Anforderungen öffentlicher Auftraggeber — Einordnung für Amturo

Dokument DS-10 · Version 1.7 · Stand 19.11.2026

Kommunale Datenschutzbeauftragte, IT-Sicherheitsbeauftragte und Vergabestellen prüfen neben der DSGVO weitere Regelwerke. Diese Übersicht ordnet ein, was sie typischerweise erwarten und wie Amturo diese Anforderungen erfüllt oder unterstützt. Die Einordnungen geben die Sicht von Amturo wieder; die rechtliche Bewertung trifft die Kommune. Die Quellen wurden am 22.10.2026 abgerufen.

1. Übersicht

Thema	Was Kommunen typischerweise erwarten	Stand bei Amturo
Auftragsverarbeitung (Art. 28 DSGVO)	Vertrag mit allen Pflichtinhalten, Unterauftragsverarbeiter mit Einspruchsrecht	AVV-Vorlage mit allen Anlagen
Verzeichnis (Art. 30 Abs. 2 DSGVO)	Verzeichnis des Auftragsverarbeiters, Ausfüllhilfe für das eigene Verzeichnis	Verzeichnis nach Art. 30 Abs. 2 DSGVO
TOM (Art. 32 DSGVO)	Beschreibung nach Standard-Datenschutzmodell (SDM) bzw. Art. 32	Maßnahmen nach Art. 32 DSGVO mit Zuordnung zu den SDM-Gewährleistungszielen
DSFA (Art. 35 DSGVO)	Unterstützung mit Systembeschreibung und Risikoanalyse	Schwellwertanalyse, Risiken und Maßnahmen je Modul
§ 203 StGB	Verpflichtung der mitwirkenden Personen zur Geheimhaltung	Geheimhaltungsverpflichtung im AVV (§ 3)
BSI C5 / IT-Grundschutz	Testat des Cloud-Anbieters, Sicherheitskonzept des SaaS-Anbieters	Hosting-Anbieter mit C5 Typ 1 und ISO 27001 auf Basis IT-Grundschutz; Amturo selbst ohne Zertifizierung
EVB-IT Cloud	Vertragsmuster des Bundes, oft auch von Kommunen genutzt	Die Unterlagen können als Datenschutzanlagen in einen EVB-IT-Cloudvertrag einbezogen werden; Zusätzliches regelt der Hauptvertrag
Barrierefreiheit (BITV 2.0)	Barrierefreie Bürgeroberflächen, Erklärung zur Barrierefreiheit	Seite für die Erklärung zur Barrierefreiheit der Kommune; ergänzend eine Werkzeugleiste zur individuellen Anpassung der Darstellung
OZG / BundID	Anbindung an das Bürgerkonto des Bundes nach OZG	optionales Modul (SAML-Anbindung)
TDDDG § 25	Keine Cookies/Speicherungen ohne Einwilligung, außer unbedingt erforderlich	Bürgerseiten ohne Tracking und ohne Speicherung zur Statistik; Speicher-Inventar unten

Thema	Was Kommunen typischerweise erwarten	Stand bei Amturo
NIS2	Lieferkettensicherheit bei Einrichtungen im Anwendungsbereich	Nach Einschätzung von Amturo nicht selbst erfasst; die Unterlagen unterstützen die Lieferkettenprüfung der Kunden
Data Act	Wechsel- und Exit-Regeln für Cloud-/SaaS-Verträge	Wechsel spätestens zwei Monate nach Verlangen, 30 Tage Übergang, mindestens 30 Tage Datenabruf, keine Wechselentgelte (Hauptvertrag); Export in offenen Formaten (AVV § 11)

2. Auftragsverarbeitung und EU-Standardvertragsklauseln

Art. 28 Abs. 3 DSGVO schreibt die Pflichtinhalte eines AVV vor (Weisungen, Vertraulichkeit, Sicherheit, Unterauftragsverarbeiter, Unterstützung bei Betroffenenrechten und bei Art. 32 bis 36, Löschung oder Rückgabe, Nachweise und Prüfungen). Die EU-Kommission hat dafür Standardvertragsklauseln erlassen (Durchführungsbeschluss (EU) 2021/915), deren Nutzung freiwillig ist. Die AVV-Vorlage von Amturo deckt die Pflichtinhalte ab; ihre Anlagen beschreiben die nach Art. 28 Abs. 3 DSGVO erforderlichen Angaben zur Verarbeitung und zu den Schutzmaßnahmen. Auf Wunsch der Kommune schließt Amturo den Vertrag auf Grundlage der Standardvertragsklauseln ab.

Quellen: DSGVO (EUR-Lex), Durchführungsbeschluss (EU) 2021/915.

3. Geheimnisschutz nach § 203 StGB

Beschäftigte in Bürgerämtern, die Aufgaben der öffentlichen Verwaltung wahrnehmen, sind regelmäßig Amtsträger und damit Geheimnisträger (§ 203 Abs. 2 Satz 1 Nr. 1 StGB). Sie dürfen Geheimnisse an mitwirkende Dienstleister nur offenbaren, wenn diese zur Geheimhaltung verpflichtet sind; sonst macht sich der Geheimnisträger strafbar (§ 203 Abs. 3 Satz 2, Abs. 4 Satz 2 Nr. 1 StGB). Soweit im Rahmen des Auftrags gesetzlich geschützte Geheimnisse zugänglich werden, stellt Amturo die hierfür erforderlichen Geheimhaltungsverpflichtungen der mitwirkenden Personen und der weiteren Verarbeitungskette sicher (AVV § 3). Für Sozialdaten gelten zusätzlich § 35 SGB I und § 80 SGB X.

Quelle: § 203 StGB, § 80 SGB X.

4. BSI: C5, Mindeststandard Cloud, IT-Grundschutz

- **C5** ist der Kriterienkatalog des BSI für Cloud-Dienste. Er kennt Testate vom Typ 1 (Ausgestaltung zu einem Stichtag) und Typ 2 (Wirksamkeit über einen Zeitraum). Es gibt kein „C5-Zertifikat“, nur Testate. Laut BSI ist neben C5:2020 die neue Fassung C5:2026 erschienen.
- Der **Mindeststandard des BSI zur Nutzung externer Cloud-Dienste** ist nur für die Bundesverwaltung verbindlich; Kommunen nutzen ihn als Orientierung. Er verlangt, dass Cloud-Anbieter mindestens die C5-Basiskriterien erfüllen.
- Für Kommunen gibt es das IT-Grundschutz-Profil **„Basis-Absicherung Kommunalverwaltung“** und den Einstieg **WiBA** („Weg in die Basis-Absicherung“).

Einordnung: Amturo betreibt die Plattform in Rechenzentren der IONOS Cloud in Deutschland. IONOS verfügt über ein ISO-27001-Zertifikat auf Basis von IT-Grundschutz (Compute Engine, S3 Object Storage) und ein C5-Testat vom Typ 1 (Details im Dokument DS-09 „Hosting und Nachweise der Anbieter“). **Amturo selbst ist nicht nach C5, ISO 27001 oder IT-Grundschutz zertifiziert oder testiert.** Formulierungen wie „C5-zertifiziert“ oder „BSI-zertifiziert“ verwendet Amturo nicht.

Quellen: BSI C5, Mindeststandard Cloud, IT-Grundschutz-Profile.

5. EVB-IT Cloud

Die EVB-IT Cloud (Cloudvertrag und Ergänzende Vertragsbedingungen für Cloudleistungen) decken auch Software-as-a-Service ab. Sie enthalten **kein eigenes AVV-Muster**; der AVV wird als Anlage beigefügt. Nach den EVB-IT Cloud-AGB sollen die C5-Basiskriterien auf allen Ebenen erfüllt sein, der Auftragnehmer soll ein ISMS nach ISO 27001 betreiben; Abweichungen sind ausdrücklich zu vereinbaren. Für Bundesbehörden sind EVB-IT verbindlich, Kommunen sind in der Regel nicht gebunden, nutzen sie aber häufig.

Die Unterlagen dieses Pakets (AVV, TOM, Unterauftragsverarbeiter, Löschkonzept) können als Datenschutzanlagen in einen EVB-IT-Cloudvertrag einbezogen werden. Zusätzliche Anforderungen und Abweichungen, etwa zu den C5-Basiskriterien oder zu einem ISMS, werden im jeweiligen Hauptvertrag festgelegt.

Quellen: IT-Planungsrat Beschluss 2022/01, Bitkom FAQ EVB-IT Cloud (2022, Verbandspublikation).

6. Barrierefreiheit

Öffentliche Stellen müssen ihre Websites und mobilen Anwendungen barrierefrei gestalten (Richtlinie (EU) 2016/2102; im Bund BGG und BITV 2.0, in den Ländern die Landesgesetze). Dazu gehört eine **Erklärung zur Barrierefreiheit** mit Feedback-Mechanismus (§ 7 BITV 2.0). Die BITV 2.0 nennt ausdrücklich auch elektronisch unterstützte Verwaltungsabläufe, also möglicherweise auch die Oberflächen der Beschäftigten.

Amturo stellt die Seite `/barrierefreiheit` bereit, auf der die Kommune ihre Erklärung hinterlegt. Ergänzend bietet eine Werkzeugleiste auf den Bürgerseiten individuelle Anpassungen (Schriftgröße, Kontrast, Legasthenie-Schrift, Abstände, Linkhervorhebung, reduzierte Bewegung); sie ergänzt die barrierefreie Gestaltung und ersetzt keine Prüfung nach WCAG bzw. EN 301 549.

Für öffentliche Bürgeroberflächen gelten die einschlägigen Barrierefreiheitsvorgaben des jeweiligen Landes. Das Barrierefreiheitsstärkungsgesetz (BFSG) erfasst eine abschließende Liste von Produkten und Dienstleistungen für Verbraucher. Ob ein gelieferter Check-in-Automat darunter fällt, richtet sich nach seiner Funktion und dem konkreten Einsatz; maßgeblich ist die konkrete Produkt- und Dienstleistungskategorie.

Quellen: BITV 2.0, § 1 BFSG, Richtlinie (EU) 2016/2102.

7. OZG und BundID

Das Bürgerkonto des Bundes (BundID, Weiterentwicklung zur DeutschlandID) ist eine Komponente nach dem Onlinezugangsgesetz. Nach der Orientierungshilfe der Datenschutzkonferenz zum OZG ist die Rechtsgrundlage für die Nutzung keine Einwilligung, sondern die „Veranlassung“ durch die Nutzerin oder den Nutzer (§ 8 OZG i. V. m. Art. 6 Abs. 1 lit. e DSGVO). Für das Nutzerkonto ist die vom Bund bestimmte Stelle verantwortlich, für den angebundenen Onlinedienst die Kommune; Amturo ist Auftragsverarbeiter. Amturo fordert per SAML nur das bereichsspezifische Kennzeichen bPK2 (verpflichtend) sowie optional Vorname, Nachname und E-Mail an.

Quellen: DSK Orientierungshilfe OZG, Version 1.1, OZG.

8. Video-Termine

Die Orientierungshilfe der Datenschutzkonferenz zu Videokonferenzsystemen verlangt mindestens eine Transportverschlüsselung nach BSI TR-02102. Bei hohem Risiko soll die Vertraulichkeit auch auf den Servern gewahrt werden, zum Beispiel durch Ende-zu-Ende-Verschlüsselung, oder durch dokumentierte kompensierende Maßnahmen. Aufzeichnungen sollen standardmäßig ausgeschaltet sein; Funktionen wie Dokumentfreigabe sind abzuwägen.

Amturo: Betrieb des Videoservers durch Amturo selbst in Deutschland, Transportverschlüsselung, keine Aufzeichnungskomponente installiert, kein Chat, Beitritt nur mit zeitlich begrenztem Token, Dokumentübergabe mit Typ- und Größenprüfung und Löschung nach 30 Tagen. Kein weiterer Dienstleister ist beteiligt; administrativen Zugriff auf die Server haben nur Administratoren von Amturo über VPN, privilegierte Zugriffe des Hosting-Anbieters sind vertraglich begrenzt.

Quellen: DSK Orientierungshilfe Videokonferenzsysteme, Checkliste.

9. Speichern auf Endgeräten (§ 25 TDDDG)

Speichern und Auslesen von Informationen auf dem Endgerät ist ohne Einwilligung nur erlaubt, wenn es unbedingt erforderlich ist, um einen ausdrücklich gewünschten Dienst bereitzustellen (§ 25 Abs. 2 Nr. 2 TDDDG). Bürgerseiten von Amturo verwenden nach aktuellem Funktionsumfang:

Speicherung	Zweck	Art	Einordnung (Empfehlung)
Anmelde-Cookie des Bürgerportals	Anmeldung im Bürgerportal	HttpOnly-Cookie, nur nach Login	unbedingt erforderlich
Buchungsfortschritt im Sitzungsspeicher	Fortsetzen einer begonnenen Buchung (Bereich, Leistung, Termin, Reservierung, Schritt)	bis zum Schließen des Browserfensters	unbedingt erforderlich
Einstellungen im Browserspeicher	Barrierefreiheits-Einstellungen, die die Person selbst wählt	dauerhaft im Browser	vom Nutzer ausdrücklich gewünscht

Analyse-, Tracking- oder Werbedienste Dritter sind auf den Bürgerseiten nicht eingebunden. Die eigene Nutzungsstatistik speichert nichts auf dem Gerät und zählt nur Tagessummen. Ein Einwilligungsbanner ist daher nach Einschätzung von Amturo nicht erforderlich.

Quelle: § 25 TDDDG.

10. NIS2

Das NIS2-Umsetzungsgesetz ist am 06.12.2025 in Kraft getreten. Die kommunale Kernverwaltung ist grundsätzlich nicht erfasst; die Länder entscheiden selbst. Eigenbetriebe (z. B. Stadtwerke) können erfasst sein. Amturo ist nach seiner Größe (unter 50 Beschäftigten und 10 Mio. Euro Umsatz) nach Einschätzung von Amturo nicht selbst erfasst (§ 28 BSIG). Kommunen, die selbst erfasst sind, müssen die Sicherheit ihrer Lieferkette berücksichtigen (§ 30 BSIG) und werden Nachweise und Meldewege verlangen; dieses Paket liefert die Grundlage.

Quellen: § 28 BSIG, BSI: NIS-2 für Land und Kommune.

11. Data Act — Anbieterwechsel

Der Data Act (VO (EU) 2023/2854) gilt seit 12.09.2025. Kapitel VI regelt den Wechsel zwischen Datenverarbeitungsdiensten; Amturo wendet diese Regeln auf seine SaaS-Leistung an. Sie stehen im Hauptvertrag (Allgemeine Geschäftsbedingungen von Amturo):

Schritt	Regel
Wechselverlangen	In Textform; der Wechsel beginnt spätestens zwei Monate nach Zugang
Übergangszeitraum	30 Kalendertage, in denen Amturo den Wechsel unterstützt und die Leistungen weiter erbringt; ist das technisch nicht möglich, Mitteilung mit Begründung binnen 14 Arbeitstagen und höchstens sieben Monate
Datenabruf	Mindestens 30 Kalendertage ab Ende des Übergangszeitraums; Export in offenen, maschinenlesbaren Formaten
Vertragsende	Mit erfolgreichem Abschluss des Wechsels, Bestätigung in Textform; bei einem reinen Löschverlangen nach Ablauf der Frist für den Wechselbeginn
Entgelte	Amturo erhebt keine Entgelte für den Wechsel oder die Datenbereitstellung

Davon getrennt ist die ordentliche Kündigung ohne Wechselverlangen: Sie richtet sich nach der vereinbarten Kündigungsfrist; Rückgabe und Löschung der Daten folgen dann AVV § 11.

Quelle: VO (EU) 2023/2854.

12. Landesrecht

Rechtsgrundlage der Kommune ist in der Regel Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit Fachrecht oder der Generalklausel des Landesdatenschutzgesetzes. Landesrecht kann zusätzliche Anforderungen enthalten (z. B. an technische Maßnahmen bei besonderen Kategorien) und eigene DSFA-Listen für öffentliche Stellen.

Änderungshistorie

Datum	Version	Änderung
22.10.2026	1.0	Erste Fassung
24.10.2026	1.1	Inhalte präzisiert
26.10.2026	1.2	Inhalte präzisiert
28.10.2026	1.3	Inhalte aktualisiert
02.11.2026	1.4	Durchgesehen; keine inhaltlichen Änderungen
09.11.2026	1.5	Durchgesehen; keine inhaltlichen Änderungen
12.11.2026	1.6	Durchgesehen; keine inhaltlichen Änderungen
19.11.2026	1.7	Inhalte aktualisiert