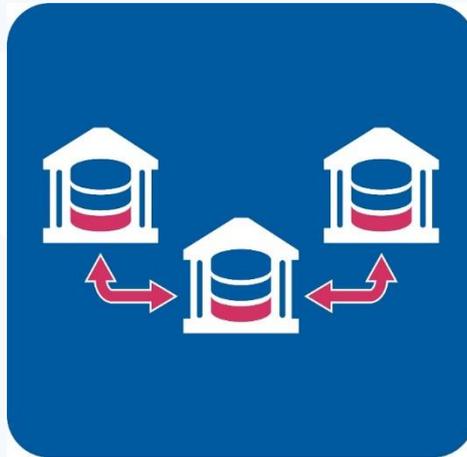


sormas

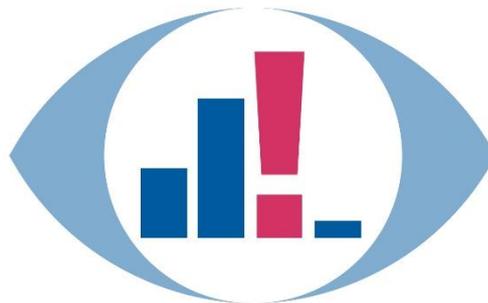
[VERTRAULICH]



Umsetzung des Löschkonzeptes für SORMAS-X

Version 1.0.1

Stand 28.04.2022



COVID-19 SORMAS-ÖGD Deutschland

Wahrung der Vertraulichkeit

Dieses Dokument darf ohne schriftliche Genehmigung des Helmholtz-Zentrums 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.

Versionsübersicht

Version	Datum	Autor	Gepr.	Beschreibung
14_SORMAS-X_Umsetzungskonzept-Löschen_V1.0.0_220308	08.03.2022	SH	KGE, GSO	Initiale Erstellung
14_SORMAS-X_Umsetzungskonzept-Löschen_V1.0.1_220428	28.04.2022	KS	DM	Wasserzeichen hinzugefügt

Inhaltsverzeichnis

Inhaltsverzeichnis

1	Klassifizierung des Umsetzungskonzeptes-Löschen.....	5
2	Geltungsbereich/Einführung.....	5
3	Allgemeine Prinzipien der Löschung von Daten in SORMAS-X.....	6
4	Bestimmung des effektiven Löschezitpunkts.....	6
	Startzeitpunkt „Entstehung der Daten“.....	6
4.1.1	Sonderfall „Zeitpunkt des Ereignisses“.....	7
4.1	Startzeitpunkt „Ende des Vorgangs“.....	7
4.2.1	Ende der Bearbeitung eines Vorgangs.....	8
4.2	4.2.2 Sonderfall „Endes der Beziehung zur betroffenen Person“.....	9
	Startzeitpunkt „Manuelle Löschkennzeichnung“.....	9
4.3.5	Automatisierter technischer Löschkprozess.....	10
	Festlegung der effektiven Löschkfrist pro Feld.....	10
5.1	Automatische Ausführung der Löschung.....	11
5.2	5.2.1 Löschen von Person und Visits.....	11
	5.2.2 Löschung aus Audit History.....	11
6	Umsetzung der Löschung im Betrieb.....	12
7.1.7	Technische Umsetzung des Löschens in Sonderfällen.....	13
7.2	Backupdaten.....	13
7.3	Doubletten.....	13
7.4	Störfälle.....	13
7.5	Löschen von eingespielten Backupdaten.....	13
7.6	Protokolldaten (Logging).....	13
7.7	Transportsysteme.....	14
	SORMAS2SORMAS.....	14
8	Manuelle Löschung von Daten in SORMAS-X.....	14
11.1	9 Information über zu löschende Daten in der Benutzungsoberfläche.....	15
11.2	10 Protokollierung von Löschvorgängen.....	16
11.3	11 Anhang.....	17
	Abkürzungsverzeichnis.....	17
	Abbildungsverzeichnis.....	17
	Tabellenverzeichnis.....	17
	Quellenverzeichnis.....	17

sormas

	Regelverzeichnis	17
12	Änderungshistorie	18
	Änderungen von der vorherigen Version zur aktuellen Version	18

11.5

12.1

sormas

1 Klassifizierung des Umsetzungskonzepts-Löschen

Die Dokumentation des Umsetzungskonzepts-Löschen ist ein wesentlicher Teil des Sicherheitsprozesses des Gesundheitsamt Musterstadt und sollte entsprechend des Klassifikationsschemas des Gesundheitsamt Musterstadt gekennzeichnet und behandelt werden.

In Anlehnung an den ‚BSI-Standard 200-2, IT-Grundschutzmethodik‘, Abschnitt 5, Dokumentation im Sicherheitsprozess‘ könnten die Informationen des Umsetzungskonzeptes-Löschen wie folgt klassifiziert werden.

Gewährleistungsziel ‚Vertraulichkeit‘	
Umsetzungskonzept-Löschen	Vertraulich
Gewährleistungsziel ‚Integrität‘	
Umsetzungskonzept-Löschen	wichtig
Gewährleistungsziel ‚Verfügbarkeit‘	
Umsetzungskonzept-Löschen	Eine Woche

Tabella 1: Klassifikation ‚Umsetzungskonzept-Löschen‘

2 Geltungsbereich/Einführung

Dieses Dokument ist ein internes Dokument im Rahmen der SORMAS-X-Datenschutz Dokumentation, das die im Dokument 14_SORMAS-X_Löschkonzept und seinen 13 Anlagen beschriebenen Anforderungen des automatisierten und manuellen Löschens in der SORMAS-X Software beschreibt. Das SORMAS-X-Löschkonzept nebst Anlagen beinhaltet die Vorgaben und Anforderungen für ein datenschutzkonformes Löschen in der Software. Beschrieben sind die verschiedenen Szenarien, in denen ein Löschen erforderlich wird. Dies betrifft nicht nur das routinemäßige Löschen nach dem Ablauf der gesetzlichen Aufbewahrungsfristen der Daten, sondern z.B. auch das Löschen in manuellen Prozessen oder von Datenträgern.

Die tatsächliche Umsetzung der in diesem Dokument beschriebenen technischen Vorgaben des automatisierten Löschens sind in einem weiteren Dokument beschrieben.

Beschrieben werden die technischen Maßnahmen, die in im Rahmen der Softwareentwicklung von SORMAS-X in der Anwendung umgesetzt werden.

3 Allgemeine Prinzipien der Löschung von Daten in SORMAS-X

Bei den in SORMAS-X verarbeiteten personenbezogenen Daten handelt es sich um Gesundheitsdaten und damit um Daten, die einem besonders hohen Schutzbedarf unterliegen. Die für das Löschen der Daten in der SORMAS-X-Software erforderlichen Löschfristen sind in der Datenfeldertabelle für jedes einzelne Feld, das sich in der Software befindet, festgelegt (Name des Dokuments und aktuelle Version Datenfeldertabelle eintragen). Diese Löschfristen werden den Gesundheitsämtern zunächst als Voreinstellung mit ausgeliefert, es ist aber möglich diese nach den individuellen Erfordernissen in den Gesundheitsämtern anzupassen.

Das Löschen in SORMAS-X erfolgt automatisiert auf Feld- bzw. Entitätsebene. Es werden immer zuerst Datenfelder in den entsprechenden Entitäten, deren Aufbewahrungsfrist abgelaufen ist, gelöscht. Im letzten Schritt wird die Entität selbst gelöscht.

Die vorgesehenen Aufbewahrungsfristen („Löschklassen“) der Daten in der Anwendung sind in Anlage 01 zum Löschkonzept im Detail beschrieben und begründet (siehe Dokument 14-01_SORMAS-X_Löschkonzept_AnI01_V2-1_211125).

In Kapitel 4 werden die Komponenten, die zum automatisierten Löschen in der Anwendung notwendig sind, beschrieben. Dies beinhaltet die Definition der Startzeitpunkte und effektiven Löschfristen sowie die Beschreibung wie diese im System konfiguriert werden können.

Kapitel 5 beschreibt anschließend den technischen Löschvorgang, der nach Ablauf der effektiven Löschfrist automatisch ausgelöst wird und in der Entfernung der Daten aus der Anwendungsdatenbank resultiert.

In Kapitel 6 wird auf die Maßnahmen beim Betrieb des Systems und der Datenbanken eingegangen, die für eine sichere Löschung der Anwendungsdaten sorgen.

In Kapitel 7 wird das Löschen in Sonderfällen beschrieben und in Kapitel 8 auf die Möglichkeit des manuellen Löschens über die Benutzungsoberfläche eingegangen.

In den Kapiteln 9 und 10 werden abschließend die Darstellung von Löschfristen auf der Benutzungsoberfläche sowie die Protokollierung von Löschvorgängen beschrieben.

4 Bestimmung des effektiven Löschzeitpunkts

Für die Umsetzung des automatisierten Löschrates in der Anwendung ist in erster Linie die effektive Löschfrist relevant, um den Löschzeitpunkt zu bestimmen (vgl. Abb. 1).

- 4.1 Der Löschzeitpunkt wird entweder relativ zur Entstehung der Daten (Kap. 4.1) oder zum Ende des Vorgangs (Kap. 4.2) berechnet. Eine Beschreibung der entsprechenden Zeitpunkte in Hinblick auf die Umsetzung ist in den folgenden Kapiteln gegeben. Diese werden jeweils als eigene Löschraten implementiert, die dann zur Konfiguration der tatsächlichen Löschraten verwendet werden können.

Startzeitpunkt „Entstehung der Daten“

Der erste Bezugstyp für die automatisierte Löschung ist die „Entstehung der Daten“ (siehe Abb. 1). Dieses wird durch den Zeitpunkt der Erstellung des Datensatzes im System definiert (Ausnahme siehe

Sonderfall Kapitel 4.1.1). Die Berechnung des effektiven Löschezitpunkts erfolgt hier also relativ zum automatisch gefüllten Datumsfeld *creationDate*.

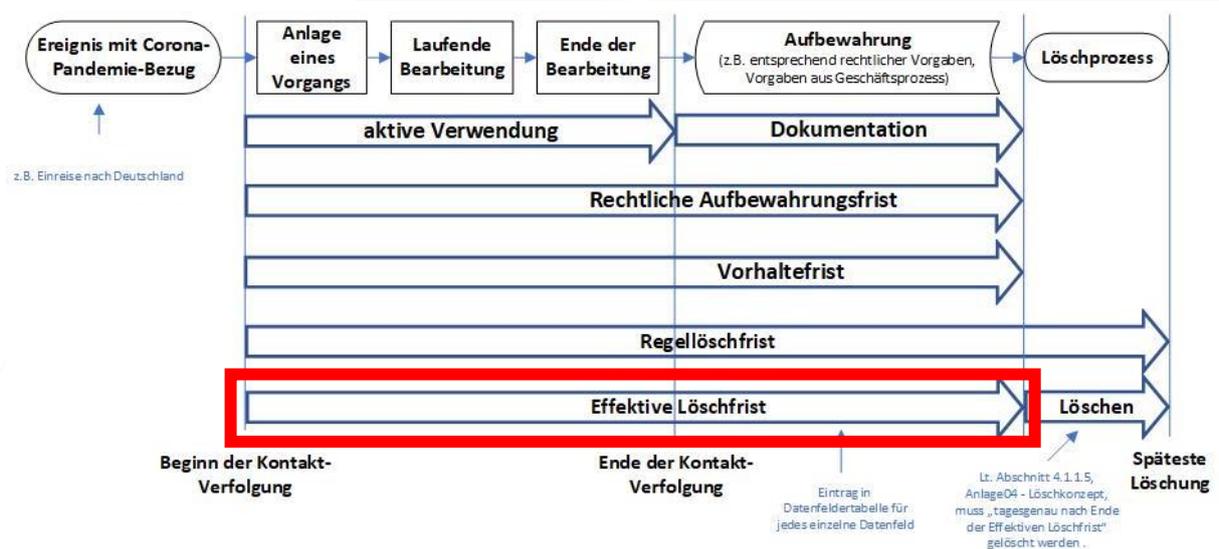


Abbildung 1: Startzeitpunkt "Entstehung der Daten"

4.1.1 Sonderfall „Zeitpunkt des Ereignisses“

Für ereignisbezogene Entitäten, bei denen der Zeitpunkt des Ereignisses relevant für die zugrundeliegende Löschrfrist ist, wird das „Ereignisdatum“ als Startzeitpunkt herangezogen. Dies betrifft derzeit das Einreisedatum (vgl. Abb. 1) – dort wird also das Pflichtfeld *arrivalDate* zur Berechnung des effektiven Löschezitpunkts verwendet. In der Umsetzung ist hierfür ein eigener Bezugstyp definiert.

Startzeitpunkt „Ende des Vorgangs“

Ein weiterer wesentlicher Bezugstyp für die automatisierte Löschung ist das „Ende des Vorgangs“ (siehe Abb.2). Hier wird das automatisch befüllte *endOfProcessDate* zur Berechnung des effektiven Löschezitpunkts verwendet. In den folgenden Abschnitten sind die hierfür relevanten Prozesse in der Anwendung beschrieben.

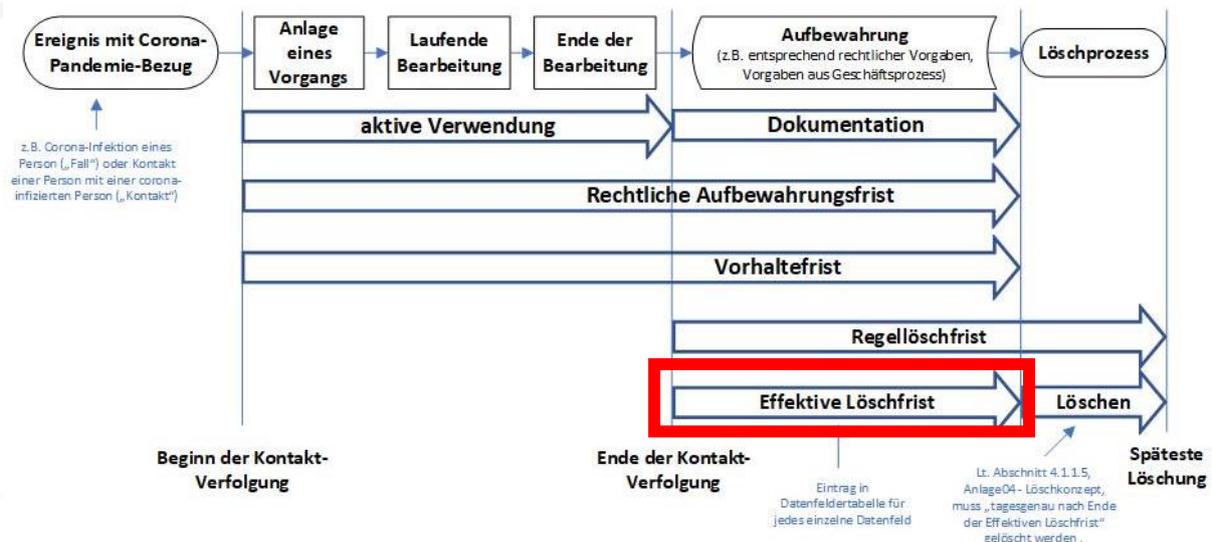


Abbildung 2: Startzeitpunkt "Ende des Vorgangs"

4.2.1 Ende der Bearbeitung eines Vorgangs

Daten deren Bearbeitung beendet ist, können manuell (bei entsprechender Berechtigung des Benutzers) oder automatisch abgeschlossen werden. Wird ein Datensatz abgeschlossen, wird dieser in einer anderen Ansicht in der Anwendung dargestellt.

Abgeschlossene Datensätze sind von der weiteren Bearbeitung ausgeschlossen und im abgeschlossenen Zustand nicht mehr editierbar. Sie lassen sich zu Dokumentations- und Informationszwecken von Benutzern mit entsprechenden Berechtigungen schreibgeschützt öffnen (Lesezugriff).

Abgeschlossen Datensätze können von Benutzern mit entsprechenden Berechtigungen entsperrt bzw. wieder aktiviert werden, um eine weitere Bearbeitung zu ermöglichen. Das Ende des Vorgangs wird damit aufgehoben und nach dem erneuten Abschließen neu gesetzt.

Bei Abschluss eines Vorgangs wird für den betreffenden Datensatz als "Ende der Bearbeitung" das letzte Änderungsdatum (*endOfProcessDate*) am Datensatz gespeichert.

4.2.1.1 Automatisches Abschließen der Bearbeitung

Alle Kernentitäten (Core Entities), die im SORMAS-X System innerhalb eines definierten Zeitraums (Default 90 Tage) nicht bearbeitet werden, werden vom System automatisch in den Status „abgeschlossen“ versetzt. Dabei wird das letzte aggregierte Änderungsdatum¹ automatisch als „Ende der Bearbeitung“ im System festgesetzt.

Dies ist durch einen täglich ausgeführten Cronjob umgesetzt, der automatisch alle Datensätze auf ihr aggregiertes Änderungsdatum überprüft. Ein CronJob ist eine Aufgabe, die automatisiert im Betriebssystem abläuft (CRON = Command Run On Notice).

¹ Letztes Änderungsdatum des Objekts bzw. seiner Unterobjekte

4.2.1.2 Manuelles Abschließen der Bearbeitung

Dem Nutzer steht in SORMAS-X die Möglichkeit zur Verfügung Datensätze manuell abzuschließen. Das Abschließen von Datensätzen unterliegt einem Systemrecht (vergleiche Dokumente „12_SORMAS-X_Berechtigungskonzept_V2-2_211101“ und „12_SORMAS-X_Umsetzungskonzept-Berechtigung_VO-5_220208“) und steht somit nur entsprechend zugewiesenen Nutzern zur Verfügung.

Der Nutzer wählt zum „Abschließen“ den entsprechenden Datensatz aus und aktiviert die Option „abschließen“ (siehe SORMAS Benutzerhandbuch, Kap. 2.1)². Das System fordert den Nutzer 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 den Nutzer setzt das System das aggregierte Änderungsdatum als „Ende der Bearbeitung“.

4.2.1.3 Aufhebung des Abschlusses

Hebt der Nutzer mit der entsprechenden Berechtigung den Abschluss eines Datensatzes auf, wird das gesetzte „Ende der Bearbeitung“ automatisch gelöscht und der Nutzer muss einen Grund für die Aufhebung des Abschlusses angeben.

4.2.2 Sonderfall „Endes der Beziehung zur betroffenen Person“

Der im Löschkonzept noch erwähnte Begriff des „Endes der Beziehung zur betroffenen Person“ als Startzeitpunkt für den Beginn der Aufbewahrungsfrist ist das Ende der Bearbeitung eines Vorgangs: endet eine Beziehung zu einer betroffenen Person, z.B. weil der Fall an ein anderes Gesundheitsamt abgegeben wird, endet auch die Bearbeitung des entsprechenden Vorgangs.

4.3 Startzeitpunkt „Manuelle Löschvormerkung“

Der Bezugstyp und Startzeitpunkt „Manuelle Löschvormerkung“ (aufgrund des vorzeitigen Endes eines Vorgangs) berechnet den effektiven Löschezitpunkt anhand der für diesen Fall definierten Löschrfrist (Standard 90 Tage) relativ zur manuellen Löschvormerkung durch einen berechtigten Benutzer.

² <https://www.sormas-oegd.de/dokumente/>

**Fristabschnitte im SORMAS-X-Löschkonzept:
Manuelle Festlegung der vorzeitigen Löschung mit
Startzeitpunkt ‚vorzeitiges Ende eines Vorgangs (vEV)‘**

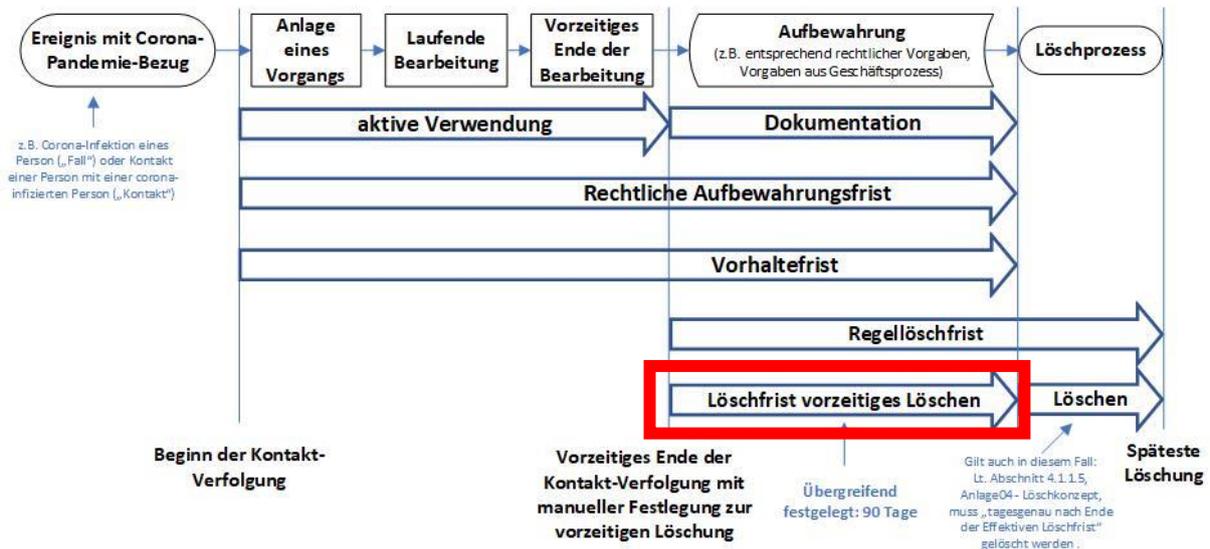


Abbildung 3: Startzeitpunkt "Manuelle Löschkonfirmation"

Dieser Fall umfasst z.B. das Löschen von unberechtigt erhobenen personenbezogenen Daten und das Löschen von personenbezogenen Daten nach einem berechtigten Löschauftrag einer betroffenen Person. Für diese Zwecke steht Benutzern der Anwendung mit entsprechenden Berechtigungen in SORMAS-X über die Benutzungsoberfläche die Funktionalität zur manuellen Löschung von Entitäten zur Verfügung (siehe Kap. 8).

Die manuelle Löschung ist im ersten Schritt eine Vormerkung zur Löschung, die dazu führt, dass die betroffenen Daten nicht mehr in den Auflistungen für aktive und abgeschlossene Vorgänge gelistet werden.

5 Automatisierter technischer Löschkonzept

Um die automatisierte Löschung einzelner Datenfelder und ganzer Entitäten durchführen zu können, muss im System eine Löschkonfiguration hinterlegt werden, die dann zur Umsetzung der automatisierten Löschung verwendet wird.

5.1

In den folgenden Kapiteln wird der technische Löschkonzept innerhalb der Anwendung SORMAS-X beschrieben. Maßnahmen zur sicheren Löschung der Daten, die den Betrieb des Systems betreffen, sind im darauffolgenden Kapitel 6 beschrieben.

Festlegung der effektiven Löschkonzept pro Feld

Die Löschkonfiguration für Entitäten und Felder wird in einer Datenbanktabelle hinterlegt. Sie gibt jeweils für eine Entität oder einzelne Felder der Entität an, welches der Löschauftragstyp und die effektive Löschkonzept in Tagen ist.

Die Löschkonfiguration erfolgt dabei für die Core Entitäten *Case*, *Contact*, *Event*, *Event Participant* und *TravelEntry* und umfassen jeweils deren untergeordnete Entitäten (z.B. *Symptoms*, *EpiData*, *Samples*). Felder von untergeordneten Entitäten werden in der Löschkonfiguration als Pfad relativ zur Core Entität konfiguriert (z.B. *Case.symptoms.temperature*).

Das Hinterlegen der Löschkonfiguration erfolgt aus Anwendersicht anhand der Datenfeldertabelle (vgl. Dokument ‚40_SORMAS_Datenfelder_Vnnn‘ in der aktuellen Version) als Konfigurationsdatei. In dieser wird jedem einzelnen Datenfeld der Anwendung die besagte effektive Löschrfrist in Tagen und der Bezugstyp für den Beginn der Löschrfrist zugewiesen (vgl. Kap. 4). Diese Konfigurationsdatei kann bei Bedarf angepasst und vom Systemadministrator auf Anfrage beim Anlagen-Betreiber Netzlink im System hinterlegt werden. Sie wird beim Start des Systems automatisch eingelesen und als Löschkonfiguration in die Datenbank übernommen.

Automatische Ausführung der Löschung

5.2 Ein täglicher Cronjob (Ausführung standardmäßig nachts) prüft alle Datensätze automatisch auf die berechneten Löschrzeitpunkte. Ist der Löschrzeitpunkt für Datensätze erreicht oder überschritten (siehe Backups, Störfälle), wird der Datensatz und alle anhängenden Daten (abhängige Daten, History Tables, etc.) gelöscht.

Eine Entität wird erst gelöscht, wenn alle ‚abwärts‘ verbundenen Entitäten auch gelöscht wurden („Löschen von außen nach innen“).

Das Löschen einer Entität bedeutet, dass diese per DELETE Befehl aus der jeweiligen Datenbanktabelle gelöscht wird. Die Löschung einzelner Felder erfolgt, indem der Datensatz per UPDATE Befehl angepasst wird. Diese Löschung erfolgt also jeweils unmittelbar bei der Ausführung des Cronjobs.

5.2.1 Löschen von Person und Visits

Ein Sonderfall bei der Löschung stellen die Entitäten *Person* und *Visit* dar, da diese zeitgleich von mehreren Core Entitäten referenziert werden können (z.B. *Person* ist sowohl *Contact*, als auch *Case verbunden*). *Person* und *Visit* haben keine eigenständige automatische Löschung, sondern werden dann gelöscht, wenn die letzte Core Entität, die auf sie verweist, gelöscht wurde.

5.2.2 Löschung aus Audit History

Protokolldaten zu Änderungen an Inhaltsdaten in SORMAS-X werden in Form von History Tables in der Anwendungsdatenbank angelegt (vergleiche Dokument ‚32_SORMAS-X_Logging_V1-4_211021‘ und ‚32_SORMAS-X_Umsetzungskonzept-Logging_V1-1_220217‘). In den History Tables werden historische personenbezogene Inhaltsdaten von SORMAS-X dokumentiert.

Erfolgt eine Löschung der Ursprungsdaten, werden alle dazugehörigen History Table Einträge entsprechend Entitäten- und feldbezogen gelöscht.

Wird ein einzelnes Feld einer Entität gelöscht stellt das System sicher, dass auch alle Einträge zu diesem Feld aus den History Tables gelöscht werden. Die Identifizierung des zu löschenden Eintrags in der jeweiligen History Table erfolgt dabei anhand der gleich lautenden Spaltennamen und der eindeutigen Datenbank ID des Datensatzes.

Wird eine ganze Entität gelöscht, so werden in der Datenbank automatisch auch alle zugehörigen Einträge in den History Tables gelöscht.

6 Umsetzung der Löschung im Betrieb

Daten, die in der Datenbank gelöscht werden, sind dadurch nicht mehr unmittelbar dem Zugriff durch Datenbankabfragen zugänglich. Die Daten sind allerdings noch nicht unmittelbar physikalisch gelöscht und könnten noch theoretisch wieder gelesen werden.

Die Datenbank-Software stellt einen Prozess bereit (VACUUM), der genutzt werden kann, um gelöschte Daten auch physisch auf der Festplatte zu löschen. VACUUM kann sowohl automatisch ausgeführt werden (AUTOVACUUM) als auch explizit per Hand gestartet werden.

Derzeit ist AUTOVACUUM so konfiguriert, dass es abhängig von bestimmten Parametern automatisch Tabellenplatz freigibt.

Die Konfigurationsparameter für AUTOVACUUM sind:

Parameter	Wert
Autovacuum	on
autovacuum_analyze_scale_factor	0.1
autovacuum_analyze_threshold	50
autovacuum_freeze_max_age	200000000
autovacuum_max_workers	3
autovacuum_multixact_freeze_max_age	400000000
autovacuum_naptime	60
autovacuum_vacuum_cost_delay	20
autovacuum_vacuum_cost_limit	-1
autovacuum_vacuum_scale_factor	0.2
autovacuum_vacuum_threshold	50
autovacuum_work_mem	-1
log_autovacuum_min_duration	-1

Die Einstellungen sind derzeit so gewählt, dass AUTOVACUUM Speicherplatz in einer Tabelle freigibt, sobald mehr als 50 gelöschte oder aktualisierte Datensätze vorhanden sind. AUTOVACUUM wird nicht explizit per cronjob zeitgesteuert gestartet.

Nach der Freigabe von Festplattenplatz durch VACUUM wird der freie Plattenplatz dem Betriebssystem zum neu Beschreiben zur Verfügung gestellt. Theoretisch ist es jetzt noch möglich, bei physikalischem Zugriff auf die Festplatte mit Hilfe von Tools zur Datenrettung Daten wieder herzustellen. Allerdings ist hierfür ein Zugriff auf die Speichersysteme des Infrastruktur-Betreibers (im Produktionsfall ITZBund) nötig. Es wird davon ausgegangen, dass dieser physische Zugang nicht erlangt werden kann. Deswegen wird von Seiten des Projektes davon ausgegangen, dass eine Wiederherstellung von Daten nach der Ausführung von VACUUM nicht mehr möglich ist.

Version 1.0.1 Stand 28.04.2022

7 Technische Umsetzung des Löschens in Sonderfällen

Abseits 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.

Backupdaten

Backupdaten unterliegen ebenfalls einer Löschregel (vgl. Anlage 02 – Umsetzungsvorgaben für Querschnittsbereiche, Dokument 14-02_SORMAS-X_Lösckonzept_An102_V1-1_211201).

- 7.1 Weiterhin kann beim Zurückspielen von Backups ins System die Löschung von zurückgespielten Daten in der Anwendung relevant sein. In diesem Fall werden Daten mit einer überschrittenen Löschrfrist zum nächstmöglichen Zeitpunkt gelöscht (siehe Kapitel 7.4).

Doubletten

- 7.2 Bei der Zusammenführung von Doubletten (zwei gleiche Fälle oder zwei gleiche Kontakte), wird jeweils ein Datensatz als führender ausgewählt, in den die korrekten Daten übernommen werden. Der andere Datensatz wird als Duplikat gelöscht. Dabei wird am zu löschenden Datensatz ein Verweis auf den zusammengeführten Datensatz eingetragen. Anschließend folgt der Datensatz dem Prozess des manuellen Löschens (siehe Kap. 8).

7.3 Störfälle

Für den Fall, dass die Löschung zeitweise ausgesetzt werden muss (Updateprozesse, unerwartete Probleme etc.) werden die Datensätze mit einer überschrittenen Löschrfrist zum nächstmöglichen Zeitpunkt gelöscht.

- 7.4 Der nächstmögliche Zeitpunkt entspricht der nächsten Ausführung des Cronjobs zur automatisierten Löschung (siehe Kapitel 5) und die Daten werden aus der Anwendung gelöscht.

Löschen von eingespielten Backupdaten

- 7.5 Um für den Fall eines Systemausfalls ein Datensicherung zu haben, die wieder zurückgespielt werden kann, werden im Betrieb von SORMAS-X regelmäßig Systembackups erstellt (vergleiche Dokument ,15_SORMAS-X_Datensicherung_ITZBünd_V1-3_211029'). Nach dem Zurückspielen der Backupdaten kann es in Abhängigkeit von der Länge des Ausfalls dazu kommen, dass Datensätze ihre Löschrfrist überschritten haben, nach dem Zurückspielen aber noch bzw. wieder im System vorliegen. In diesem Fall erkennt der automatisierte Löschrprozess von SORMAS-X diese Daten automatisch beim nächsten Durchlauf des Cronjobs (siehe Kap. 5) und die Daten werden aus der Anwendung gelöscht.

Protokolldaten (Logging)

Das SORMAS-X System legt entsprechend den Vorgaben Protokolldaten von Aktivitäten im System an (vergleiche Dokument ,32_SORMAS-X_Logging_V1-4_211021'). Auch diese unterliegen den Löschanforderungen.

Neben der Protokollierung der Inhaltsdaten (siehe Kap. 5.2.2) legt SORMAS-X ein Protokoll sämtlicher Aktivitäten auf den Daten an, das Audit Log. Das Audit Log enthält keine expliziten Inhaltsdaten, sondern nur Referenzen auf UUIDs. Darüber hinaus sind im Audit Log Informationen der SORMAS-X

Benutzer protokolliert (z.B. Benutzername). Die Umsetzung der hierfür relevanten Löschfristen obliegt dem Betrieb von SORMAS-X, in dessen Kontext die Daten des Audit Logs gespeichert werden (vgl. Anlage 02 – Umsetzungsvorgaben für Querschnittsbereiche).

Transportsysteme

SORMAS-X erhält und übermittelt Daten an externe Systeme (z.B. Climedo, SurvNet). Dabei werden die Daten über eine ReST API übermittelt, die keine Daten speichert und somit keine Löschung erfordert.

- 7.6 Für den Datenaustausch mit SurvNet kommt zusätzlich die Komponente SurvNet Connector zum Einsatz. Auch dort werden keine personenbezogenen Daten gespeichert und lediglich UUIDs als Referenzen in eine Logdatenbank geschrieben (vergleiche Dokument ‚32_SORMAS-X_Logging_V1-4_211021‘ und ‚32_SORMAS-X_Umsetzungskonzept-Logging_V1-1_220217‘).

SORMAS2SORMAS

- 7.7 Datensätze, die mittels SORMAS2SORMAS Funktionalität zwischen SORMAS Instanzen transferiert werden, unterliegen den Löschfristen, die den jeweiligen Datentypen zugeordnet sind. Dh. es finden für diese Datensätze keine gesonderten Löschfristen Anwendung. Die automatisierte sowie die manuelle Löschung dieser Datensätze richtet sich damit nach den festgelegten Löschregeln des jeweiligen GA.

8 Manuelle Löschung von Daten in SORMAS-X

Benutzern mit entsprechenden Berechtigungen in der Anwendung steht in SORMAS-X 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 geschulten Nutzern zur Verfügung.

Der Nutzer wählt zum Löschen den entsprechenden Datensatz aus und wählt die Option „Löschen“. Das System fordert den Nutzer auf, den Löschauftrag zu bestätigen und eine Begründung für die Löschung anzugeben. Dabei ist es erforderlich aus folgenden Optionen zu wählen oder eine Begründung in einem Freitextfeld anzugeben:

- Löschen auf Anforderung der betroffenen Person nach DSGVO
- Löschen auf Anforderung einer anderen Behörde
- Entität (z.B. Fall) ohne Rechtsgrund angelegt
- Abgabe eines Vorgangs bei Nicht-Zuständigkeit des GA
- Löschen von Doubletten
- Andere Begründung

Bestätigt der Nutzer die Löschung des gewählten Datensatzes, wird diese im System als gelöscht markiert, aber noch nicht aus dem System gelöscht (*soft delete*). Die Löschkennzeichnung sorgt dafür, dass der Datensatz in der Anwendung nicht mehr gelistet wird, er kann aber noch durch Benutzer geöffnet werden, die die Löschberechtigung haben.

Die Funktionalität des manuellen Löschsens ist für folgende Entitäten im System verfügbar:

- Fall
- Kontakt
- Ereignis
- Ereignisteilnehmer
- Einreisemeldung

Die tatsächliche Löschung aus dem System (*hard delete*) des Datensatzes erfolgt durch den automatisierten Löschrprozess nach der definierten Löschrfrist, wie in Kapitel 4.3 und 5 beschrieben.

9 Information über zu löschende Daten in der Benutzungsoberfläche

Dem Nutzer werden Informationen über den Löschrzeitpunkt von Daten in der Benutzungsoberfläche zur Verfügung gestellt. Dies ist vor allem für kurzlebige Entitäten, wie z.B. Einreisemeldungen von Bedeutung, die eine Löschrfrist von nur 14 Tagen haben können. Informationen über die Löschrfrist sind für jeden Datensatz erkennbar:

Hinweis innerhalb eines Datensatzes

- mit einem Löschrdatum innerhalb von 180 Tagen oder weniger
 - farbliche Markierung
 - Einblendung des errechneten Löschrzeitpunktes als Datumsangabe
- mit einem Löschrdatum von über 180 Tage
 - keine gesonderte Darstellung
 - Einblendung des errechneten Löschrzeitpunktes als Datumsangabe

Weitergehende Informationen zum Löschrdatum

Auf Nachfrage kann der User weitere Informationen zur Löschrfrist des gewählten Datensatzes erhalten:

- Datum der geplanten Löschung (10.11.2031)
- Datum der Startzeitpunktes (09.11.2031)

- Definierte Löschfrist (10 Jahre)
- Auskunft darüber, welche Felder gelöscht werden

10 Protokollierung von Löschvorgängen

Alle Löschvorgänge werden im System protokolliert. Eine Beschreibung der Protokollierungsfunktionen findet sich im Loggingkonzept (vergleiche Dokument ‚32_SORMAS-X_Logging_V1-4_211021‘ und ‚32_SORMAS-X_Umsetzungskonzept-Logging_V1-1_220217‘).

11 Anhang

Abkürzungsverzeichnis

Abkürzung	Beschreibung
11.1 CRON	Command Run On Notice; automatisierte Aufgabe Berechtigungskonzeptim Betriebssystem
DSGVO	Datenschutz-Grundverordnung
GA	Gesundheitsamt
GÄ	Gesundheitsämter
SORMAS	Surveillance Outbreak Response Management and Analysis System
SORMAS-X	SORMAS eXchange

Abbildungsverzeichnis

11.2	Abbildung 1: Startzeitpunkt "Entstehung der Daten"	7
	Abbildung 2: Startzeitpunkt "Ende des Vorgangs"	8
	Abbildung 3: Startzeitpunkt "Manuelle Löschvormerkung"	10

11.3 Tabellenverzeichnis

	Tabelle 1: Klassifikation ‚Umsetzungskonzept-Löschen‘	5
--	---	---

11.4

Quellenverzeichnis

Abkürzung	Titel	Herausgeber/Verlag	Jahr
11.5			

Regelverzeichnis

Bezeichnung	Regel/Norm/Standard/Richtlinie	Jahr

12 Änderungshistorie

Version	Datum	Beschreibung
14_SORMAS-X_Umsetzungskonzept-Löschen_ V1-0_vg_220228	28.02.2022	Initialfassung

Änderungen von der vorherigen Version zur aktuellen Version

Das vorliegende Dokument ist die Initialversion. Deswegen gibt es noch keine Änderungsangaben.

12.1