Datenschutz-Rollen- und Datenflusskonzept

Virtueller Bürger-Schreibtisch & Schuldnerberatung

Version 1.0 · Stand 09.10.2026

Dieses Konzept beschreibt Rollen und Datenflüsse. Es ersetzt weder die Datenschutzerklärung noch die konkrete Rollen-/Rechtsgrundlagenprüfung je Pilot und Verarbeitung.

1. Grundprinzip

Der Virtuelle Bürger-Schreibtisch ist nicht lediglich ein von einer Kommune geführtes Fachverfahren.

Aus der bisherigen Architektur ergibt sich vielmehr ein eigenständiger persönlicher Arbeitsbereich des Bürgers, aus dem dieser gezielt einzelne Vorgänge für weitere Beteiligte freigeben kann.

Deshalb darf datenschutzrechtlich nicht pauschal angenommen werden, dass eine Kommune oder Beratungsstelle für sämtliche innerhalb des Bürger-Schreibtischs stattfindenden Verarbeitungen Verantwortlicher ist.

Die datenschutzrechtliche Rolle ist für den jeweiligen Verarbeitungsvorgang zu bestimmen.

Status: ROLLEN JE VERARBEITUNGSVORGANG UND PILOTMODELL ENDGÜLTIG FESTLEGEN

2. Die Beteiligten

Für den vorgesehenen Betrieb werden zunächst fünf Akteure unterschieden:

- A – Bürger: Nutzer und regelmäßig betroffene Person
- B – Sentinel / Betreiber: Betreiber und technischer Anbieter des Virtuellen Bürger-Schreibtischs
- C – Schuldnerberatungsstelle: kommunale oder freie Beratungsstelle
- D – Externe Kommunikationspartner: beispielsweise Behörden, Gerichte, Gläubiger oder andere Empfänger
- E – Technische Dienstleister: insbesondere Hosting und – sofern für eine konkrete Funktion aktiviert – weitere externe Dienste

Diese Rollen sind nicht für sämtliche Verarbeitungsvorgänge identisch.

3. Datenflussübersicht

Der zentrale Ablauf lässt sich als kontrollierte Kette darstellen. Entscheidend ist: Es gibt keinen automatischen Durchgriff von der Beratungsstelle in den Bürger-Schreibtisch.

Bürger → Anmeldung → Persönlicher Bürger-Schreibtisch → Upload / digitaler Eingang → Dokumentenspeicher → technische Verarbeitung → OCR / Metadaten / Aktenzeichen / Zuordnung → Vorgang + Verfahrenslinie → optional und gesondert aktiviert: KI-Auswertung → Bürger prüft / korrigiert / ergänzt → ausdrückliche Vorgangsfreigabe → Schuldnerberatung → Beratung / Bearbeitung → gegebenenfalls Export / Schreiben / eBO / andere Kommunikation

4. Bürgerkonto

Der Bürger legt ein persönliches Konto an. Darin können unter anderem gespeichert werden:

- Kontodaten
- Dokumente
- Vorgänge
- Fristen
- Verfahrenslinien
- persönliche Notizen
- Kommunikationsinformationen
- Freigaben

Der Bürger bestimmt grundsätzlich selbst, welche Inhalte er dort einstellt.

Für diesen allgemeinen persönlichen Schreibtisch spricht vieles dafür, dass Sentinel nicht einfach Auftragsverarbeiter einer später hinzukommenden Kommune ist.

Die genaue Rolle des Betreibers und die einschlägigen Rechtsgrundlagen müssen anhand des konkreten Nutzungs- und Vertragsmodells festgelegt und in den Datenschutzhinweisen beschrieben werden.

Status: ROLLE UND RECHTSGRUNDLAGEN FÜR DAS KONKRETE NUTZUNGS-/VERTRAGSMODELL FESTLEGEN

5. Dokumentenupload

Datenfluss: Bürger → Sentinel-Dokumentenspeicher.

Das Dokument wird dem jeweiligen Bürgerkonto und gegebenenfalls einem Vorgang zugeordnet.

Es findet dadurch noch keine Freigabe an eine Beratungsstelle statt.

Das Hochladen eines Dokuments in den persönlichen Bürger-Schreibtisch stellt keine Übermittlung dieses Dokuments an eine Beratungsstelle, Behörde oder sonstige dritte Stelle dar.

6. OCR und lokale Dokumentenverarbeitung

Nach der bisherigen technischen Dokumentation können Dokumente lokal beziehungsweise innerhalb der Sentinel-Infrastruktur verarbeitet werden.

Hierzu gehören beispielsweise: PDF/Bild → OCR → Text → Metadaten → Aktenzeichen → mögliche Dokumentart → Vorgangszuordnung.

Solange hierfür kein externer Dienst verwendet wird, verlässt das Dokument für diesen Verarbeitungsschritt nicht allein aufgrund der OCR die Sentinel-Infrastruktur.

7. Verfahrenslinie

Aus erkannten Dokumentinformationen können Vorgänge und Verfahrenslinien aufgebaut beziehungsweise fortgeführt werden. Dabei können insbesondere verarbeitet werden:

- Dokumentdatum
- Absender
- Empfänger
- Aktenzeichen
- Dokumentart
- Beteiligte
- erkannte Zusammenhänge
- Fristen
- chronologische Beziehungen

Die Verfahrenslinie bleibt Bestandteil des Bürgerkontos.

Eine Beratungsfreigabe des Bürgers muss deshalb nicht automatisch dessen gesamte Verfahrenshistorie umfassen.

8. Bürgerkorrektur

Automatisch extrahierte Informationen können vom Bürger korrigiert oder ergänzt werden.

Technisch und datenschutzrechtlich werden drei Ebenen unterschieden: Originaldokument → technische Extraktion → vom Bürger bestätigte/korrigierte Information.

Dadurch bleibt nachvollziehbar, woher eine Information stammt.

9. KI-Auswertung

Die bisherige Architektur sieht vor, dass KI für Bürgerkonten standardmäßig deaktiviert und kontospezifisch aktiviert werden kann.

Dokument hochladen bedeutet damit nicht automatisch externe KI-Verarbeitung.

Vor einer produktiven Veröffentlichung wird für jede KI-Funktion eine Datenflussbeschreibung erstellt:

- Funktion
- Anbieter
- übermittelte Daten
- Zweck
- Speicherbedingungen
- Verarbeitungsort
- Rechtsgrundlage
- Löschung

Erst danach kann korrekt beschrieben werden, welche Daten tatsächlich die Sentinel-Infrastruktur verlassen.

Status: PRODUKTIVE EXTERNE KI-DATENFLÜSSE JE FUNKTION VOLLSTÄNDIG DOKUMENTIEREN

10. Private Bürgernotizen

Private Notizen besitzen eine besonders klare Zweckgrenze.

Sie bleiben im persönlichen Bürgerbereich.

Eine spätere Freigabe eines Schuldnerberatungsvorgangs umfasst sie nicht.

Persönlicher Arbeitsraum und Beratungsraum bleiben getrennt.

11. Beginn der Schuldnerberatung

Der Bürger entscheidet: Diesen konkreten Vorgang möchte ich dieser Beratungsstelle zugänglich machen.

Die Beratungsstelle erhält nicht den gesamten Sentinel-Account.

Die Freigabe folgt dem Modell: Bürger A → Vorgang X → Beratungsstelle Y → definierte Rechte.

12. Freigabeumfang

Eine Freigabe kann insbesondere umfassen:

- Forderungen
- Gläubigerinformationen
- ausgewählte Dokumente
- Haushalt

- Einnahmen/Ausgaben
- Pfändungsinformationen
- P-Konto-Angaben
- Vergleichsvorbereitung
- Insolvenzvorbereitungsinformationen

Nicht automatisch enthalten sind andere Bürgerangelegenheiten, andere Verfahren, private Notizen, nicht freigegebene Dokumente und interne Sicherheitsinformationen.

13. Rolle der Beratungsstelle

Sobald eine Beratungsstelle personenbezogene Informationen für die eigene Durchführung der Schuldnerberatung verarbeitet, ist sorgfältig zu unterscheiden, ob sie für diese fachliche Verarbeitung selbst Verantwortlicher ist. Das ist bei einer klassischen Beratungsleistung naheliegend.

Sentinel könnte hinsichtlich des von der Beratungsstelle verwendeten technischen Arbeitsbereichs als Auftragsverarbeiter tätig werden, soweit Sentinel Daten ausschließlich für die Beratungsstelle verarbeitet.

Mögliche Struktur: Bürger ↔ Sentinel als persönlicher digitaler Schreibtisch; Bürger → Beratungsstelle als gezielte Offenlegung eines Vorgangs; Beratungsstelle in eigener fachlicher Verantwortung; Sentinel → Beratungsstelle als technische Bereitstellung des geschützten Beratungsarbeitsbereichs.

Status: JE PILOTVERTRAG ENDGÜLTIG FESTLEGEN

14. Persönlicher Berater

Nach der Freigabe an eine Institution kann ein konkreter Berater dem Vorgang zugeordnet werden.

Der vorgesehene Einmalcode funktioniert nicht als alleinige Authentisierung.

Der Berater muss bereits angemeldet, der richtigen Institution zugeordnet und entsprechend berechtigt sein.

Erst anschließend kann der kurzlebige Code für die vorgesehene Zuordnung verwendet werden.

15. Widerruf

Der Bürger kann eine Freigabe zurückziehen.

Der weitere Zugriff über Sentinel wird dann unmittelbar gesperrt.

Ein Widerruf verhindert zukünftige Zugriffe über die Plattform. Daten, die eine Beratungsstelle zuvor rechtmäßig heruntergeladen oder in eigene Systeme übernommen hat, können dadurch nicht technisch aus diesen Fremdsystemen zurückgerufen werden.

Für diese Kopien gelten anschließend die Datenschutz- und Löschpflichten der Beratungsstelle.

16. Beratungsmappe

Der Bürger beziehungsweise die berechtigte Beratungsstelle kann eine strukturierte Beratungsmappe erhalten.

Sie kann Dokumente, Gläubigerliste, strukturierte Daten, Erläuterungen und Integritätsinformationen enthalten.

Private Bürgernotizen und unnötige technische Interna werden nicht Bestandteil des Exports.

Damit lässt sich konkret dokumentieren, welche Daten Sentinel beim Export verlassen.

17. Kommunikation

Bei einem bewussten Versand entsteht ein neuer Datenfluss: Bürger/Berater → Sentinel Communication → ausgewähltes Dokument → ausgewählter Empfänger → Mail/eBO/anderer Kanal.

Das Speichern oder Erstellen eines Schreibens löst dagegen keinen Versand aus.

Diese Trennung ist datenschutzrechtlich und technisch wesentlich.

18. eBO / SAFE / Zertifikat

Bei einer eBO-Kommunikation können zusätzliche Identitäts- und Kommunikationsdaten verarbeitet werden, beispielsweise SAFE-ID, Zertifikatsinformationen, Empfänger, Versandmetadaten und Zustellinformationen.

Zertifikate und zugehörige Geheimnisse erhalten deshalb einen eigenen Schutzbereich.

Der Controller soll keine P12-Datei beziehungsweise das zugehörige Passwort benötigen.

19. Sentinel Controller

Der Controller soll insbesondere technische und betriebliche Informationen verwalten: Instanz → Produkt → Konfiguration → Entitlements → Betriebszustand → gegebenenfalls Abrechnung.

Er soll nicht zum zentralen Sammelpunkt sämtlicher Bürgerdokumente werden.

Architekturprinzip: Zentrale Betriebssteuerung und dezentrale Fachinhalte werden soweit technisch möglich getrennt.

20. Hosting

Für den gegenwärtigen Bürger-Schreibtisch ergibt sich der Datenweg: Bürger → TLS → Hetzner-Infrastruktur Nürnberg → Reverse Proxy → Bürger-Schreibtisch :8104 → kontobezogene Fach- und Dokumentdaten.

Sentinel System und der Bürger-Schreibtisch teilen sich derzeit eine Serverinstanz, sind jedoch unterschiedliche Anwendungsdienste.

Für die datenschutzrechtliche Bewertung ist nicht lediglich der Server ausschlaggebend, sondern insbesondere die tatsächliche logische Zugriffstrennung.

21. Rollenmatrix

Die folgende Matrix ist eine Arbeitsgrundlage. Die Rolle von Sentinel ist in den gekennzeichneten Verarbeitungsschritten vor Pilot- beziehungsweise Vertragsschluss endgültig festzulegen.

[illegible]	[illegible]	[illegible]	[illegible]
Persönliches Konto	Betroffener / Nutzer	Rolle endgültig festzulegen	kein Zugriff
Dokumentensafe	Nutzer	Betreiber / Verarbeitung	kein Zugriff
OCR	initiiert Verarbeitung	technische Verarbeitung	kein Zugriff
Verfahrenslinie	Nutzer	technische Verarbeitung	nur wenn freigegeben
Private Notizen	Nutzer	technische Speicherung	kein Zugriff
KI	optional aktiviert	technische Vermittlung / Verarbeitung	grundsätzlich kein Zugriff
Schuldenvorgang	Nutzer	Plattform	nach Freigabe

Verarbeitung	Rolle	Partner	Bemerkung
Fachberatung	Betroffener	technische Plattform	regelmäßig eigene fachliche Verantwortung
Beraterworkspace	Betroffener	potenziell Auftragsverarbeiter	Verantwortlicher
Export	veranlasst / berechtigt	technische Erstellung	Empfänger
eBO	veranlasst / berechtigt	technischer Versand	abhängig vom Absender
Hosting	Betroffener	Betreiber	kein unmittelbarer Hostingzugriff

Status: ARBEITSMATRIX / keine pauschale Rollenfestlegung für sämtliche Verarbeitungen