

sormas

Dokumentation zur Umsetzung des Löschkonzepts in SORMAS

Version 2.3

Stand 22.11.2022

sormas

Hintergrund

Diese Dokumentation bezieht sich auf den aktuellen Umsetzungsstand des Löschkonzepts. Sie haben nun die Möglichkeit, Löschungen in SORMAS durchzuführen, sobald Sie das Einspielen der von Ihnen gewählten Fristen in der Löschkonfigurationstabelle bei Netzlink in Auftrag gegeben haben.

In dieser Dokumentation erklären wir Ihnen die Hintergründe, wie der Löschmechanismus in SORMAS arbeitet und beschreiben eine Empfehlung für die Löschung von Daten, die in SORMAS hinterlegt sind.

Bitte beachten Sie: Die Verantwortung für den DSGVO-konformen Umgang mit den Daten in Ihrer SORMAS-Instanz und damit auch die Verantwortung für die Löschung dieser Daten liegt bei den Verantwortlichen der Gesundheitsämter.

Wahrung der Vertraulichkeit

Dieses Dokument darf ohne schriftliche Genehmigung des Helmholtz Zentrum für Infektionsforschung weder ganz noch teilweise dupliziert, an Dritte weitergegeben oder anderweitig veröffentlicht werden. Dies gilt nicht für Kopien, die für die interne Verwendung bestimmt sind.

Versionshistorie

Datum/ Uhrzeit	Beschreibung	Kürzel Autor	Version
14.04.2022	Entwurf	bin	0.1
04.05.2022	Entwurf	owi	0.2
12.05.2022	Entwurf	owi	0.3
13.05.2022	Review, inhaltliche Qualitätssicherung HZI	owi	0.4
13.05.2022	Finalisierung des Entwurfs	owi, aha	0.5
09.11.2022	Überarbeitung des Entwurfs, Die aktuelle Dokumentation bildet den Stand der SORMAS-Version 1.76.3 ab.	owi	0.6
10.11.2022	Finale Überarbeitung – Ergänzen eines Disclaimers, Hinzufügen der Handreichung, Bearbeitung letzter Kommentare	Kas	1.0
11.11.2022	Umstrukturierung des Aufbaus	Kas + dma	2.0
14.11.2022	Abstimmung mit gek, aha, KC	Kas	2.1
17.11.2022	Finalisierung	Kas	2.2
22.11.2022	Finalisierung	Owi, kas, jam, aha, KC	2.3

Inhaltsverzeichnis

Hintergrund	2
Wahrung der Vertraulichkeit.....	2
Versionshistorie.....	2
Zielgruppe des Dokumentes.....	4
1. Hintergründe zum Löschen und Begriffserklärungen	4
2.1 Allgemeine Prinzipien der Löschung	4
3 Technische Umsetzung des Löschkonzeptes.....	5
3.1 Benutzeroberfläche	5
3.2 Löschberechtigung	5
3.3 Manuelle Löschung.....	6
3.4 Automatische Löschung	8
3.4.1 Funktionsweise automatisches unwiderrufliches Löschen	9
3.4.2 Referenz-Zeitpunkte für automatisierte Löschrprozesse („deletionreference“).....	9
3.5 Nachweis von Löschvorgängen	10
3.6 Sonderfälle	10
3.6.1 Dubletten.....	10
3.6.2 Störfälle	10
3.6.3 Löschen von eingespielten Backupdaten	10
3.6.4 Protokolldaten	11
3.6.5 Transportsysteme.....	11
3.6.6 SORMAS2SORMAS.....	11
4 Anwendung des Löschkonzepts	11
4.1 Löschrfristen in SORMAS konfigurieren und ändern	11
4.2 Anwendungsempfehlung für in SORMAS gespeicherte Vorgänge.....	13
4.2.1 SARS-CoV-2 infizierte Personen, Indexpersonen (Fall)	13
4.2.2 Enge Kontaktpersonen (Kontakt)	14
4.2.3 Sonstige personenbezogene Daten, die im Rahmen der Kontaktpersonen-	
nachverfolgung erhoben wurden (Kontakt).....	14
4.2.4 Verdachtspersonen und positiv getestete Personen, die nicht von den Ziffern 2 und 3	
des Konzepts erfasst werden (Fall).....	15
4.2.5 Leiharbeitnehmer, Beschäftigte eines Werkunternehmers und Saisonarbeitskräfte ..	16
4.2.6 Einreisende (Einreise)	16

Zielgruppe des Dokumentes

Mit der vorliegenden Dokumentation sollen Gesundheitsämter die Umsetzung des Löschens in SORMAS nachvollziehen und produktiv damit arbeiten können. Grundlage für die Umsetzung in SORMAS ist das Löschkonzept. Dieses ist mit seinen Anlagen Teil des Datenschutzkonzeptes, das im Rahmen von SORMAS entwickelt wurde. Zielgruppe des Datenschutzkonzeptes sind die Datenschutzbeauftragten der Gesundheitsämter, die SORMAS einsetzen. Das vorliegende Dokument basiert auf dem „Umsetzungskonzept Löschen“ und der technischen Dokumentation in GitHub (Wiki: [„Manual & Automatic Deletion“](#)). Im Anhang finden Sie Erläuterung zu den verwendeten Begriffen / Definitionen. Die Beschreibung der Umsetzung des Löschkonzeptes in SORMAS richtet sich an Administrator:innen aller Gesundheitsämter, die SORMAS einsetzen. Ebenfalls kann es für Datenschutzbeauftragte der Gesundheitsämter zum besseren Verständnis zur Festlegung von Löschfristen verwendet werden.

1. Hintergründe zum Löschen und Begriffserklärungen

2.1 Allgemeine Prinzipien der Löschung

Bei den in SORMAS verarbeiteten Daten handelt es sich um personenbezogene Gesundheitsdaten und deshalb um Daten, die einem besonders hohen Schutzbedarf unterliegen.

Um diesem Bedarf gerecht zu werden, wurde ein Datenschutzkonzept ausgearbeitet. Speziell im Löschkonzept wurde festgelegt, in welchen Fällen und in welcher Art und Weise eine Löschung von Vorgängen in SORMAS erfolgen muss.

Zunächst muss es den Benutzer:innen in SORMAS möglich sein, dass **fälschlicherweise angelegte Vorgänge unwiderruflich gelöscht** werden können oder Sie einem **berechtigten Löschrückruf** nachkommen können. Um dies umzusetzen, muss es möglich sein, eine **manuelle Löschung** der Vorgänge durchzuführen. Das bedeutet, dass die Daten aus der Benutzeroberfläche verschwinden, in der Datenbank jedoch zunächst mit einer **Löschvormerkung** versehen werden und für einen bestimmten Zeitraum vorgehalten werden. Dies ermöglicht es, bei einer versehentlichen Löschung, die Vorgänge durch berechnigte Benutzer:innen wiederherstellen zu können. **Nach dem Verstreichen dieser Vorhaltefrist**, werden die Daten ohne Zutun der Benutzer:innen **automatisch unwiderruflich aus SORMAS gelöscht**.

Dieser **automatische Löschrückruf** findet zudem bei Vorgängen Anwendung, die für das Fall- und Kontaktpersonen-Management essentiell sind, eine dauerhafte Speicherung der erhobenen Daten aber nicht rechtskonform ist. Diese Daten müssen nach dem Verstreichen einer Frist ebenfalls automatisch und unwiderruflich aus der Datenbank gelöscht werden. Diese Frist ist jedoch aufgrund geltender Aufbewahrungsfristen deutlich länger, als die Frist bei der manuellen Löschung.

Daten, die in einer Datenbank gelöscht werden, sind für Benutzer:innen in SORMAS nicht mehr verfügbar und damit auch nicht mehr dem unmittelbaren Zugriff durch Datenbankabfragen zugänglich. Bei einer jeden Löschung sind die Daten nicht unmittelbar unwiderruflich gelöscht und können unter bestimmten Umständen durch IT-Spezialisten wiederhergestellt werden. In SORMAS wird dafür gesorgt, dass bei der unwiderruflichen Löschung die gelöschten Daten durch Überschreibung des zuvor für die Speicherung genutzten Speicherplatzes auf dem Server gelöscht werden. Dies führt dazu, dass eine Wiederherstellung durch IT-Spezialisten nach einer unwiderruflichen Löschung nicht mehr möglich ist.

3 Technische Umsetzung des Löschkonzeptes

3.1 Benutzeroberfläche

Den Benutzer:innen werden Informationen über den Löschzeitpunkt von Entitäten in der Benutzeroberfläche angezeigt. Dies ist vor allem für kurzlebige Entitäten, wie z. B. Einreisen von Bedeutung, die eine kurze Löschfrist haben können.

Der Hinweis innerhalb eines Datensatzes enthält den errechneten Löschzeitpunkt als Datumsangabe. Dieses Datum wird bei mehr als 180 Tagen bis zum Löschzeitpunkt in grau angezeigt. Liegt der Löschzeitpunkt 180 oder weniger Tage entfernt, so wird das Datum in rot angezeigt.

Beim Halten des Mauszeigers über das Info-Symbol können die Benutzer:innen weitere Informationen zur Löschfrist des gewählten Datensatzes erhalten (siehe *Abbildung 1*):

Löschung geplant für: (TT.MM.JJJJ)

Datum der letzten Änderung (TT.MM.JJJJ)

Löschzeitraum (XX Jahre)

Wird eine Kernentität in der Benutzeroberfläche geöffnet, zeigt das System das berechnete Löschdatum der Entität an. Ist die geplante Löschung in sechs Monaten oder weniger (180 Tagen) fällig, wird der Text in roter Schrift angezeigt.

Die für Ihre Instanz geltenden Löschfristen können im Menüpunkt Statistik anhand des Datenbankexport über die Checkbox „Löschkonfigurationen“ von berechtigten Benutzer:innen heruntergeladen und eingesehen werden. Diese wird beim manuellen und automatischen Löschen herangezogen und kann durch die Firma Netzlink auf Anweisung einer weisungsberechtigten Person des Gesundheitsamtes angepasst werden (siehe Kapitel 4.1).



Abbildung 1: Anzeige des Löschzeitpunkts („Löschung geplant für 06.11.2032“), des Referenz-Zeitpunkts („Datum der letzten Änderung“) und der Löschfrist („Löschzeitraum“) in der Benutzeroberfläche von SORMAS

3.2 Löschberechtigung

Benutzer:innen mit den Standard-Benutzerrollen „Nationaler Benutzer“ und „Admin“, können die für Deutschland relevanten Kernentitäten löschen. Benutzer:innen mit der Standard-Benutzerrolle „Administrator Überwachungsleitung“ können „Fälle“, „Immunisierungen“, „Ereignisse“ und „Einreisen“ löschen. Diese Rollen besitzen ebenfalls die Berechtigung zum Wiederherstellen der jeweiligen Datensätze.

Die Benutzerrechte, die einer Benutzerrolle zugeordnet werden müssen, um eine Löschung vornehmen zu können sind logisch benannt; es wird die Entität genannt und nach dem Unterstrich ‚delete‘ (engl. für löschen): CASE_DELETE, TASK_DELETE, etc.

Hinweis: Bitte achten Sie darauf, dass eine Benutzerrolle, die Entitäten löschen soll, ebenfalls das Benutzerrecht erhalten muss, die Entitäten anzusehen (z. B. CASE_VIEW, TASK_VIEW, etc.).

Weitere Informationen zur Konfiguration von Benutzerrollen und –rechten finden Sie in der entsprechenden Dokumentation [Benutzerrollenkonzept und Benachrichtigungsfunktion in SORMAS](#), die Beschreibung der Benutzerrechte und der Abhängigkeiten entnehmen Sie bitte folgender Tabelle [SORMAS Standardrollen und Benutzerrechte](#).



Abbildung 2: Pop-Up Fenster "Löschen bestätigen"; "Grund des Löschens"

3.3 Manuelle Löschung

Benutzer:innen mit entsprechenden Berechtigungen steht in SORMAS die Möglichkeit zur Verfügung, einzelne Datensätze (Entitäten) manuell zu löschen. Dies gilt insbesondere für Sondersituationen, wie das Löschen von unberechtigt erhobenen personenbezogenen Daten oder das Löschen von personenbezogenen Daten nach einem berechtigten Löschbegehren einer betroffenen Person. Das manuelle Löschen von einzelnen Datensätzen unterliegt gesonderten Anforderungen und steht somit nur berechtigten Benutzer:innen zur Verfügung.

Diese Benutzer:innen wählen zum Löschen den entsprechenden Datensatz aus und wählen die Option „Löschen“. SORMAS fordert die Benutzer:innen auf, den Löschauftrag zu bestätigen (siehe *Abbildung 2*). Wird dieser bestätigt, so wird der gewählte Datensatz zunächst **in der Datenbank als gelöscht markiert**, aber noch nicht unwiderruflich aus der Datenbank gelöscht. Diese sogenannte **Löschvormerkung** sorgt dafür, dass der Datensatz in der Benutzeroberfläche für Personen ohne Berechtigung, gelöschte Entitäten einzusehen, nicht mehr angezeigt wird. Benutzer:innen, deren Benutzerrolle das Benutzerrecht zum Löschen bzw. Datensätze wiederherzustellen beinhaltet, haben weiterhin Zugriff auf die Daten und können diese wiederherstellen. Die unwiderrufliche Löschung eines Datensatzes aus der Datenbank im Anschluss an die manuelle Löschung erfolgt durch den automatisierten Löschmodus (Cronjob) nach der in der Löschkonfigurations-Tabelle definierten Löschrfrist (siehe Kapitel 3.4).

Folgende **Kernentitäten** können manuell gelöscht werden:

- Fall
- Kontakt
- Ereignis
- Ereignisteilnehmer
- Einreisemeldung

Auch **untergeordnete Entitäten**, die als Inhaltsdaten betrachtet werden, können manuell gelöscht werden und werden entweder 30 Tage (oder der für die jeweilige Entität in der Löschkonfigurationen-Tabelle hinterlegten Löschrfrist) nach der manuellen Löschung oder mit der Löschung der übergeordneten Entität automatisiert unwiderruflich gelöscht.

Dies gilt für die folgenden Entitäten, die in Listen verwaltet werden und direkte oder indirekte untergeordnete Entitäten einer Kernentität sind:

- Aktionen
- Betreuung/Unterbringung/Tätigkeit in Einrichtung
- Klinischer Besuch
- Ereignisgruppe
- Exposition
- Ort (Adressen)
- Personenkontaktdetails
- Vorheriger Krankenhausaufenthalt
- Meldungen
- Aufgaben
- Anrufe

Dies gilt ebenso für Dokumente, diese werden nach der manuellen Löschung durch einen nächtlichen Cronjob aus der Datenbank entfernt.

Eine manuelle Löschung folgender Entitäten führt dazu, dass **verknüpfte Entitäten** ebenfalls zur Löschung vorgemerkt werden:

- **Fall:** Kontakte und Proben, die nicht mit anderen Entitäten verknüpft sind, werden ebenfalls gelöscht.
- **Kontakt:** Proben, die nicht mit anderen Entitäten verknüpft sind, werden gelöscht.
- **Ereignisteilnehmer:** Proben, die nicht mit anderen Entitäten verknüpft sind, werden gelöscht.
- **Ereignis:** Ereignisteilnehmer werden gelöscht.

Auch die Verknüpfung zu anderen Entitäten wird durch eine manuelle Löschung wie folgt entfernt:

- **Fall:** Entfernt die Verknüpfung von verbundenen Kontakten, Proben, Ereignisteilnehmern, Einreisen und Impfungen.
- **Kontakt:** Entfernt die Verknüpfung von verbundenen Proben und Fallexpositionen.
- **Ereignis:** Entfernt die Verknüpfung aller untergeordneter Ereignisse

Eine **Person** (und die damit verknüpfte Impfung) wird immer dann gelöscht, wenn die letzte mit der Person verknüpften Entität (Fall/Kontaktperson/Ereignisteilnehmer) gelöscht wird. Personen, die mit gelöschten Entitäten verknüpft sind, werden den Benutzer:innen also nur dann angezeigt, wenn sie mit einer weiteren nicht gelöschten Entität verknüpft sind.

Wenn eine Entität als gelöscht vorgemerkt ist, kann sie nicht mehr über die **ReST-API** bereitgestellt werden. Dies gilt auch für untergeordnete Entitäten dieser Kernentitäten (z. B. Aufgaben von zur Löschung vorgemerkten Fällen).

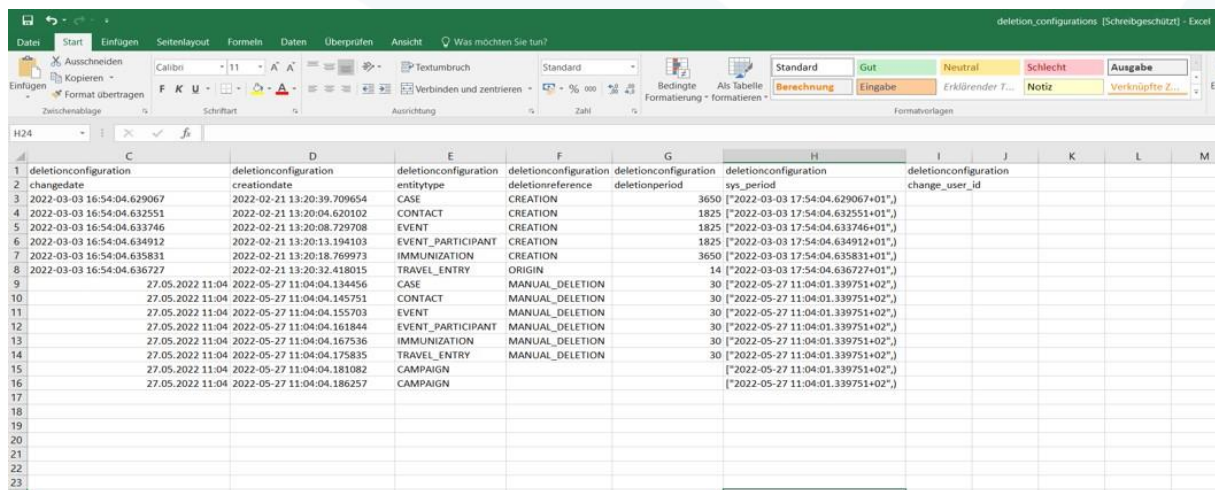
Hinweis für SurvNet: Für manuell gelöschte Fälle und Ereignisse, die ebenfalls in SurvNet vorliegen, wird ein Löschantrag an SurvNet gesendet, sodass die entsprechenden Datensätze auch in SurvNet gelöscht werden.

3.4 Automatische Löschung

Die automatische Löschung setzt die **automatisierte unwiderrufliche Löschung** von Entitäten auf der Grundlage von Löschrufen um, die in der Löschkonfigurationen-Tabelle definiert sind (siehe Abbildung 3). Anhand dieser Löschrufen prüft ein nächtlicher Cronjob in jeder Nacht automatisch, ob ein Datensatz in der Datenbank gelöscht werden muss. Wenn die Löschrufe erreicht oder überschritten (z. B. bei Störfällen siehe Kapitel 3.6.2) wird, wird der Datensatz und alle anhängenden Daten (verknüpfte Entitäten, Dokumente, Änderungshistorie der Entität etc.) unwiderruflich aus der Datenbank gelöscht.

Die **Änderungshistorie** über die vorgenommenen Änderungen an Entitäten wird in Form von Tabellen im Hintergrund der Anwendung angelegt (sog. Logging, siehe auch Wiki in GitHub: [Auditing & Data History](#)). Erfolgt eine Löschung der Entität, werden in dieser Tabelle alle dazugehörigen Felder, Verknüpfungen und verknüpfte untergeordnete Entitäten ebenfalls gelöscht (siehe Kapitel 3.6.4).

Hinweis zu SurvNet: Es werden nur manuelle Löschungen als Löschauftrag an SurvNet übermittelt, da hier davon auszugehen ist, dass die Daten sowohl in SORMAS als auch in SurvNet gelöscht werden müssen (z. B. bei Falscheingaben). Bei Dublettenzusammenführungen wird der obsoletere Datensatz ebenfalls automatisch in SurvNet gelöscht. Automatische Löschungen in SORMAS lösen keinen Löschauftrag in SurvNet aus, die Datensätze in SurvNet folgen den in SurvNet geltenden Löschvorgängen und Löschrufen.



deletionconfiguration	deletionconfiguration	deletionconfiguration	deletionconfiguration	deletionconfiguration	deletionconfiguration	deletionconfiguration	deletionconfiguration	deletionconfiguration	deletionconfiguration
changedate	creationdate	entitytype	deletionreference	deletionperiod	sys_period	change_user_id			
2022-03-03 16:54:04.629067	2022-02-21 13:20:39.709654	CASE	CREATION	3650	("2022-03-03 17:54:04.629067+01")				
2022-03-03 16:54:04.632551	2022-02-21 13:20:04.620102	CONTACT	CREATION	1825	("2022-03-03 17:54:04.632551+01")				
2022-03-03 16:54:04.633746	2022-02-21 13:20:08.729708	EVENT	CREATION	1825	("2022-03-03 17:54:04.633746+01")				
2022-03-03 16:54:04.634912	2022-02-21 13:20:13.194103	EVENT_PARTICIPANT	CREATION	1825	("2022-03-03 17:54:04.634912+01")				
2022-03-03 16:54:04.635831	2022-02-21 13:20:18.769973	IMMUNIZATION	CREATION	3650	("2022-03-03 17:54:04.635831+01")				
2022-03-03 16:54:04.636727	2022-02-21 13:20:32.418015	TRAVEL_ENTRY	ORIGIN	14	("2022-03-03 17:54:04.636727+01")				
27.05.2022 11:04	2022-05-27 11:04:04.134456	CASE	MANUAL_DELETION	30	("2022-05-27 11:04:01.339751+02")				
27.05.2022 11:04	2022-05-27 11:04:04.145751	CONTACT	MANUAL_DELETION	30	("2022-05-27 11:04:01.339751+02")				
27.05.2022 11:04	2022-05-27 11:04:04.155703	EVENT	MANUAL_DELETION	30	("2022-05-27 11:04:01.339751+02")				
27.05.2022 11:04	2022-05-27 11:04:04.161844	EVENT_PARTICIPANT	MANUAL_DELETION	30	("2022-05-27 11:04:01.339751+02")				
27.05.2022 11:04	2022-05-27 11:04:04.167536	IMMUNIZATION	MANUAL_DELETION	30	("2022-05-27 11:04:01.339751+02")				
27.05.2022 11:04	2022-05-27 11:04:04.175835	TRAVEL_ENTRY	MANUAL_DELETION	30	("2022-05-27 11:04:01.339751+02")				
27.05.2022 11:04	2022-05-27 11:04:04.181082	CAMPAIGN			("2022-05-27 11:04:01.339751+02")				
27.05.2022 11:04	2022-05-27 11:04:04.186257	CAMPAIGN			("2022-05-27 11:04:01.339751+02")				

Abbildung 3: Löschkonfigurationstabelle mit Empfehlungen für Löschrufen in Tagen.

Um die automatische Löschung zu aktivieren, müssen die Löschrufen durch Netzlink auf Weisung des jeweiligen Gesundheitsamts über eine **Löschkonfigurationen-Tabelle** konfiguriert werden. Eine detaillierte Beschreibung des Prozesses finden Sie in Kapitel 4.1. Für jeden Entitätstyp sind zwei separate Löschrufen vorgesehen. Eine Löschrufe für das automatische unwiderrufliche Löschen von manuell gelöschten Entitäten und eine Löschrufe für die automatische unwiderrufliche Löschung nach Ablauf der Aufbewahrungsfrist (siehe Abbildung 3).

In dieser Löschkonfigurationen-Tabelle sind folgende Spalten von Relevanz:

- „**entitytype**“ beschreibt die zu löschende Entität (z. B. Fall, Kontakt, Einreisen, Ereignis etc.).
- „**deletionreference**“ beschreibt die Löschrufe, also den Startzeitpunkt, ab dem die Löschrufe gezählt wird, und damit die Berechnungsgrundlage für den Löschrufezeitpunkt. Hierfür werden die untenstehenden Zeitpunkte herangezogen (siehe auch Kapitel 3.4.2):
 - „**CREATION**“: automatisch hinterlegtes Datum, an dem die Entität in SORMAS angelegt wurde (Erstellungsdatum)
 - „**ORIGIN**“: Datum des Ereignisses, welchem die Daten zugrunde liegen (z.B. Einreisedatum)

- „**END**“: Datum, an dem die Bearbeitung der Entität abgeschlossen wurde
- „**MANUAL_DELETION**“: Datum, an dem die Entität manuell gelöscht, also in der Datenbank als gelöscht markiert wurde und in der Benutzeroberfläche nicht mehr angezeigt wurde.
- „**deletionperiod**“ beschreibt die Löschfrist in Tagen

3.4.1 Funktionsweise automatisches unwiderrufliches Löschen

Die automatische unwiderrufliche Löschung der Daten folgt nachfolgendem Prozess: Zunächst werden der zu löschenden Entität untergeordnete Entitäten und Daten aus der Datenbank gelöscht, z. B. Aufgaben, Proben, Behandlungen, Verordnungen, Klinische Besuche, Anrufe. Dies gilt gleichermaßen für Dokumente. Im Detail wird wie folgt gelöscht:

- SORMAS2SORMAS-Metadaten, die gemeinsam genutzt werden, werden gelöscht.
- Fälle und Kontakte werden von zusammengeführten Fällen/Kontakten entkoppelt.
- Verknüpfungen zu anderen Entitäten werden entfernt.
- Die Entität selbst wird aus der Datenbank gelöscht.
- Wenn eine Entität aus der Datenbank gelöscht wird, werden die zugehörigen Einträge in der Historientabelle automatisch mit gelöscht

3.4.2 Referenz-Zeitpunkte für automatisierte Löschrprozesse („deletionreference“)

Für die Umsetzung des automatisierten Löschrprozesses in der Anwendung, ist in erster Linie die effektive Löschrfrist relevant, um den Löschrzeitpunkt zu bestimmen. Der Löschrzeitpunkt wird entweder relativ zur Entstehung der Daten oder zum Verarbeitungsende berechnet.

3.4.2.1 Entstehung der Daten („CREATION“ und „ORIGIN“)

Ein Startzeitpunkt für die automatisierte Löschung ist die „Entstehung der Daten“. Dieser wird durch den Zeitpunkt der Erstellung des Datensatzes in SORMAS definiert („CREATION“). Bitte bedenken Sie, dass das Erstellungsdatum in SORMAS, möglicherweise von dem tatsächlichen Erstellungsdatum, also der initialen Erhebung des Datensatzes abweichen kann (verzögerte Verarbeitung von Labormeldungen, initiale Erfassung von Daten außerhalb von SORMAS). Ggf. sollte eine manuelle Löschung bereits vor Ablauf der hinterlegten Löschrfrist vorgenommen werden.

Ausnahme: Für ereignisbezogene Entitäten, bei denen der Zeitpunkt des Ereignisses relevant für die zugrundeliegende Löschrfrist ist, wird das „Ereignisdatum“ als Startzeitpunkt herangezogen („ORIGIN“).

3.4.2.2 Verarbeitungsende („END“)

Ein weiterer Startzeitpunkt für die automatisierte Löschung ist das „Verarbeitungsende“. Dazu wird der Zeitpunkt herangezogen, ab dem die Daten nicht mehr bearbeitet werden.

Datensätze, deren Bearbeitung beendet ist, können manuell (bei entsprechender Berechtigung der Benutzer:innen) oder automatisch abgeschlossen werden. Abgeschlossene Datensätze lassen sich ausschließlich schreibgeschützt öffnen (Lesezugriff). Sie können nur von Benutzer:innen mit entsprechenden Berechtigungen entsperrt bzw. wiedereröffnet werden, um eine weitere Bearbeitung zu ermöglichen; das zuvor gesetzte Verarbeitungsende wird damit aufgehoben und nach dem erneuten Abschließen neu gesetzt, sofern eine Änderung vorgenommen wurde.

Wenn das **automatische Abschließen** („AUTOMATIC_ARCHIVING“=true) konfiguriert ist und die Daten einer Entität über einen bestimmten Zeitraum nicht bearbeitet werden, werden sie (wenn keine Änderung an der Frist zum automatischen Abschließen bei Netzlink beauftragt wurde) **nach 90 Tagen** abgeschlossen. Dabei wird das letzte aggregierte Änderungsdatum (d. h. das letzte Änderungsdatum des Objekts bzw. seiner Unterobjekte) automatisch als „Verarbeitungsende“ definiert.

Benutzer:innen mit entsprechender Berechtigung können Datensätze **manuell abschließen**. Hierzu muss im Dropdown-Menü die Auswahl „abschließen“ gewählt werden. SORMAS fordert die Benutzer:innen auf das Abschließen des Datensatzes zu bestätigen und informiert darüber, dass der Vorgang den ausgewählten Datensatz nicht löscht, sondern nur für die weitere Bearbeitung schließt. Nach Bestätigung durch die Benutzer:innen wird das aggregierte Änderungsdatum als „Verarbeitungsende“ gespeichert.

Bei einer **Aufhebung des ‚Abgeschlossen‘-Status der Entität** durch berechtigte Benutzer:innen wird das ursprünglich gesetzte „Verarbeitungsende“ automatisch gelöscht.

3.4.2.3 Manuelle Löschung („MANUAL_DELETION“)

Der Referenz-Zeitpunkt „Manuelle Löschung“ berechnet den effektiven Löszeitpunkt anhand der konfigurierten Lösfrist, die mit der manuellen Löschvormerkung beginnt.

Anwendungsfälle sind z. B. das Löschen von unberechtigt erhobenen personenbezogenen Daten und das Löschen von personenbezogenen Daten nach einem berechtigten Löschbegehren einer betroffenen Person. Dazu steht berechtigten Benutzer:innen in SORMAS die manuelle Löschung von Entitäten zur Verfügung. Die manuelle Löschung im ersten Schritt ist eine Vormerkung zur Löschung, die dazu führt, dass die betroffenen Daten nicht mehr in der Benutzeroberfläche zu sehen sind (siehe Kapitel 3.3). In der Datenbank werden die Daten bis Ablauf der in Löschkonfigurationen-Tabelle hinterlegten Lösfristen für manuell gelöschte Entitäten vorgehalten, um bspw. bei versehentlich gelöschten Vorgängen eine Wiederherstellung zu ermöglichen.

3.5 Nachweis von Löschvorgängen

Alle Löschvorgänge werden in SORMAS protokolliert. Auf GitHub steht Ihnen ein Wiki zum Logging zur Verfügung: [Auditing & Data History](#)

3.6 Sonderfälle

Neben der routinemäßigen, automatisierten Umsetzung der Regellöschfristen gibt es eine Reihe von Sonderfällen, in denen ebenfalls das Löschen von personenbezogenen Daten erforderlich ist, dieses aber nicht als Teil der Umsetzung der Regellöschfristen geschehen kann. Die technische Umsetzung dieser Sonderfälle ist nachfolgend beschrieben.

3.6.1 Dubletten

Bei der Zusammenführung von Dubletten (Fälle oder Kontakte) wird jeweils ein Datensatz als führender ausgewählt. Der andere Datensatz wird als Duplikat manuell zur Löschung vorgemerkt und nach Verstreichen der Lösfrist für die jeweilige Entität unwiderruflich aus der Datenbank gelöscht.

3.6.2 Störfälle

Für den Fall, dass die Löschung zeitweise ausgesetzt werden muss (Updateprozesse, unerwartete Probleme etc.) werden die Datensätze mit einer überschrittenen Lösfrist zum nächstmöglichen Zeitpunkt gelöscht. Der nächstmögliche Zeitpunkt entspricht der nächsten Ausführung des Cronjobs zur automatisierten Löschung und die Daten werden aus der Anwendung gelöscht. Dieser Cronjob kann allerdings auch manuell gestartet werden.

3.6.3 Löschen von eingespielten Backupdaten

Um für den Fall eines Systemausfalls eine Datensicherung zu haben, anhand derer eine Instanz wiederhergestellt werden kann, werden im Betrieb von SORMAS regelmäßig Sicherheitskopien der Instanz erstellt. Nach dem Wiederherstellen einer Instanz aus dieser Sicherheitskopie kann es in Abhängigkeit von der Länge des Ausfalls dazu kommen, dass die Lösfrist für einen Datensatz abgelaufen ist, dieser aber durch das Einspielen der Sicherheitskopie eines früheren Zeitpunkts, fälschlicherweise in der Datenbank vorliegt. In diesem Fall erkennt der automatisierte Lösprozess

von SORMAS diese Daten automatisch beim nächsten Durchlauf des nächtlichen Cronjobs und löscht die Daten aus der Anwendung. Ein direkter Durchlauf des Cronjobs, um unmittelbar die zum Löschen markierten Daten unwiderruflich zu löschen kann manuell bei der Wiederherstellung ihrer Instanz bei der Firma Netzlink beauftragt werden.

3.6.4 Protokolldaten

SORMAS legt entsprechend den Vorgaben Protokolldaten von Aktivitäten im System an. Auch diese unterliegen den Löschanforderungen.

Neben der Protokollierung der Inhaltsdaten, legt SORMAS ein Protokoll sämtlicher Aktivitäten auf den Daten an, das sog. AuditLog. Das AuditLog enthält keine expliziten Inhaltsdaten, sondern nur Referenzen auf UUIDs. Darüber hinaus sind im AuditLog Informationen der SORMAS Benutzer:innen protokolliert (z. B. Benutzername). Die Umsetzung der hierfür relevanten Löschfristen erfolgt durch die für den Betrieb beauftragte Firma (im SORMAS@DEMIS Projekt Firma Netzlink Informationstechnik GmbH), auf deren Server die Daten des AuditLogs gespeichert werden.

3.6.5 Transportsysteme

SORMAS erhält und übermittelt Daten an externe Systeme (z. B. Climedo, SurvNet). Dabei können die Daten über eine ReST-API übermittelt werden. Diese Transportdateien werden in SORMAS nicht gespeichert, es bedarf dementsprechend keiner Löschung. Für den Datenaustausch mit SurvNet kommt zusätzlich der SurvNet Konverter zum Einsatz. Über den Konverter werden keine personenbezogenen Daten an die SurvNet Transportverwaltung übertragen.

Hinweis: Es werden nur manuelle Löschungen als Löschauftrag an SurvNet übermittelt, da hier davon auszugehen ist, dass die Daten sowohl in SORMAS als auch in SurvNet gelöscht werden sollen z. B. bei Falscheingaben. Bei Dublettenzusammenführungen wird der obsolete Datensatz ebenfalls automatisch in SurvNet gelöscht. Automatische Löschungen in SORMAS lösen keinen Löschauftrag in SurvNet aus, die Datensätze in SurvNet folgen den in SurvNet geltenden Löschvorgängen und Löschfristen.

3.6.6 SORMAS2SORMAS

Datensätze, die durch SORMAS2SORMAS zwischen SORMAS Instanzen übergeben werden, unterliegen den Löschfristen, die den jeweiligen Datentypen zugeordnet sind. Diese können sich von Gesundheitsamt zu Gesundheitsamt unterscheiden.

Die automatisierte sowie die manuelle Löschung dieser geteilten Datensätze, richtet sich damit nach den festgelegten Löschregeln des Gesundheitsamtes mit Besitz und auch dem mit Leserecht. Damit kann z. B. ein Fall, der im Besitz von Gesundheitsamt A ist, bereits aufgrund der Löschregeln des Gesundheitsamtes A gelöscht sein und gleichzeitig im Gesundheitsamt B, das Leserecht hat und andere Löschregeln als Gesundheitsamt A hat, denselben Fall noch lesen.

4 Anwendung des Löschkonzepts

4.1 Löschfristen in SORMAS konfigurieren und ändern

Die Verantwortung für den rechtmäßigen Umgang mit den erhobenen Daten liegt bei den Gesundheitsämtern. **Wir empfehlen jedoch dringend, die Netzlink Informationstechnik GmbH vor Projektende mit der Konfiguration der Löschfristen und -referenzen zu beauftragen, um die zurzeit gelöscht-markierten Daten nun unwiderruflich aus der Datenbank zu löschen.** Spätestens zum Zeitpunkt der Datenübergabe, sollten die Datenbank bereinigt sein.

Um eine informierte Entscheidung zu ermöglichen, werden den Gesundheitsämtern vier Dokumente zur Verfügung gestellt:

- das inhaltliche *Löschkonzept*
- das technische *Umsetzungskonzept Löschen*
- die für die Gesundheitsämter zusammengefasste *Dokumentation zur Umsetzung des Löschkonzepts in SORMAS* (dieses Dokument)
- eine Anwendungsempfehlung für die Löschkonfiguration als Excel-Datei (entsprechend der Empfehlungen in diesem Dokument)

In Absprache mit den amtsinternen Datenschutzbeauftragten können die empfohlenen Löschkonfigurationen entweder übernommen oder individuell angepasst werden.

Die Konfiguration der unwiderruflichen Löschung kann ausschließlich durch weisungsberechtigte Personen gegenüber Netzlink (im AV-Vertrag benannt) beauftragt werden. Das bedeutet, dass die weisungsberechtigte Person die Löschkonfigurationen-Tabelle, die für das Amt gelten soll, mit folgendem Text an den Netzlink-Support unter support@sormas-oegd.de zurückschickt (die zu befüllenden Textpassagen sind gelb hinterlegt):

Betreff: „Beauftragung zur Konfiguration der Löschfristen und -referenzen“

Hiermit weise ich,, die Firma Netzlink Informationstechnik GmbH an, für das Gesundheitsamt, die Löschfristen gemäß [der vorliegenden Empfehlung / laut der von uns spezifizierten Vorgabe] in die SORMAS Instanz unseres Gesundheitsamtes zu übernehmen.

Wichtig: Solange keine Weisung an die Netzlink Informationstechnik GmbH erfolgt, wird keine Löschung der vorliegenden Daten durchgeführt. Als verantwortliche Stelle obliegt es dem Gesundheitsamt die Löschung von Daten in SORMAS anzuweisen.

Hinweis: Die Löschkonfigurationen-Tabelle, die für die jeweilige Instanz gilt, wird ab der Version 1.76 im Datenbank-Export unter den „Konfigurationsdaten“ zum Download bereitgestellt.

Bei auftretenden Fragen zum Löschen steht der inhaltlichen Support über sormas-covid@helmholtz-hzi.de oder über die Rufnummer **0531-61811109** zur Verfügung.

Der notwendige, manuelle Vorgang zur Anpassung der Löschfristen durch Update Statements auf der Datenbank wurde erfolgreich getestet und als sog. Playbook auf der Automationsplattform hinterlegt. Dieses Playbook wird bei Bedarf mit den Vorgaben des beauftragenden Gesundheitsamtes auf der Datenbank der jeweiligen Instanz im Livebetrieb ausgeführt. Durch die Automation ist die Qualität gesichert und ein unnötiger manueller Zugriff auf die Datenbank ausgeschlossen. Ein Restart der Instanz ist nicht notwendig.

Folgende Statements werden aufgrund der Entwicklervorgaben mittels des Playbook ausgeführt:

- Für Einreisemeldedaten

```
UPDATE public.deletionconfiguration SET deletionreference='ORIGIN',  
deletionperiod=TT WHERE entitytype='TRAVEL_ENTRY' and  
deletionreference IS NULL;
```

(TT=Angabe der Löschfrist in Tagen)

- Für endgültige Löschung nach manueller Löschung über die Oberfläche

```
UPDATE public.deletionconfiguration SET deletionperiod=TT WHERE  
deletionreference='MANUAL_DELETION';
```

(TT=Angabe der Löschfrist in Tagen)

4.2 Anwendungsempfehlung für in SORMAS gespeicherte Vorgänge

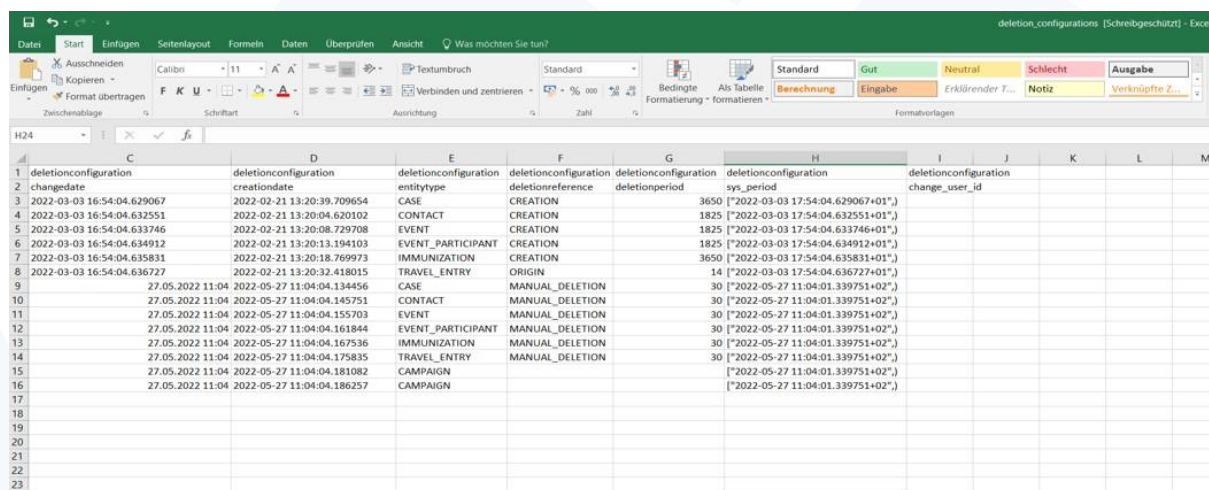
In Zusammenarbeit mit den Datenschutzbehörden wurden Empfehlungen für eine Löschung der in SORMAS hinterlegten Vorgänge erarbeitet.

Nachdem wir Ihnen nun die Grundlagen des Löschsens beschrieben haben, möchten wir Ihnen nun eine Anwendungsempfehlung an die Hand geben, wie eine Umsetzung des Löschkonzeptes in SORMAS praktisch umgesetzt aussehen kann.

Die erarbeiteten Löschkonfigurationen erhalten Sie als Orientierung. Im Folgenden wird ein Bezug zu den in SORMAS hinterlegten Vorgänge hergestellt und die Löschung dieser Vorgänge erläutert.

In der vorliegenden Löschkonfigurationen-Tabelle wird die jeweilige Entität in Spalte E genannt (,entitytype'), das herangezogene Referenzdatum in Spalte F (,deletionreference') und die Löschrfrist in Tagen in Spalte G (,deletionperiod'). Die automatische Löschrfrist beträgt für Fälle und Immunisierungen 10 Jahre und für Kontakte, Ereignisse und Ereignisteilnehmer 5 Jahre nach Erstellungszeitpunkt (deletionreference = ,CREATION'). Einreisen werden bereits 14 Tage nach dem Einreisedatum (,deletionreference = ,ORIGIN') gelöscht. Im zweiten Teil ab Zeile 9 wird beschrieben, wann manuell gelöschte Entitäten unwiderruflich aus der Datenbank gelöscht werden. Dies beträgt für alle Entitäten 30 Tage nach der manuellen Löschung. Die in Spalte 14 und 15 benannte Entität ,CAMPAIGN' ist für Deutschland nicht relevant und deshalb nicht gefüllt.

Hinweis: Bitte bedenken Sie, dass das Erstellungsdatum in SORMAS, möglicherweise von dem tatsächlichen Erstellungsdatum, also der initialen Erhebung des Datensatzes abweichen kann (verzögerte Verarbeitung von Labormeldungen, initiale Erfassung von Daten außerhalb von SORMAS). Ggf. sollte eine manuelle Löschung bereits vor Ablauf der hinterlegten Löschrfrist vorgenommen werden.



A	B	C	D	E	F	G	H	I	J	K	L	M
1	deletionconfiguration	creationdate	entitytype	deletionreference	deletionperiod	sys_period	deletionconfiguration	change_user_id				
2	changedate											
3	2022-03-03 16:54:04.629067	2022-02-21 13:20:39.709654	CASE	CREATION	3650	["2022-03-03 17:54:04.629067+01"]						
4	2022-03-03 16:54:04.632551	2022-02-21 13:20:04.620102	CONTACT	CREATION	1825	["2022-03-03 17:54:04.632551+01"]						
5	2022-03-03 16:54:04.633746	2022-02-21 13:20:08.729708	EVENT	CREATION	1825	["2022-03-03 17:54:04.633746+01"]						
6	2022-03-03 16:54:04.634912	2022-02-21 13:20:13.194103	EVENT_PARTICIPANT	CREATION	1825	["2022-03-03 17:54:04.634912+01"]						
7	2022-03-03 16:54:04.635831	2022-02-21 13:20:18.769973	IMMUNIZATION	CREATION	3650	["2022-03-03 17:54:04.635831+01"]						
8	2022-03-03 16:54:04.636727	2022-02-21 13:20:32.418015	TRAVEL_ENTRY	ORIGIN	14	["2022-03-03 17:54:04.636727+01"]						
9	27.05.2022 11:04	2022-05-27 11:04:04.134456	CASE	MANUAL_DELETION	30	["2022-05-27 11:04:01.339751+02"]						
10	27.05.2022 11:04	2022-05-27 11:04:04.145751	CONTACT	MANUAL_DELETION	30	["2022-05-27 11:04:01.339751+02"]						
11	27.05.2022 11:04	2022-05-27 11:04:04.155703	EVENT	MANUAL_DELETION	30	["2022-05-27 11:04:01.339751+02"]						
12	27.05.2022 11:04	2022-05-27 11:04:04.161844	EVENT_PARTICIPANT	MANUAL_DELETION	30	["2022-05-27 11:04:01.339751+02"]						
13	27.05.2022 11:04	2022-05-27 11:04:04.167536	IMMUNIZATION	MANUAL_DELETION	30	["2022-05-27 11:04:01.339751+02"]						
14	27.05.2022 11:04	2022-05-27 11:04:04.175835	TRAVEL_ENTRY	MANUAL_DELETION	30	["2022-05-27 11:04:01.339751+02"]						
15	27.05.2022 11:04	2022-05-27 11:04:04.181082	CAMPAIGN			["2022-05-27 11:04:01.339751+02"]						
16	27.05.2022 11:04	2022-05-27 11:04:04.186257	CAMPAIGN			["2022-05-27 11:04:01.339751+02"]						

Abbildung 4: Löschkonfigurationen-Tabelle mit Empfehlungen für Referenzen und Löschrfristen in Tagen.

4.2.1 SARS-CoV-2 infizierte Personen, Indexpersonen (Fall)

Wir empfehlen, die personenbezogenen Daten von positiv auf SARS-CoV-2 getestete und dementsprechend mit SARS-CoV-2 infizierten Personen (gemäß der Falldefinition des Robert-Koch-Instituts) **zehn Jahre nach der Erhebung der Daten** zu löschen.

Hierfür müssen die Löschrparameter wie folgt definiert werden:

entitytype	deletionreference	deletionperiod
CASE	CREATION	3650

4.2.2 Enge Kontaktpersonen (Kontakt)

Wir empfehlen die Daten von engen Kontaktpersonen **fünf Jahren nach der Erhebung** aus der Datenbank zu löschen.

Auch Kontaktpersonen, die positiv auf SARS-CoV-2 getestet wurden, werden derart behandelt. Es bestehen zwei Datensätze (Kontakt, Fall) zur gleichen Person. Um diese Daten zu löschen, müssen die Datensätze beider Entitäten gelöscht werden. Mit der bereits durchgeführten Konfiguration der Löschparameter für SARS-CoV-2 Infizierte Personen (s. Kapitel 4.2.1) ist für die Entität „Fall“ keine weitere Aktion erforderlich.

Hierfür müssen die Löschparameter wie folgt definiert werden:

entitytype	deletionreference	deletionperiod
CONTACT	CREATION	1825

4.2.3 Sonstige personenbezogene Daten, die im Rahmen der Kontaktpersonennachverfolgung erhoben wurden (Kontakt)

Werden im Rahmen der Kontaktpersonennachverfolgung personenbezogene Daten von Personen erhoben, die vom Gesundheitsamt nachträglich nicht als enge Kontaktperson eingestuft wurden und die weder nach einer bei Ihnen geltender Verordnung oder Allgemeinverfügung noch durch sonstige behördliche Anordnung einer Absonderungspflicht, einem Selbst-Monitoring oder Tätigkeitsverbot unterworfen wurden, empfehlen wir **diese Daten umgehend zu löschen**, sobald diese für die unmittelbare Kontaktnachverfolgung nicht mehr benötigt werden.

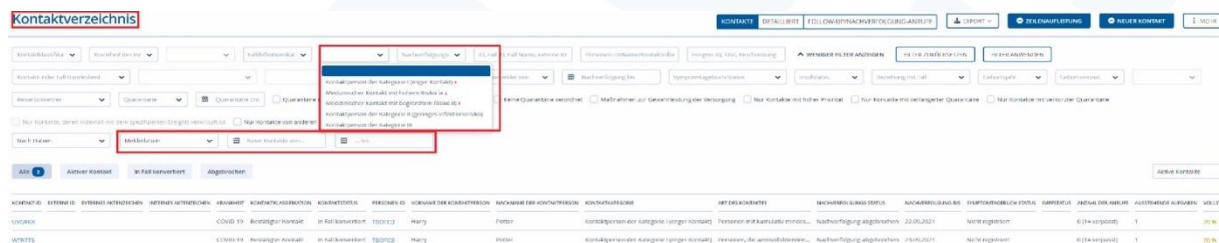


Abbildung 5: Filtereinstellungen zur Änderung der Kontaktkategorie (1)

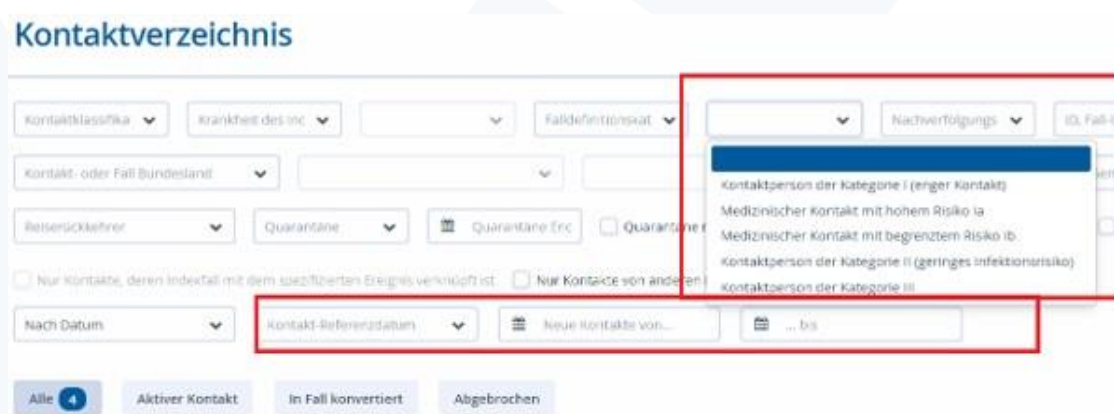


Abbildung 6: Filtereinstellungen zur Änderung der Kontaktkategorie (2)

Dies gilt beispielsweise auch für personenbezogene Daten von Kunden, Gästen oder Veranstaltungsteilnehmern, die von den Verantwortlichen i. R. d. Kontaktdatenerhebung erhoben

worden sind, und die die Gesundheitsämter zum Zwecke der Kontaktpersonennachverfolgung angefordert haben, sofern diese Personen nicht in eine der o. g. Kategorien fallen.

Die o. g. Gruppen werden in SORMAS als „Kontaktpersonen der Kategorie II (geringes Infektionsrisiko)“ oder „Kontaktpersonen der Kategorie III“ gekennzeichnet. Diese müssen ebenfalls über das Kontaktverzeichnis durch die Angabe des Filters „Meldedatum“ tagesgenau herausgefiltert werden. Abhängig vom Löschintervall ist der Filter-Zeitraum in folgenden Einheiten zu setzen (Tag, Woche, Monat). Der Filter ist auf jede der Kategorien anzuwenden (siehe *Abbildung 5* und *Abbildung 6*).

Anschließend an die Filterung sind die Vorgänge über den Massенbearbeitungsmodus zu löschen (siehe *Abbildung 7* und *Abbildung 8*). Sollten Sie die Personen nicht als Kontaktpersonen der Kategorie II (geringes Infektionsrisiko)“ oder „Kontaktpersonen der Kategorie III“ erfasst worden sein, sind die Filtereinstellungen entsprechend anzupassen.

Hinweis: Alle manuell gelöschten Daten werden erst nach dem Verstreichen der für die manuelle Löschung festgelegte Löschfrist unwiderruflich gelöscht.

4.2.4 Verdachtspersonen und positiv getestete Personen, die nicht von den Ziffern 2 und 3 des Konzepts erfasst werden (Fall)

Bei der Dokumentation von Verdachtsfälle in SORMAS gibt es kein einheitliches Vorgehen. Die Klassifizierung kann sich unterscheiden. Diese Verdachtsfälle müssen ebenfalls manuell durch Auswahl dieser anhand von Filtereinstellungen gelöscht werden.

Wir empfehlen Ihnen die erhobenen Daten sind innerhalb von **vier Jahren** nach Erhebung zu löschen.

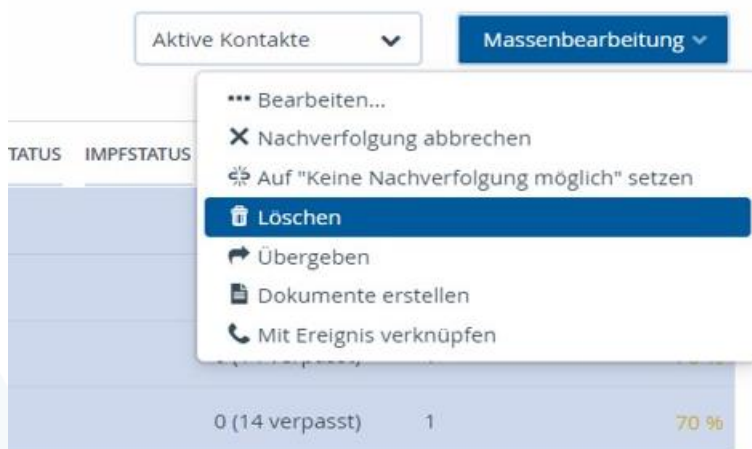


Abbildung 7: Auswahl der manuellen Löschvormerkung über die Massenbearbeitung

Die o. g. Gruppen können in SORMAS als Kategorie „0. nicht klassifiziert“ oder „X. kein Fall“ klassifiziert werden. Diese Datensätze können über das Fallverzeichnis durch die Angabe des Filters „Meldedatum“ tagesgenau herausgefiltert werden. Abhängig vom Löschintervall ist der Filter-Zeitraum in folgenden Einheiten zu setzen (Tag, Woche, Monat). Nach dem Herausfiltern der betroffenen Fälle können diese markiert und über die Massenbearbeitung manuell gelöscht werden.

Hinweis: Sollten Sie die Datensätze nicht einheitlich in einer Kategorie gekennzeichnet worden sein, empfehlen wir die Kategorisierung nachzuziehen bzw. die Filtereinstellungen entsprechend anzupassen.



Abbildung 8: Auswahl des "Grund des Löschsens" zur manuellen Löschvormerkung.

4.2.5 Leiharbeitnehmer, Beschäftigte eines Werkunternehmers und Saisonarbeitskräfte

Wir empfehlen Ihnen Daten zur Kontaktnachverfolgung von Leiharbeitnehmern, Beschäftigten eines Werkunternehmers und Saisonarbeitskräften in landwirtschaftlichen Betrieben **vier Wochen nach dem Zeitpunkt des Verlassens des Betriebs** bzw. **nach Außerkrafttreten einer Verordnung, die zum Erfassen dieser Daten aufruft**, zu löschen.

Für diese Personengruppe konnte ebenfalls kein standardisiertes Vorgehen für die Erfassung in SORMAS festgelegt werden. Aus diesem Grund empfehlen wir Ihnen diese Daten unter Berücksichtigung der Erfassung manuell zu filtern und zu löschen.

4.2.6 Einreisende (Einreise)

Wir empfehlen Ihnen personenbezogene Daten von Einreisenden **14 Tage nach dem mitgeteilten Datum der Einreise** zu löschen. Entsprechendes gilt für personenbezogene Daten bzw. Testergebnisse Einreisender, die nach früherer Rechtslage an die Gesundheitsämter übermittelt wurden.

Die Löschung der Daten von Einreisenden kann ebenfalls automatisiert erfolgen. Hierfür müssen die Löschparameter wie folgt definiert werden:

entitytype	deletionreference	deletionperiod
TRAVEL_ENTRY	ORIGIN	14