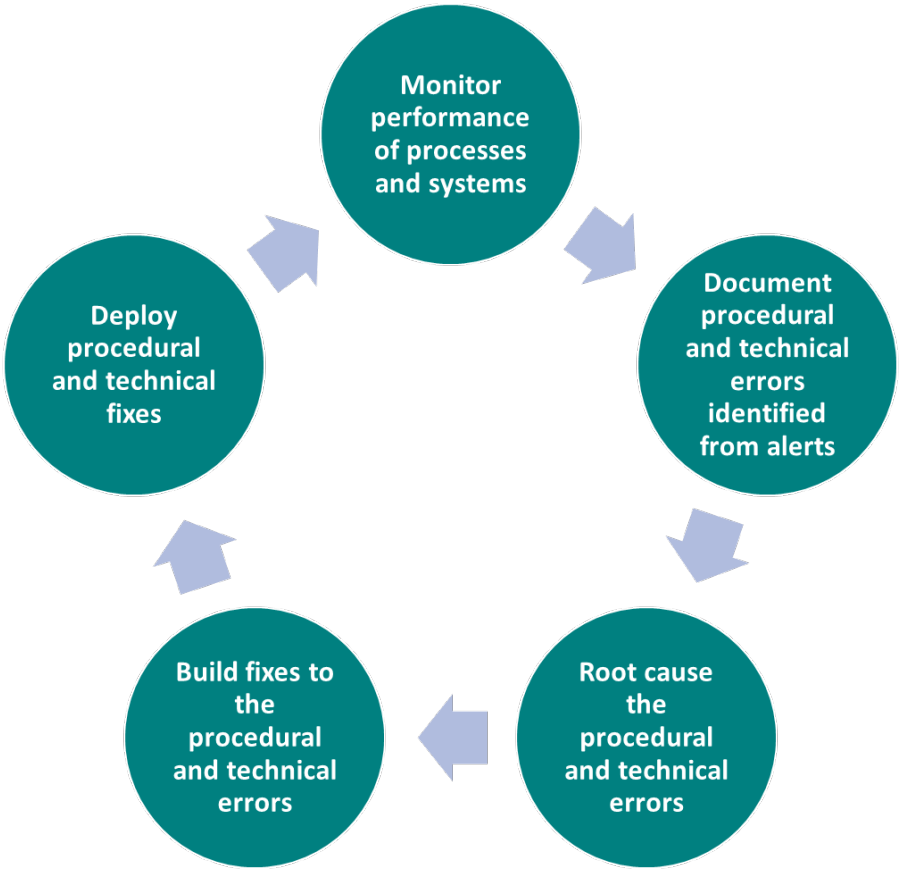
The EU-FMD requires a complex set of systems and business processes.

These are operated by a large number of users and stakeholders across the European supply chain.

With such complexity and volume of serialised packs it is expected that there will be both errors due to processes and technical issues.

Over time alerts may help to highlight these issues and allow organisations to review and improve their master data, processes and systems.

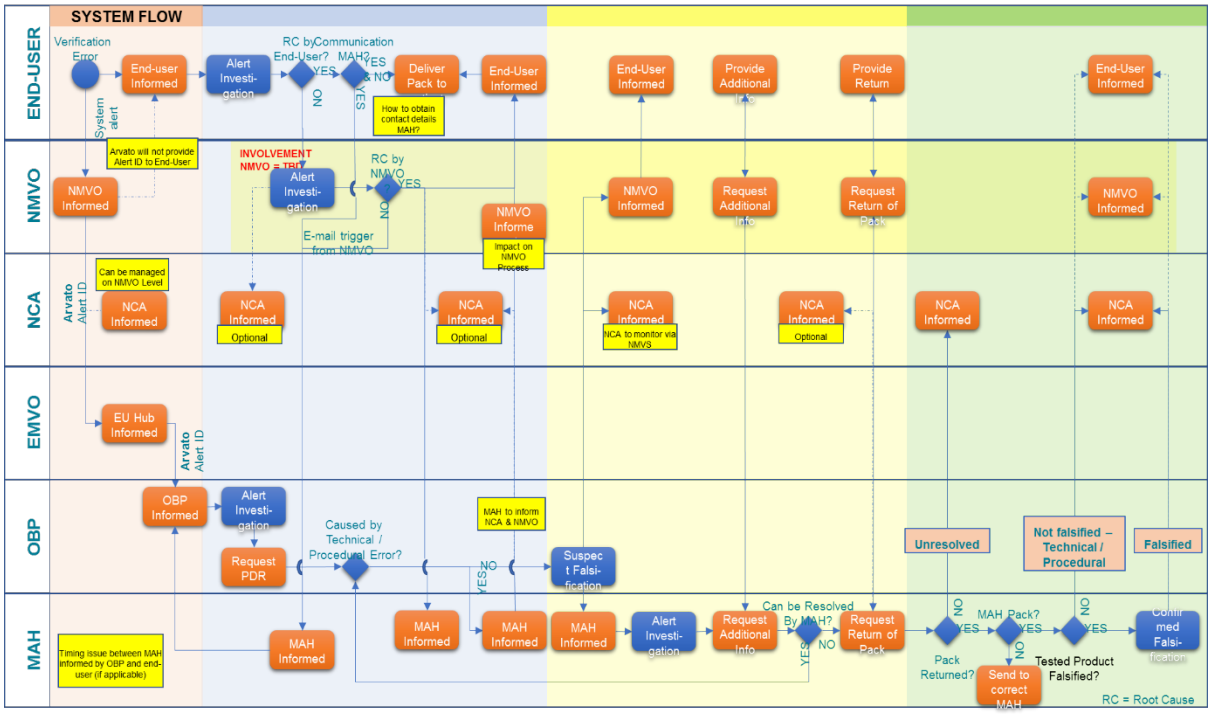
Establishing a monitoring and improvement cycle such as the one shown will help ensure that unnecessary alerts can be reduced over time.



© EMVO 2019

D. Appendix

1. Process flows



© EMVO 2019

Uncontrolled when printed

E. Glossary

3PL	Third Party Logistics. A party managing on behalf of the OBP the storage and / or distribution of products
Business days	Are standing for Monday to Friday
End-user	An actor in the process performing a verification, dispensing and / or decommissioning activity.
EU Hub	The central system operated by the EMVO connecting the OBP with the NMVSs.
MAH	**Marketing Authorisation Holder** and/or the holders of parallel import or parallel distribution licenses that operate and place medicines on the market for sale, and responsible for data upload into the Hub.
NMVS	National Medicines Verification System
OBP	**On-boarding Partner,** single entity representing one or more MAH's and owns the interface between the MAH's and the EMVS. It is understood that MAHs have delegated the tasks of data upload to the EU Hub and receipt of alerts from the EU Hub to the OBP
OBP's local representative	Within the OBPs organisation it is possible that country specific organizations do exists for contacts with / for end-users, such as: affiliate services, customer services etc. As each OBPs company may use different terminology, for the ease of reading, OBP local representative is used.

© EMVO 2019