

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Vertragszuordnung

dataMatters GmbH, Pilgrimstr. 6, 50674 Köln

Auftraggeber / Verantwortlicher - vollständiger Name / Firma / Organisation

Anschrift

Vertreten durch (Name und Funktion)

Zugehörige Leistungsvereinbarung / Angebot (Nummer, Datum und Fassung)

Diese Vertragsunterlage enthält den vollständigen nachfolgenden Rechtstext. Die Vertragszuordnung erfolgt auf diesem Blatt, die Unterzeichnung auf dem letzten Blatt. Individuelle Vereinbarungen und deren Rangfolge bleiben unberührt.

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

dataMatters GmbH

Pilgrimstr. 6

50674 Köln

zwischen dem in der zugehörigen Leistungsvereinbarung bezeichneten Kunden („Verantwortlicher“ oder „Auftraggeber“) und der dataMatters GmbH, Pilgrimstr. 6, 50674 Köln („Auftragsverarbeiter“ oder „dataMatters“).

Dieser AVV gilt nur, soweit dataMatters personenbezogene Daten im Auftrag des Kunden verarbeitet. Für eigene Zwecke von dataMatters gilt die Datenschutzerklärung.

1. Gegenstand, Rangfolge und Begriffe

(1) Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus der Leistungsvereinbarung über die urbanOS Services. Er gilt für alle Verarbeitungsvorgänge, bei denen dataMatters personenbezogene Daten ausschließlich im Auftrag des Verantwortlichen verarbeitet. Art, Zweck und Umfang ergeben sich ergänzend aus Anlage 1.

(2) Die Begriffe „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“, „Verletzung des Schutzes personenbezogener Daten“ und „Aufsichtsbehörde“ haben die Bedeutung der DSGVO. „Kundendaten“ sind die vom Auftraggeber oder seinen Nutzern bereitgestellten oder durch angebundene Geräte und Systeme in dessen Verantwortungsbereich erzeugten Daten.

(3) Bei Widersprüchen geht dieser AVV einschließlich seiner Anlagen den allgemeinen Vertragsbedingungen vor. Individuelle datenschutzrechtliche Vereinbarungen gehen diesem AVV vor. Zwingendes Datenschutzrecht bleibt unberührt.

(4) Die Leistungsvereinbarung, dieser AVV und seine Anlagen 1 bis 3 bilden den dokumentierten Auftrag. Jede einbezogene Organisation verantwortet die Verarbeitung in ihrem Zuständigkeitsbereich und benennt ihre weisungsberechtigten Personen. Eine zentrale Beschaffungs- oder Verwaltungsstelle darf für andere Organisationen nur aufgrund einer dokumentierten Bevollmächtigung handeln. Gemeinsame Beschaffung oder zentrale Administration allein begründen keine Weisungsbefugnis über Daten anderer Verantwortlicher. Zuordnung, Bevollmächtigungen und deren Änderungen werden in der Organisationsverwaltung oder in Textform dokumentiert und sind Bestandteil der auftragsbezogenen Festlegungen zu Anlage 1. Weitere Verantwortliche treten dem AVV vor Beginn ihrer Verarbeitung bei oder lassen sich hierfür wirksam vertreten.

2. Dauer und Beendigung

(1) Dieser AVV tritt mit der Leistungsvereinbarung in Kraft und gilt, solange dataMatters im Auftrag personenbezogene Daten verarbeitet. Er endet erst, wenn alle auftragsbezogenen Daten nach Ziffer 14 zurückgegeben oder gelöscht sind, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

(2) Weisungen und datenschutzrechtliche Verpflichtungen, die ihrer Natur nach fortwirken, bleiben nach Vertragsende bestehen. Die Vertraulichkeitspflichten gelten zeitlich unbeschränkt.

3. Verantwortlichkeit des Auftraggebers

- (1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, die Auswahl und Konfiguration der urbanOS Services, die Richtigkeit seiner Weisungen und die Wahrung der Rechte betroffener Personen verantwortlich. Er bestimmt insbesondere Zwecke und Mittel der fachlichen Verarbeitung.
- (2) Der Auftraggeber stellt die erforderlichen Rechtsgrundlagen, Informationen, Einwilligungen, Interessenabwägungen, Löschregeln und gegebenenfalls Datenschutz-Folgenabschätzungen sicher. Er prüft besondere Kategorien personenbezogener Daten, Beschäftigtendaten, Kamera-, Telekommunikations-, Standort- und Bewegungsdaten sowie KI- oder Überwachungsszenarien vor ihrer Nutzung gesondert.
- (3) Der Auftraggeber vergibt Rollen, Mandate, Freigaben und technische Zugänge nach dem Erforderlichkeitsprinzip und widerruft sie rechtzeitig. Er übermittelt keine Daten, deren Verarbeitung nicht vom Auftrag umfasst oder für die die Services nach der Dokumentation nicht vorgesehen sind.
- (4) Erkennt der Auftraggeber Fehler oder Unregelmäßigkeiten in Auftragsergebnissen, Weisungen oder Daten, informiert er dataMatters unverzüglich und wirkt an einer risikogerechten Behebung mit.

4. Weisungsgebundene Verarbeitung

- (1) dataMatters verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers und innerhalb der vereinbarten Zwecke und Verarbeitungsorte. Es gilt die EU-Beschränkung nach Ziffer 9. Gesetzlich gebotene Verarbeitung nach Unionsrecht oder dem Recht eines Mitgliedstaats bleibt unberührt; dataMatters informiert den Auftraggeber vorab, soweit das Recht dies nicht aus wichtigen öffentlichen Interessen verbietet.
- (2) Anfängliche Weisungen ergeben sich aus diesem AVV, der Leistungsvereinbarung, der vereinbarten Konfiguration und der bestimmungsgemäßen Nutzung durch berechtigte Nutzer. Weitere Weisungen werden grundsätzlich in Textform über vereinbarte Kontakt- oder Supportwege erteilt. Mündliche Eilweisungen sind unverzüglich zu dokumentieren.
- (3) Hält dataMatters eine Weisung für datenschutzrechtswidrig, informiert dataMatters den Auftraggeber unverzüglich und darf ihre Ausführung bis zur Bestätigung oder Änderung aussetzen. Besteht trotz Hinweis ein erheblicher Rechtsverstoß fort, bleiben gesetzliche und vertragliche Sperr- und Kündigungsrechte unberührt.
- (4) Weisungen, die den vereinbarten Leistungsumfang wesentlich überschreiten, können als Zusatzleistung vergütet werden. Gesetzlich geschuldete Unterstützung wird dadurch nicht eingeschränkt.

5. Pflichten von dataMatters

- (1) dataMatters verarbeitet die Daten nur im vereinbarten Umfang. Alle Beschäftigten haben eine Geheimhaltungsvereinbarung (NDA) unterzeichnet. Auch sonstige zur Verarbeitung befugte Personen werden vor ihrem Zugriff zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht.
- (2) dataMatters trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen und hält ein dem Risiko angemessenes Schutzniveau aufrecht. Maßnahmen dürfen dem technischen Fortschritt angepasst werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird.
- (3) dataMatters unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der verfügbaren Informationen bei der Einhaltung der Art. 32 bis 36 DSGVO sowie bei Anfragen betroffener Personen nach Maßgabe dieses Vertrags.

(4) dataMatters führt die gesetzlich erforderlichen Verzeichnisse und stellt die für den Nachweis der Pflichten nach Art. 28 DSGVO erforderlichen Informationen bereit. Anfragen von Aufsichtsbehörden zum Auftragsgegenstand werden in Abstimmung mit dem Auftraggeber beantwortet, soweit keine unmittelbare gesetzliche Pflicht von dataMatters besteht.

(5) dataMatters nutzt auftragsbezogene Kundendaten nicht für eigene Werbung, Profilbildung, unabhängiges Benchmarking oder eigene Produktentwicklung. Weder dataMatters noch eingesetzte Unterauftragsverarbeiter dürfen diese Daten zum Trainieren oder Verbessern eigener oder fremder KI-Modelle verwenden. Das gilt auch für aus Kundendaten erzeugte anonymisierte Aggregate. Beauftragte Analyse und KI-Inferenz für den Auftraggeber bleiben innerhalb der dokumentierten Weisungen zulässig. Unabhängig von Kundendaten erzeugte synthetische Testdaten sind hiervon nicht erfasst. Eine allgemeine Einwilligung in Produktanalyse hebt die Zweckbindung dieses AVV nicht auf. Bei AWS Bedrock werden Kundeneingaben und Ausgaben nicht für Modelltraining freigegeben; bei direkter Nutzung von Mistral ist die Nutzung für Training und Modellverbesserung deaktiviert (Opt-out). Funktionen, Feedbackübermittlungen oder Testangebote, die diese Zweckbindung nicht einhalten, werden nicht mit Kundendaten genutzt.

6. Berechtigungen und Vertraulichkeit

(1) dataMatters beschränkt den Zugriff auf solche Beschäftigten und sonstigen Personen, die ihn für Betrieb, Support, Sicherheit oder die beauftragte Leistung benötigen. Berechtigungen werden rollenbezogen vergeben, regelmäßig überprüft und bei Aufgabenwechsel oder Ausscheiden entzogen.

(2) Personen mit Zugriff werden vor Tätigkeitsbeginn angemessen zum Datenschutz und zur Informationssicherheit verpflichtet und geschult. Geheimhaltungs- und Vertraulichkeitspflichten gelten auch nach Ende ihrer Tätigkeit fort.

(3) Produktivzugriffe für Support oder Fehleranalyse erfolgen nur durch autorisierte Personen im erforderlichen, dokumentierten Umfang und innerhalb der vereinbarten Zugriffsländer. dataMatters protokolliert Zugriffe und begrenzt sie zeitlich oder sachlich. Der Auftraggeber stellt Testdaten oder anonymisierte Daten bereit, wenn diese für den Zweck genügen. Administrative Berechtigung allein ersetzt weder die Weisung noch eine geografische Zugriffsbeschränkung.

7. Sicherheit der Verarbeitung

(1) Die Parteien berücksichtigen bei Auswahl und Bewertung der Maßnahmen insbesondere Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere der Risiken für betroffene Personen.

(2) dataMatters schützt insbesondere Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, stellt die Wiederherstellbarkeit nach physischen oder technischen Zwischenfällen sicher und überprüft die Wirksamkeit seiner Maßnahmen regelmäßig. Die konkret zugesagten Maßnahmen ergeben sich aus Anlage 2.

(3) Der Auftraggeber ist für die Sicherheit seiner Endgeräte, Netzwerke, Identitätsanbieter, API-Clients, Sensoren und Integrationen sowie für sichere Rollen-, Freigabe- und Schlüsselverwaltung verantwortlich. Gemeinsam genutzte oder kundenseitig betriebene Komponenten werden in der Leistungsvereinbarung abgegrenzt.

(4) Beide Parteien melden sicherheitsrelevante Änderungen und Schwachstellen über die vereinbarten Kontaktwege und koordinieren erforderliche Abhilfemaßnahmen ohne unangemessene Verzögerung.

8. Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt die allgemeine schriftliche Genehmigung für die im verbindlichen Verarbeitungsverzeichnis nach Anlage 3 benannten Unterauftragsverarbeiter. Weitere Unterauftragsverarbeiter dürfen nur nach dem Verfahren der folgenden Absätze eingesetzt werden. Verlangt eine individuelle Vereinbarung eine vorherige Zustimmung in Textform für jeden neuen Anbieter, gilt stattdessen dieses Verfahren. dataMatters bleibt für die Erfüllung der Datenschutzpflichten seiner Unterauftragsverarbeiter verantwortlich.

(2) dataMatters informiert den Auftraggeber mindestens 14 Tage vor einer beabsichtigten Hinzuziehung oder Ersetzung über Vertragsgesellschaft, Leistung, betroffene Daten, Verarbeitungs- und Zugriffsländer innerhalb der Europäischen Union. Der Auftraggeber kann innerhalb dieser Frist aus datenschutzrechtlichen Gründen widersprechen. Ein Wechsel darf keine ausdrücklich vereinbarten Standort-, Zugriffs- oder Zweckbeschränkungen umgehen.

(3) Die Parteien bemühen sich bei einem berechtigten Widerspruch um eine zumutbare Alternative. Ist eine Alternative nicht verfügbar oder wirtschaftlich unverhältnismäßig, kann jede Partei die hiervon betroffene Leistung außerordentlich zum Einsatzzeitpunkt beenden; weitergehende Rechte bleiben unberührt.

(4) dataMatters legt jedem Unterauftragsverarbeiter vertraglich dieselben einschlägigen Datenschutzpflichten auf, einschließlich Zweckbindung, Verbot von KI-Training und Modellverbesserung, Zugriffsbeschränkungen, Löschung und rechtzeitiger Vorfallinformation. Die Meldewege müssen dataMatters die Einhaltung der Fristen dieses AVV ermöglichen. Hilfsleistungen ohne Zugriffsmöglichkeit auf personenbezogene Daten sind keine Unterauftragsverarbeitung. Eigenständig Verantwortliche und vom Kunden selbst beauftragte Empfänger werden nach ihrer tatsächlichen Rolle gesondert ausgewiesen.

9. Verarbeitungsorte und Ausschluss von Drittlandverarbeitung

(1) Die Verarbeitung im Auftrag einschließlich Speicherung, Sicherungskopien sowie administrativer Support- und Fernzugriffe erfolgt ausschließlich innerhalb der Europäischen Union. dataMatters nutzt deutsche Standorte, soweit der betreffende Dienst dort angeboten wird; andernfalls werden ausschließlich Standorte in anderen EU-Mitgliedstaaten genutzt. Für die Plattforminfrastruktur gilt Deutschland (AWS Frankfurt, eu-central-1); für AWS Bedrock je nach Modell Deutschland (eu-central-1) oder Schweden (eu-north-1). Die Zuordnung der weiteren Dienste ergibt sich aus Anlage 3. Eine ausdrücklich vereinbarte Beschränkung auf Deutschland geht vor.

(2) Eine Speicherung oder Verarbeitung außerhalb der EU sowie administrative Zugriffe aus Drittstaaten sind ausgeschlossen, auch im Support, bei Störungen oder im Ausnahmebetrieb. Dies gilt für eigenes Personal und eingesetzte Unterauftragsverarbeiter. Allgemeine Transferklauseln, Standardvertragsklauseln oder Angemessenheitsbeschlüsse erweitern diesen Verarbeitungsraum nicht. Nicht zur EU gehörende EWR-Staaten sind nicht eingeschlossen. Dienste, Funktionen und Ausweichwege, die diese Beschränkung nicht erfüllen, dürfen für auftragsbezogene personenbezogene Daten nicht eingesetzt werden.

(3) Kundenseitig eingerichtete Integrationen und Datenquellen dürfen den vereinbarten Verarbeitungsraum nicht erweitern. Eine Weisung zur Verarbeitung außerhalb der EU wird nicht im Rahmen dieses AVV ausgeführt. Behördenanfragen werden auf ihre Rechtmäßigkeit einschließlich Art. 48 DSGVO geprüft; dataMatters informiert den Auftraggeber, soweit rechtlich zulässig. Zwingende Pflichten nach Unionsrecht oder dem Recht eines Mitgliedstaats bleiben unberührt.

10. Rechte betroffener Personen

- (1) Geht bei dataMatters eine Anfrage einer betroffenen Person ein, die erkennbar Kundendaten betrifft, leitet dataMatters sie ohne unangemessene Verzögerung an den Auftraggeber weiter und beantwortet sie nicht selbst, sofern dataMatters nicht gesetzlich dazu verpflichtet oder vom Auftraggeber angewiesen ist.
- (2) dataMatters unterstützt den Auftraggeber durch geeignete Funktionen und, soweit erforderlich, zusätzliche Maßnahmen bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und der Bearbeitung von Entscheidungen nach Art. 22 DSGVO.
- (3) Der Auftraggeber prüft Identität, Berechtigung, Umfang und Frist der Anfrage. Zusätzlicher Aufwand außerhalb der vereinbarten Standardfunktionen kann nach Aufwand vergütet werden, sofern er nicht auf einer Pflichtverletzung von dataMatters beruht.

11. Datenschutzverletzungen

- (1) dataMatters informiert den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, über Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten, die die auftragsbezogenen Daten oder ihre Verarbeitung betreffen. Die Erstmeldung wartet nicht auf den Abschluss der Untersuchung; noch ungesicherte Erkenntnisse werden als solche gekennzeichnet und nachgereicht. Die Frist läuft unabhängig von Servicezeiten, Wochenenden und Feiertagen. Eine strengere gesetzliche Pflicht zur unverzüglichen Information bleibt unberührt.
- (2) Die Meldung enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten- und Personengruppen, ungefähre Zahl der Datensätze, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen sowie eine Ansprechstelle. dataMatters dokumentiert Untersuchung und Abhilfe.
- (3) dataMatters unterstützt den Auftraggeber angemessen bei dessen Risikoanalyse, Meldungen nach Art. 33 DSGVO und Benachrichtigungen nach Art. 34 DSGVO. Meldungen an Behörden oder Betroffene für den Auftraggeber erfolgen nur auf Weisung, soweit dataMatters nicht selbst gesetzlich verpflichtet ist.
- (4) Der Auftraggeber meldet dataMatters unverzüglich Vorfälle in seiner Sphäre, die Kundendaten oder die Sicherheit der urbanOS Services berühren, und stellt die für Schutz- und Aufklärungsmaßnahmen erforderlichen Informationen bereit.
- (5) Zentrale Ansprechstelle für Datenschutz- und Sicherheitsvorfälle ist mail@datamatters.io. Meldungen können rund um die Uhr eingehen. dataMatters organisiert Überwachung, interne Weiterleitung und Vertretung so, dass die unverzügliche Bearbeitung und die 24-Stunden-Frist unabhängig von den Servicezeiten gewährleistet sind. Der Auftraggeber hinterlegt einen aktuellen Empfängerkontakt und eine Vertretung in der Organisationsverwaltung oder teilt diese in Textform mit.

12. Unterstützung und Datenschutz-Folgenabschätzung

- (1) dataMatters stellt dem Auftraggeber verfügbare Informationen über Architektur, Datenflüsse, Sicherheitsmaßnahmen und Unterauftragsverarbeiter bereit, soweit diese für eine Datenschutz-Folgenabschätzung oder vorherige Konsultation erforderlich sind und keine Rechte Dritter oder Sicherheitsinteressen entgegenstehen.
- (2) Der Auftraggeber bleibt für Erforderlichkeit, Durchführung und Ergebnis einer Datenschutz-Folgenabschätzung sowie die Konsultation der Aufsichtsbehörde verantwortlich. dataMatters unterstützt im angemessenen Umfang bezogen auf die von dataMatters betriebene Verarbeitung.

13. Nachweise und Kontrollen

(1) dataMatters stellt alle Informationen bereit, die erforderlich sind, um die Einhaltung dieses AVV und des Art. 28 DSGVO nachzuweisen. Geeignete aktuelle Zertifikate, Prüfberichte, Sicherheitsfragebögen oder zusammenfassende Auditberichte sollen vorrangig verwendet werden.

(2) Der Auftraggeber darf selbst oder durch einen unabhängigen, fachkundigen und zur Vertraulichkeit verpflichteten Prüfer Kontrollen durchführen. Prüfungen sind grundsätzlich mindestens 30 Tage vorher anzukündigen, auf Geschäftszeiten und den erforderlichen Umfang zu beschränken und so durchzuführen, dass Betrieb, Sicherheit, Geheimnisse und Daten anderer Kunden nicht beeinträchtigt werden.

(3) Bei konkretem Verdacht eines erheblichen Verstoßes, einem relevanten Datenschutzvorfall oder behördlicher Anordnung ist eine kürzere Frist zulässig. Der Auftraggeber trägt angemessene Kosten zusätzlicher Audits, soweit kein von dataMatters zu vertretender wesentlicher Verstoß festgestellt wird.

(4) Festgestellte Abweichungen werden risikogerecht bewertet und innerhalb einer angemessenen Frist behoben. Sicherheitskritische Einzelheiten dürfen in geschützter Form, durch Einsicht ohne Kopie oder gegenüber dem Prüfer offengelegt werden.

(5) Kontroll- und Nachweisanfragen richten Sie an mail@datamatters.io. dataMatters koordiniert die Prüfung und benennt für den jeweiligen Vorgang eine verantwortliche Ansprechperson. Eine gesonderte Auditabteilung ist hierfür nicht erforderlich.

14. Rückgabe, Export und Löschung

(1) Der Auftraggeber entscheidet nach Ende der Verarbeitungsleistung über Rückgabe oder Löschung der personenbezogenen Daten. dataMatters ermöglicht die vollständige Rückgabe der vom Auftrag erfassten personenbezogenen Daten einschließlich zugehöriger Metadaten, Dateien und übertragbarer Konfigurationen, Dashboards und Regelwerke in vereinbarten offenen, maschinenlesbaren Formaten. Je Datenart kommen insbesondere CSV, Excel, JSON, GeoJSON und XML sowie das ursprüngliche Dateiformat in Betracht. Die Übergabe erfolgt über einen zugriffsgeschützten Download oder einen vereinbarten sicheren Übertragungsweg. Ein allgemeiner Vorbehalt technischer Exportierbarkeit oder ein automatischer Wegfall nach 30 Tagen schränkt diese Pflicht nicht ein. Umfang und Termine der Übergabe werden dokumentiert; während der Übergangsphase darf dataMatters Daten nur für die vereinbarte Übergabe, Sicherung und Löschung verarbeiten.

(2) Bei Rückgabe erfolgt die Löschung nach vollständiger Übergabe und Bestätigung durch den Auftraggeber. Nach Löschfreigabe löscht dataMatters die betroffenen Daten unverzüglich, spätestens innerhalb von 14 Kalendertagen aus aktiven Systemen. Für einzeln freigegebene Nutzerkonten gilt die besondere Frist aus Anlage 1; sie verlängert nicht die 14-Tage-Frist bei vollständiger Löschung des Kundenbestands. Der Auftraggeber kann eine frühere Löschung anweisen; zwingende Löschpflichten bleiben unberührt. Eine Anonymisierung anstelle der Rückgabe oder Löschung setzt eine dokumentierte Weisung voraus und begründet kein eigenes Nutzungsrecht. Sicherungskopien werden nach der 30-tägigen Backup-Rotation entfernt, spätestens 30 Kalendertage nach der aktiven Löschung. Bis dahin bleiben gelöschte Daten gegen produktive Nutzung gesperrt; bei einer Wiederherstellung werden dokumentierte Löschungen vor erneuter produktiver Nutzung wieder angewendet.

- (3) Gesetzlich aufzubewahrende Daten werden von operativen Kundendaten getrennt, für andere Zwecke gesperrt und nach Ablauf der einschlägigen Frist gelöscht. dataMatters dokumentiert Ausnahmen und bestätigt dem Auftraggeber den Abschluss der Löschung einschließlich verbleibender gesetzlicher Ausnahmen und des Zeitplans für noch vorhandene Sicherungskopien. Der Löschungsnachweis nennt Datenumfang, Datum der aktiven Löschung, Abschluss der Backup-Löschung und gegebenenfalls gesetzlich verbleibende Bestände mit Rechtsgrundlage und Löschtermin.
- (4) Die Vergütung zusätzlicher Arbeiten richtet sich nach der Leistungsvereinbarung und zwingendem Recht. Gesetzlich oder vertraglich geschuldete Rückgabe, Löschung, Exporte und Anbieterwechselunterstützung werden nicht allein wegen ihres Aufwands zu einer Zusatzleistung. Darüber hinausgehende Sonderleistungen bedürfen einer vorherigen Beauftragung. Eine vereinbarte kostenfreie Migration oder Datenrückgabe geht vor.

15. Haftung und Schlussbestimmungen

- (1) Für die Haftung der Parteien gelten Art. 82 DSGVO, sonstiges zwingendes Recht und ergänzend die Haftungsregelungen der Leistungsvereinbarung. Keine Bestimmung dieses AVV beschränkt Ansprüche betroffener Personen oder behördliche Befugnisse.
- (2) Änderungen und Ergänzungen dieses AVV bedürfen mindestens der Textform, soweit nicht ein strengeres gesetzliches Formerfordernis gilt. Dies gilt auch für eine Änderung dieser Formklausel.
- (3) Es gilt deutsches Recht. Eine individuelle Gerichtsstandsvereinbarung geht vor; ansonsten ist Köln Gerichtsstand, soweit gesetzlich zulässig. Sollte eine Bestimmung unwirksam sein, bleibt der übrige Vertrag wirksam.
- (4) Stand: 10. September 2026.

Anlage 1 – Beschreibung der Auftragsverarbeitung

Festlegung	Beschreibung
Gegenstand	Bereitstellung und Betrieb der urbanOS Plattform einschließlich aller gegenwärtigen und künftig bereitgestellten urbanOS Apps, KI-Funktionen, Integrationen und Supportleistungen, soweit der Auftraggeber sie im Rahmen seiner Leistungsvereinbarung nutzt. Der AVV erfasst neue Funktionen innerhalb der hier beschriebenen Zwecke, Datenarten und Personengruppen ohne separate Vereinbarung je App. Wesentliche Erweiterungen dieser Kategorien oder neue Empfänger werden vor ihrer Nutzung in den Anlagen dokumentiert; für Unterauftragsverarbeiter gilt Ziffer 8. Der AVV allein begründet keine Lizenz oder Vergütungspflicht für zusätzliche Apps.
Dauer	Dauer der beauftragten Verarbeitung zuzüglich der dokumentierten Übergabe- und Löschphase; konkrete Vertragsdaten ergeben sich aus der Leistungsvereinbarung. Der AVV gilt bis zum Abschluss der Rückgabe oder Löschung fort.

Festlegung	Beschreibung
Zwecke	Erfassung, Übertragung, Speicherung, Strukturierung, Anzeige, Analyse, Aggregation, Alarmierung, Automatisierung, Export, Support, Sicherung und Löschung nach Weisung des Auftraggebers.
Verarbeitung	Insbesondere Hosting, Datenbank- und Objektspeicherbetrieb, API- und Gerätekommunikation, Rollen- und Berechtigungsprüfung, Karten- und Dashboarddarstellung, Protokollierung, Fehlersuche, Support, Sicherung und Wiederherstellung.
Datenarten	Stamm-, Kontakt-, Organisations-, Konto-, Rollen-, Mandats-, Authentifizierungs-, Nutzungs-, Protokoll-, Geräte-, Sensor-, Zeitreihen-, Standort-, Karten-, Dashboard-, Dokument-, Kommunikations-, Support-, Integrations- und Inhaltsdaten; weitere vom Auftraggeber konfigurierte Daten.
Besondere Kategorien	Nicht regelhaft vorgesehen. Nur nach ausdrücklicher Vereinbarung, geeigneter Konfiguration, Rechtsgrundlage und zusätzlicher Schutzprüfung des Auftraggebers.
Betroffene	Beschäftigte und Nutzer des Auftraggebers, Einwohner, Besucher, Verkehrsteilnehmer, Vertragspartner, Ansprechpartner, Einsatz- und Serviceteams sowie weitere Personen, deren Daten der Auftraggeber rechtmäßig verarbeitet.
Fachliche Grenzen	Noise verarbeitet keine Audioaufnahmen; Counting soll keine identifizierbaren Bilder, Videos, Gesichter oder Kennzeichen speichern, sondern Edge-seitig erzeugte Zählwerte; Fleet soll keine namentlichen Fahrerprofile bilden; CityPulse soll nur pseudonymisierte bzw. aggregierte Signale verarbeiten. Abweichungen bedürfen gesonderter Prüfung.
Ort	Ausschließlich Europäische Union einschließlich Backups, Support und administrativer Fernzugriffe. Plattformhosting: Deutschland, AWS Frankfurt (eu-central-1). AWS Bedrock: Deutschland oder Schweden je Modell. Weitere Dienste: Deutschland, soweit verfügbar, andernfalls EU gemäß Anlage 3. Drittlandverarbeitung und Drittlandzugriffe sind nach Ziffer 9 ausgeschlossen.

Festlegung	Beschreibung
Löschung	Der Auftraggeber bestimmt die zulässige Aufbewahrung seiner Fachdaten. Vereinbarte Rohsensorhistorien dürfen nicht ohne Freigabe gelöscht oder verdichtet werden; zwingende Datenschutzpflichten bleiben unberührt. Für Konten, Protokolle, Support und KI gelten die nachfolgend festgelegten Standardfristen. Eine vollständige Rohsensorhistorie verlängert diese Fristen nicht. Rückgabe, Löschfreigabe und Löschungsnachweis richten sich nach Ziffer 14.
Organisationen und Weisungen	Jede Organisation benennt ihre weisungsberechtigten Personen. Zentraler Einkauf und zentrale Administration begründen keine Weisungsbefugnis für fremde Daten. Eine Vertretung setzt dokumentierte Bevollmächtigung voraus. Die Organisationsverwaltung oder eine Mitteilung in Textform dokumentiert Zuordnung und Befugnisse; weitere Verantwortliche werden nach Ziffer 1 Absatz 4 einbezogen. Datenschutz-, Sicherheits- und Kontrollanfragen an mail@datamatters.io.

Daten und Zwecke nach Funktion

Verarbeitung	Daten und Zweck
Konten und Berechtigungen	Namen, geschäftliche Kontaktdaten, Organisation, Rollen, Einladungen, Authentisierungsdaten und Loginereignisse zur Anmeldung und Zugangsverwaltung nach Weisung der Organisation.
Sensoren und Fachanwendungen	Gerätekennungen, Messwerte, Zeitreihen, Standorte und Metadaten für die eingerichteten Auswertungen, Karten, Dashboards, Alarmer und Steuerungen. Personenbezug und betroffene Personengruppen richten sich nach der Datenquelle; reine Umweltmesswerte sind nicht allein durch ihre Speicherung personenbezogen.
Support und Kommunikation	Kontaktdaten, Nachrichten, Anhänge, technischer Kontext und Bearbeitungsverlauf zur Bearbeitung auftragsbezogener Supportfälle. Amazon SES versendet Transaktions- und Supportnachrichten; Microsoft 365 / Exchange Online hostet die für Kunden- und Supportkommunikation genutzten Postfächer.
Karten und Informationsdienste	HERE stellt Grundkarten, Routen, Adresssuche und Höhendaten bereit. CityPulse bezieht Flächennutzungs- und Straßendaten über Overpass; Open-Meteo liefert Wetterdaten und OpenHolidays Kalenderdaten. Anlage 3 beschreibt die jeweiligen Abfrageparameter und unterscheidet Browserabrufe von serverseitigen Abrufen.

Verarbeitung	Daten und Zweck
KI und Automationen	Texteingaben, freigegebene Organisations- und Fachdaten, Kontext, Ergebnisse und Ausführungsprotokolle für angeforderte Assistenz und freigegebene Automationen. Kein Training und keine Modellverbesserung mit Kundendaten.
Abgrenzung eigener Zwecke	Eigene Vertriebs-, Abrechnungs- und Websiteverarbeitung von dataMatters richtet sich nach der Datenschutzerklärung. Eine Einwilligung in Produktanalyse erweitert den Auftrag nicht und erlaubt keine unabhängige Nutzung der Fachdaten einer Kundenorganisation.

Aufbewahrungs- und Löschfristen

Diese Fristen sind Standard-Höchstfristen, keine Mindestaufbewahrung. Frühere berechnete Löschungen und dokumentierte kürzere Kundenweisungen gehen vor. Gesetzlich erforderliche Aufbewahrung und eine für einen konkreten Rechtsstreit oder Sicherheitsvorfall notwendige Beweissicherung werden begründet, auf die erforderlichen Daten beschränkt und getrennt dokumentiert. Die Bestände bleiben für andere Zwecke gesperrt und werden nach Wegfall des Grundes gelöscht. Bei Wiederherstellung von Backups werden Löschungen vor produktiver Nutzung erneut angewendet.

Daten / Vorgang	Standardfrist
Datenbanken und hochgeladene Dateien: Sicherung	Mindestens alle 24 Stunden, unabhängig von Servicezeiten.
Sicherungskopien	30 Kalendertage ab Erstellung, danach endgültige Löschung. Nach aktiver Löschung verbleibende Kopien werden spätestens binnen weiterer 30 Kalendertage entfernt.
Aktive Kundendaten nach Löschfreigabe	Unverzüglich, spätestens innerhalb von 14 Kalendertagen. Bei Rückgabe beginnt die Frist nach vollständiger Übergabe und Bestätigung.
Nutzerkonten	Bei Entzug der Nutzungsberechtigung sofort sperren. Nach endgültiger Löschfreigabe unverzüglich, spätestens innerhalb von 30 Kalendertagen löschen. Die vollständige Löschung eines Kundenbestands nach Ziffer 14 bleibt auf 14 Kalendertage begrenzt.
Einladungen	Nach 7 Kalendertagen ungültig; spätestens 30 Kalendertage nach Ablauf löschen.
Zugriffsprotokolle	30 Kalendertage ab Ereignis.

Daten / Vorgang	Standardfrist
Sicherheitsprotokolle	90 Kalendertage ab Ereignis.
Erledigte Supporttickets einschließlich Anhängen	6 Monate nach Abschluss des Supportfalls.
Gespeicherte KI-Chatverläufe einschließlich Eingaben und Antworten	30 Kalendertage ab der jeweiligen Nachricht. Keine zusätzliche Speicherung der Inhalte in technischen Protokollen.

Anlage 2 – Technische und organisatorische Maßnahmen

dataMatters verpflichtet sich zu den folgenden technischen und organisatorischen Maßnahmen. Diese Anlage ist Bestandteil des AVV. Ergänzungen zur eingesetzten Betriebsumgebung hält dataMatters in der vereinbarten Fassung dieser Anlage fest. Technische Anpassungen dürfen das vereinbarte Schutzniveau nicht unterschreiten.

Festlegung	Beschreibung
Governance	Alle Beschäftigten haben NDAs unterzeichnet. dataMatters verantwortet die Datenschutz- und Sicherheitsorganisation, rollenbezogene Schulung, geregelten Eintritt, Rollenwechsel und Austritt. Zentrale Datenschutz-, Sicherheits- und Auditkoordination über mail@datamatters.io.
Zutrittskontrolle	Angemessene physische Sicherung der von dataMatters genutzten Arbeitsbereiche; Rechenzentren werden durch die jeweiligen Hostinganbieter physisch geschützt.
Zugangskontrolle	Personengebundene Konten und rollenbezogene Zugriffe; Zwei-Faktor-Authentifizierung für administrative und steuerungsberechtigte Rollen; geregelte Vergabe, Überprüfung und Entziehung von Berechtigungen; Schutz und Rotation von Zugangsdaten und Schlüsseln.
Zugriffskontrolle	Least-Privilege-Prinzip, getrennte administrative Rollen und zweckgebundene Supportzugriffe. Vereinbarte Zugriffsländer gelten für eigenes Personal und Unterauftragsverarbeiter; Freigaben und Kontrollen werden dokumentiert.
Mandantentrennung	Organisationen werden logisch getrennt. Berechtigungsprüfungen begrenzen Zugriffe auf freigegebene Daten und Funktionen. Gemeinsame Datenräume und organisationsübergreifende Freigaben erfordern eine Autorisierung der datenverantwortlichen Organisation. Entwicklungs- und Testzugriffe auf produktive personenbezogene Daten unterliegen denselben Schutzanforderungen.
Übertragung	TLS 1.3, mindestens TLS 1.2, für die von dataMatters betriebenen unterstützten Transportverbindungen; authentifizierte APIs und kontrollierte Freigaben. Abweichende Geräte- oder Funkprotokolle werden im Integrationsauftrag mit ihren Schutzmaßnahmen und Verantwortlichkeiten beschrieben.

Festlegung	Beschreibung
Speicherung	Produktive personenbezogene Daten und Sicherungskopien werden bei Speicherung verschlüsselt. dataMatters verantwortet die Verwaltung, Zugriffsberechtigungen und Rotation der für den Plattformbetrieb eingesetzten Schlüssel; Hostinganbieter stellen die vereinbarten technischen Verschlüsselungsdienste bereit. Schlüsselzugriffe sind auf berechnigte Betriebsverantwortliche beschränkt.
Protokollierung	Protokollierung von Zugriffen, Änderungen, Steuerungsbefehlen und Exporten mit Zeitbezug und Zugriffsschutz. Zugriffsprotokolle: 30 Kalendertage; Sicherheitsprotokolle: 90 Kalendertage. Berechnigte Administratoren erhalten Einblick für ihren Verantwortungsbereich. Protokolle enthalten keine unnötigen Inhalte oder Geheimnisse; KI-Eingaben und -Antworten werden nicht zusätzlich in technischen Protokollen gespeichert.
Verfügbarkeit	dataMatters sichert Datenbanken und hochgeladene Dateien mindestens alle 24 Stunden, auch außerhalb der Servicezeiten. Sicherungskopien werden 30 Kalendertage aufbewahrt und anschließend endgültig gelöscht. dataMatters verantwortet Überwachung der Sicherungsläufe, Fehlerbehandlung und dokumentierte Wiederherstellungstests. Numerische RPO- und RTO-Zusagen richten sich nach dem ausdrücklich einbezogenen urbanOS Standard-SLA (https://urbanos.de/legal/sla).
Schwachstellen	Sicherheitsupdates, Abhängigkeits- und Codeprüfungen, dokumentiertes Schwachstellenmanagement, risikobezogene Penetrationstests und Incident-Response. Umfang und Ergebnisse werden dokumentiert; geeignete Nachweise werden auf Anforderung unter Schutz sicherheitskritischer Informationen bereitgestellt.
Datensparsamkeit	Privacy by Design und Default, konfigurierbare Berechtigungen und Aufbewahrungsregeln sowie Datenklassifikation nach öffentlich, intern, vertraulich und personenbezogen. Löschung, Pseudonymisierung und Anonymisierung erfolgen zweckbezogen nach Weisung. Beauftragte Rohdatenhistorien dürfen nicht ohne Freigabe verdichtet werden; zwingende Datenschutzpflichten bleiben unberührt.

Festlegung	Beschreibung
Löschung	Kontrollierte Übergabe und weisungsgebundene Löschung nach Ziffer 14 und Anlage 1. Aktive Kundenbestände werden nach Löschfreigabe unverzüglich, spätestens innerhalb von 14 Kalendertagen gelöscht. Backups werden innerhalb der 30-tägigen Rotation entfernt. Löschungen werden bei Wiederherstellung erneut angewendet und deren Abschluss nachgewiesen; gesetzlich aufzubewahrende Daten bleiben getrennt und zweckgebunden.
Prüfung	Regelmäßige Wirksamkeitskontrollen, Wiederherstellungstests und dokumentierte Vorfallnachbereitung. Für vertraglich zugesagte Rechenzentrumszertifizierungen werden gültige Nachweise mit passendem Dienst- und Regionsumfang vorgelegt. Eine Anbieterzertifizierung belegt keine eigene Zertifizierung von dataMatters.
KI und MCP	Kein Training und keine Modellverbesserung mit auftragsbezogenen Kundendaten. KI-/MCP-Zugriffe folgen den Rollen- und Organisationsrechten; einzeln erteilbare, befristbare und widerrufbare Zugänge sowie Protokollierung. Schreib- und Steuerungsaktionen bleiben bis zur organisationsbezogenen Freigabe deaktiviert; Steuerbefehle erfordern einen dokumentierten Bestätigungsschritt.
Vorfalldmeldung	Zentrale Meldestelle mail@datamatters.io; geregelte interne Weiterleitung und Vertretung. Erstinformation unverzüglich und spätestens innerhalb von 24 Stunden nach Kenntniserlangung gemäß Ziffer 11, unabhängig von Servicezeiten. Untersuchung, Abhilfe und Folgeinformationen werden dokumentiert.

Anlage 3 – Unterauftragsverarbeiter, externe Empfänger und Verarbeitungsverzeichnis

Diese Anlage enthält die Dienste, ihre Vertragsgesellschaften, Rollen, Aufgaben, Verarbeitungsräume und Datenflüsse. dataMatters führt sie als versioniertes Verarbeitungsverzeichnis innerhalb dieses AVV, ohne separate Aufteilung nach Apps. Es gilt für die jeweils genutzten Dienste. Für die Genehmigung und Änderungen von Unterauftragsverarbeitern gilt Ziffer 8. Die Aufnahme eines externen Empfängers begründet keine pauschale Genehmigung als Unterauftragsverarbeiter. Die ausschließliche EU-Verarbeitung nach Ziffer 9 gilt auch für nachgelagerte Auftragsverarbeiter und deren Supportzugriffe.

Daten übermitteln wir im Umfang der von Ihnen genutzten Leistungen. Karten- und Informationsdienste erhalten die unten beschriebenen Abfragen; von Ihnen angebundene Datenquellen bestimmen Sie in den Integrationseinstellungen. Die Datenschutzerklärung erläutert unsere eigene Website- und Vertragskommunikation.

Bei einem Browserabruf erhält der Anbieter die IP-Adresse und technischen Verbindungsdaten Ihres Endgeräts. Bei einem serverseitigen Abruf erhält er die Verbindungsdaten unseres Servers und die für die Abfrage erforderlichen Parameter. Die einzelnen Datenflüsse beschreibt die folgende Tabelle. Die Anbieteranschriften sind keine Angaben zu Speicher- oder Zugriffsorten; für diese gelten die Vereinbarungen nach Ziffer 9.

Dienst / Betriebsmodell	Verwendung	Verarbeitete Daten und Abrufweg
AWS Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg Luxemburg Datenschutzkontakt (https://aws.amazon.com/privacy/)	Hosting und Betrieb der urbanOS Infrastruktur. Rolle: Unterauftragsverarbeiter. Verarbeitungsraum: Deutschland, Frankfurt (eu-central-1).	Konto-, Organisations-, Anwendungs- und Protokolldaten sowie gespeicherte Dateien und Sicherungskopien. Die vertraglich vereinbarten Speicher- und Zugriffsländer gelten für diese Verarbeitung.
Supabase Cloud (Managed Service) Supabase Pte. Ltd. 65 Chulia Street #38-02/03 OCBC Centre Singapore 049513 Singapur Datenschutzkontakt (https://supabase.com/privacy)	Datenbanken, Anmeldung, Dateispeicherung und Echtzeitfunktionen der mit Supabase Cloud betriebenen Apps. Rolle: Unterauftragsverarbeiter. Verarbeitungsraum: Deutschland bei verfügbarer deutscher Projektregion, andernfalls ausschließlich EU.	Supabase verarbeitet Konto- und Authentisierungsdaten, Organisations- und Anwendungsdaten, Dateien und technische Protokolle als Unterauftragsverarbeiter.
PostHog PostHog, Inc. 2261 Market Street #4008 San Francisco, CA 94114 USA Datenschutzkontakt (https://posthog.com/privacy)	Produktanalyse und, nach Ihrer Einwilligung, Sitzungswiedergabe. Rolle: Für beauftragte Analyse Unterauftragsverarbeiter; eigene Produktanalyse von dataMatters richtet sich nach der Datenschutzerklärung. Verarbeitungsraum: Deutschland, Frankfurt (PostHog Cloud EU).	Nutzungsereignisse, Seitenaufrufe, Browser- und Geräteinformationen sowie Fehlerdaten; bei eingewilligter Sitzungswiedergabe maskierte Interaktionen. Die Datenaufnahme erfolgt über EU-Endpunkte.

Dienst / Betriebsmodell	Verwendung	Verarbeitete Daten und Abrufweg
AWS Bedrock / Mistral Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg Luxemburg Mistral AI (SAS) 15 rue des Halles 75001 Paris Frankreich AWS Datenschutzkontakt (https://aws.amazon.com/privacy/) Mistral Datenschutzkontakt (https://legal.mistral.ai/terms/privacy-policy/)	KI-Auswertungen für NOVA, Assistenz und Automationen. Rolle: Unterauftragsverarbeiter; bei ausschließlich über Bedrock bereitgestellten Modellen erhält Mistral nicht allein aufgrund seiner Rolle als Modellhersteller Kundendaten. Verarbeitungsraum: Bedrock: Deutschland (eu-central-1) oder Schweden (eu-north-1). Direkte Mistral-API: EU; keine US-Endpunkte oder Drittlandfunktionen.	Eingaben, freigegebene Organisations- und Fachdaten, Kontext, Antworten und Ausführungsprotokolle. Kein Training und keine Modellverbesserung mit Kundendaten.
Amazon Simple Email Service (Amazon SES) Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg Luxemburg Datenschutzkontakt (https://aws.amazon.com/privacy/)	Versand von Transaktions- und Supportnachrichten. Rolle: Unterauftragsverarbeiter für beauftragte Kommunikation. Verarbeitungsraum: Deutschland bei verfügbarer deutscher Versandregion, andernfalls ausschließlich EU.	Amazon SES verarbeitet Absender- und Empfängeradressen, Betreff, Nachrichteninhalte, Anhänge sowie Versand- und Zustellmetadaten.
Microsoft 365 / Exchange Online (Outlook) Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown, Dublin 18 D18 P521 Irland Datenschutzkontakt (https://privacy.microsoft.com/de-de/privacystatement)	Hosting unserer E-Mail-Postfächer sowie Versand, Empfang und Verwaltung der Kunden- und Supportkommunikation über Outlook. Rolle: Unterauftragsverarbeiter für beauftragte Supportkommunikation; eigene Geschäftskorrespondenz richtet sich nach der Datenschutzerklärung. Verarbeitungsraum: Deutschland bei verfügbarer deutscher Bereitstellung, andernfalls ausschließlich EU.	Microsoft verarbeitet Absender- und Empfängeradressen, Kontaktdaten, Betreff, Nachrichten, Anhänge und Kommunikationsmetadaten.

Dienst / Betriebsmodell	Verwendung	Verarbeitete Daten und Abrufweg
HERE Maps / HERE APIs HERE Europe B.V. Kennedyplein 222-226 5611 ZT Eindhoven Niederlande HERE WeGo: HERE Global B.V. Kennedyplein 222-226 5611 ZT Eindhoven Niederlande Datenschutzkontakt (https://www.here.com/en-us/privacy/)	Grundkarten mit Vektor- und Rasterkacheln, Straßenkarten und Satellitenbildern; Adresssuche, Stadtteilzuordnung, Routing, Routenoptimierung sowie Höhenansicht und geländebezogene Schattenberechnung. Rolle: Externer Karten- und Informationsanbieter; bei weisungsgebundener Verarbeitung Unterauftragsverarbeiter. Die Nutzung von HERE WeGo nach Öffnen eines externen Links ist gesondert von den integrierten APIs zu behandeln. Verarbeitungsraum: Für die Verarbeitung im Auftrag ausschließlich EU nach Ziffer 9.	Die integrierten Grundkarten einschließlich Straßen-, Dunkel- und Satellitenansichten verwenden ausschließlich HERE. Browserabrufe von maps.hereapi.com, assets.vector.hereapi.com und den im Kartenstil referenzierten Ressourcen übermitteln IP-Adresse, Kartenbereich, Zoomstufe und technische Abrufdaten. Routenberechnung und Wegpunktoptimierung über router.hereapi.com und wps.hereapi.com übermitteln aus dem Browser Adressen, Koordinaten, Wegpunkte und Suchparameter. Für Adresssuche und Stadtteilzuordnung fragen unsere Server geocode.search.hereapi.com und revgeocode.search.hereapi.com ab; für HERE DEM rufen sie Höhenkacheln über maps.hereapi.com ab und übermitteln Kachelkoordinaten und Zoomstufe. Dabei erhält HERE die Abfrageparameter und Server-Verbindungsdaten, keine von uns weitergeleitete Nutzer-IP, Nutzernamen oder Sensormesswerte. Beim Öffnen eines HERE WeGo-Links erhält HERE die gewählte Route. Bei Nichtverfügbarkeit zeigen wir einen Hinweis an und wechseln nicht zu einem anderen Kartenanbieter.

Dienst / Betriebsmodell	Verwendung	Verarbeitete Daten und Abrufweg
Overpass-Dienste (overpass-api.de) FOSSGIS e.V. Bundesallee 23 10717 Berlin Deutschland info@fossgis.de	Öffentliche Flächennutzungs- und Straßenanalyse in CityPulse mit OpenStreetMap-Daten, unabhängig vom Anbieter der Kartendarstellung. Rolle: Externer Empfänger von Abfrage- und Verbindungsdaten; nicht allein durch den Datenabruf Unterauftragsverarbeiter. Verarbeitungsraum: Für die Verarbeitung im Auftrag ausschließlich EU nach Ziffer 9.	Der CityPulse-Server verwendet ausschließlich overpass-api.de/api/interpreter. Der Betreiber erhält Standortkoordinaten, bei Straßenabfragen den Suchradius, festgelegte Kartenfilter und technische Server-Verbindungsdaten. Wir leiten keine Nutzer-IP, Anmeldedaten, Organisations- oder Sensor-IDs, Sensormesswerte oder Bewegungsverläufe weiter. Standortangaben können personenbezogen oder vertraulich sein. CityPulse begrenzt die Abfragen und verwendet erfolgreiche Ergebnisse aus einem Zwischenspeicher mit 24 Stunden Gültigkeit. Bei Ausfall erfolgt kein Wechsel zu anderen Overpass-Betreibern; die nicht verfügbare Flächennutzungsanalyse wird gekennzeichnet.
Open-Meteo OpenMeteo GmbH Hintere Schilligmatte 6 6463 Bürglen (UR) Schweiz info@open-meteo.com	Wettervorhersagen und historische Wetterdaten über api.open-meteo.com und archive-api.open-meteo.com. Rolle: Externer Empfänger von Abfrage- und Verbindungsdaten; nicht allein durch den Datenabruf Unterauftragsverarbeiter. Verarbeitungsraum: Für die Verarbeitung im Auftrag ausschließlich EU nach Ziffer 9.	Koordinaten, Abfragezeitraum und technische Verbindungsdaten. Bei serverseitigen Abrufen erhält der Dienst die Verbindung unseres Servers.

Dienst / Betriebsmodell	Verwendung	Verarbeitete Daten und Abrufweg
OpenHolidays API STÜBER SYSTEMS GmbH Grabbeallee 31 13156 Berlin Deutschland hello@stueber.de	Kalenderabfragen über openholidaysapi.org zur Einordnung von Auslastungs- und Betriebskennzahlen. Die App-Server rufen für Parken, Abfall und Stadtgrün öffentliche Feiertage ab; Parken und Stadtgrün beziehen auch Schulferien. Rolle: Externer Empfänger von Abfrage- und Verbindungsdaten; nicht allein durch den Datenabruf Unterauftragsverarbeiter. Verarbeitungsraum: Deutschland (Hosting bei STRATO); weitere auftragsbezogene Verarbeitung ausschließlich EU.	Unsere Server übermitteln Land (DE), Bundesland (DE-NW), Kalenderjahr, Sprache und technische Server-Verbindungsdaten, keine Nutzer-IP, Anmeldedaten, Organisations- oder Sensor-IDs und keine Sensormesswerte. Erfolgreiche Antworten verwenden sie aus einem Zwischenspeicher mit 24 Stunden Gültigkeit. Bei Ausfall wechseln sie nicht den Anbieter. In Dashboard-Auswertungen erfolgen direkte Browserabrufe: Der Betreiber erhält die IP-Adresse, technische Abrufdaten, Land, Region, Zeitraum und Sprache.
GIS-Dienste (WMS/WFS und GeoJSON) Geobasis NRW Land Nordrhein-Westfalen Vertreten durch die Bezirksregierung Köln Zeughausstraße 2-8 50667 Köln Deutschland poststelle@bezreg-koeln.nrw.de	Darstellung der von Ihrer Organisation ausgewählten Geodaten. Die voreingestellten NRW-Dienste über wms.nrw.de und wfs.nrw.de stammen von Geobasis NRW. Für weitere von Ihrer Organisation eingerichtete WMS-, WFS- und GeoJSON-Quellen ist der jeweilige Quellenbetreiber der Empfänger. Rolle: Vom Auftraggeber bestimmter externer Quellenbetreiber; keine automatische Beauftragung als Unterauftragsverarbeiter von dataMatters. Verarbeitungsraum: Für über urbanOS verarbeitete personenbezogene Auftragsdaten ausschließlich EU nach Ziffer 9.	Kartenausschnitte, Layernamen, Filter und technische Verbindungsdaten. Bei Browserabrufen erhält der Betreiber die Endgeräteverbindung, bei Proxyabrufen die Serververbindung. Ihre Organisation legt die Datenquelle und den Empfänger durch die Einrichtung der Integration fest.

Ergänzung zu HERE: Die aktivierbare Gateway-Standortplanung verwendet serverseitig browse.search.hereapi.com. Übermittelt werden Kartenbereich, Einrichtungskategorien und Server-Verbindungsdaten, keine weitergeleiteten Nutzer-IP-Adressen, Organisationskennungen oder Sensormesswerte. Verfügbare Gebäudehöhen stammen aus bereits geladenen HERE-Vektorkarten. Ergebnisse und Kandidaten verbleiben nur vorübergehend im geöffneten Planungsfenster.

CloudRF-Admin-Pilot: Plattform-Administratoren können Funkabdeckung über api.cloudrf.com berechnen. Unsere Server übermitteln Standortkoordinaten bestehender oder geplanter Gateways, Funk- und Antennenparameter sowie technische Server-Verbindungsdaten. Sensorpositionen, Messwerte, Gerätekennungen, Organisationsnamen und Nutzer-IP-Adressen werden nicht weitergeleitet. Der Sensorvergleich erfolgt lokal im Browser. CloudRF gibt Serverstandorte in Großbritannien an und speichert Berechnungen nach seinen tarifabhängigen Aufbewahrungsbedingungen. Ergebnisse mit Abdeckungsbild, Legende und Berechnungszeit werden in der bestehenden Supabase-Datenbank organisationsbezogen dauerhaft gespeichert, bis sie ersetzt oder gelöscht werden. Zugriff haben ausschließlich Plattform-Administratoren. Bei unveränderten Einstellungen können die Ergebnisse ohne erneute Berechnung wiederverwendet werden. Berechnungen erfolgen nur nach ausdrücklicher Auslösung; der Pilot ist nicht für andere Nutzer freigegeben.

Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Vereinbarung und Unterschriften

Dokumentkennung: avv / 1f53da62cce7fef2

Die Parteien vereinbaren diesen AVV einschließlich der Anlagen 1 bis 3 für die auf dem Zuordnungsblatt genannte Leistungsvereinbarung. Die Anlagen enthalten die Verarbeitungsbeschreibung, die technischen und organisatorischen Maßnahmen sowie das Verarbeitungsverzeichnis. Auftragspezifische Ergänzungen werden in der vereinbarten Fassung dieser Anlagen festgehalten.

Die Unterschriften beziehen sich auf diese vollständige, durchgehend nummerierte Dokumentfassung. Ausfüllbare Textfelder dienen der Vertragszuordnung; sie sind keine elektronische Signatur.

Auftraggeber / Verantwortlicher

Name und Funktion der unterzeichnenden Person

Ort und Datum

Unterschrift

dataMatters GmbH

Name und Funktion der unterzeichnenden Person

Ort und Datum

Unterschrift