Auftragsverarbeitung (AV)

Standardisierte Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO für das Citivo Webprojekt

Dokumenttyp	**Mustervertrag / Standard-AV mit Anlagen**
Version und Stand	**Version 1.0, 02.06.2026**
Geltungsbereich	**Betrieb, Wartung, Hosting, Support und optionale Zusatzmodule des Webprojekts**
Vertragsparteien	**Vor Unterzeichnung in Abschnitt 1 zu ergänzen**

> Diese Vorlage ist eine standardisierte Arbeitsgrundlage für eine Auftragsverarbeitung. Sie muss vor Vertragsschluss mit den tatsächlichen Parteien, Unterauftragsverarbeitern, technischen und organisatorischen Maßnahmen sowie den konkret aktivierten Modulen abgeglichen werden. Sie ersetzt keine individuelle rechtliche Prüfung.

1. Vertragsparteien

Zwischen

Rolle	Angaben
Auftraggeber / Verantwortlicher	*[Name der Kommune / Organisation, Anschrift, Vertretungsberechtigte, Datenschutzkontakt eintragen]*
Auftragnehmer / Auftragsverarbeiter	*[Name des Betreibers / Dienstleisters, Anschrift, Vertretungsberechtigte, Datenschutzkontakt eintragen]*

wird die folgende Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag geschlossen.

2. Gegenstand, Rangfolge und Hauptvertrag

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Auftraggebers, soweit dies für Betrieb, Wartung, Support, Hosting, Fehleranalyse, Sicherheit und Weiterentwicklung des Webprojekts erforderlich ist.
2. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien für den zugrunde liegenden Hauptvertrag über das Webprojekt. Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieser AV für Verarbeitungsvorgänge im Auftrag vor.
3. Gegenstand, Dauer, Art, Zweck, Datenkategorien und betroffene Personengruppen ergeben sich aus dieser Vereinbarung und insbesondere aus Anlage 1.

3. Dauer der Verarbeitung

1. Die Verarbeitung beginnt mit Einrichtung oder produktiver Bereitstellung des Webprojekts und läuft für die Dauer des Hauptvertrags.
2. Nach Ende des Hauptvertrags hat der Auftragnehmer personenbezogene Daten nach Wahl und Weisung des Auftraggebers zurückzugeben oder zu löschen, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.
3. Backups und technische Protokolle werden nach den vereinbarten Lösch- und Rotationszyklen entfernt, sofern eine sofortige Löschung technisch nicht mit angemessenem Aufwand möglich ist.

4. Art und Zweck der Verarbeitung

Die Verarbeitung dient dem sicheren und nachvollziehbaren Betrieb eines kommunalen Webprojekts mit Verwaltungs- und Bürgerfunktionen. Je nach aktivierten Modulen umfasst dies insbesondere:

- Annahme, Bearbeitung und Dokumentation von Meldungen, Hinweisen, Support- und Kontaktanfragen,
- Nutzer-, Melder- und Administrationskonten einschließlich Berechtigungs- und Rollenverwaltung,
- Bürgerbeteiligung, Verfahren, Kommentare, Beiträge, Umfragen, Petitionen und Veranstaltungsanmeldungen,
- Baustellen-, Planungs-, Liegenschafts- und Raumverwaltungsfunktionen einschließlich Buchungs- und Kalenderdaten,
- E-Mail-Benachrichtigungen, Statuskommunikation, Bestätigungen und Passwortprozesse,
- Sicherheitsmaßnahmen wie Protokollierung, Missbrauchserkennung, Rate-Limiting, Spam- und Bot-Schutz,
- optionale KI-gestützte Analyse, sofern vom Auftraggeber aktiviert und freigegeben.

Eine Verarbeitung zu eigenen Zwecken des Auftragnehmers findet nicht statt.

5. Weisungen des Auftraggebers

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Betroffenenrechte und die dokumentierten Weisungen verantwortlich.
2. Weisungen können im Hauptvertrag, in dieser AV, in Konfigurationsentscheidungen, in Tickets, per E-Mail oder in sonstiger Textform erfolgen.
3. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Ansicht ist, dass eine Weisung gegen Datenschutzrecht verstößt. Die Ausführung der Weisung kann bis zur Klärung ausgesetzt werden, soweit dies erforderlich ist.

6. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers, auch in Bezug auf Übermittlungen in Drittstaaten oder an internationale Organisationen.
2. Der Auftragnehmer verpflichtet alle Personen, die Zugriff auf personenbezogene Daten erhalten, auf Vertraulichkeit, soweit keine gesetzliche Verschwiegenheitspflicht besteht.
3. Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Die standardisierten Maßnahmen sind in Anlage 2 beschrieben.
4. Der Auftragnehmer unterstützt den Auftraggeber angemessen bei Betroffenenanfragen, Datenschutz-Folgenabschätzungen, Sicherheitsprüfungen und Anfragen von Aufsichtsbehörden, soweit die Verarbeitung im Auftrag betroffen ist.
5. Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden an den Auftraggeber und stellt die zur Bewertung und Meldung erforderlichen Informationen bereit.
6. Der Auftragnehmer stellt dem Auftraggeber die erforderlichen Informationen zum Nachweis der Einhaltung dieser AV bereit und ermöglicht angemessene Prüfungen nach Abschnitt 10.

7. Technische und organisatorische Maßnahmen

Der Auftragnehmer unterhält ein Sicherheitsniveau, das dem Risiko der Verarbeitung angemessen ist. Die Maßnahmen werden regelmäßig überprüft und bei Bedarf weiterentwickelt. Die in Anlage 2 dokumentierten Maßnahmen bilden den Mindeststandard für das Webprojekt.

8. Unterauftragsverarbeiter

1. Der Auftraggeber erteilt eine allgemeine Genehmigung für den Einsatz von Unterauftragsverarbeitern, soweit diese in Anlage 3 aufgeführt oder in Textform freigegeben sind.
2. Der Auftragnehmer informiert den Auftraggeber rechtzeitig über beabsichtigte Änderungen, insbesondere Hinzufügung oder Ersetzung von Unterauftragsverarbeitern. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.
3. Der Auftragnehmer verpflichtet Unterauftragsverarbeiter auf dieselben wesentlichen Datenschutzpflichten, die in dieser AV geregelt sind. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Pflichten verantwortlich.
4. Eine Verarbeitung in Drittstaaten oder durch Anbieter mit Drittstaatenbezug erfolgt nur nach Maßgabe von Abschnitt 9 und Anlage 3.

9. Drittlandübermittlungen

1. Personenbezogene Daten sollen grundsätzlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeitet werden.
2. Eine Übermittlung in Drittstaaten ist nur zulässig, wenn der Auftraggeber sie dokumentiert angewiesen oder genehmigt hat und die Voraussetzungen der DSGVO, insbesondere Kapitel V, eingehalten werden.
3. Geeignete Garantien können insbesondere ein Angemessenheitsbeschluss, Standardvertragsklauseln, zusätzliche Schutzmaßnahmen oder eine andere zulässige Grundlage sein.

10. Nachweise und Prüfungen

1. Der Auftragnehmer stellt auf Anfrage geeignete Nachweise zur Einhaltung dieser AV zur Verfügung, etwa Sicherheitskonzepte, technische Dokumentationen, TOM-Übersichten oder Zertifikate, soweit vorhanden.
2. Prüfungen erfolgen nach vorheriger Abstimmung, während üblicher Geschäftszeiten und unter Wahrung von Vertraulichkeit, Betriebsgeheimnissen und Sicherheitsinteressen.
3. Vor-Ort-Prüfungen sind nur erforderlich, wenn dokumentenbasierte Nachweise oder Remote-Prüfungen zur angemessenen Kontrolle nicht ausreichen.

11. Löschung, Rückgabe und Berichtigung

1. Der Auftragnehmer berichtigt, sperrt, anonymisiert, löscht oder exportiert personenbezogene Daten nach dokumentierter Weisung des Auftraggebers, soweit dies technisch möglich und zumutbar ist.

2. Nach Vertragsende werden personenbezogene Daten nach Wahl des Auftraggebers zurückgegeben oder gelöscht. Gesetzliche Aufbewahrungspflichten und technisch notwendige Backup-Zyklen bleiben unberührt.
3. Der Auftragnehmer bestätigt die Löschung auf Wunsch in Textform.

12. Verantwortlichkeiten und Haftung

1. Der Auftraggeber bleibt Verantwortlicher im Sinne der DSGVO und entscheidet über Zwecke und Mittel der Verarbeitung, soweit diese nicht rein technische Umsetzung im Auftrag sind.
2. Die Haftung richtet sich nach den gesetzlichen Vorschriften und den Vereinbarungen des Hauptvertrags. Zwingende datenschutzrechtliche Ansprüche bleiben unberührt.

13. Schlussbestimmungen

1. Änderungen und Ergänzungen dieser AV bedürfen der Textform, soweit keine strengere Form gesetzlich vorgeschrieben ist.
2. Sollte eine Regelung unwirksam sein, bleibt die Wirksamkeit der übrigen Regelungen unberührt. Die Parteien ersetzen die unwirksame Regelung durch eine wirksame Regelung, die dem datenschutzrechtlichen Zweck möglichst nahekommt.
3. Soweit rechtlich zulässig, gilt deutsches Recht. Der Gerichtsstand richtet sich nach dem Hauptvertrag oder den gesetzlichen Vorschriften.

14. Unterschriften

Ort, Datum, Unterschrift Auftraggeber / Verantwortlicher	Ort, Datum, Unterschrift Auftragnehmer / Auftragsverarbeiter

Anlage 1 - Beschreibung der Verarbeitung

A. Gegenstand und Zweck

Bereich	Beschreibung
Webprojekt	Betrieb eines kommunalen Webportals mit öffentlichen Formularen, Verwaltungsbackend, Kommunikationsfunktionen und optionalen Zusatzmodulen.
Zwecke	Bereitstellung digitaler Verwaltungs- und Bürgerdienste, Bearbeitung von Meldungen und Anfragen, Beteiligung, Raum- und Liegenschaftsverwaltung, Benachrichtigung, Support, Sicherheit, Protokollierung und Missbrauchsprävention.
Verarbeitungsarten	Erheben, Speichern, Anzeigen, Ändern, Übermitteln, Protokollieren, Löschen, Exportieren, Sichern, Wiederherstellen und Auswerten nach Weisung des Auftraggebers.

B. Kategorien personenbezogener Daten

- Kontakt- und Stammdaten: Name, Vorname, E-Mail-Adresse, Telefonnummer, Organisationszugehörigkeit, Rolle.
- Kontodaten: Login-Daten, Passwort-Hash, Rollen, Berechtigungen, Bestätigungs- und Reset-Tokens, Registrierungs- und Login-Zeitpunkte.
- Meldungs- und Vorgangsdaten: Beschreibung, Status, interne und öffentliche Kommentare, Zuständigkeiten, Prioritäten, Aktenzeichen, Zeitpunkte.
- Standort- und Inhaltsdaten: Adresse, GPS-Koordinaten, Kartenbezug, Fotos, Dateianhänge, Dokumente und hochgeladene Inhalte.
- Beteiligungsdaten: Beiträge, Kommentare, Umfrageantworten, Unterstützungen, Petitionsteilnahmen, Veranstaltungsanmeldungen und zugehörige Bestätigungen.
- Raum-, Buchungs- und Liegenschaftsdaten: Buchungsanfragen, Kontaktangaben, Termine, Kalender- und Nutzungsdaten.
- Kommunikationsdaten: E-Mail-Versanddaten, Benachrichtigungen, Supportnachrichten und Bearbeitungsvermerke.
- Technische Daten: IP-Adresse, Zeitstempel, Browser- und Geräteinformationen, Sicherheits- und Fehlerprotokolle, Rate-Limit-Informationen, Bot-Schutz-Prüfdaten.

- Optionale Analysedaten: KI-Analyseergebnisse oder Klassifikationen, sofern das Modul aktiviert und freigegeben ist.

C. Kategorien betroffener Personen

- Bürgerinnen und Bürger, Melderinnen und Melder, registrierte Nutzerinnen und Nutzer,
- Teilnehmende an Beteiligungen, Umfragen, Petitionen und Veranstaltungen,
- Raum- und Buchungsinteressierte, Kontaktpersonen und Anfragende,
- Mitarbeitende, Administrierende, Sachbearbeitende und sonstige berechtigte Personen des Auftraggebers,
- Dienstleister, Ansprechpartner, Bauherrn, Träger oder andere in Vorgängen genannte Personen.

D. Besondere Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nicht Zweck des Webprojekts. Da öffentliche Formulare Freitextfelder und Uploads enthalten können, kann eine unbeabsichtigte Eingabe solcher Daten durch Nutzer nicht vollständig ausgeschlossen werden. Der Auftraggeber legt fest, wie solche Inhalte zu behandeln sind.

E. Lösch- und Aufbewahrungslogik

Die konkrete Speicherdauer richtet sich nach den Weisungen des Auftraggebers, gesetzlichen Aufbewahrungspflichten, Fachverfahrensanforderungen und den im Webprojekt konfigurierten Lösch- und Archivierungsregeln. Technische Protokolle und Sicherheitsdaten werden nur so lange aufbewahrt, wie dies für Sicherheit, Nachvollziehbarkeit und Betrieb erforderlich ist.

Anlage 2 - Technische und organisatorische Maßnahmen

1. Vertraulichkeit

Maßnahme	Standard
Zutrittskontrolle	Rechenzentrums- und Serverzugang nur für berechtigte Personen des jeweiligen Hosting- oder Infrastrukturbetreibers; physische Sicherheitsmaßnahmen nach dem Standard des eingesetzten Providers.
Zugangskontrolle	Personalisierte Benutzerkonten, Passwortschutz, Session-Timeouts, administrative Zugriffsbeschränkungen und nach Möglichkeit starke Authentisierung für privilegierte Konten.
Zugriffskontrolle	Rollen- und Rechtekonzept, gemeinde- oder modulbezogene Berechtigungen, Least-Privilege-Prinzip und Trennung öffentlicher sowie administrativer Funktionen.
Vertraulichkeitspflichten	Verpflichtung der eingesetzten Personen auf Vertraulichkeit und Begrenzung des Zugriffs auf Personen, die diesen zur Aufgabenerfüllung benötigen.

2. Integrität

Maßnahme	Standard
Transportverschlüsselung	Verschlüsselte Übertragung über HTTPS/TLS im Produktivbetrieb; sichere SMTP- oder API-Übertragung nach Konfiguration des Auftraggebers.
Eingabe- und Änderungskontrolle	Protokollierung relevanter administrativer Vorgänge, Zeitstempel, technische Logs und nachvollziehbare Bearbeitungsstände, soweit im System vorgesehen.
Schutz vor Manipulation	CSRF-Schutz, serverseitige Validierung, Bereinigung von HTML-Inhalten, Zugriffsbeschränkungen für Uploads und Sicherheitsprüfungen gegen Missbrauch.

3. Verfügbarkeit und Belastbarkeit

Maßnahme	Standard
Backups	Regelmäßige Sicherungen nach vereinbartem Betriebsmodell; Wiederherstellung nach Weisung und technischer Möglichkeit.
Betriebssicherheit	Monitoring, Fehlerprotokollierung, Wartungsmodus, Updates nach Betriebsvereinbarung und Schutzmechanismen gegen Überlastung oder automatisierten Missbrauch.
Notfallfähigkeit	Dokumentierte Wiederherstellungswege, technische Ansprechpartner und geordnete Eskalation bei Sicherheits- oder Verfügbarkeitsvorfällen.

4. Trennung, Datenschutz durch Technikgestaltung und Standardvorgaben

Maßnahme	Standard
Mandanten- und Modultrennung	Logische Trennung nach Rollen, Gemeinden, Modulen und Zuständigkeiten, soweit im Projekt aktiviert.
Datenminimierung	Pflichtfelder nur soweit für den jeweiligen Vorgang erforderlich; optionale Kontaktdaten und konfigurierbare Veröffentlichung von Inhalten.
Löschung und Anonymisierung	Konfigurierbare Lösch-, Papierkorb- und Bereinigungsprozesse; temporäre Rate-Limit- und Sicherheitsdaten werden nach Zweckfortfall gelöscht oder rotiert.
Auftragskontrolle	Verarbeitung nur nach Weisung, dokumentierte Unterauftragsverarbeiter und regelmäßige Überprüfung der getroffenen Maßnahmen.

Die TOMs sind vor Vertragsschluss gegen das konkrete Hosting-, Betriebs- und Supportmodell zu prüfen und bei Bedarf projektspezifisch zu ergänzen.

Anlage 3 - Unterauftragsverarbeiter und Drittlandbezug

Die folgende Tabelle ist vor Unterzeichnung mit den tatsächlich eingesetzten Anbietern zu vervollständigen. Nicht aktivierte optionale Dienste sind zu streichen.

Leistung / Dienst	Anbieter	Sitz / Verarbeitungsort	Zweck	Status
Hosting / Server / Rechenzentrum	*[eintragen]*	*[eintragen]*	Betrieb des Webprojekts, Datenbank, Dateispeicher, Backups	*freizugeben*
E-Mail-Versand / SMTP	*[eintragen]*	*[eintragen]*	Benachrichtigungen, Bestätigungsmails, Passwortprozesse	*freizugeben*
Bot-Schutz / Spam-Schutz	*[z. B. Cloudflare Turnstile, falls aktiviert]*	*[eintragen]*	Missbrauchsprävention bei öffentlichen Formularen	*optional*
Karten-, Geocoding- oder Geodatendienste	*[eintragen, falls personenbezogene Daten übermittelt werden]*	*[eintragen]*	Standortsuche, Kartenanzeige, Lagebezug	*optional*
KI- oder Analyse-Dienst	*[eintragen, falls aktiviert]*	*[eintragen]*	Klassifikation oder Analyse von Meldungsinhalten nach Freigabe des Auftraggebers	*optional*
Support-, Wartungs- oder Monitoringdienst	*[eintragen]*	*[eintragen]*	Fehleranalyse, Betriebsüberwachung, technische Unterstützung	*freizugeben*

Freigabe und Änderung

Der Auftraggeber genehmigt die in dieser Anlage aufgeführten Unterauftragsverarbeiter. Änderungen sind dem Auftraggeber in Textform mitzuteilen. Der Auftraggeber kann innerhalb einer angemessenen Frist widersprechen, wenn ein wichtiger datenschutzrechtlicher Grund vorliegt.

Drittlandbezug

Besteht bei einem Unterauftragsverarbeiter ein Drittlandbezug, sind die konkrete Rechtsgrundlage, geeignete Garantien und zusätzliche Schutzmaßnahmen in der Tabelle oder einer Ergänzung zu dokumentieren.