Anlage TOM-BS

Virtueller Bürger-Schreibtisch einschließlich Schuldnerberatung – Ergänzung zu den zentralen TOMs gemäß Art. 32 DSGVO

Fassung 1.0 – Stand: 09.10.2026

Produktspezifische Anlage zur zentralen Sentinel-TOM. Offen markierte Prüfpositionen sind keine bestätigten Maßnahmen.

1. Gegenstand und Schutzbedarf

Der Virtuelle Bürger-Schreibtisch ist eine geschützte digitale Arbeitsumgebung zur persönlichen Organisation von Dokumenten, Vorgängen, Fristen, Verfahrenslinien und Kommunikation.

Ein besonderer Funktionsbereich unterstützt die Vorbereitung und Zusammenarbeit mit Schuldner- und Insolvenzberatungsstellen.

Verarbeitet werden können deshalb Daten mit teilweise hohem Schutzbedarf, insbesondere:

- Identitäts- und Kontodaten
- Korrespondenz mit Behörden, Gerichten und anderen Stellen
- Akten- und Geschäftszeichen
- Dokumente und Nachweise
- Fristen und Verfahrensinformationen
- Gläubiger- und Forderungsinformationen
- Einkommens-, Ausgaben-, Vermögens- und Pfändungsinformationen
- P-Konto-bezogene Angaben
- Kommunikationsdaten
- vom Bürger angelegte private Notizen

Der Schutz dieser Daten wird insbesondere durch Kontentrennung, Zugriffskontrolle, restriktive Freigaben und nachvollziehbare Sicherheitsereignisse umgesetzt.

2. Technische Bereitstellung

Der Bürger-Schreibtisch wird derzeit auf derselben Hetzner-Serverinstanz in Nürnberg wie Sentinel System betrieben.

Er stellt jedoch einen eigenständigen, hostbasierten Python-Anwendungsdienst dar.

Interner Anwendungsport: 8104.

Der Dienst wird durch systemd unter dem dedizierten Unix-Benutzer sentinel-portal betrieben. Das Capability-Set ist leer; NoNewPrivileges, Seccomp, MemoryDenyWriteExecute, privates IPC und weitere systemd-Schutzmaßnahmen sind aktiv.

Port 8104 bindet ausschließlich an das interne Docker-Gateway 172.18.0.1. Der vorgeschaltete Caddy-Reverse-Proxy erreicht den Dienst über dieses interne Ziel; auf Loopback und der öffentlichen Host-IP besteht kein Listener für Port 8104.

Die öffentliche Erreichbarkeit erfolgt ausschließlich über die vorgeschaltete Web-/TLS-Infrastruktur mit HTTP-zu-HTTPS-Umleitung und HSTS.

Die Host-Firewall arbeitet mit INPUT DROP und FORWARD DROP. Eine zusätzliche persistente Docker-Ingress-Allowlist verhindert die unbeabsichtigte Veröffentlichung weiterer Containerports.

Die fachlichen Bürgerdaten werden gegenwärtig in getrennten JSON-Stores sowie einem konten- und vorgangsbezogenen Dateibaum gehalten. Es wird keine eigenständige relationale Bürgerdatenbank verwendet.

Die gemeinsame physische beziehungsweise virtuelle Serverbasis bedeutet ausdrücklich nicht, dass Benutzer der unterschiedlichen Anwendungen gegenseitig auf ihre Daten zugreifen können.

Status: TECHNISCH VERIFIZIERT AM 09.10.2026 / Prozess-, Bind-, Proxy-, Firewall-, Store- und Dienstgrenze

3. Konten- und Objektisolation

Der Bürger-Schreibtisch verwendet eine kontobezogene Fachstruktur.

Fachobjekte werden einer account_id zugeordnet. Dazu gehören insbesondere Dokumente, Vorgänge, Fristen, Freigaben und weitere personenbezogene Arbeitsdaten.

Die Berechtigung wird serverseitig geprüft.

Die Kenntnis oder Manipulation einer Objekt-ID darf keinen Zugriff auf Daten eines anderen Bürgerkontos ermöglichen.

Entsprechende Isolation wird mit mehreren getrennten Testkonten automatisiert überprüft.

4. Registrierung und Authentisierung

Der Zugang zum Bürger-Schreibtisch kann über Passwort und Passkeys erfolgen.

Für Passkeys gelten insbesondere:

- WebAuthn-basierte Authentisierung
- verpflichtende User Verification
- RP-ID-/Origin-Bindung
- zeitlich begrenzte Challenges
- einmalige Verwendung von Challenges
- automatische Bereinigung abgelaufener Challenge-Dateien bei der nächsten Challenge-Erzeugung
- accountgebundene Sitzungen

Registrierung und Verwaltung sicherheitsrelevanter Zugangsmittel erfolgen ausschließlich innerhalb hierfür vorgesehener Prozesse.

5. Recovery und Verlust von Zugangsmitteln

Für den Verlust eines regulären Zugangsmittels besteht ein kontrolliertes Recovery-Verfahren.

Recovery-Codes werden nur einmal angezeigt und nicht als wiederverwendbarer Klartext gespeichert. Nach der vorliegenden Implementationsdokumentation werden sie einzeln mittels Scrypt abgeleitet beziehungsweise gehasht.

Eine erfolgreiche Wiederherstellung setzt das Passwort neu und widerruft bestehende Sitzungen.

Mehrere fehlgeschlagene Recovery-Versuche führen zu einer zeitweisen Sperre.

Passkey- und Recovery-Ereignisse werden sicherheitsbezogen protokolliert.

6. Dokumentenupload

Bürger können Dokumente in ihren persönlichen Schreibtisch übernehmen.

Dabei werden technische Dateiinformationen und die kontobezogene Zuordnung gespeichert.

Zu den vorgesehenen Metadaten gehören insbesondere:

- Konto
- Vorgang
- MIME-Typ
- Dateigröße
- SHA-256-Prüfwert

- Speicherstatus
- Freigabestatus
- Löschstatus
- Verschlüsselungsmodus

Uploads unterliegen Kontingent- beziehungsweise Quotenprüfungen.

Die Quotenreservierung erfolgt vor Abschluss eines Uploads, damit auch parallele Uploadvorgänge nicht zur unbeabsichtigten Überschreitung der zulässigen Speichermenge führen sollen.

Persistente Bürger-Stores und Dokumentdateien sind ausschließlich für den dedizierten Dienstbenutzer lesbar (Dateien 0600; dienstbezogene Verzeichnisse ohne Rechte für sonstige lokale Benutzer). Quellcode ist root-besessen und für den Dienst nicht schreibbar.

Beratungs-ZIP-Dateien werden beim Abruf im Arbeitsspeicher erzeugt und nicht als dauerhafte serverseitige Exportdatei abgelegt.

7. Originalerhalt und Dokumentenverarbeitung

Originaldokumente werden bei OCR-, Analyse-, Konvertierungs- und Zuordnungsvorgängen nicht lediglich durch das erzeugte Ergebnis ersetzt.

Technisches Extraktionsergebnis, Original und spätere Bürgerkorrektur werden voneinander unterschieden.

Damit bleibt nachvollziehbar, welche Information aus dem ursprünglichen Dokument stammt und welche Information später ergänzt oder korrigiert wurde.

8. OCR und automatische Erkennung

Dokumente können automatisiert analysiert werden. Hierzu gehören insbesondere:

- Texterkennung
- Dokumenttyp
- Datum
- Absender/Empfänger
- Aktenzeichen
- mögliche Beteiligte/Rollen
- Fristen
- mögliche Vorgangszuordnung

OCR- beziehungsweise Analyseergebnisse stellen technische Extraktionen oder Vorschläge dar.

Fehlerhafte Erkennungen können korrigiert werden.

Ein Dokument wird nicht allein deshalb verändert oder gelöscht, weil seine automatische Klassifizierung verworfen wurde.

9. Automatische Verfahrenslinien

Aus den erkannten und bestätigten beziehungsweise korrigierten Dokumentinformationen kann der Bürger-Schreibtisch fortlaufend Verfahrenslinien aufbauen.

Die Verfahrenslinie beginnt grundsätzlich bereits mit den ersten Dokumenten eines Vorgangs und kann mit neu hinzukommenden Unterlagen fortgeschrieben werden.

Dadurch können insbesondere zeitliche und sachliche Beziehungen zwischen Dokumenten, Aktenzeichen und Vorgängen sichtbar gemacht werden.

Die Verfahrenslinie ist eine Organisations- und Nachvollziehbarkeitsfunktion.

Automatisch erkannte Zusammenhänge stellen nicht ohne Weiteres eine rechtliche Bewertung eines Verfahrens dar.

10. KI-gestützte Dokumentenauswertung

Neben der technischen beziehungsweise regelbasierten Verarbeitung können KI-gestützte Funktionen angeboten werden.

Für Bürgerkonten ist die KI-Nutzung nach der dokumentierten Architektur grundsätzlich standardmäßig deaktiviert und kontospezifisch freizugeben.

Der Benutzer kann damit entscheiden, ob hierfür vorgesehene KI-Funktionen genutzt werden.

KI-Vorschläge werden von den ursprünglichen Dokumentinformationen und menschlichen Korrekturen getrennt behandelt.

Wo KI-Ergebnisse für sensible Folgeprozesse verwendet werden könnten, sollen sie nicht ungeprüft als verbindliche Tatsachen übernommen werden.

11. Private Bürgernotizen

Private Notizen gehören zum persönlichen Arbeitsbereich des Bürgers.

Eine Freigabe eines Vorgangs an eine Beratungsstelle führt nicht automatisch zur Freigabe privater Bürgernotizen.

Dies gilt auch für Beratungs- und Exportprozesse.

Damit wird zwischen dem persönlichen Arbeitsraum und bewusst zur Beratung freigegebenen Informationen unterschieden.

12. Schuldnerberatungsbereich

Der Schuldnerberatungsbereich ermöglicht die strukturierte Vorbereitung einer Beratung. Hierzu können gehören:

- Gläubiger
- ursprünglicher und aktueller Gläubiger
- Inkasso-/Vertretungsinformationen
- Akten- beziehungsweise Referenznummern
- Forderungsart
- Hauptforderung
- Kosten
- Zinsen
- Zahlungen
- aktueller Saldo
- Vollstreckungsstatus
- bestrittene beziehungsweise bestätigte Forderungen
- zugehörige Dokumente

Eine Zusammenführung von Forderungen erfolgt nicht ausschließlich aufgrund einer KI- oder Regelannahme.

Originalinformationen bleiben erhalten.

13. Dringlichkeit

Das System kann Forderungen beziehungsweise Situationen hinsichtlich ihrer Bearbeitungsdringlichkeit strukturieren.

Diese Kennzeichnung dient der Arbeitspriorisierung.

Sie stellt keine verbindliche rechtliche Beurteilung dar.

Maschinell ermittelte Gründe sollen nachvollziehbar gespeichert werden. Eine manuelle Änderung ist mit entsprechender Begründung möglich.

14. Haushalts- und Finanzinformationen

Für die Vorbereitung der Schuldnerberatung können Angaben erfasst werden zu:

- Haushaltsmitgliedern und Unterhaltspflichten
- Einnahmen
- Ausgaben
- Vermögen
- Pfändungen
- Kontosituation

Automatisierte Berechnungen beschränken sich auf dafür vorgesehene mathematische beziehungsweise strukturierende Funktionen.

Eine Kennzeichnung eines Gegenstandes als geschützt oder existenziell erforderlich stellt keine verbindliche Feststellung seiner rechtlichen Pfändbarkeit dar.

15. P-Konto

Der Bürger kann Informationen zu einem Pfändungsschutzkonto erfassen. Hierzu können gehören:

- P-Konto-Status
- Kreditinstitut
- gekürzte Kontokennung
- Bedarf einer Bescheinigung
- ausdrücklich bestätigte Schutzbeträge

Das System soll keine gesetzlichen Freibeträge lediglich aufgrund eigener Annahmen als verbindlichen individuellen Schutzbetrag ausgeben.

16. Außergerichtlicher Vergleich

Der Schreibtisch kann bei der Vorbereitung eines außergerichtlichen Einigungsversuchs unterstützen.

Berechnungen erfolgen nur mit bestätigten, offenen Forderungen.

Eine proportionale Verteilung wird centgenau berechnet; Einzelangebote werden auf die jeweilige Forderung begrenzt.

Vorgänge können unter anderem als Entwurf → vorbereitet → Versand dokumentiert → abgeschlossen/gescheitert geführt werden.

Das Speichern eines Entwurfs löst keinen automatischen Versand aus.

Ein tatsächlicher Versand beziehungsweise dessen Dokumentation erfordert einen gesonderten Vorgang.

17. Vorbereitung eines Insolvenzverfahrens

Eine Checkliste kann bei der Zusammenstellung notwendiger Unterlagen und Informationen unterstützen.

Das System entscheidet nicht automatisch über:

- das Vorliegen einer Insolvenz
- die Zulässigkeit eines Insolvenzantrags
- die richtige Verfahrensart
- die rechtliche Wirksamkeit eines Einigungsversuchs

Besondere Sachverhalte wie frühere Selbstständigkeit, frühere Insolvenzverfahren oder besondere Forderungsarten werden als Prüfhinweise behandelt.

Solange definierte Pflichtbestandteile fehlen, darf ein Vorgang nicht allein durch die Software als vollständig eingereicht dargestellt werden.

18. Trennung von Bürger und Beratungsstelle

Die Beratungsstelle besitzt eine vom Bürgerkonto getrennte Vertrauens- beziehungsweise Identitätsdomäne.

Berater erhalten keinen generellen Zugriff auf den gesamten Bürger-Schreibtisch.

Eine Freigabe bezieht sich auf:

- einen Bürger
- einen bestimmten Schuldenvorgang
- eine bestimmte Beratungsstelle
- gegebenenfalls einen konkreten Berater
- definierte Rechte

Freigaben können zeitlich begrenzt werden.

19. Beraterrollen

Innerhalb einer Beratungsstelle können unterschiedliche Rollen verwendet werden, beispielsweise:

- Manager
- Berater
- Viewer

Die jeweilige Rolle bestimmt nicht allein den Zugriff auf beliebige Bürgerdaten.

Zusätzlich muss der betreffende Bürger beziehungsweise Vorgang für die Einrichtung oder Person freigegeben sein.

20. Einmalcode für persönliche Übergabe

Für vorgesehene persönliche Beratungsprozesse kann ein kurzlebiger Einmalcode verwendet werden.

Nach der dokumentierten Implementierung:

- achtstelliger Code
- zehn Minuten gültig
- einmal verwendbar
- nur innerhalb eines bereits authentisierten Beraterkontos
- nur innerhalb der richtigen Beratungsinstitution
- zeitweilige Sperre nach fünf Fehlversuchen

Der Einmalcode ersetzt nicht die Identitätsprüfung beziehungsweise Anmeldung des Beraters.

21. Sofortiger Widerruf

Der Bürger kann eine Beratungsfreigabe widerrufen.

Der Widerruf soll den weiteren Zugriff der Beratungsstelle auf den betreffenden Vorgang unmittelbar sperren.

Dies betrifft auch den weiteren Download zuvor nur über die Freigabe erreichbarer Inhalte.

Bereits rechtmäßig heruntergeladene beziehungsweise anderweitig übergebene Kopien können technisch nicht durch einen späteren Widerruf aus dem Herrschaftsbereich des Empfängers zurückgerufen werden. Dieser Unterschied wird organisatorisch berücksichtigt.

22. Beratungsmappe / Export

Für eine Beratung kann eine vorgangsbezogene Übergabemappe erstellt werden. Diese kann beispielsweise enthalten:

- Gläubigerliste als CSV
- strukturierte JSON-Daten
- README beziehungsweise Erläuterungen
- ausgewählte Dokumente
- Hashwerte zur Integritätsprüfung

Nicht Bestandteil der Beratungsmappe sollen insbesondere private Bürgernotizen, unnötige interne Identifikatoren und interne Auditinformationen sein.

Die Erstellung und der Download setzen entsprechende Berechtigungen voraus.

23. Kommunikation und eBO

Der Bürger-Schreibtisch kann an die vorhandene Sentinel-Communication-Infrastruktur angebunden werden.

Für eBO-bezogene Funktionen werden insbesondere SAFE-Zuordnung und Zertifikate berücksichtigt.

Ohne erforderliches Zertifikat beziehungsweise ohne erforderliche Zuordnung werden entsprechende Funktionen technisch gesperrt.

Das SAFE-Recipient-Cert wird als klassischer Empfaenger-Keyslot auf Gueltigkeit, CA-Status, RSA-Staerke und Key Encipherment geprueft. Sein erwarteter SHA-256-Fingerprint wird bis in die Java-/Governikus-Engine gebunden; der API-Sendepfad erzwingt OSCI-Transportverschluesselung.

Die Transportverschluesselung ist nicht mit dem Browser-CryptoKey-Modus gleichzusetzen: Sentinel Communication verarbeitet eBO-Inhalte vor dem Send im Klartext. Ein ML-KEM-/Hybridmodus bleibt gesperrt, solange die Gegenstelle keinen verifizierten PQC-Empfaengerschluessel bereitstellt.

Ein Zertifikat wird nicht allein deshalb als qualifizierte elektronische Signatur bezeichnet, weil eine PDF-Datei kryptografisch signiert werden kann.

Der gegenwärtig dokumentierte Status ist daher gegebenenfalls als „SAFE-Zertifikat gebunden“ und nicht als abschließend geprüfte Personenidentität auszuweisen.

24. P12-Zertifikate und Geheimnisse

Soweit P12-Zertifikate für Kommunikations- beziehungsweise Signaturprozesse eingesetzt werden, sind Zertifikat und zugehörige Geheimnisse besonders geschützt aufzubewahren.

Nach der technischen Dokumentation werden P12-Passwörter verschlüsselt gespeichert und Dateiberechtigungen restriktiv gesetzt.

Der zentrale Controller soll weder P12-Dateien noch zugehörige Passwörter erhalten.

Status: VOR VERÖFFENTLICHUNG TECHNISCH ERNEUT VERIFIZIEREN

25. Kontrollierte Stellenrecherche

Der Bürger kann eine Recherche nach geeigneten Stellen beziehungsweise Funktionsträgern ausdrücklich anstoßen.

Der hierfür vorgesehene KI-Executor erhält nach der dokumentierten Schnittstelle keine Bürgerdokumente, Aktenzeichen, Bürgernotizen sowie keine Konto-, Nutzer- oder Vorgangskennungen.

Rechercheergebnisse werden zunächst als ungeprüfter Vorschlag gespeichert.

Eine automatische Veröffentlichung in das gemeinsame Stellenverzeichnis findet nicht statt.

26. Aggregierter Eskalationsradar

Soweit mehrere Bürger vergleichbare strukturierte Auffälligkeiten melden beziehungsweise entsprechende Signale entstehen, kann eine aggregierte Betrachtung vorgesehen werden.

Dabei werden keine Dokumente, Namen, Aktenzeichen, Konto- oder Vorgangskennungen oder freie Bürgertexte in den aggregierten Datensatz übernommen.

Ein Signal wird erst ab einer definierten Mindestzahl unterschiedlicher Bürgerkonten gebildet.

Das Ergebnis ist ein Prüfindikator, keine Tatsachenfeststellung über eine Behörde, ein Gericht oder eine andere Stelle.

27. Pilotbetrieb

Pilotumgebungen werden von produktiven Bürgerdaten unterschieden.

Das derzeit vorbereitete Bayern-Präsentationskonto verwendet fest definierte Demo-Identitäten und künstliche beziehungsweise für die Vorführung bestimmte Daten.

Ein Demo-Reset ist nur über den geschützten Backendbereich und zusätzliche Bestätigung möglich.

Vor dem Reset werden die betreffenden Demo-Stores gesichert; bestehende Demo-Sitzungen werden beendet und neue Zugangsdaten erzeugt.

Die automatische Präsentation verändert keine Fachdaten.

28. Automatisierte technische Prüfungen

Der aktuelle Entwicklungsstand dokumentiert 397 erfolgreiche Bürger-Schreibtisch-Checks. Diese umfassen unter anderem Account-Isolation, IDOR-Schutz, Host-Isolation, Rollen und Freigaben, CSRF, Passwort-/Passkey-Authentisierung, Recovery, normale und clientseitig verschlüsselte Dateiablage, CryptoKey-Container, kontrollierten Unterlagenversand, Schuldnerberatung, Beraterzugriffe, Sofortwiderruf, Zertifikats- und eBO-Prozesse sowie den Demo- und Pilotbereich.

Diese Prüfungen sind interne automatisierte Regressionstests.

Sie werden nicht als externe Sicherheitszertifizierung oder unabhängiger Penetrationstest dargestellt.

Status: INTERNE TECHNISCHE REGRESSIONSTESTS / keine externe Zertifizierung

29. Betreiberzugriff

Die zentrale Sentinel-Verwaltung soll für den regulären Betrieb grundsätzlich technische Status-, Konfigurations- und Abrechnungsinformationen verarbeiten.

Sie ist nicht als allgemeiner Arbeitsplatz zum Lesen fremder Bürgerdokumente vorgesehen.

Der laufende Bürger-Schreibtisch-Prozess verwendet den dedizierten Benutzer sentinel-portal statt root, besitzt keine Linux-Capabilities und ist über systemd unter anderem gegen Privilegienausweitung, Gerätezugriff sowie Kernel-, Control-Group- und Namespace-Manipulation eingeschränkt.

Technisch privilegierte administrative Hostzugriffe, die für Betrieb, Fehlerbehebung oder Wiederherstellung erforderlich sein können, sind davon zu unterscheiden und weiterhin entsprechend zu begrenzen und zu protokollieren.

Status: PROZESSBETRIEB VERIFIZIERT; administrative Hostzugriffe und vollständige Dateirechtematrix vor Pilotbeginn weiter prüfen

30. Löschung

Löschung muss mehrere Ebenen berücksichtigen:

- Bürgerkonto
- Vorgänge
- Dokumente
- Freigaben
- Kommunikationsdaten
- Auditinformationen
- Backups

Eine fachliche Löschung darf nicht fälschlich als sofortige physische Entfernung aus sämtlichen Sicherungskopien dargestellt werden.

Für aktive Systeme, Logs und Sicherungen werden deshalb jeweils eigene Aufbewahrungs- und Löschfristen festgelegt.

Konkrete Fristen folgen im zentralen Löschkonzept.

Status: KONKRETE FRISTEN IM ZENTRALEN LÖSCHKONZEPT OFFEN

31. Datenschutzfreundliche Voreinstellungen

Für den Bürger-Schreibtisch gelten insbesondere folgende Grundsätze:

- keine allgemeine Freigabe des Schreibtisches
- keine automatische Beratungsfreigabe
- private Notizen bleiben privat
- KI standardmäßig deaktiviert
- Freigaben vorgangsbezogen
- Freigaben widerrufbar
- externe Übermittlungen bewusst ausgelöst
- Speicherung eines Entwurfs bedeutet keinen Versand
- technische Vorschläge ersetzen keine fachliche Entscheidung

32. Grenzen des Systems

Der Virtuelle Bürger-Schreibtisch ersetzt insbesondere keine:

- Rechtsberatung
- Schuldner- oder Insolvenzberatung
- anwaltliche Prüfung
- behördliche Entscheidung
- gerichtliche Entscheidung

Automatisierte Hinweise, Verfahrenslinien, Priorisierungen und KI-Auswertungen dienen der Organisation, Vorbereitung und Unterstützung des Benutzers.

33. Noch vor einem Pilot mit Echtdaten zu schließen

Für die endgültige Fassung werden folgende Punkte als offene Prüfpositionen geführt:

- Löschfristen nach Datenkategorien und Post-Restore-Reconciliation
- zusätzliche immutable beziehungsweise projektgetrennte Offsite-Kopie des Borg-Repositories
- vollständige externe KI-Datenflüsse
- vollständige Unterauftragnehmerliste
- konkrete administrative Root-/Hostzugriffe und deren Protokollierung
- verbindlicher Incident-Response-Prozess
- Anwendungsschicht-Verschlüsselung der gespeicherten Bürgerdateien und getrennte Schlüsselverwaltung

Status: OFFENE PRÜFPOSITIONEN VOR ECHTDATEN-PILOT