

Gemeinsame Leitlinie für Apotheken/Großhändler/Krankenhäuser/Hersteller

Alarm-Bearbeitung in Deutschland

(Stand: 3.11.2025, MB)

1	Präambel	2
2	Grundlegende Informationen	3
2.1	Grundsätze	3
2.2	Wissenswertes zu Alarmen	3
2.3	Ansprechstellen für die Systembeteiligten in Deutschland	3
2.4	Das Alarm-Management-System (AMS)	4
3	Alarm-Typ spezifisches Vorgehen	5
3.1	Doppelte Ausbuchung, gleiche (PCK_19) bzw. abweichende Aktion (PCK_22)	5
3.2	Unbekannte Packung (Alarme aufgrund unbekannter Datenelemente)	6
	Anlage 1 - Mapping der häufigsten Alarm-Codes (Return-Codes)	8

1 Präambel

In diesem Dokument sind die gemeinsamen Leitlinien für Hersteller, Apotheken, Krankenhäuser und Großhändler beschrieben, wie Alarmer in Deutschland bearbeitet werden sollten.

Alarmer werden anhand fester Kriterien klassifiziert und zusammengefasst. Wenn bestimmte Kriterien erfüllt sind, findet eine automatische Kommentierung und Bearbeitung der Alarmer statt. Je nach Klassifizierung wird ein anderes Vorgehen empfohlen.

Ziel ist, dass Hersteller, Apotheken, Krankenhäuser und Großhändler gemeinsam eine größtmögliche Anzahl an Alarmen auflösen, um so einen wirksamen Beitrag zum Schutz vor Arzneimittelfälschungen zu leisten.

Diese Leitlinie wird von den Mitgliedern von securPharm, darunter ABDA, BPI, Pharma Deutschland und vfa, unterstützt.

Hinweis

Beachten Sie, dass sich dieses Dokument ändern kann. Die jeweils aktuelle Version finden Sie unter: <https://www.securpharm.de/downloads/>

2 Grundlegende Informationen

2.1 Grundsätze

In Bezug auf Alarme gelten folgende Grundsätze:

- Alarme sind Warnhinweise an unterschiedliche Nutzer im securPharm-System.
- Sofern die Ursache für einen Alarm nicht gefunden werden kann, stellt die Packung, zu der dieser Alarm aufgetreten ist, einen Fälschungsverdachtsfall dar. Daher sollten die Systembeteiligten stets die Ursache von Alarmen ermitteln und überprüfen, ob das Ergebnis der Untersuchung entsprechend im System dokumentiert ist.
- Auch ohne Alarm kann ein Fälschungsverdacht bestehen.

2.2 Wissenswertes zu Alarmen

In Bezug auf die Alarme und ihre Bearbeitung gilt folgendes:

- Ein Alarm, der durch einen Fehler entstanden ist, wird als Fehlalarm bezeichnet. Fehlalarme lassen sich anhand der mitgelieferten Informationen in zwei Gruppen klassifizieren:
 - Alarme, die aufgrund fehlender Übereinstimmung der abgefragten zu den hinterlegten Packungsdaten entstehen: **Technische Alarme**
 - Alarme, die bei einem nicht erfolgreichen Statuswechsel entstehen, weil der gewünschte Packungsstatus bereits gesetzt ist: **Handhabungsalarme**
- Der Systemnutzer, der den Alarm auslöst, ist nicht zwangsläufig derselbe wie der, der den Alarm verursacht hat.
- Je nach Ort der Systemanbindung kann ein Alarm eine andere Codierung besitzen (siehe dazu Anlage 1), der Inhalt des Alarms ist aber jeweils der gleiche.
- Den Betriebsstätten¹ wird mit der Alarmauslösung der Alarm und eine Handlungsempfehlung im Warenwirtschaftssystem angezeigt.
- Alarme werden in Deutschland in einem Alarm-Management-System (AMS) dokumentiert und verwaltet.

2.3 Ansprechstellen für die Systembeteiligten in Deutschland

Sollten die in diesem Dokument vorgeschlagenen Maßnahmen und Vorgehensweisen in Einzelfällen nicht ausreichen, können Sie folgende Ansprechpartner um Unterstützung bitten:

- **Behörden** melden sich bei support@securpharm.de
- **MAHs / Kunden** der ACS Pharmaprotect melden sich bei support@pharmaprotect.de
- **Apotheken:**
 - Weiterführende Informationen:
 - FAQ und die SOP "securPharm – Vorgehen in der Apotheke" unter www.abda.de/sp
 - Generelle Fragen/Anmerkungen/Kritik:
 - securpharm@abda.de
 - Fragen zu einer einzelnen Packung / N-ID: Helpdesk der NGDA

¹ Apotheken, Krankenhausapotheken, Großhändler

2.4 Das Alarm-Management-System (AMS)

Alle Alarme und die dazugehörigen Informationen werden in Deutschland in einem zentralen Alarm-Management-System gespeichert.

Sämtliche Aktionen im Alarm-Management-System werden dokumentiert. Ebenfalls wird eine manchmal notwendige manuelle Alarm-Auflösung durch dieses System unterstützt.

- Im Alarm-Management-System wird eine automatische Alarmbearbeitung durchgeführt. Das Alarm-Management-System prüft, ob es sich wahrscheinlich um einen Fehlalarm handelt. Kommt das System zu dieser Einschätzung, wird der Alarm automatisch geschlossen und ein entsprechender Kommentar zugeordnet. Kann der Alarm nicht geschlossen werden, werden weitere Informationen bereitgestellt, die für die weitere Bewertung durch die zuständigen Personen genutzt werden können.
- Die Vorgehensweisen des Alarm-Management-Systems basieren auf den Erfahrungen der securPharm-Mitglieder im Systembetrieb. Sie ersetzen jedoch keine sorgfältige Prüfung des Alarms. Erst wenn die Fehlerursache zweifelsfrei identifiziert wurde, kann der Alarm auf Basis der vorliegenden Informationen als Fehlalarm eingestuft werden. Grundsätzlich gilt: Sollten nachträglich Informationen bekannt werden, die einen Fälschungsverdacht erneut aufkommen lassen, ist dies den Aufsichtsbehörden zu melden. Optional kann der Alarm im Alarm-Management-System jederzeit auf "eskaliert" gesetzt werden.
- Eine Packung darf nur dann ausgebucht werden, wenn kein Verdacht auf Fälschung besteht und ihr Status "aktiv" ist.

Die Alarmbearbeitung über das angebotene Alarm-Management-System ist für die Systemnutzer (Hersteller und Betriebsstätten) freiwillig.

Es wird jedoch nachdrücklich empfohlen, das von der NGDA (securPharm GUI), ACS (Nationale AMS) und der EMVO (EAMS-Portal) angebotene Alarm-Management-System zu nutzen. In diesem System werden alle Statusänderungen und Kommentare miteinander synchronisiert. Sowohl der Hersteller als auch die alarmanlösende Betriebsstätte können ihre Alarme einsehen und bearbeiten. Die Identität der alarmanlösenden Betriebsstätte bleibt dem Hersteller dank eines Pseudonyms verborgen. Dadurch ist ein anonymer Austausch zwischen Herstellern und Betriebsstätten möglich.

Behörden haben derzeit nur lesenden Zugriff auf dieses System.

Hinweis

Im Falle eines "sich konkretisierenden Fälschungsverdachts" reicht es nicht aus, den Alarmstatus im Alarm-Management-System auf „eskaliert“ zu setzen. Die vorgegebenen Meldewege bei Fälschungsverdacht sind unabhängig von der Dokumentation im System einzuhalten.

3 Alarm-Typ spezifisches Vorgehen

3.1 Doppelte Ausbuchung, gleiche (PCK_19) bzw. abweichende Aktion (PCK_22)

Ein **PCK_19**- oder **PCK_22**-Alarm wird ausgelöst, wenn versucht wird, eine bereits inaktive Packung erneut auf *inaktiv* zu setzen.

- Beim **PCK_19**-Alarm entspricht die auslösende Ausbuchungsaktion exakt der vorherigen Aktion, durch die die Packung ursprünglich inaktiv gesetzt wurde.
- Beim **PCK_22**-Alarm handelt es sich hingegen um eine andere Aktion als die ursprüngliche Inaktivierung.

Das Alarm-Management-System analysiert diese Alarmer, ergänzt einen Kommentar mit weiteren Informationen und schließt den Alarm unter bestimmten Umständen automatisch.

3.1.1 Empfehlungen für die Betriebsstätte

Mithilfe der Transaktionshistorie in der Software kann die Betriebsstätte überprüfen, ob diese Packung bereits ausgebucht wurde.

Sollte eine Packung versehentlich ausgebucht worden sein, kann sie unter gewissen Voraussetzungen (10-Tagesfrist, Kontrollbereich, kein Fälschungsverdacht) zurückgebucht werden. Führen Sie anschließend eine **Rückbuchung** durch, um die Packung wieder aktiv zu setzen. Das System sichert automatisch ab, dass nur diejenige Betriebsstätte eine Rückbuchung durchführen kann, die die Packung in den inaktiven Zustand versetzt hat.

In der Betriebsstätte entstandene Alarmer aufgrund doppelter Ausbuchungsversuche werden mit der Rückbuchung automatisch geschlossen. Der Vorgang wird durch die Rückbuchung im System dokumentiert und ist somit abgeschlossen. Eine zusätzliche Dokumentation ist nicht erforderlich. Sollte die Rückbuchung nicht erfolgreich sein, wird als Rückmeldung angegeben, warum dies nicht möglich war. Die Alarmerdetails können möglicherweise weitere Hinweise liefern.

Wenn sich die Packung auch auf Basis der Transaktionshistorie oder weiterer Informationen nicht wieder in einen aktiven Packungsstatus überführen lässt, ist sie nicht abgabefähig.

Sollte die Fehlerursache in der Betriebsstätte gefunden werden, wird eine Schließung des Alarms in der securPharm-GUI empfohlen.

Sollte keine Fehlerursache in der Betriebsstätte gefunden werden, ist abzuwägen, ob zunächst eine Kontaktaufnahme mit dem NGDA-Helpdesk und/oder mit dem Hersteller zur internen Untersuchung abgewartet wird oder ob unverzüglich ein Fälschungsverdacht gemeldet wird.

Hinweis

Wenn eine Ursache für den Alarm gefunden wurde und eine Rückbuchung nicht möglich ist, sollte dies auch in der securPharm-GUI vermerkt werden. Das unterstützt sowohl den Hersteller als auch die Aufsichtsbehörden bei der Aufklärung von Verdachtsfällen von Arzneimittelfälschungen.

3.1.2 Handlungen beim Hersteller der Packung:

Sofern ein interner Fehler als Ursache der doppelten Ausbuchung ausgeschlossen werden kann und solange keine konkreteren Hinweise auf eine mögliche Fälschung vorliegen (z. B. durch weitere Quellen oder eine manuelle Alarmkommentierung in der Betriebsstätte), ist **keine** zusätzliche Bearbeitung des Alarms erforderlich. Dem Hersteller liegen in der Regel die notwendigen Informationen zur Bewertung des Alarms nicht vor.

3.2 Unbekannte Packung (Alarme aufgrund unbekannter Datenelemente)

Bei einer unbekannten Packung sind ein oder mehrere Datenelemente unbekannt, das heißt, die ausgelesenen Daten stimmen nicht mit den hinterlegten Daten überein. Dies löst einen Alarm aus und die Betriebsstätte erhält keinen Packungsstatus.

Das Gleiche gilt für Packungen, die nicht für das europäische Fälschungsschutzsystem hergestellt wurden. In diesem Fall sind die Rückmeldungen der Software zu beachten und die Gestattungsdokumente sind zu prüfen.

Erkennt das System, dass die Packungen verifikationspflichtig sind, kommen drei Ursachen für die Rückmeldung "unbekannte Packung" in Betracht: Die aufgedruckten Packungsdaten sind fehlerhaft, die Packung wird durch Scanner oder Software nicht richtig ausgelesen, oder die hinterlegten Packungsdaten im System sind nicht korrekt.

Die nachfolgenden Empfehlungen befassen sich mit Alarmen zu den drei Datenelementen Seriennummer, Charge oder Verfalldatum. Bei einem Alarm aufgrund eines unbekannten Produktcodes (PC_01, #A1) fehlt die Zuordnung zu einem Hersteller. Eine Bearbeitung im Alarm-Management der securPharm-GUI ist deshalb nicht möglich. Lässt sich die Ursache nicht vor Ort finden, kann eine Kontaktaufnahme zum Hersteller über die konventionellen Kommunikationswege erforderlich sein.

Die Alarm-Codes für unbekannte Packungen lauten wie folgt:

- **PC_02-Alarme** entstehen, wenn die übermittelte Seriennummer unbekannt ist oder nicht übereinstimmt. Die übermittelte Charge wird jedoch gefunden.
- **LOT_13-Alarme** entstehen, wenn die übermittelte Charge unbekannt ist oder nicht übereinstimmt. Die übermittelte Seriennummer wird hingegen gefunden.
- **LOT_12-Alarme** entstehen, wenn das übermittelte Verfalldatum unbekannt ist oder nicht übereinstimmt.
- **LOT_03-Alarme** entstehen, wenn die Seriennummer und die Charge unbekannt sind bzw. nicht übereinstimmen.

Das Alarm-Management-System analysiert diese Alarme, ergänzt bei Bedarf einen Kommentar mit weiteren Informationen und schließt den Alarm unter bestimmten Umständen.

3.2.1 Handlungen in der Betriebsstätte:

Versuchen Sie herauszufinden, ob die Fehlerquelle in Ihrer Betriebsstätte liegt.

Gleichen Sie dazu die aufgedruckten Daten mit den ausgelesenen Daten ab. Eine entsprechende Ansicht der ausgelesenen Packungsdaten finden Sie in der Software sowie in der securPharm-GUI.

Sollten Sie die Fehlerquelle noch nicht gefunden haben, überprüfen Sie, ob eine manuelle Eingabe zum gewünschten Ergebnis führt.

Empfehlung: Scannertest. Dieser deckt typische Auslesefehler schnell auf — auch korrekt eingestellte Scanner können sich im Laufe der Zeit wieder verstellen.

Wenn die Packung dennoch nicht erkannt werden kann, wird empfohlen mit dem Hersteller Kontakt aufzunehmen. Dies ist schnell und ohne weitere Dateneingaben über die securPharm-GUI möglich.

Selbst wenn die Ursache des Alarms identifiziert und behoben wurde sowie die Packung ordnungsgemäß ausgebucht und abgegeben wurde, bleibt der Alarm aufgrund der unbekannten Packung möglicherweise als unbearbeitet im System bestehen. In diesem Fall

wird eine manuelle Bearbeitung durch die Betriebsstätte erbeten. Dies hilft den Aufsichtsbehörden den Fall zu bewerten und stärkt somit das Arzneimittelfälschungsschutzsystem.

Ein Teil der Alarme wird automatisch kommentiert und geschlossen. Liegt kein Fälschungsverdacht vor, sind seitens der Betriebsstätte keine weiteren Maßnahmen zur Alarmbearbeitung erforderlich. Die Handhabung der Packung, u.a. die Verifizierung und Ausbuchung vor der physischen Abgabe, bleibt davon unberührt.

3.2.2 Handlung des Herstellers, zu dem die Packung gehört:

Prüfen Sie, ob die ausgelesenen Daten valide oder ob die hochgeladenen Daten für diese Packung/Charge möglicherweise fehlerhaft sind.

Insbesondere wenn das Alarm-Management-System vermutet, dass die Charge nicht hochgeladen wurde (dies wird als Kommentar hinterlegt und der Alarm wird in den Status „under investigation“ gesetzt), sollten Sie prüfen, ob die Charge erfolgreich hochgeladen wurde. Sollte dies nicht der Fall sein, ist ein Kommentar zum Alarm zu hinterlegen. Der Upload ist unverzüglich nachzuholen. Nach erfolgreichem Upload ist dies ebenfalls als Kommentar zu dokumentieren und der Alarm ist zu schließen. So sehen die Betriebsstätten, dass die Ursache behoben wurde.

Sind die Daten korrekt hochgeladen, können Sie einen Kommentar mit Hinweisen zur vermuteten Fehlerursache in der Betriebsstätte eingeben (Bspw. „Unsere Seriennummern haben XX Stellen“).

Bei vermehrten Alarmen sollten die Druckqualität und die Zeichenwahl der Datenelemente geprüft werden. Die Codierregeln liefern dazu Hinweise (<https://www.securpharm.de/securpharm-system/codierung/>).

Anlage 1 - Mapping der häufigsten Alarm-Codes (Return-Codes)

Nachfolgend aufgeführt sind die häufigsten Return-Codes, die im Zusammenhang mit Alarmen auftreten.

Dabei unterscheiden sich die Return-Codes, je nachdem ob sie in einem Nationalen System von arvato (für Kunden der ACS), dem Concentrator (für Kunden der NGDA) oder im EU-Hub (für sogenannte Onboarding Partner) bzw. Nationalen System von SolidSoft Reply (SSR) angezeigt werden.

Ein automatisches Mapping sorgt dabei für die reibungslose Übersetzung der verschiedenen Codes.

Return Code			Beschreibung	Erläuterung
Arvato	SSR	NGDA		
NMVS_NC_PCK_19	#A7	SP-201	Eigenschaft bereits gesetzt	Der Status, der versucht wird, zu setzen, ist bereits für diese Packung gesetzt.
NMVS_NC_PCK_22	#A24	SP-201	Packung ist bereits inaktiv	Die Packung ist bereits inaktiv, allerdings mit einem anderen Status als derjenige, der versucht wird zu setzen
NMVS_NC_PCK_27	#A24	SP-252	Statusänderung nicht möglich	Statusänderung im Rahmen einer Intermarket-Anfrage ist nicht möglich
NMVS_NC_PCK_06	#A24	SP-252	Die zu entfernende Eigenschaft ist an der Packung nicht gesetzt	Es wird versucht einen Status zurückzunehmen, der nicht für diese Packung gesetzt worden ist.
NMVS_NC_PC_02	#A3	SP-102	Seriennummer nicht bekannt	Die angefragte Seriennummer wurde nicht im System gefunden, wohl aber die Charge
NMVS_FE_LOT_03	#A2	SP-212	Keine Charge gefunden	Die angefragte Seriennummer und Charge sind sowohl im DE-System als auch im EU-Hub unbekannt
NMVS_FE_LOT_13	#A68	SP-212	Chargennummer ungleich	Die angefragte Charge wurde nicht gefunden, die Seriennummer hingegen schon
NMVS_FE_LOT_12	#A52	SP-216	Verfalldatum ungleich	Das angefragte Verfalldatum unterscheidet sich zu dem in System hinterlegtem Verfalldatum zu dieser Packung im Monat oder Jahr
NMVS_NC_PCK_21	#A5	SP-254	Undo von Eigenschaft kann nur der User, der diese gesetzt hat, wirken	Die Packung ist inaktiv und ein anderer User versucht diese wieder aktiv zu setzen

Return Code			Beschreibung	Erläuterung
Arvato	SSR	NGDA		
NMVS_NC_PCK_20	#A4	SP-253	Zeitfenster zwischen Setzen und Undo überschritten	Es wurde nach mehr als 10 Tagen versucht eine inaktive Packung wieder auf aktiv zu setzen
NMVS_NC_PC_01	#A1	SP-101	Produktcode nicht bekannt	Der angefragte Produktcode ist weder im DE-System noch im EU-Hub bekannt