Lösch- und Aufbewahrungskonzept

Sentinel System / Virtueller Bürger-Schreibtisch / Schuldnerberatung

Version 1.0 · Stand 09.10.2026
Anlage zum Datenschutz- und Sicherheitskonzept

Offene Fristen und Arbeitswerte sind ausdrücklich keine produktiven Zusagen. Sie werden erst nach technischer und rechtlicher Verifikation festgelegt.

1. Zweck

Dieses Konzept beschreibt die Grundsätze für Aufbewahrung, Sperrung, Löschung und technische Bereinigung personenbezogener Daten innerhalb des Virtuellen Bürger-Schreibtischs und der angeschlossenen Schuldnerberatungsfunktionen.

Es ergänzt die zentralen technischen und organisatorischen Maßnahmen von Sentinel System sowie die produktspezifischen TOMs.

Grundprinzip ist:

Personenbezogene Daten werden nicht allein deshalb dauerhaft gespeichert, weil technisch Speicherplatz zur Verfügung steht.

Aufbewahrungsdauer und Löschung richten sich nach Zweck, Vertragsverhältnis, gesetzlichen Pflichten und erforderlichen Sicherheits- beziehungsweise Nachweisinteressen.

2. Unterschiedliche Arten von Löschen

Für Sentinel werden vier Zustände ausdrücklich unterschieden.

Fachliche Löschung

Ein Objekt steht dem Bürger beziehungsweise der Beratungsstelle nicht mehr zur Verfügung und wird aus dem aktiven Fachbestand entfernt.

Zugriffsentzug

Die Daten bleiben technisch vorhanden, ein bestimmter Benutzer oder Empfänger darf aber nicht mehr darauf zugreifen. Der Widerruf einer Beratungsfreigabe ist zunächst kein Löschen des Bürgerdokuments.

Technische Löschung

Das Objekt wird aus dem produktiven Datenspeicher entfernt.

Backup-Rotation

Bereits vorhandene Sicherungskopien werden nicht zwingend synchron mit dem Produktivbestand verändert. Gelöschte Produktivdaten verschwinden entsprechend der jeweiligen Aufbewahrungsfrist zeitversetzt aus Sicherungssystemen.

Es wird deshalb nicht behauptet, dass Daten in derselben Sekunde aus sämtlichen Sicherungskopien verschwinden.

3. Grundsätze

Für die Löschung gelten insbesondere:

- Zweckbindung: Daten werden nicht länger als für ihren Zweck erforderlich gespeichert.
- Datenminimierung: Nicht benötigte Daten werden nicht vorsorglich unbegrenzt aufbewahrt.
- Mandantentrennung: Eine Löschung in einem Bürgerkonto darf keine Daten eines anderen Kontos beeinträchtigen.
- Nachvollziehbarkeit: Sicherheitsrelevante Löschvorgänge können protokolliert werden.
- Backupsicherheit: Eine Löschung im Produktivsystem führt nicht zur nachträglichen Manipulation unveränderter Sicherungskopien.
- Gesetzliche Pflichten: Gesetzlich erforderliche Aufbewahrung hat Vorrang vor einer vertraglichen Löschfrist, soweit sie tatsächlich einschlägig ist.

4. Löschmatrix

Die Arbeitsmatrix unterscheidet Ereignis, Behandlung im Produktivsystem, Backup und Umsetzungsstatus.

Offene Fristen bleiben bewusst offen, bis die tatsächlichen technischen Jobs und gesetzlichen Anforderungen festgelegt wurden.

Bürgerkonto	Kontolöschung/Vertragsende	zu löschen	Rotation	Frist festlegen
Dokumente	Löschung durch Berechtigten	zu löschen	Rotation	Frist festlegen
private Notizen	Löschung/Kontolöschung	zu löschen	Rotation	Frist festlegen
Verfahrenslinien	Vorgang/Konto gelöscht	zu löschen	Rotation	Frist festlegen
OCR-Daten	Dokument gelöscht	mit Dokumentbezug löschen	Rotation	prüfen
KI-Ergebnisse	Dokument/Vorgang gelöscht	zu löschen	Rotation	Anbieter prüfen
Schuldendaten	Vorgang/Konto gelöscht	zu löschen	Rotation	Frist festlegen
Beratungsfreigabe	Widerruf	sofort Zugriff entziehen	Historie ggf. erhalten	umgesetzt
Beraterzuordnung	Widerruf/Entfernung	sofort entziehen	Audit	umgesetzt
Sessions	Logout/Sperre/Entfernung	widerrufen	–	umgesetzt
Passkeys	Widerruf/Kontolöschung	deaktivieren/löschen	ggf. Audit	umgesetzt
Recovery-Codes	Verwendung/Neuerstellung	ungültig	–	umgesetzt
Beratungs-ZIP	Ablauf/Widerruf	Zugriff sperren/löschen	ggf. Rotation	Frist festlegen
Demo-Daten	Reset	ersetzen	Reset-Sicherung	gesondert
Security-Logs	Fristablauf	löschen/anonymisieren	Rotation	Frist festlegen
Abrechnungsdaten	Vertragsende	gesetzliche Fristen	Backup	gesetzlich bestimmen
Supportdaten	Abschluss + Frist	löschen	Rotation	Frist festlegen
Kommunikationsdaten	Zweckende + Frist	löschen	Rotation	kanalabhängig

Offener Prüfpunkt: Fristen, Anbieterretention und gesetzliche Anforderungen technisch und rechtlich verifizieren.

5. Löschung durch den Bürger

Der Bürger soll im Rahmen der angebotenen Funktionen eigene Inhalte löschen können.

Eine Löschung darf dabei nicht nur die Darstellung im Browser entfernen.

Serverseitig muss der betreffende Datensatz beziehungsweise das betreffende Dokument dem Löschprozess zugeführt werden.

Bei miteinander verknüpften Objekten ist zu prüfen, ob abhängige Daten ebenfalls gelöscht werden müssen oder aus Gründen der Datenintegrität lediglich die Verbindung entfernt wird.

6. Dokumentlöschung und Verfahrenslinie

Wenn ein Bürger ein Dokument löscht, dürfen daraus nicht unbemerkt vollständige Dokumentinhalte in der Verfahrenslinie dauerhaft weiterleben.

Unterschieden werden:

- Originaldokument
- OCR-/Extraktionsdaten
- Dokumentmetadaten
- Verknüpfungen
- Verfahrenslinien-Eintrag
- KI-Auswertung

Beim Löschen eines Dokuments muss festgelegt werden, welche davon ebenfalls gelöscht werden und welche Informationen gegebenenfalls aus zwingenden Integritäts- oder Nachweisgründen erhalten bleiben.

Die Oberfläche darf einen verbleibenden Verfahrenslinien-Eintrag nicht so darstellen, als existiere das gelöschte Original weiterhin.

Offener Prüfpunkt: Abhängige Löschregeln für Dokument, OCR, Metadaten, Verfahrenslinie und KI-Ergebnis technisch festlegen.

7. Beratungsfreigabe ist keine Datenübertragung des gesamten Kontos

Wird eine Beratungsfreigabe widerrufen, wird nicht das zugrunde liegende Bürgerdokument gelöscht.

Bürgerdokument bleibt beim Bürger → Freigaberecht wird entzogen → Berater verliert Zugriff → zukünftiger Download wird gesperrt

8. Bereits heruntergeladene Daten

Ein späterer Widerruf kann keine Datei von einem fremden Computer oder Fachsystem technisch zurückholen.

Der Widerruf beendet den weiteren Zugriff über Sentinel. Bereits rechtmäßig an einen Empfänger übermittelte oder von ihm heruntergeladene Daten unterliegen anschließend dessen eigenen datenschutzrechtlichen Pflichten.

Das gilt insbesondere für Beratungsstellen, Behörden und sonstige Empfänger.

9. Ende einer Beratung

Das Ende einer Schuldnerberatung führt nicht automatisch zur Löschung des gesamten Bürgerkontos.

Stattdessen können getrennt beendet werden:

Beraterzugriff → Beraterzuordnung → Beratungsfreigabe → gegebenenfalls institutioneller Arbeitsbestand

Der persönliche Bürger-Schreibtisch kann unabhängig davon weiterbestehen.

10. Löschen eines Bürgerkontos

Bei vollständiger Kontolöschung müssen mindestens geprüft beziehungsweise entfernt werden:

- Account
- Profileinstellungen
- Dokumente
- Dokumentmetadaten

- Vorgänge
- Verfahrenslinien
- Fristen
- private Notizen
- Gruppenmitgliedschaften
- Freigaben
- Beraterverknüpfungen
- Passkeys
- Recovery-Daten
- aktive Sessions
- KI-Ergebnisse
- personenbezogene Rechercheaufträge
- noch vorhandene Exportpakete

Gesetzlich erforderliche Abrechnungs- oder Nachweisdaten werden getrennt vom aktiven Bürgerkonto aufbewahrt.

11. Authentisierungsdaten

Sessions

Bei Logout, Kontosperre, sicherheitsrelevanter Passwortänderung, erfolgreicher Recovery oder Benutzerentfernung werden die jeweils vorgesehenen Sitzungen widerrufen.

Passkeys

Passkeys können einzeln beziehungsweise vollständig widerrufen werden. Bei Kontolöschung werden die zugehörigen aktiven Credentials entfernt beziehungsweise dauerhaft ungültig gemacht.

Recovery-Codes

Ein verwendeter Recovery-Code kann nicht erneut eingesetzt werden. Neu erzeugte Recovery-Codes ersetzen beziehungsweise invalidieren die vorherige Serie entsprechend der Implementierung.

12. Gruppen und Freigaben

Wird ein Mitglied entfernt, werden dessen Gruppenzugehörigkeiten, direkte Rechte, Sessions, Passkeys beziehungsweise entsprechende Zugriffsmittel und Freigaben nach dem dokumentierten Lebenszyklus bereinigt beziehungsweise widerrufen.

Das Entfernen eines Mitglieds darf nicht lediglich dessen Menüeintrag ausblenden.

13. Exporte

Exportpakete, insbesondere Beratungs-ZIPs, sind keine dauerhaften Primärspeicher.

Für temporär serverseitig erzeugte Exporte wird als technischer Arbeitswert eine kurze automatische Lebensdauer von 24 Stunden vorgeschlagen.

Danach soll das serverseitige Exportartefakt automatisch gelöscht werden. Der Export kann bei fortbestehender Berechtigung erneut erzeugt werden.

Offener Prüfpunkt: Arbeitswert von 24 Stunden gegen tatsächliche Exportablage und Bereinigungsjobs prüfen, bevor er produktiv zugesichert wird.

14. KI-Daten

Sentinel-seitige KI-Ergebnisse

Gespeicherte KI-Auswertungen werden mit dem zugehörigen Objekt beziehungsweise Vorgang verbunden und entsprechend dessen Löschlebenszyklus behandelt.

Externe KI-Anbieter

Sentinel kann eine Löschung nur entsprechend den technischen und vertraglichen Möglichkeiten des jeweiligen Anbieters gewährleisten.

Vor produktiver Aktivierung jedes externen KI-Dienstes werden übertragene Daten, Eingabespeicherung, Speicherdauer, Trainingsnutzung, Verarbeitungsort und Löschmöglichkeiten dokumentiert.

Offener Prüfpunkt: Unterauftragnehmer- und KI-Anlage je produktivem Anbieter vervollständigen.

15. Kommunikationsdaten

Kommunikationsdaten können anderen gesetzlichen und praktischen Anforderungen unterliegen als normale Dokumente.

Zu unterscheiden sind beispielsweise:

- Entwurf
- gesendete Nachricht
- empfangene Nachricht
- Versandnachweis
- Zustellinformation
- technisches Transportprotokoll

Ein Versandnachweis kann länger benötigt werden als eine temporäre Versanddatei. Hierfür werden kanalabhängige Fristen festgelegt.

Offener Prüfpunkt: Kanalabhängige Aufbewahrungsfristen festlegen.

16. eBO-Kommunikation

Für eBO-/EGVP-bezogene Kommunikation können Nachweise über Versand, Empfänger, Zeitpunkt und Zustellstatus fachlich relevant sein.

Diese werden deshalb nicht automatisch mit kurzfristigen technischen Logs gleichgesetzt.

Zertifikatsgeheimnisse werden nur so lange gespeichert, wie sie für die entsprechende Funktion erforderlich und vom Nutzer hinterlegt sind.

17. Security- und Audit-Logs

Die Aufbewahrung soll ausreichend Historie bieten, um Angriffe, unberechtigte Zugriffe, Freigabeänderungen, Recovery-Vorgänge und Sicherheitsvorfälle untersuchen zu können, aber nicht unbegrenzt erfolgen.

- normale technische Logs: 30 Tage als Arbeitswert
- sicherheitsrelevante Auditdaten: 180 Tage als Arbeitswert
- besondere nachweispflichtige Vorgänge: gegebenenfalls länger

Offener Prüfpunkt: Arbeitswerte sind noch keine festgelegte Sentinel-Regel und müssen gegen Log-Rotation, Zwecke und Rechtsgrundlagen geprüft werden.

18. Backups

Produktiv gelöschte Daten können entsprechend der Borg-Retention noch Bestandteil verschlüsselter Sicherungskopien sein.

Sicherungskopien werden nicht als Archiv zur weiteren regulären Verarbeitung verwendet.

Die technische Retention umfasst sieben tägliche, vier wöchentliche und sechs monatliche Archive.

Ein vollständiger Datencheck und eine Testextraktion konsistenter JSON- und SQLite-Stores wurden erfolgreich durchgeführt.

Bei einer Wiederherstellung eines älteren Backups muss verhindert werden, dass bereits gelöschte oder widerrufene Daten unbeabsichtigt wieder produktiv verfügbar werden.

Offener Prüfpunkt: Backup und technischer Restore verifiziert; fachliche Post-Restore-Reconciliation bleibt umzusetzen.

19. Demo- und Testdaten

Für Präsentationsumgebungen sollen grundsätzlich künstliche beziehungsweise hierfür freigegebene Testdaten verwendet werden.

Das Bayern-Demokonto besitzt einen kontrollierten Resetmechanismus.

Vor einem Reset werden Demo-Stores gesichert, bestehende Sitzungen beendet und neue Zugangsdaten erzeugt.

Demo-Sicherungen dürfen nicht unbegrenzt anwachsen und erhalten eine kurze Rotation.

Offener Prüfpunkt: Rotation der Demo-Zwischensicherungen technisch festlegen; sieben Tage sind ein Arbeitsvorschlag.

20. Ende eines kommunalen Piloten

Nach Pilotende läuft ein kontrollierter Abschluss:

1. Keine neuen Pilotzugriffe.
2. Sitzungen und Pilotberechtigungen widerrufen.
3. Beratungsfreigaben prüfen.
4. Erforderliche Datenexporte bereitstellen.
5. Auftraggeber bestätigt Übernahme beziehungsweise Abschluss.
6. Pilotdaten entsprechend vereinbarter Frist löschen.
7. Backup-Rotation läuft aus.
8. Abschluss wird dokumentiert.

21. Gesetzliche Aufbewahrungspflichten

Nicht sämtliche Daten dürfen bei Vertragsende automatisch vernichtet werden.

Insbesondere geschäftliche und steuerrechtlich relevante Unterlagen können gesetzlichen Aufbewahrungspflichten unterliegen.

Diese Daten werden vom aktiven Bürgerkonto beziehungsweise Fachsystem getrennt behandelt.

Eine gesetzliche Aufbewahrungsfrist wird nicht pauschal auf sämtliche Bürgerdokumente angewendet, nur weil zwischen Sentinel und dem Nutzer ein Vertragsverhältnis bestand.

22. Sperrung statt Löschung

Ist eine Löschung aufgrund gesetzlicher Verpflichtungen oder eines konkret bestehenden Nachweisinteresses vorübergehend nicht zulässig, kann eine Einschränkung der Verarbeitung erfolgen.

Die Daten dürfen dann nicht weiterhin wie aktive Fachdaten genutzt werden.

23. Löschprotokoll

Ein Löschvorgang kann selbst einen minimalen Nachweis erzeugen.

Objektklasse → Zeitpunkt → Löschgrund → technische Durchführung → Ergebnis

Der Löschbeleg enthält nicht den gelöschten Dokumentinhalt erneut.

24. Backup-Wiederherstellung

Nach Wiederherstellung eines Sicherungsstandes müssen insbesondere geprüft werden:

- inzwischen gelöschte Konten
- widerrufene Freigaben
- gesperrte Benutzer
- widerrufene Passkeys
- ungültige Sessions
- entfernte Gruppenmitglieder
- inzwischen gelöschte Exportartefakte

Ein Restore darf keinen dauerhaft aufgehobenen Zugriff unbeabsichtigt wieder aktivieren.

Offener Prüfpunkt: Post-Restore-Reconciliation konzipieren und testen.

25. Empfohlene erste technische Fristen

Die folgenden Werte bilden eine Arbeitskonfiguration und werden erst nach Prüfung gegen Jobs, Backup-Konfiguration, Logs und gesetzliche Anforderungen produktiv veröffentlicht.

Kategorie	Aufbewahrung
Temporäre Export-ZIPs	24 Stunden
Web-/technische Standardlogs	30 Tage
Security-/Access-Audit	180 Tage
abgelaufene Sessions	kurzfristige automatische Bereinigung
verbrauchte Recovery-Challenges	unmittelbar ungültig
widerrufene Freigaben	Zugriff sofort
Demo-Zwischensicherungen	7 Tage als Vorschlag

Kategorie	Richtwert
gelöschte Bürgerdaten in Backups	abhängig von Backup-Rotation
Rechnungs-/Steuerdaten	gesetzliche Frist

Offener Prüfpunkt: Zeitwerte sind Vorschläge, keine produktiven Zusagen.

26. Pilot-Sonderregel

Nach Ende des Piloten wird dem Pilotpartner zunächst die Möglichkeit gegeben, die für ihn erforderlichen Daten zu exportieren. Anschließend werden die pilotbezogenen Zugriffsrechte deaktiviert und die vereinbarten produktiven Pilotdaten gelöscht. Verbleibende Kopien in Sicherungssystemen werden mit der dokumentierten Backup-Rotation entfernt und bis dahin nicht für reguläre Verarbeitungszwecke verwendet.

27. Offene technische Verifikation

Vor einer endgültigen Fassung sind die tatsächlichen Werte und Verfahren zu ermitteln für:

- Log-Rotation
- temporäre Exportablage
- Communication-Aufbewahrung
- Support-/Ticketdaten
- KI-Anbieterretention
- Abrechnungsdaten
- physische Entfernung gelöschter Dateien
- Post-Restore-Reconciliation
- zusätzliche immutable/offsite Backupkopie

Damit kann das Löschkonzept gegen die technische Implementierung geprüft werden.

Offener Prüfpunkt: OFFENE TECHNISCHE VERIFIKATION