

Datenschutzerklärung

für urbanos.de und die urbanOS Services

dataMatters GmbH

Pilgrimstr. 6

50674 Köln

Diese Erklärung informiert darüber, wie dataMatters personenbezogene Daten verarbeitet, wenn Sie unsere Website, ein eigenes urbanOS Angebot, ein Nutzerkonto, den urbanOS Store, Support- oder Vertriebswege nutzen. Verarbeitet dataMatters Daten ausschließlich im Auftrag einer Kundenorganisation, ist diese Organisation verantwortlich und ihre Datenschutzinformation maßgeblich.

1. Verantwortlicher und Kontakt

(1) Verantwortlicher im Sinne der DSGVO ist die dataMatters GmbH, Pilgrimstr. 6, 50674 Köln, E-Mail: mail@datamatters.io, soweit wir nachfolgend eigene Zwecke und Mittel der Verarbeitung bestimmen.

(2) Geschäftsführer ist Dr. Daniel Trauth. Einen Datenschutzbeauftragten haben wir derzeit nicht bestellt. Datenschutzanfragen können unter mail@datamatters.io oder postalisch an die vorstehende Anschrift gerichtet werden.

(3) Die jeweilige Kundenorganisation verantwortet die von ihr bestimmten fachlichen Verarbeitungen in urbanOS. dataMatters verarbeitet diese Daten nach dem vereinbarten Auftrag und dem AVV. In einem Verbund können mehrere Organisationen eigene Verantwortliche sein; eine zentrale Beschaffungs- oder Administrationsstelle ist nicht allein deshalb für sämtliche Daten verantwortlich. Freigaben gemeinsamer Datenräume und weisungsberechtigte Stellen ergeben sich aus der dokumentierten Organisation. Bitte wenden Sie sich bei Fragen zu solchen Daten an die Organisation, die den jeweiligen Bereich betreibt.

(4) Bei klar gekennzeichneten Partnerangeboten ist der jeweilige Partner für seine Leistung, seinen Vertrag und die von ihm bestimmten Datenverarbeitungen eigenständig verantwortlich. Informationen zu Partner und Rollen werden im Angebot oder Store bereitgestellt.

2. Grundsätze, Zwecke und Rechtsgrundlagen

(1) Wir verarbeiten personenbezogene Daten nur, soweit dies erforderlich ist und eine Rechtsgrundlage besteht. Je nach Vorgang stützen wir uns insbesondere auf Art. 6 Abs. 1 Buchst. a DSGVO (Einwilligung), Buchst. b (Vertrag und vorvertragliche Maßnahmen), Buchst. c (rechtliche Pflicht) oder Buchst. f (berechtigzte Interessen). Bei Behörden können zusätzlich die für die jeweilige Aufgabe geltenden öffentlich-rechtlichen Grundlagen maßgeblich sein.

(2) Unsere berechtigten Interessen liegen insbesondere in einem sicheren und wirtschaftlichen Betrieb, der technischen Stabilität und Weiterentwicklung der Services, der Verhinderung von Missbrauch, der Bearbeitung von Anfragen, der Vertrags- und Kundenverwaltung, der Reichweitenmessung ohne unnötige Personenbezüge sowie der Durchsetzung und Verteidigung von Ansprüchen. Wir wägen diese Interessen mit Ihren Rechten ab.

(3) Soweit eine Einwilligung Grundlage ist, können Sie sie jederzeit mit Wirkung für die Zukunft über die angebotenen Einstellungen oder die oben genannten Kontakte widerrufen. Die Rechtmäßigkeit der Verarbeitung bis zum Widerruf bleibt unberührt.

3. Aufruf der Website und technische Protokolle

(1) Beim Aufruf von urbanos.de oder öffentlich erreichbaren urbanOS Seiten verarbeiten unsere Systeme technisch erforderliche Daten, etwa IP-Adresse, Datum und Uhrzeit, angeforderte Ressource, Referrer soweit übertragen, Browser- und Geräteinformationen, Antwortstatus sowie Sicherheits- und Fehlerdaten. Dies ist erforderlich, um Inhalte auszuliefern, Angriffe abzuwehren, Fehler zu analysieren und Stabilität sicherzustellen.

(2) Rechtsgrundlage ist Art. 6 Abs. 1 Buchst. f DSGVO; unser berechtigtes Interesse liegt im sicheren, funktionsfähigen und missbrauchsgeschützten Betrieb. Soweit ein Zugriff auf Informationen in Ihrem Endgerät oder deren Speicherung unbedingt erforderlich ist, richtet er sich nach § 25 Abs. 2 TDDDG.

(3) Technische Protokolle werden nur so lange aufbewahrt, wie dies für Betrieb, Sicherheit, Fehleranalyse und Nachweiszwecke erforderlich ist. Längere Aufbewahrung erfolgt bei einem konkreten Sicherheitsereignis, zur Rechtsverfolgung oder aufgrund gesetzlicher Pflichten.

4. Konten, Organisationen und Anmeldung

(1) Bei Registrierung und Kontonutzung verarbeiten wir insbesondere Namen, geschäftliche Kontaktdaten, Organisation, Rollen, Mandate, Einladungen, Konto- und Authentisierungsdaten, Loginzeitpunkte, Spracheinstellungen, Sicherheitsereignisse und die von Ihnen vorgenommenen administrativen Handlungen.

(2) Soweit wir Konten und Berechtigungen nach Weisung einer Kundenorganisation verwalten, verarbeiten wir diese Daten als Auftragsverarbeiter; die Organisation informiert über die für sie geltende Rechtsgrundlage. Für davon getrennte eigene Vertragsbeziehungen und Vertragsverwaltung gilt Art. 6 Abs. 1 Buchst. b DSGVO, für gesetzliche Nachweise Buchst. c und für erforderliche eigene Sicherheits- oder Verwaltungszwecke Buchst. f mit dokumentierter Interessenabwägung. Support oder Sicherheitsbezug allein machen eine auftragsbezogene Verarbeitung nicht zur eigenen Verarbeitung von dataMatters.

(3) Wenn ein Kunde oder Identitätsanbieter Ihr Konto einrichtet, erhalten wir Daten von dieser Stelle. Die jeweilige Organisation entscheidet über Rollen und Zugriffsrechte. Sie darf nur berechtigte Nutzer einladen und muss deren Angaben aktuell halten.

5. Verträge, Angebote, Store und Abrechnung

(1) Bei Angeboten, Bestellungen und Verträgen verarbeiten wir Kontakt-, Organisations-, Angebots-, Bestell-, Leistungs-, Liefer-, Rechnungs-, Zahlungsstatus-, Steuer-, Lizenz-, Support- und Kommunikationsdaten. Bei Hardware können Lieferanschrift, Empfangsbestätigung, Seriennummer, Gewährleistungs- und Rückrufinformationen hinzukommen.

(2) Zwecke sind Vertragsanbahnung und -durchführung, Bereitstellung, Abrechnung, Lieferung, Gewährleistung, Rückabwicklung, Betrugsprävention, Buchhaltung und die Erfüllung steuer-, handels-, produkt- und verbraucherrechtlicher Pflichten. Rechtsgrundlagen sind Art. 6 Abs. 1 Buchst. b und c DSGVO sowie für Missbrauchsschutz Art. 6 Abs. 1 Buchst. f DSGVO.

(3) Bei einem Partnerangebot übermitteln wir die für Vertragsanbahnung, Vertragsschluss, Bereitstellung, Support und Abrechnung erforderlichen Daten an den ausgewiesenen Partner. dataMatters und Partner handeln grundsätzlich jeweils für ihre eigenen Vertrags- und Rechtspflichten; abweichende Rollen werden im Angebot erklärt.

(4) Bei Zahlungen über Stripe erhält Stripe die für die Zahlungsabwicklung erforderlichen Zahlungs-, Geräte-, Transaktions- und Prüfungsdaten. Stripe verarbeitet bestimmte Daten in eigener Verantwortlichkeit nach seinen Datenschutzinformationen.

6. Kontakt, Vertrieb, Support und Veranstaltungen

(1) Wenn Sie uns per E-Mail, Kontaktformular, Support-Widget, Telefon im Rahmen eines Projekts oder auf anderem Weg kontaktieren, verarbeiten wir Ihre Kontaktdaten, Organisation, Inhalt, Anhänge, technische Kontextdaten und den Bearbeitungsverlauf. Bitte übermitteln Sie keine nicht erforderlichen vertraulichen oder besonderen personenbezogenen Daten.

(2) Wir bearbeiten allgemeine Kontakt- und Vertriebsanfragen zur Kommunikation, Vertragsanbahnung und Nachweisführung auf Grundlage von Art. 6 Abs. 1 Buchst. b beziehungsweise f DSGVO; gesetzliche Aufbewahrung beruht auf Buchst. c. Soweit Support Einsicht in Daten einer Kundenorganisation erfordert, erfolgt diese Verarbeitung nach deren Auftrag und dem AVV. Wir trennen die jeweiligen Zwecke und beschränken den Zugriff auf die erforderlichen Informationen.

(3) Wir versenden keinen allgemeinen Marketing-Newsletter. Individuelle geschäftliche Ansprache erfolgt im gesetzlich zulässigen Rahmen.

(4) Für Bestätigungen und Benachrichtigungen zu Websiteanfragen setzen wir Resend ein, betrieben von Plus Five Five, Inc., USA. Resend verarbeitet Empfängeradresse, Nachrichteninhalte und Versandmetadaten. Wir speichern Website-Anfragedaten in Supabase. Anbieterinformationen: Resend Datenschutz (<https://resend.com/legal/privacy-policy>) und Supabase Datenschutz (<https://supabase.com/privacy>). Informationen zu Drittlandübermittlungen finden Sie in Ziffer 14.

(5) Für Transaktions- und Supportnachrichten verwenden wir Amazon Simple Email Service (Amazon SES). Unsere E-Mail-Postfächer hostet Microsoft 365 / Exchange Online; wir nutzen Outlook zum Versand, Empfang und zur Verwaltung unserer Kunden- und Supportkommunikation. Amazon SES und Microsoft verarbeiten dabei Absender- und Empfängeradressen, Betreff, Nachrichteninhalte, Anhänge sowie Versand- und Zustellmetadaten. Rechtsgrundlagen sind Art. 6 Abs. 1 Buchst. b DSGVO für Vertragsangelegenheiten und vorvertragliche Anfragen, Art. 6 Abs. 1 Buchst. f DSGVO für sonstige geschäftliche Kommunikation und Art. 6 Abs. 1 Buchst. c DSGVO für gesetzliche Aufbewahrungspflichten. Für Support im Kundenauftrag gelten die Weisungen und der AVV. Informationen zu Drittlandübermittlungen finden Sie in Ziffer 14. Anbieterinformationen: AWS Datenschutz (<https://aws.amazon.com/privacy/>) und Microsoft Datenschutz (<https://privacy.microsoft.com/de-de/privacystatement>).

(6) Für Onlineveranstaltungen versenden wir Besprechungslinks zu Microsoft Teams. Beim Öffnen des Links oder bei Ihrer Teilnahme erhält Microsoft Verbindungs- und Kontodaten sowie Ihren Anzeigenamen. Wenn Sie Chat, Mikrofon, Kamera oder Bildschirmfreigabe nutzen, verarbeitet Microsoft die von Ihnen geteilten Inhalte. Über Aufzeichnungen oder Transkriptionen informieren wir vor Beginn und holen die erforderliche Einwilligung ein.

(7) Nach einer erfolgreichen Anfrage können Websiteformulare Ihre E-Mail-Adresse im lokalen Browserspeicher unter `urbanos_lead_email` merken, um weitere Formulare auf demselben Browser vorzubelegen. Dieser lokale Eintrag hat derzeit keine automatische Ablaufzeit. Sie können ihn über die Website-Daten Ihres Browsers löschen; das Löschen dieses Eintrags entfernt nicht die bereits versandte Anfrage bei uns oder unseren Versand- und Speicherdiensten. Die lokale Speicherung übermittelt die Adresse für sich genommen nicht an einen weiteren Anbieter. Für eine nicht technisch erforderliche Speicherung und das spätere Auslesen ist eine Einwilligung nach § 25 Abs. 1 TDDDG erforderlich; die Verarbeitung der Adresse auf dieser Grundlage richtet sich nach Art. 6 Abs. 1 Buchst. a DSGVO.

7. Produktanalyse, Einwilligungen und Sitzungswiedergabe

(1) Auf urbanos.de verwenden wir PostHog mit EU-Endpunkten für die Websiteanalyse. Erst nach Ihrer ausdrücklichen Auswahl „Analyse erlauben“ laden wir die Analysesoftware und beginnen mit der Messung. Ohne diese Einwilligung wird auch keine Analyseerkennung angelegt oder an PostHog übermittelt. Ein EU-Endpunkt allein bedeutet keine Anonymität. Weitere Informationen zum Anbieter: PostHog Datenschutz (<https://posthog.com/privacy>).

(2) Wir erfassen festgelegte Ereignisse wie Seitenaufrufe, geöffnete Anwendungsfälle, Betätigung von Kontakt- oder Informationslinks, Beginn und Fehlschläge einer Formularübermittlung, Lade- und Reaktionszeiten sowie grob kategorisierte technische Fehler und wiederholte Klicks. Hinzu kommen Sprache, eine grobe Gerätekategorie, die Einstellung für reduzierte Bewegung, die Herkunftskategorie des Besuchs (etwa Suche oder direkter Aufruf) und gegebenenfalls ein festgelegtes Interessengebiet, zum Beispiel Abfallentsorgung. Wir übermitteln dabei keine vollständigen Seiten- oder Herkunftsadressen mit Suchparametern, Suchbegriffe, frei eingegebenen Texte oder vollständigen Browserkennungen an die Ereignisanalyse. Beim Verbindungsaufbau erhält der Dienst technische Verbindungsdaten.

(3) Nach Ihrer Analyse-Einwilligung vergeben wir eine zufällige pseudonyme Browserkennung. Ein signiertes, für Seitenskripte nicht lesbares Cookie speichert diese Kennung bis zu 120 Tage. Die Einwilligungsauswahl speichern wir bis zu 180 Tage in einem gesonderten Cookie. Wir erstellen für diese Websiteanalyse keine benannten Personenprofile und führen Geräte nicht anhand Ihrer E-Mail-Adresse oder eines Nutzerkontos zusammen.

(4) Kontakt- und Dokumentanfragen speichern wir zur Bearbeitung unabhängig davon, ob Sie in die Websiteanalyse einwilligen; siehe Ziffer 6. Mit Ihrer Analyse-Einwilligung können wir einer pseudonymen Browserkennung zusätzlich zuordnen, dass eine Anfrage gespeichert, als fachlich passend eingestuft oder ein Gespräch tatsächlich durchgeführt wurde. Hierfür übermitteln wir eine nicht sprechende Anfrageerkennung und Zeitpunkte. Namen, E-Mail-Adressen, Betreff und Nachrichtentext werden nicht als Analyseereignisse an PostHog übermittelt. Ohne Analyse-Einwilligung wird die Anfrage nicht für diese Zuordnung an PostHog übermittelt.

(5) Sitzungswiedergabe ist auf dieser Website standardmäßig deaktiviert. Eine Freischaltung setzt zusätzlich Ihre gesonderte Einwilligung in die Sitzungswiedergabe voraus. In dieser Funktion werden Text und Eingaben maskiert sowie Formulare und sensible Bereiche ausgeschlossen; Formularinhalte, Netzwerk-Nachrichteninhalte, Konsolenausgaben und die Zeichenfläche der 3D-Darstellung werden nicht aufgezeichnet. In anderen urbanOS Angeboten werden personenbezogene Produktprofile, geräteübergreifende Zuordnung und maskierte Sitzungswiedergaben nur nach ausdrücklicher Einwilligung aktiviert. Für diese einwilligungsbasierten Verarbeitungen gelten Art. 6 Abs. 1 Buchst. a DSGVO und, soweit anwendbar, § 25 Abs. 1 TDDDG.

(6) Über „Datenschutzeinstellungen“ im Footer können Sie Ihre Auswahl ändern und eine Einwilligung mit Wirkung für die Zukunft widerrufen. Die Website stoppt die weitere Analyse auf diesem Gerät unmittelbar. Auf unserem Server entfernen wir die Zuordnung zu gespeicherten Anfragen und verwerfen noch nicht versandte zugeordnete Analyseereignisse. Kann dieser serverseitige Schritt nicht bestätigt werden, zeigt die Website dies an und bietet eine Wiederholung an. Bereits übermittelte Daten werden durch den Widerruf allein nicht rückwirkend gelöscht; für eine gesonderte Löschanfrage nutzen Sie bitte die Kontakte in Ziffer 1. Notwendige Sicherheits-, Authentisierungs- und Spracheinstellungen bleiben hiervon unberührt, soweit sie für den gewünschten Dienst erforderlich sind.

(7) Eine Einwilligung in Website- oder Produktanalyse erlaubt keine unabhängige Nutzung der Fachdaten einer Kundenorganisation. Soweit Analysedaten im Auftrag einer Organisation verarbeitet werden, gelten zusätzlich deren Weisungen, der AVV und die dort vereinbarte Zweckbindung. Kundendaten und daraus abgeleitete Aggregate werden nicht für unabhängiges Benchmarking oder zur Verbesserung eigener oder fremder KI-Modelle verwendet.

8. Support-Widget Mendaro

(1) Über das Support-Widget Mendaro können Sie uns Anfragen senden. Wir verarbeiten Ihre Kontakt- und Nachrichtendaten, Anhänge, technischen Kontext und den Bearbeitungsverlauf, um Ihre Anfrage zu beantworten.

(2) Rechtsgrundlagen sind Art. 6 Abs. 1 Buchst. b DSGVO für vertragsbezogene Hilfe und Art. 6 Abs. 1 Buchst. f DSGVO für die Bearbeitung allgemeiner Anfragen.

(3) dataMatters bearbeitet die Anfragen. Soweit der Support Zugriff auf Daten Ihrer Organisation benötigt, gelten deren Weisungen und der AVV. Für den Versand von Supportnachrichten nutzen wir die in Ziffer 6 beschriebenen E-Mail-Dienste.

9. Karten, Geodaten, Wetter und externe Informationsdienste

(1) Je nach App und Kartenansicht verwenden wir HERE Maps/HERE APIs für Vektor- und Rasterkarten, Straßenkarten, Satellitenbilder sowie Routing, Routenoptimierung, Geocoding und Umgebungssuche. Overpass-Dienste liefern Umgebungsdaten zu Flächennutzungen und Straßen unabhängig vom Anbieter der Kartendarstellung; Open-Meteo liefert Wettervorhersagen und historische Wetterdaten. Diese Anbieter sind nicht in jeder App aktiv. OpenStreetMap als Datenquelle ist von dem Betreiber zu unterscheiden, der eine Karte oder Abfrage bereitstellt. HERE-Straßen- und Dunkelansichten verwenden HERE auch für Vektorkarten und Gebäude. Ein HERE-Fehler löst in diesen Ansichten keinen Wechsel zu einem anderen Kartenanbieter aus. Die integrierten Grundkarten einschließlich Straßen-, Dunkel- und Satellitenansichten verwenden ausschließlich HERE. Bei Nichtverfügbarkeit zeigen wir einen Hinweis an und wechseln nicht zu einem anderen Kartenanbieter.

(2) Bei direkten Browserabrufen von Kartenkacheln, Stilen, Schrift- oder Bildressourcen erhält der Anbieter insbesondere Ihre IP-Adresse, Zeitpunkt, technische Abrufdaten, den angeforderten Kartenbereich und die Zoomstufe. Das gilt auch für HERE-Karten und -Satellitenbilder. Routing und Geocoding können Adressen, Koordinaten, Wegpunkte und Suchparameter übermitteln. Bei serverseitigen Abrufen erhält der Anbieter grundsätzlich die Verbindungsdaten unseres Servers und die Abfrageparameter; Standortangaben können dennoch personenbezogen sein. Wenn Sie einen HERE-WeGo-Link öffnen, übergeben Sie die gewählte Route an HERE WeGo. Für die Adresssuche und Stadtteilzuordnung fragen unsere Server `geocode.search.hereapi.com` beziehungsweise `revgeocode.search.hereapi.com` ab. Wir senden die Suchadresse oder Koordinaten mit Server-Verbindungsdaten und leiten dabei keine Nutzer-IP weiter. Die CityPulse-Adresssuche verwendet HERE über unseren Server. Für die öffentliche Flächennutzungs- und Straßenanalyse ruft der CityPulse-Server ausschließlich `overpass-api.de/api/interpreter` ab. Er sendet Standortkoordinaten, bei Straßenabfragen den Suchradius und festgelegte Kartenfilter. Der Betreiber erhält die Serververbindung; wir leiten dabei keine Nutzer-IP, Anmeldedaten, Organisations- oder Sensor-IDs, Sensormesswerte oder Bewegungsverläufe weiter. Standortangaben können dennoch personenbezogen oder vertraulich sein. Wir begrenzen die Abfragen und nutzen erfolgreiche Ergebnisse aus einem Zwischenspeicher mit 24 Stunden Gültigkeit. Bei Ausfall wechselt diese Analyse nicht zu einem anderen Overpass-Betreiber. Wir kennzeichnen die nicht verfügbare Flächennutzungsanalyse; verfügbare HERE-Ergebnisse bleiben nutzbar. Für die aktivierbare Gateway-Standortplanung fragen unsere Server `browse.search.hereapi.com` mit dem sichtbaren Kartenbereich und Einrichtungskategorien (Schulen, Feuerwehr, Verwaltung) ab. HERE erhält Server-Verbindungsdaten und Suchparameter, keine weitergeleiteten Nutzer-IP-Adressen, Organisationskennungen oder Sensormesswerte. Gebäudehöhen stammen, soweit verfügbar, aus den bereits geladenen HERE-Vektorkarten. Suchergebnisse und vorgemerkte Kandidaten werden nur vorübergehend im geöffneten Planungsfenster gehalten.

(3) 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. Weitere Informationen: CloudRF Datenschutz und Bedingungen (<https://cloudrf.com/terms-and-conditions/>).

(4) Für Wetterdaten nutzen wir `api.open-meteo.com` und `archive-api.open-meteo.com`. Die CityPulse-Analyse nutzt für Overpass nur `overpass-api.de`. HERE-Karten verwenden `maps.hereapi.com`, `assets.vector.hereapi.com` und die im Kartenstil referenzierten Ressourcen; für Routing und Suche kommen die jeweiligen HERE-APIs hinzu. Weitere Informationen: HERE Datenschutz (<https://www.here.com/en-us/privacy>).

(5) In den Routenfunktionen für Abfall und Stadtgrün verwenden wir HERE Routing (`router.hereapi.com`) und Wegpunktoptimierung (`wps.hereapi.com`). Ihr Browser übermittelt Koordinaten der Routenstopps, Start und Ziel, Fahrzeugmodus und technische Verbindungsdaten einschließlich Ihrer IP-Adresse. Wenn HERE keine Route berechnen kann, zeigen wir einen Fehler an; wir wechseln nicht zu einem anderen Routinganbieter.

(6) Für die Höhenansicht und geländebezogene Schattenberechnung der Plattformkarte verwenden wir Höhenkacheln von HERE DEM über maps.hereapi.com. Unser Server übermittelt Kachelkoordinaten und Zoomstufe. HERE erhält dabei die Verbindung unseres Servers, keine von uns weitergeleitete Nutzer-IP und in diesen Abfragen keine Nutzernamen oder Sensormesswerte. Kartenbewegungen können bei aktiviertem Werkzeug neue Abfragen auslösen. Standortangaben können dennoch personenbezogen sein. Bei einem HERE-Fehler wechseln wir nicht zu einem anderen Höhendatenanbieter. Weitere Dienstinformationen: HERE Datenschutz (<https://www.here.com/en-us/privacy/>).

(7) Für Kalendervergleiche nutzen die App-Server für Parken, Abfall und Stadtgrün OpenHolidays API (openholidaysapi.org). Sie fragen öffentliche Feiertage ab; Parken und Stadtgrün beziehen dort auch Schulferien. Der Betreiber erhält Land (DE), Bundesland (DE-NW), Kalenderjahr, Sprache und technische Verbindungsdaten unserer Server. Wir leiten dabei keine Nutzer-IP, Anmeldedaten, Organisations- oder Sensor-IDs und keine Sensormesswerte weiter. Unsere Server verwenden erfolgreiche Kalenderantworten aus einem Zwischenspeicher mit 24 Stunden Gültigkeit. Bei Ausfall wechseln sie nicht zu einem anderen Kalenderanbieter. In entsprechenden Dashboard-Auswertungen ruft Ihr Browser OpenHolidays API weiterhin mit Land, Region, Zeitraum und Sprache ab. Dabei erhält der Betreiber Ihre IP-Adresse und technische Abrufdaten.

(8) Organisationen können zusätzliche GIS-Dienste über WMS/WFS oder GeoJSON einbinden, etwa Geobasisdienste des Landes Nordrhein-Westfalen über wms.nrw.de und wfs.nrw.de. Je nach Dienst betreffen Abfragen Kartenausschnitte, Layernamen, Such- oder Filterparameter. Direkte Abrufe legen dem Betreiber die Browserverbindung offen; über unsere Server vermittelte Abrufe legen die Serververbindung und Abfrageparameter offen. Die Organisation bestimmt die verwendeten Datenquellen; konkrete Betreiber, Rollen und Übermittlungen richten sich nach der freigegebenen Integration.

(9) Einzelne Karten und öffentliche Ansichten enthalten Navigationslinks zu Google Maps oder Apple Maps. Erst wenn Sie einen solchen Link öffnen, übermitteln Sie die darin enthaltenen Ziel- oder Routenkoordinaten an Google beziehungsweise Apple. Dort gelten die jeweiligen Datenschutzzinformationen.

(10) Rechtsgrundlage ist Art. 6 Abs. 1 Buchst. b DSGVO, soweit die Funktion von Ihnen angefordert und vertraglich geschuldet ist, andernfalls Art. 6 Abs. 1 Buchst. f DSGVO für eine zweckmäßige Darstellung. Eine einwilligungsbedürftige Endgeräteverarbeitung erfolgt nur nach Art. 6 Abs. 1 Buchst. a DSGVO und § 25 Abs. 1 TDDDG.

10. Videos und eingebettete Inhalte

(1) YouTube-Videos oder vergleichbare externe Inhalte werden, soweit eingesetzt, im erweiterten Datenschutzmodus oder als zunächst blockierte Vorschau eingebunden und erst nach Ihrer Auswahl geladen. Beim Laden erhält der Anbieter jedenfalls Ihre IP-Adresse und technische Abrufdaten; bei einem eingeloggten Konto kann er den Abruf zuordnen.

(2) Rechtsgrundlagen sind Ihre Einwilligung nach Art. 6 Abs. 1 Buchst. a DSGVO und § 25 Abs. 1 TDDDG. Alternativ können wir auf Inhalte lediglich verlinken; dann findet eine Übermittlung erst statt, wenn Sie dem Link folgen.

(3) YouTube-Videooplayer laden wir über youtube-nocookie.com, Vorschaubilder über img.youtube.com. Auch ein extern geladenes Vorschaubild übermittelt bereits Verbindungsdaten an den Anbieter. Der erweiterte Datenschutzmodus bedeutet nicht, dass beim Abruf keine Verbindung zu Google entsteht.

(4) Die Integrationsübersicht zeigt Logos von GitHub (avatars.githubusercontent.com) und The Things Network (thethingsnetwork.org). Bei direkten Browserabrufen erhält der jeweilige Betreiber Ihre IP-Adresse, die angeforderte Ressource, Zeitpunkt und technische Abrufdaten, gegebenenfalls einen vom Browser übertragenen Referrer. Bei Abruf über einen eigenen Bildproxy erhält der Ursprungsanbieter dessen Verbindungsdaten; lokal bereitgestellte Bilder lösen keinen Abruf beim ursprünglichen Bildanbieter aus. Inhalte innerhalb eines fremden eingebetteten Dienstes richten sich zusätzlich nach dessen Datenschutzinformationen.

(5) Für erforderliche Inhaltsauslieferung kommt Art. 6 Abs. 1 Buchst. f DSGVO auf Grundlage einer Interessenabwägung in Betracht. Soweit eingebettete Dienste eine Einwilligung für die Verarbeitung oder einen Zugriff auf Ihr Endgerät benötigen, gelten Art. 6 Abs. 1 Buchst. a DSGVO und § 25 Abs. 1 TDDDG.

11. KI-Funktionen, NOVA und Automationen

(1) Für NOVA, Assistenz-, Analyse- und Automationsfunktionen nutzen wir AWS Bedrock und Mistral. Die Funktionen verarbeiten Ihre Texteingaben, freigegebenen Organisations- und Fachdaten, Berechtigungs- und Kontextinformationen, Ergebnisse, Feedback sowie Sicherheits- und Ausführungsprotokolle.

(2) Die Verarbeitung erfolgt auf Nutzeranfrage oder aufgrund einer durch berechtigte Administratoren freigegebenen Automation. KI- und MCP-Zugriffe unterliegen den jeweiligen Organisations-, Rollen-, App- und Datenberechtigungen. Zwecke sind die angeforderte Zusammenfassung, Analyse, Inhaltserzeugung, Abfrage oder Ausführung. Bei Verarbeitung im Auftrag bestimmt die Kundenorganisation die Rechtsgrundlage; für eine eigene Vertragsnutzung gilt Art. 6 Abs. 1 Buchst. b DSGVO. MCP-Zugänge können befristet und widerrufen werden; Aufrufe werden protokolliert. Schreib- und Steuerungsaktionen benötigen eine organisationsbezogene Freigabe, Steuerbefehle zusätzlich einen dokumentierten Bestätigungsschritt.

(3) dataMatters und die eingesetzten Modellanbieter verwenden Kundendaten einschließlich Eingaben, Ausgaben und daraus abgeleiteter anonymisierter Aggregate nicht zum Trainieren oder Verbessern eigener oder fremder KI-Modelle. Die angeforderte KI-Inferenz für die Kundenorganisation bleibt zulässig. Auch unabhängige Werbung, Benchmarking oder eigene Produktentwicklung mit auftragsbezogenen Kundendaten sind ausgeschlossen. Diese Zweckbindung entfällt nicht durch eine allgemeine Einwilligung in Produktanalyse. Bei direkter Mistral-Nutzung ist Training deaktiviert (Opt-out). Funktionen oder Feedbackübermittlungen, die eine Nutzung von Kundendaten für Modellverbesserung erlauben, werden nicht mit Kundendaten genutzt.

(4) KI-Ausgaben können fehlerhaft oder unvollständig sein. Die verantwortliche Stelle prüft Ergebnisse vor ihrer Verwendung und stellt bei Entscheidungen über Personen die erforderliche menschliche Prüfung sicher. Gespeicherte KI-Chatverläufe einschließlich Eingaben und Antworten werden standardmäßig spätestens 30 Kalendertage nach der jeweiligen Nachricht gelöscht. Inhalte werden nicht zusätzlich in technischen Protokollen gespeichert; für Zugriffs- und Sicherheitsprotokolle gelten die getrennten Fristen nach Ziffer 15.

(5) Bei Interaktion mit einem KI-System wird die KI-Natur der Funktion kenntlich gemacht, soweit sie nicht offensichtlich ist. Synthetische oder manipulierte Inhalte werden nach den anwendbaren gesetzlichen Anforderungen gekennzeichnet.

12. Sensor-, Geräte- und Fachdaten in Kundenorganisationen

(1) Organisationen können Datenquellen, Sensoren, Geräte, Gateways, Mobilfunk- oder LoRaWAN-Dienste, APIs, Dokumente und andere Systeme anbinden. Je nach Konfiguration können dabei Gerätekennungen, Zeitreihen, Standorte, Bewegungen, Zählwerte, Umwelt- und Betriebsdaten sowie mitgelieferte Metadaten verarbeitet werden.

(2) Die jeweilige Organisation entscheidet über Zweck, Rechtsgrundlage, Datenquellen, Berechtigungen, Veröffentlichungen, Aufbewahrung und Betroffeneninformation. dataMatters verarbeitet diese Daten regelmäßig als Auftragsverarbeiter; Einzelheiten regelt der AVV. Daten, die eine Organisation in öffentlichen Dashboards oder Bürgerfunktionen veröffentlicht, werden durch die Organisation zur Veröffentlichung bestimmt.

(3) Die Noise-App speichert bestimmungsgemäß keine Audioaufnahmen. Counting-Lösungen sollen identifizierbare Bilder oder Videos, Gesichter und Kennzeichen nicht an urbanOS übertragen, sondern Zählwerte am Rand des Netzes erzeugen. Fleet ist nicht für namentliche Fahrerprofile vorgesehen. CityPulse verarbeitet in urbanOS grundsätzlich aggregierte Ergebnisse aus vorgelagerter Erfassung pseudonymisierter, rotierender oder privater MAC-Adressen. Die tatsächliche Sensorkonfiguration und Rechtmäßigkeit verantwortet die einsetzende Organisation.

(4) Wenn Ihre Organisation Integrationen wie The Things Network, Helium, ChirpStack, Mobilfunk, Gateways, n8n, Node-RED, externe APIs oder MCP-Dienste einrichtet, übermittelt urbanOS die für diese Verbindung erforderlichen Daten an die von Ihrer Organisation ausgewählten Betreiber.

13. Empfänger und Auftragsverarbeiter

(1) Innerhalb von dataMatters erhalten nur Personen Zugriff, die ihn für Vertrieb, Vertrag, Betrieb, Support, Sicherheit, Abrechnung oder rechtliche Pflichten benötigen. Darüber hinaus erhalten Daten je nach Vorgang Kundenorganisationen, Partner, Zahlungs- und Versanddienstleister, Hosting- und IT-Anbieter, Kommunikations-, Analyse-, Support-, Karten-, Wetter-, KI-, IoT- und Integrationsdienste sowie Berater, Versicherer, Behörden und Gerichte.

(2) Wir nutzen PostHog über EU-Endpunkte für Produktanalyse, Resend für Website-E-Mails, Amazon SES für Transaktions- und Supportnachrichten sowie Microsoft 365 / Exchange Online für unsere Postfächer. Supabase speichert Website-Anfragedaten. urbanOS verwendet je nach App und Komponente Supabase Cloud und selbst betriebene Supabase-Installationen. Innerhalb einer Kundenorganisation können beide Betriebsmodelle zusammentreffen. AWS stellt Hosting und Infrastruktur bereit. Bei Zahlungen über Stripe erhält Stripe die für die Abwicklung erforderlichen Daten. Die einzelnen Verarbeitungen beschreiben die Ziffern 5 bis 12.

(3) Für Kundenaufträge enthält Anlage 3 des AVV das versionierte Verarbeitungsverzeichnis mit Vertragsgesellschaften, Diensten, Rollen, Datenarten sowie Verarbeitungs- und Zugriffsländern innerhalb der EU. Die Genehmigung von Unterauftragsverarbeitern und Änderungen regelt der AVV. Datenschutzanfragen richten Sie bitte an mail@datamatters.io.

(4) Bei der Veröffentlichung von Blogbeiträgen melden wir öffentliche Seitenadressen über api.indexnow.org an IndexNow. Die Meldung enthält die veröffentlichten URLs und technische Serverdaten, keine Besucherprofile oder Kundensensordaten.

14. Übermittlungen in Drittländer

(1) Personenbezogene Daten aus urbanOS Kundenaufträgen werden ausschließlich in Deutschland oder anderen EU-Mitgliedstaaten verarbeitet, einschließlich Backups und administrativer Support- und Fernzugriffe. Deutsche Standorte werden genutzt, soweit der jeweilige Dienst dort angeboten wird. Plattformhosting erfolgt in AWS Frankfurt; AWS Bedrock nutzt je Modell Deutschland oder Schweden. Die Einzelheiten und der Ausschluss von Drittlandverarbeitung ergeben sich aus Ziffer 9 und Anlage 3 des AVV. Davon getrennte Verarbeitung für eigene Website-, Vertriebs- und Zahlungszwecke sowie vom Nutzer geöffnete externe Angebote wird durch die nachfolgenden Transferregeln beschrieben.

(2) Für die vorgenannten eigenen Zwecke kommen Anbieter mit Sitz außerhalb der EU zum Einsatz, darunter Resend. Soweit dabei personenbezogene Daten in Drittländer übermittelt werden, gelten die Voraussetzungen der Art. 44 ff. DSGVO, insbesondere ein Angemessenheitsbeschluss oder geeignete Garantien wie Standardvertragsklauseln und erforderliche ergänzende Maßnahmen. Diese Regelung erweitert nicht den ausschließlich auf die EU beschränkten Verarbeitungsraum für Auftragsdaten nach dem AVV.

15. Speicherdauer

(1) Wir speichern Daten nur so lange, wie dies für den jeweiligen Zweck, die Vertragsdurchführung, Sicherheit und gesetzliche Nachweise erforderlich ist. Kriterien sind insbesondere Kontolaufzeit, vereinbarte Mess- und Speicherfristen, Abschluss eines Supportfalls, gesetzliche handels- und steuerrechtliche Fristen, Verjährung sowie ein konkreter Rechtsstreit oder Sicherheitsvorfall.

(2) Bei auftragsbezogenen Daten bestimmt die Kundenorganisation die zulässige Aufbewahrung ihrer Fachdaten und die Rückgabe oder Löschung nach dem AVV. Nach vollständiger Übergabe und Löschfreigabe löschen wir aktive Kundenbestände unverzüglich, spätestens innerhalb von 14 Kalendertagen. Backups werden spätestens 30 Kalendertage nach der aktiven Löschung entfernt und bis dahin gegen produktive Nutzung gesperrt. Ein fortbestehendes Konto begründet keine unbegrenzte Speicherung von Support-, Protokoll- oder KI-Daten.

(3) Für die nachfolgend genannten urbanOS Daten gelten die Standardfristen der Tabelle. Frühere berechtigte Löschungen bleiben möglich. Einwilligungsnachweise, Analyseereignisse sowie eigenständige Vertrags- und Zahlungsunterlagen werden zweckbezogen und nach den jeweils erforderlichen gesetzlichen Nachweisfristen behandelt; eine Rohsensorhistorie verlängert deren Aufbewahrung nicht.

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 des AVV 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.

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.

16. Ihre Rechte

(1) Sie haben nach Maßgabe der gesetzlichen Voraussetzungen das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Widerspruch. Erteilte Einwilligungen können Sie jederzeit mit Wirkung für die Zukunft widerrufen.

(2) Soweit wir Daten auf Art. 6 Abs. 1 Buchst. f DSGVO stützen, können Sie aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit widersprechen. Gegen Verarbeitung für Direktwerbung können Sie jederzeit ohne Angabe besonderer Gründe widersprechen; dann verarbeiten wir die Daten nicht mehr zu diesem Zweck.

(3) Zur Ausübung können Sie mail@datamatters.io kontaktieren. Wir dürfen angemessene Informationen zur Identitätsprüfung verlangen. Betrifft die Anfrage Daten, die wir nur im Auftrag einer Organisation verarbeiten, leiten wir sie an diese Organisation weiter oder unterstützen sie bei der Bearbeitung.

(4) Sie können sich bei einer Datenschutzaufsichtsbehörde beschweren, insbesondere in dem Mitgliedstaat Ihres gewöhnlichen Aufenthaltsorts, Ihres Arbeitsplatzes oder des mutmaßlichen Verstoßes. Für dataMatters ist grundsätzlich die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen zuständig.

17. Pflicht zur Bereitstellung, Minderjährige und automatisierte Entscheidungen

(1) Für Registrierung, Vertrag, Bestellung und Support benötigen wir die jeweils als erforderlich gekennzeichneten Angaben. Ohne sie können wir den gewünschten Dienst möglicherweise nicht bereitstellen. Freiwillige Angaben sind als solche erkennbar oder für die angeforderte Zusatzfunktion erforderlich.

(2) Kostenpflichtige urbanOS Verträge richten sich nicht gezielt an Minderjährige. Öffentliche Bürgerfunktionen können allgemein zugänglich sein; sie sollen grundsätzlich ohne Profilbildung oder unnötige Erhebung von Daten Minderjähriger funktionieren. Erkennen wir eine unzulässige Erhebung, ergreifen wir angemessene Lös- und Schutzmaßnahmen.

(3) Wir treffen als eigener Verantwortlicher keine ausschließlich automatisierten Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung im Sinne von Art. 22 DSGVO. Kundenorganisationen dürfen entsprechende Entscheidungen nur bei eigener Rechtsgrundlage, Transparenz, Schutzmaßnahmen und vereinbarter technischer Eignung konfigurieren.

18. Sicherheit und Änderungen dieser Erklärung

(1) Wir setzen risikogerechte technische und organisatorische Maßnahmen ein, insbesondere rollenbezogene Zugriffe, Mandantentrennung, Transportverschlüsselung, Schutz von Geheimnissen, Protokollierung, Sicherungen, geregelte Änderungen, Schwachstellenbehandlung und Vorfallprozesse. Kein internetbasierter Dienst kann absolute Sicherheit garantieren.

(2) Wir aktualisieren diese Datenschutzerklärung, wenn sich Dienste, Anbieter, Rechtslage oder Verarbeitung ändern. Wesentliche Änderungen werden über geeignete Kanäle bekannt gemacht. Die jeweils aktuelle Fassung ist auf unserer Website abrufbar.

(3) Stand: 9. Oktober 2026.