Datenschutz- und Sicherheitsinformation für Pilotpartner

Virtueller Bürger-Schreibtisch & digitale Schuldnerberatung

Version 1.0 · Stand 09.10.2026
Sentinel System

Transparenzinformation für die fachliche und datenschutzrechtliche Bewertung eines Piloten. Sie ersetzt weder die Datenschutzerklärung noch TOM, AVV oder die konkrete Rollenprüfung.

1. Worum geht es?

Der Virtuelle Bürger-Schreibtisch ist eine digitale Arbeitsumgebung, mit der Bürger ihre Dokumente und Vorgänge strukturiert verwalten und bei Bedarf gezielt mit einer Beratungsstelle zusammenarbeiten können.

Für die Schuldnerberatung können beispielsweise Dokumente hochgeladen, Forderungen strukturiert, Gläubiger erfasst, Haushalts- und Finanzinformationen vorbereitet und ausgewählte Informationen für eine Beratungsstelle freigegeben werden.

Ein wesentliches Architekturprinzip lautet dabei:

Der Bürger gibt nicht seinen gesamten digitalen Schreibtisch frei. Er gibt einen bestimmten Vorgang für einen bestimmten Zweck an eine bestimmte Stelle frei.

Der persönliche Arbeitsbereich und der Beratungsbereich bleiben voneinander getrennt.

2. Wo werden die Daten verarbeitet?

Die derzeitige Infrastruktur des Virtuellen Bürger-Schreibtischs wird auf Serverinfrastruktur von Hetzner in Nürnberg, Deutschland betrieben.

Der Bürger-Schreibtisch wird gegenwärtig gemeinsam mit Sentinel System auf einer Serverinstanz betrieben, bildet dort jedoch einen eigenständigen Anwendungsdienst.

Der interne Anwendungsdienst des Bürger-Schreibtischs verwendet Port 8104.

Die Trennung der Bürgerkonten erfolgt nicht lediglich über unterschiedliche Webseiten oder Benutzeroberflächen, sondern durch serverseitige Konto-, Objekt- und Berechtigungsprüfungen.

3. Wie werden Bürgerkonten voneinander getrennt?

Fachobjekte des Bürger-Schreibtischs werden einem account_id zugeordnet.

Hierzu gehören insbesondere Dokumente, Vorgänge, Freigaben und weitere persönliche Arbeitsdaten.

Der Server prüft die Berechtigung auf die angeforderten Objekte.

Die Kenntnis oder Manipulation einer Objektkennung darf keinen Zugriff auf ein anderes Bürgerkonto ermöglichen.

Diese Isolation wird mit getrennten Testkonten in den automatisierten Regressionstests überprüft.

4. Was kann die Beratungsstelle sehen?

Eine teilnehmende Beratungsstelle erhält keinen allgemeinen Zugriff auf Bürgerkonten.

Der Bürger gibt einen konkreten Vorgang gezielt frei.

Eine Freigabe kann beispielsweise umfassen:

- ausgewählte Dokumente
- Gläubiger und Forderungen
- Haushaltsinformationen
- Einnahmen und Ausgaben
- Pfändungsinformationen
- P-Konto-bezogene Angaben
- Informationen zur Vergleichsvorbereitung
- Informationen zur Vorbereitung eines möglichen Insolvenzverfahrens

Andere Angelegenheiten des Bürgers bleiben davon unberührt.

Private Notizen bleiben privat.

Sie werden nicht allein deshalb an eine Beratungsstelle übermittelt, weil ein Schuldnerberatungsvorgang freigegeben wurde.

5. Wie werden Berater authentisiert?

Berater verwenden einen von Bürgerkonten getrennten Zugang.

Innerhalb einer Beratungsstelle können unterschiedliche Rollen vorgesehen werden, beispielsweise Manager, Berater und ausschließlich leseberechtigte Nutzer.

Eine Rolle allein berechtigt nicht automatisch zum Zugriff auf sämtliche Bürgerfälle.

Zusätzlich muss der betreffende Vorgang für die Institution beziehungsweise den jeweiligen Berechtigten freigegeben sein.

Für bestimmte persönliche Übergabeprozesse kann ein kurzlebiger Einmalcode eingesetzt werden.

Dieser ersetzt ausdrücklich nicht die Anmeldung des Beraters.

6. Was passiert bei einem Widerruf?

Der Bürger kann eine Beratungsfreigabe widerrufen.

Der weitere Zugriff über den Virtuellen Bürger-Schreibtisch wird daraufhin gesperrt.

Das betrifft auch zukünftige Downloads über die widerrufene Freigabe.

Bereits zuvor rechtmäßig von einer Beratungsstelle heruntergeladene oder in deren eigenes System übernommene Daten können technisch nicht nachträglich von Sentinel aus diesem Fremdsystem entfernt werden.

Für diese Daten ist anschließend die jeweilige Beratungsstelle nach den für sie geltenden datenschutzrechtlichen Vorgaben verantwortlich.

7. Wie kommen Dokumente in das System?

Der Bürger kann Dokumente selbst hochladen beziehungsweise über hierfür vorgesehene digitale Kommunikationswege übernehmen.

Zu einem Dokument können technische Informationen wie Dateityp, Größe, Kontozuordnung und kryptografischer SHA-256-Prüfwert gespeichert werden.

Das Hochladen eines Dokuments bedeutet nicht, dass dieses automatisch an eine Beratungsstelle oder Behörde weitergeleitet wird.

Eine Übermittlung erfordert einen dafür vorgesehenen Freigabe- beziehungsweise Versandvorgang.

8. Was macht Sentinel mit einem Dokument?

Dokumente können technisch verarbeitet werden, um den Bürger bei ihrer Organisation zu unterstützen.

Dazu können gehören:

Texterkennung → Dokumenttyp → Datum → Absender/Empfänger → Aktenzeichen → Vorgang → Verfahrenslinie

Der Bürger muss seine Verfahrensgeschichte dadurch nicht vollständig manuell zusammensuchen.

Neu hinzukommende Dokumente können anhand erkannter Informationen bestehenden Vorgängen und Verfahrenslinien zugeordnet werden.

Originaldokument, technische Extraktion und spätere Benutzerkorrektur werden konzeptionell voneinander unterschieden.

9. Werden Dokumente für OCR an fremde Anbieter geschickt?

Für die dokumentierte Sentinel-Architektur stehen lokale OCR- und Dokumentverarbeitungswege zur Verfügung.

Dokumente müssen daher für eine normale Texterkennung nicht allein zu diesem Zweck an einen externen OCR-Dienst übertragen werden.

Das ist von optionalen KI-Funktionen zu unterscheiden.

10. Wird künstliche Intelligenz eingesetzt?

KI ist nicht mit der normalen Speicherung oder OCR gleichzusetzen.

Für Bürgerkonten ist die KI-Nutzung nach der derzeitigen Produktarchitektur grundsätzlich standardmäßig deaktiviert und kontospezifisch aktivierbar.

Damit gilt insbesondere:

Ein Dokumentenupload bedeutet nicht automatisch eine Übermittlung des Dokuments an einen externen KI-Dienst.

Vor produktiver Nutzung eines externen KI-Anbieters werden der jeweilige Zweck, die übermittelten Daten, Verarbeitungsort, Speicherbedingungen und datenschutzrechtliche Einbindung dokumentiert.

Für bestimmte Recherchefunktionen ist bereits eine datensparsame Schnittstelle vorgesehen: Bürgerdokumente, Aktenzeichen, private Notizen sowie Konto-, Benutzer- und Vorgangskennungen dürfen dabei nicht an den Recherche-Executor übermittelt werden.

Rechercheergebnisse werden zunächst als Vorschläge behandelt und nicht automatisch veröffentlicht.

Offener Konkretisierungspunkt: Externe KI-Datenflüsse sind vor produktiver Aktivierung je Funktion konkret zu dokumentieren.

11. Trifft das System rechtliche Entscheidungen?

Nein.

Der Bürger-Schreibtisch kann strukturieren, rechnen, Hinweise erzeugen und Informationen zur Prüfung aufbereiten.

Das System ersetzt keine:

- Schuldnerberatung
- Rechtsberatung
- anwaltliche Prüfung
- behördliche Entscheidung
- gerichtliche Entscheidung

Eine Dringlichkeitskennzeichnung dient beispielsweise der Arbeitspriorisierung und ist keine verbindliche rechtliche Bewertung.

Ebenso entscheidet eine Insolvenz-Checkliste nicht darüber, ob die rechtlichen Voraussetzungen eines Insolvenzverfahrens erfüllt sind.

12. Was passiert bei der Vorbereitung eines Vergleichs?

Das System kann bestätigte Forderungen strukturiert für einen außergerichtlichen Einigungsversuch aufbereiten und rechnerische Verteilungen erstellen.

Ein gespeicherter Entwurf wird dadurch nicht automatisch versendet.

Entwurf → Vorbereitung → tatsächlicher Versand → Dokumentation des Versands

Dadurch soll eine unbeabsichtigte externe Kommunikation verhindert werden.

13. Wie werden Passkeys und Recovery geschützt?

Neben Passwörtern unterstützt der Bürger-Schreibtisch Passkeys.

Die dokumentierte Implementierung umfasst unter anderem:

- verpflichtende Benutzerverifikation
- Origin-/RP-ID-Bindung
- zeitlich begrenzte Challenges
- einmalige Verwendung von Challenges
- accountgebundene Sitzungen

Recovery-Codes werden nicht als dauerhaft verwendbare Klartext-Zugangscodes gespeichert.

Nach erfolgreicher Wiederherstellung werden bestehende Sitzungen widerrufen.

14. Was sieht der zentrale Sentinel-Betrieb?

Die zentrale Betriebssteuerung soll insbesondere technische und organisatorische Informationen verarbeiten, beispielsweise:

Produkt/Instanz → Konfiguration → Berechtigungsumfang → Betriebszustand → technische Administration

Der Controller ist nicht als zentraler Arbeitsplatz zur routinemäßigen Einsicht in Bürgerdokumente vorgesehen.

Technisch privilegierte Betreiberzugriffe, die beispielsweise für Fehlerbehebung oder Wiederherstellung erforderlich sein können, sind von normalen Fachzugriffen zu unterscheiden und entsprechend zu begrenzen beziehungsweise zu protokollieren.

15. Was passiert mit den Daten nach dem Pilot?

Nach Beendigung eines Pilotprojekts erfolgt ein kontrollierter Abschluss.

Zunächst werden erforderliche Daten beziehungsweise Exporte entsprechend der vereinbarten Verantwortlichkeiten bereitgestellt.

Anschließend werden Pilotzugänge und -berechtigungen deaktiviert, bestehende Freigaben überprüft und die vereinbarten produktiven Pilotdaten dem Löschprozess zugeführt.

Daten können anschließend noch für einen begrenzten Zeitraum Bestandteil vorhandener Sicherungskopien sein.

Diese Sicherungen werden nicht als reguläres Archiv weiterverwendet. Die endgültige Entfernung erfolgt mit der festgelegten Backup-Rotation.

Offener Konkretisierungspunkt: Löschfristen und Backup-Rotation sind für den konkreten Pilot vertraglich festzulegen.

16. Was passiert bei einer Sicherheitsstörung?

Sicherheitsrelevante Ereignisse werden untersucht und dokumentiert.

Der vorgesehene Prozess umfasst grundsätzlich:

Erkennung → Eindämmung → Analyse → Sicherung relevanter Informationen → Wiederherstellung → Dokumentation → datenschutzrechtliche Bewertung

Betrifft eine Verletzung des Schutzes personenbezogener Daten einen Pilotpartner beziehungsweise dessen Auftragsverarbeitung, wird dieser entsprechend der AV-Vereinbarung unverzüglich informiert.

17. Wie wird die Software getestet?

Für den Virtuellen Bürger-Schreibtisch sind derzeit 397 erfolgreiche automatisierte Prüfungen dokumentiert.

Die Tests umfassen unter anderem Kontentrennung, IDOR-Schutz, Host-Isolation, Authentisierung, Passkeys, Recovery, CSRF-Schutz, Rollenwechsel, Freigaben, unmittelbaren Zugriffsentzug, Schuldnerberatungsfunktionen, Beraterzugriffe sowie Zertifikats- und eBO-Prozesse.

Diese Prüfungen sind automatisierte Entwicklungs- und Regressionstests. Sie werden nicht als unabhängiges Sicherheitsaudit, Penetrationstest oder Zertifizierung dargestellt.

18. Wird eBO unterstützt?

Für entsprechende Anwendungsfälle ist die Anbindung an die Sentinel-Communication-Infrastruktur einschließlich SAFE-/Zertifikatsprozessen vorgesehen beziehungsweise im Produktstand technisch abgebildet.

Eine entsprechende Funktion wird nur bei Vorliegen der erforderlichen Voraussetzungen freigegeben.

Ein vorhandenes Zertifikat wird nicht allein aufgrund seiner technischen Verwendbarkeit als qualifizierte elektronische Signatur oder abschließende Identitätsprüfung bezeichnet.

19. Welche Unterauftragnehmer werden eingesetzt?

Für die gegenwärtige Serverinfrastruktur wird Hetzner, Nürnberg/Deutschland eingesetzt.

Für den konkreten Pilot wird eine vollständige Unterauftragnehmerübersicht bereitgestellt.

Externe Dienste werden dort mit Zweck, Datenkategorien und Verarbeitungsort aufgeführt.

Insbesondere optionale externe KI- oder Kommunikationsdienste werden nicht stillschweigend unter dem allgemeinen Begriff ‚Sentinel' verborgen.

Offener Konkretisierungspunkt: Vollständige Unterauftragnehmerübersicht für den konkreten Pilot bereitstellen.

20. Datenschutzrechtliche Rollen

Die Rollen werden nach dem konkreten Verarbeitungsvorgang bestimmt.

Insbesondere wird nicht pauschal davon ausgegangen, dass eine teilnehmende Kommune für sämtliche Inhalte eines persönlichen Bürger-Schreibtischs Verantwortlicher ist.

Für einen Pilot wird deshalb zwischen dem persönlichen Arbeitsbereich des Bürgers, der fachlichen Verarbeitung einer Beratungsstelle und den durch Sentinel im Auftrag erbrachten technischen Verarbeitungen unterschieden.

Die konkrete Rollenverteilung wird vor Pilotbeginn vertraglich dokumentiert.

Offener Konkretisierungspunkt: Rollenverteilung vor Pilotbeginn je Verarbeitungsvorgang vertraglich dokumentieren.

21. Dokumente für Datenschutz und IT

Einem Pilotpartner können insbesondere bereitgestellt werden:

- Zentrale TOMs Sentinel System
- Produktspezifische TOMs Bürger-Schreibtisch / Schuldnerberatung
- AVV-Muster nach Art. 28 DSGVO
- Rollen- und Datenflusskonzept
- Lösch- und Aufbewahrungskonzept
- Unterauftragnehmerübersicht
- Pilot-Onboarding und technischer Pilotablauf

Damit muss eine kommunale Datenschutzstelle ihre Bewertung nicht ausschließlich anhand einer Produktpräsentation durchführen.

22. Pilotgrundsatz

Der Virtuelle Bürger-Schreibtisch soll dem Bürger digitale Handlungsfähigkeit geben, ohne ihm dafür die Kontrolle über seine Daten zu nehmen. Dokumente bleiben zunächst in seinem persönlichen Arbeitsbereich; fachliche Stellen erhalten nur diejenigen Vorgänge und Rechte, die für die konkrete Zusammenarbeit freigegeben wurden.