Joint guideline for pharmacies/wholesalers/hospitals/manufacturers

Alert Handling in Germany

(as of 3 November 2025, MB)

1 Preamble

This document describes the common guidelines for manufacturers, pharmacies, hospitals and wholesalers on how alerts should be handled in Germany.

Alerts are classified and summarised according to fixed criteria. If certain criteria are met, the alerts are automatically commented on and processed. Depending on the classification, a different procedure is recommended.

The aim is for manufacturers, pharmacies, hospitals and wholesalers to work together to resolve as many alerts as possible in order to make an effective contribution to protecting against counterfeit medicines.

This guideline is supported by the members of securPharm, including ABDA, BPI, Pharma Deutschland and vfa.

Note

Please note that this document is subject to change. The current version can be found at: https://www.securpharm.de/downloads/

2 Basic Information

2.1 Principles

The following principles apply to alerts:

- Alerts are warnings sent to various users in the securPharm system.
- If the cause of an alert cannot be found, the pack for which the alert occurred is suspected of being counterfeit. Therefore, system participants should always determine the cause of alerts and check whether the result of the investigation is documented accordingly in the system.
- Even without an alert, there may still be a suspicion of counterfeiting.

2.2 Important information about alerts

The following applies to alerts and their processing:

- An alert caused by an error is referred to as a false alert. False alerts can be classified into two groups based on the information provided:
    - Alerts caused by a mismatch between the queried and stored pack data: **Technical alerts**
    - Alerts that occur when a status change is unsuccessful because the desired pack status is already set: **Handling alerts**
- The system user who triggers the alert is not necessarily the same as the user who caused the alert.
- Depending on the location of the system connection, an alert may have a different code (see Appendix 1), but the content of the alert is the same in each case.
- When the alert is triggered, the alert and a recommended action are displayed in the merchandise management system at the operating sites[1] .
- Alerts are documented and managed in Germany in an alert management system (AMS).

2.3 Contact points for system participants in Germany

If the measures and procedures proposed in this document are not sufficient in individual cases, you can contact the following for support:

- **Authorities** should contact support@securpharm.de
- **MAHs** / customers of ACS Pharmaprotect should contact support@pharmaprotect.de
- **Pharmacies**:
    - Further information:
        - FAQ and the SOP "securPharm – Procedure in pharmacies" at www.abda.de/sp
    - General questions/comments/criticism:
        - securpharm@abda.de
    - Questions about an individual pack/N-ID: NGDA helpdesk

[1] Pharmacies, hospital pharmacies, wholesalers

2.4 The Alert Management System (AMS)

All alerts and the associated information are stored in a central alert management system in Germany.

All actions in the alert management system are documented. This system also supports the manual resolution of alerts, which is sometimes necessary.

- The alert management system performs automatic alert processing. The alert management system checks whether the alert is likely to be a false alert. If the system comes to this conclusion, the alert is automatically closed and a corresponding comment is assigned. If the alert cannot be closed, further information is provided that can be used for further evaluation by the responsible persons.
- The procedures of the alert management system are based on the experience of securPharm members in system operation. However, they do not replace careful examination of the alert. Only when the cause of the error has been identified beyond doubt can the alert be classified as a false alert on the basis of the available information. As a general rule, if information subsequently becomes available that raises renewed suspicion of falsification, this must be reported to the supervisory authorities. Optionally, the alert can be set to "escalated" in the alert management system at any time.
- A pack may only be dispensed if there is no suspicion of counterfeiting and its status is "active".

Alert processing via the alert management system provided is voluntary for system users (manufacturers and operating sites).

However, it is strongly recommended that the alert management system offered by the NGDA (securPharm GUI), ACS (National AMS) and EMVO (EAMS portal) be used. In this system, all status changes and comments are synchronised with each other. Both the manufacturer and the operating site that triggered the alert can view and process their alerts. The identity of the operating site that triggered the alert remains hidden from the manufacturer thanks to a pseudonym. This enables anonymous communication between manufacturers and operating sites.

Authorities currently only have read access to this system.

Note

In the event of a "concrete suspicion of counterfeiting", it is not sufficient to set the alert status in the alert management system to "escalated". The specified reporting procedures for suspected counterfeiting must be followed regardless of the documentation in the system.

3 Alert type-specific guidelines

3.1 Double deactivation, same (PCK_19) or different action (PCK_22)

A PCK_19 or **PCK_22** alert is triggered when an attempt is made to set an already inactive pack to *inactive* again.

- In the case of a PCK_19 alert, the deactivation action corresponds exactly to the previous action that originally set the pack to deactivate.
- In the case of a PCK_22 alert, however, the action is different from the original deactivation.

The alert management system analyses these alerts, adds a comment with further information and, under certain circumstances, closes the alert automatically.

3.1.1 Recommendations for the operating site

The operating site can use the transaction history in the software to check whether this pack has already been dispensed.

If a pack has been accidentally dispensed, it can be reversed under certain conditions (10-day period, control area, no suspicion of falsification). Then perform an **undo** to reactivate the pack. The system automatically ensures that only the site that set the pack to inactive can perform a reversal (called “undo”).

Alerts generated at the operating site due to duplicate dispense attempts are automatically closed with the undo. The process is documented in the system by the undo and is thus completed. No additional documentation is required. If the undo is not successful, feedback is provided explaining why this was not possible. The alert details may provide further information.

If the pack cannot be restored to active pack status based on the transaction history or other information, it cannot be dispensed.

If the cause of the alert is found on the operating site, it is recommended that the alert be closed in the securPharm GUI.

If no cause for the alert can be found at the facility, it must be considered whether to first contact the NGDA helpdesk and/or the manufacturer for an internal investigation or whether to immediately report a suspected counterfeit.

Note

If a cause for the alert has been found and a reversal (undo) is not possible, this should also be noted in the securPharm GUI. This supports both the manufacturer and the supervisory authorities in investigating suspected cases of counterfeit medicines.

3.1.2 Actions to be taken by the manufacturer of the pack

If an internal error can be ruled out as the cause of the double dispense and as long as there are no concrete indications of a possible counterfeit (e.g. from other sources or a manual alert comment at the production site), **no** further action is required. The manufacturer does not usually have the information necessary to evaluate the alert.

3.2 Unknown pack (alerts due to unknown data elements)

In the case of an unknown pack, one or more data elements are unknown, i.e. the data read out does not match the stored data. This triggers an alert and the operating site does not receive a pack status.

The same applies to packs that were not manufactured for the European anti-counterfeiting system. In this case, the feedback from the software must be noted and the authorisation documents must be checked.

If the system recognises that the packs are subject to verification, there are three possible causes for the "unknown pack" feedback: The printed pack data is incorrect, the printed code on the pack is not read correctly by the scanner or software, or the pack data stored in the system is incorrect.

The following recommendations deal with alerts relating to the three data elements: serial number, batch or expiry date. In the case of an alert due to an unknown product code (PC_01, #A1), the assignment to a manufacturer is missing. It is therefore not possible to process this in the alert management of the securPharm GUI. If the cause cannot be found on site, it may be necessary to contact the manufacturer via conventional communication channels.

The alert codes for unknown packs are as follows:

- **PC_02 alerts** occur when the transmitted serial number is unknown or does not match. However, the transmitted batch is found.
- **LOT_13 alerts** occur when the transmitted batch is unknown or does not match. However, the transmitted serial number is found.
- **LOT_12 alerts** occur when the transmitted expiry date does not match.
- **LOT_03 alerts** occur when the serial number and batch are unknown or do not match.

The alert management system analyses these alerts, adds a comment with further information if necessary, and closes the alert under certain circumstances.

3.2.1 Actions at the operating site:

Try to find out whether the source of the error is at your site.

To do this, compare the printed data with the data read out. You can find a corresponding view of the read-out pack data in the software and in the securPharm GUI.

If you have not yet found the source of the alert, check whether manual entry leads to the desired result.

Recommendation: Scanner test. This quickly reveals typical read errors — even correctly adjusted scanners can become misaligned over time.

If the pack still cannot be recognised, it is recommended that you contact the manufacturer. This can be done quickly and without further data entry via the securPharm GUI.

Even if the cause of the alert has been identified and rectified and the pack has been properly checked out and dispensed, the alert may remain unprocessed in the system due to the unknown pack. In this case, manual processing by the operating site is requested. This helps the national competent authorities to evaluate the case and thus strengthens the drug counterfeiting protection system.

Some of the alerts are automatically commented on and closed. If there is no suspicion of counterfeiting, no further action is required on the part of the operating site to process the alert. The handling of the pack, including verification and deregistration prior to physical dispensing, remains unaffected.

3.2.2 Action to be taken by the manufacturer to whom the pack belongs:

Check whether the data read out is valid or whether the data uploaded for this pack/batch may be incorrect.

In particular, if the alert management system suspects that the batch has not been uploaded (this is noted as a comment and the alert is set to "under investigation" status), you should check whether the batch has been successfully uploaded. If this is not the case, a comment should be added to the alert. The upload must be completed immediately. Once the upload has been successful, this should also be documented as a comment, and the alert should be closed. This allows the operating sites to see that the cause has been rectified.

Once the data has been uploaded correctly, you can enter a comment with information about the suspected cause of the error at the operating site (e.g. "Our serial numbers have XX digits").

If there are frequent alerts, the print quality and character selection of the data elements should be checked. The coding rules provide information on this (https://www.securpharm.de/securpharm-system/codierung/).

Appendix 1 – Mapping of the most common alert codes (return codes)

The most common return codes that occur in connection with alerts are listed below.

The return codes differ depending on whether they are displayed in a national system from arvato (for ACS customers), the concentrator (for NGDA customers) or in the EU hub (for so-called onboarding partners) or a national system from SolidSoft Reply (SSR).

Automatic mapping ensures the smooth translation of the various codes.

Return code			Description	Explanation
Arvato	**SSR**	**NGDA**		
NMVS_NC_PCK_19	#A7	SP-201	Property already set	The status that is being attempted to be set is already set for this pack.
NMVS_NC_PCK_22	#A24	SP-201	Pack is already inactive	The pack is already inactive, but with a different status than the one being attempted to set.
NMVS_NC_PCK_27	#A24	SP-252	Status change not possible	Status change within the scope of an intermarket request is not possible.
NMVS_NC_PCK_06	#A24	SP-252	The property to be removed is not set on the pack	An attempt is being made to revert a status that has not been set for this pack.
NMVS_NC_PC_02	#A3	SP-102	Serial number not known	The requested serial number was not found in the system, but the batch was found.
NMVS_FE_LOT_03	#A2	SP-212	No batch found	The requested serial number and batch are unknown in both the DE system and the EU hub.
NMVS_FE_LOT_13	#A68	SP-212	Batch number does not match	The requested batch was not found, but the serial number was.
NMVS_FE_LOT_12	#A52	SP-216	Expiry date does not match	The requested expiry date differs from the expiry date stored in the system for this pack in terms of month or year.
NMVS_NC_PCK_21	#A5	SP-254	Only the user who set the property can undo it.	The pack is inactive and another user is attempting to reactivate it.
NMVS_NC_PCK_20	#A4	SP-253	Time window between setting and undo exceeded	An attempt was made to reactivate an inactive pack after more than 10 days.

Return code			Description	Explanation
Arvato	SSR	NGDA		
NMVS_NC_PC_01	#A1	SP-101	Product code unknown	The requested product code is not known in either the DE system or the EU hub.