Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 DSGVO – Muster

Version 1.0 · Stand 09.10.2026

[Name des Auftraggebers / Kommune / Träger]

[Anschrift]

– nachfolgend „Auftraggeber“ –

und

Christian Reimer, handelnd unter der Bezeichnung: Sentinel Welt

Wittenberger Str. 91, 12689 Berlin

– nachfolgend „Auftragnehmer“ –

Hinweis zum Vertragsstatus: Sentinel Welt ist nach dem derzeitigen Stand keine eigenständige juristische Person. Vertragspartner ist daher der Inhaber als natürliche Person beziehungsweise Einzelunternehmer unter seiner Geschäftsbezeichnung.

MUSTERSTATUS: Vor Unterzeichnung sind Rollen, Leistungsumfang, Anlagen, Unterauftragnehmer und Löschfristen für den konkreten Einsatz zu prüfen und auszufüllen.

§ 1 Gegenstand und Dauer

Der Auftragnehmer stellt dem Auftraggeber die vertraglich vereinbarten Sentinel-Dienste zur Verfügung.

Im Rahmen eines Pilotbetriebs kann dies insbesondere den Virtuellen Bürger-Schreibtisch einschließlich der Schnittstelle zur Schuldnerberatung umfassen.

Soweit der Auftragnehmer hierbei personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers verarbeitet, erfolgt diese Verarbeitung auf Grundlage dieser Vereinbarung.

Die Dauer der Auftragsverarbeitung entspricht grundsätzlich der Dauer des zugrunde liegenden Hauptvertrags beziehungsweise Pilotverhältnisses, soweit sich aus gesetzlichen Aufbewahrungspflichten oder gesonderten Vereinbarungen nichts anderes ergibt.

§ 2 Art und Zweck der Verarbeitung

Abhängig vom vereinbarten Leistungsumfang können insbesondere folgende Verarbeitungsvorgänge stattfinden:

- Erheben beziehungsweise Entgegennehmen
- Speichern
- Strukturieren
- Ordnen
- Auslesen
- Anzeigen
- technisches Analysieren
- OCR-Verarbeitung
- Verknüpfen
- Bereitstellen
- Übermitteln nach ausdrücklicher Auslösung
- Berechtigen
- Sperren
- Exportieren
- Sichern
- Löschen personenbezogener Daten

Beim Virtuellen Bürger-Schreibtisch können die Verarbeitungsvorgänge insbesondere der digitalen Organisation von Dokumenten und Vorgängen, der Erstellung und Fortschreibung von Verfahrenslinien sowie der Vorbereitung und kontrollierten Durchführung einer Zusammenarbeit mit Beratungsstellen dienen.

Eine eigenständige Nutzung der Daten für sachfremde Zwecke durch den Auftragnehmer ist nicht Gegenstand dieser Vereinbarung.

§ 3 Betroffene Personen

Abhängig vom vereinbarten Einsatz können insbesondere Daten folgender Personengruppen verarbeitet werden:

- Bürger beziehungsweise Nutzer des Dienstes
- Mitglieder ihres Haushalts oder sonstige in Dokumenten genannte Personen
- Gläubiger und deren Ansprechpartner

- Beschäftigte und Ansprechpartner des Auftraggebers
- Berater und sonstige berechtigte Fachkräfte
- Kommunikationspartner
- sonstige Personen, deren Daten Bestandteil der vom Nutzer eingebrachten Dokumente sind

Der konkrete Umfang wird in Anlage 1 – Gegenstand der Verarbeitung festgelegt.

§ 4 Kategorien personenbezogener Daten

Abhängig vom konkreten Anwendungsfall können insbesondere verarbeitet werden:

- Stamm- und Kontaktdaten
- Benutzer- und Kontodaten
- Authentisierungs- und Sicherheitsdaten
- Dokumente und Dokumentmetadaten
- Akten-, Geschäfts- und Referenzzeichen
- Kommunikationsdaten
- Vorgangs- und Fristinformationen
- Forderungs- und Gläubigerdaten
- Einkommens-, Ausgaben-, Vermögens- und Schuldendaten
- Angaben zu Pfändungen und P-Konten
- technische Protokoll- und Sicherheitsdaten

Dokumente können darüber hinaus personenbezogene Daten enthalten, deren Inhalt der Auftragnehmer bei der Bereitstellung des Systems nicht abschließend vorherbestimmen kann.

Soweit besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder besonders schutzbedürftige Informationen verarbeitet werden können, sind Schutzbedarf und Zulässigkeit im konkreten Einsatz gesondert zu berücksichtigen.

§ 5 Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, soweit keine gesetzliche Verpflichtung zu einer darüber hinausgehenden Verarbeitung besteht.

Weisungen können insbesondere erteilt werden durch:

- vertragliche Festlegungen
- Systemeinstellungen
- Administrationshandlungen
- dokumentierte Supportanforderungen

Hält der Auftragnehmer eine Weisung für datenschutzrechtlich unzulässig, informiert er den Auftraggeber unverzüglich. Die Durchführung kann bis zur Klärung ausgesetzt werden.

§ 6 Vertraulichkeit

Personen, die Zugang zu personenbezogenen Daten erhalten können, werden zur Vertraulichkeit verpflichtet beziehungsweise unterliegen einer entsprechenden gesetzlichen Verpflichtung.

Zugriffsberechtigungen werden nach Erforderlichkeit vergeben.

Personenbezogene Inhalte dürfen nicht allein aufgrund bestehender technischer Administrationsmöglichkeiten für sachfremde Zwecke eingesehen oder verwendet werden.

§ 7 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft angemessene technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO.

Diese werden insbesondere dokumentiert in Anlage 2 – Zentrale technische und organisatorische Maßnahmen von Sentinel System sowie, soweit eingesetzt, Anlage 3 – Produktspezifische TOM Virtueller Bürger-Schreibtisch einschließlich Schuldnerberatung.

Zu den Maßnahmen gehören abhängig vom eingesetzten Dienst insbesondere:

- TLS-gesicherte Kommunikation
- Firewall- und Netzwerkschutz
- Authentisierung und Passkeys
- serverseitige Rollen- und Berechtigungsprüfung
- Konten- und Objektisolation
- widerrufbare Vorgangsfreigaben
- Protokollierung sicherheitsrelevanter Vorgänge
- kontrollierte Dokumentenverarbeitung
- Datensicherung und Wiederherstellung
- technische Regressionstests

Der Auftragnehmer darf technische und organisatorische Maßnahmen weiterentwickeln, sofern das vereinbarte Schutzniveau dadurch nicht unterschritten wird.

§ 8 Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung dieser Vereinbarung im gesetzlich erforderlichen Umfang zu überprüfen.

Der Auftragnehmer stellt hierfür geeignete Informationen und Nachweise zur Verfügung. Hierzu können insbesondere gehören:

- aktuelle TOMs
- Architektur- und Sicherheitsbeschreibungen
- Unterauftragnehmerübersichten
- dokumentierte technische Prüfungen
- Nachweise über wesentliche Sicherheitsverfahren

Vor-Ort-Prüfungen sind bei berechtigtem Anlass und angemessener Vorankündigung abzustimmen.

Dabei sind Betriebs- und Geschäftsgeheimnisse sowie die Daten anderer Auftraggeber und Nutzer zu schützen.

§ 9 Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang bei der Erfüllung datenschutzrechtlicher Pflichten, soweit diese die Auftragsverarbeitung betreffen. Dies umfasst insbesondere Unterstützung bei:

- Betroffenenanfragen
- Berichtigung und Löschung
- Einschränkung der Verarbeitung
- Datenexport beziehungsweise Herausgabe
- Sicherheitsvorfällen
- Datenschutz-Folgenabschätzungen, soweit erforderlich
- Konsultationen der Aufsichtsbehörde, soweit die Verarbeitung durch den Auftragnehmer betroffen ist

§ 10 Meldung von Sicherheitsverletzungen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, soweit diese die im Auftrag verarbeiteten Daten betrifft.

Die Information enthält, soweit zu diesem Zeitpunkt verfügbar: Art des Vorfalls, betroffene Systeme beziehungsweise Datenkategorien, voraussichtliche Auswirkungen, bereits ergriffene oder vorgesehene Gegenmaßnahmen und einen Ansprechpartner für die weitere Abstimmung.

Noch nicht verfügbare Informationen können nachgereicht werden.

Die gesetzliche Bewertung und gegebenenfalls erforderliche Meldung nach Art. 33 DSGVO bleibt Aufgabe des jeweils hierfür Verantwortlichen.

§ 11 Betroffenenrechte

Geht beim Auftragnehmer eine Anfrage einer betroffenen Person ein, die erkennbar eine Verarbeitung des Auftraggebers betrifft, wird die Anfrage grundsätzlich an den Auftraggeber weitergeleitet, soweit keine anderweitige rechtliche Verpflichtung besteht.

Der Auftragnehmer entscheidet nicht eigenständig über die materiell-rechtliche Berechtigung einer solchen Anfrage, soweit dies Aufgabe des Auftraggebers als Verantwortlichem ist.

§ 12 Berichtigung, Einschränkung und Löschung

Der Auftragnehmer ermöglicht beziehungsweise unterstützt die vertraglich und technisch vorgesehenen Verfahren zur Berichtigung, Einschränkung und Löschung personenbezogener Daten.

Das Löschen aktiver Fachdaten ist von der zeitversetzten Entfernung aus Sicherungssystemen zu unterscheiden.

Konkrete Aufbewahrungs- und Löschfristen werden in der entsprechenden Anlage beziehungsweise dem Löschkonzept festgelegt.

§ 13 Unterauftragnehmer

Der Auftragnehmer darf weitere Auftragsverarbeiter einsetzen, sofern die Voraussetzungen des Art. 28 Abs. 2 und 4 DSGVO eingehalten werden.

Die jeweils eingesetzten Unterauftragnehmer werden in einer aktuellen Übersicht geführt.

Nach gegenwärtigem Stand gehört hierzu insbesondere der für die Serverinfrastruktur eingesetzte Hostinganbieter Hetzner.

Vor Vertragsabschluss wird dem Auftraggeber die vollständige, für den konkreten Dienst maßgebliche Unterauftragnehmerliste zur Verfügung gestellt.

Für neue beziehungsweise ausgetauschte Unterauftragnehmer wird ein Verfahren zur Information und gegebenenfalls zum Widerspruch entsprechend der vertraglichen Ausgestaltung festgelegt.

§ 14 Verarbeitung außerhalb EU/EWR

Eine Verarbeitung außerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums findet nur statt, wenn die gesetzlichen Voraussetzungen hierfür erfüllt sind.

Insbesondere externe KI-, Kommunikations- oder sonstige Cloud-Dienste sind vor ihrer Aufnahme in die produktive Verarbeitung hinsichtlich Datenübermittlung, Verarbeitungsort und gegebenenfalls erforderlicher Garantien gesondert zu dokumentieren.

Dieser Punkt wird für den konkreten Pilot anhand der tatsächlich aktivierten Dienste ausgefüllt.

§ 15 Datenstandort und Hosting

Die gegenwärtig für den Bürger-Schreibtisch verwendete Serverinfrastruktur wird bei Hetzner am Standort Nürnberg, Deutschland betrieben.

Der Virtuelle Bürger-Schreibtisch und Sentinel System befinden sich derzeit auf derselben Serverinstanz, werden jedoch als getrennte Anwendungsdienste betrieben.

Der Bürger-Schreibtisch verwendet derzeit intern den Anwendungsport 8104.

Die produktspezifische technische Trennung wird in den TOMs näher beschrieben.

§ 16 Einsatz von KI-Funktionen

Der Einsatz von KI-Funktionen ist von der regulären Speicherung und regelbasierten Dokumentenverarbeitung zu unterscheiden.

Soweit personenbezogene Daten an einen externen KI-Anbieter übermittelt werden sollen, wird der entsprechende Datenfluss hinsichtlich Zweck, Datenumfang, Anbieter, Speicherbedingungen und Verarbeitungsort dokumentiert.

Beim Bürger-Schreibtisch ist die kontospezifische KI-Nutzung nach dem dokumentierten Produktstand standardmäßig deaktiviert.

Die Aktivierung einer KI-Funktion bedeutet nicht automatisch, dass sämtliche Inhalte eines Bürgerkontos oder Vorgangs an einen externen Dienst übermittelt werden.

§ 17 Ende der Auftragsverarbeitung

Nach Beendigung des Vertragsverhältnisses werden personenbezogene Daten entsprechend der Weisung des Auftraggebers zurückgegeben beziehungsweise gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Dies umfasst auch vorhandene Kopien nach Maßgabe des vereinbarten Lösch- und Sicherungskonzepts.

Technisch unvermeidbare Restbestände in Sicherungssystemen werden spätestens im Rahmen der vorgesehenen Backup-Rotation entfernt und bis dahin nicht für den regulären Betrieb wiederhergestellt oder anderweitig verarbeitet, soweit keine Wiederherstellung aus Sicherheits- oder Notfallgründen erforderlich ist.

§ 18 Nachweis und Dokumentation

Der Auftragnehmer führt die für seine Verpflichtungen erforderlichen Nachweise und Dokumentationen.

Interne automatisierte Tests können hierbei als technischer Entwicklungs- und Regressionsnachweis herangezogen werden.

Sie werden nicht als unabhängiges Audit, Zertifizierung oder externer Penetrationstest bezeichnet.

§ 19 Haftung

Für die Haftung gelten Art. 82 DSGVO sowie die Regelungen des zugrunde liegenden Hauptvertrags und die gesetzlichen Vorschriften.

Diese Vereinbarung erweitert eine gesetzlich nicht bestehende Haftung nicht automatisch.

§ 20 Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung einschließlich ihrer Anlagen sind nachvollziehbar zu dokumentieren.

Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag haben hinsichtlich der datenschutzrechtlichen Auftragsverarbeitung die zwingenden Anforderungen der DSGVO und diese Vereinbarung Vorrang.

Sollten einzelne Bestimmungen unwirksam sein oder werden, bleiben die übrigen Bestimmungen hiervon unberührt.

Anlagen zum AVV

- Anlage 1: Gegenstand, Dauer, Art und Zweck der konkreten Verarbeitung
- Anlage 2: Zentrale TOM Sentinel System
- Anlage 3: TOM Virtueller Bürger-Schreibtisch / Schuldnerberatung
- Anlage 4: Unterauftragnehmer
- Anlage 5: Lösch- und Aufbewahrungskonzept
- Anlage 6: Ansprechpartner und Weisungsberechtigte

Anlage 1 – Pilot Bürger-Schreibtisch / Schuldnerberatung

Leistung: Bereitstellung des Virtuellen Bürger-Schreibtischs und der geschützten Beratungsoberfläche.

Zweck: Digitale Vorbereitung, Strukturierung und kontrollierte Übergabe eines durch den Bürger freigegebenen Schuldnerberatungsvorgangs.

Betroffene: Teilnehmende Bürger, gegebenenfalls Haushaltsangehörige beziehungsweise weitere in Unterlagen genannte Personen, Gläubiger, Mitarbeiter und Berater des Pilotpartners sowie Kommunikationspartner.

Daten: Konto- und Stammdaten, Dokumente, Forderungsinformationen, Haushalts- und Finanzinformationen, Pfändungs-/P-Konto-Angaben, Vorgangsinformationen, Kommunikations- und Sicherheitsdaten.

Besondere Begrenzung: Eine Beratungsstelle erhält nicht allein aufgrund ihrer Teilnahme Zugriff auf Bürgerkonten. Der Zugriff setzt eine entsprechende Freigabe des konkreten Vorgangs voraus. Private Bürgernotizen sind nicht Bestandteil dieser Freigabe.

Speicherort: Gegenwärtig Hetzner, Nürnberg, Deutschland.

Dauer: Dauer des Pilotprojekts zuzüglich vereinbarter Export-, Rückgabe- und Löschphase.

Zwingende Rollenklärung vor Vertragsschluss

Dieses Muster ist vor Veröffentlichung und Unterzeichnung rechtlich und tatsächlich auf das konkrete Bereitstellungsmodell anzupassen.

Wenn ein Bürger selbst ein Konto eröffnet und Daten für eigene Zwecke verarbeitet, ist eine Kommune nicht automatisch Auftraggeber der gesamten Verarbeitung.

Erhält eine kommunale Schuldnerberatung nur einen vom Bürger freigegebenen Vorgang, muss für jeden Verarbeitungsschritt geprüft werden, wer Verantwortlicher und wer Auftragsverarbeiter ist.

Mögliche Struktur: Sentinel ↔ Bürger als eigenes Vertrags-/Datenschutzverhältnis; Beratungsstelle ↔ Bürger in eigener Verantwortlichkeit; Sentinel ↔ Beratungsstelle als Auftragsverarbeitung für den geschützten Beratungsbereich.