

Muster

Auftragsverarbeitungsvertrag (AVV)

für von der Stadtverwaltung Worms vergebene Dienstleistungen

zwischen

Stadtverwaltung Worms,
vertreten durch den Oberbürgermeister,
Marktplatz 2
67547 Worms
– nachfolgend „Verantwortlicher“ –

und

[Name des Auftragnehmers]
[Rechtsform, Anschrift]
vertreten durch [Name/Funktion]
– nachfolgend „Auftragsverarbeiter“ –

1. Gegenstand des Vertrages

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Sinne des Art. 28 DSGVO.

(2) Dieser Vertrag gilt für Dienstleistungen, die der Verantwortliche im Wege eines Vergabeverfahrens beschafft und bei deren Erbringung personenbezogene Daten im Auftrag verarbeitet werden. Dies betrifft insbesondere Cloud-Dienstleistungen, Software-as-a-Service, Hosting-Leistungen, Wartungs- und Supportleistungen, IT-Betriebsleistungen, Verfahrens- und Plattformleistungen sowie sonstige technische oder organisatorische Dienstleistungen mit Datenverarbeitung im Auftrag.

(3) Die Vergabestelle des Verantwortlichen führt das Vergabeverfahren organisatorisch durch und stellt insbesondere Vergabeunterlagen auf einer Vergabeplattform bereit. Sie beschafft nicht selbst als eigene fachliche Bedarfsträgerin Leistungen, sondern handelt für den Verantwortlichen im Rahmen des Beschaffungsprozesses.

(4) Die konkreten Einzelheiten der Verarbeitung, insbesondere Leistung, Zweck, Art der Verarbeitung, Datenkategorien, betroffene Personengruppen, Systeme, Verarbeitungsorte und Speicher- bzw. Löschrufen, ergeben sich aus Anlage 1.

2. Rechtsgrundlagen und Einordnung

(1) Die Verarbeitung erfolgt auf Grundlage der Datenschutz-Grundverordnung, insbesondere Art. 28 DSGVO. Für den Verantwortlichen als öffentliche Stelle in Rheinland-Pfalz gelten ergänzend die einschlägigen Vorschriften des Landesdatenschutzgesetzes Rheinland-Pfalz.

(2) Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien im Hinblick auf die Verarbeitung personenbezogener Daten im Auftrag.

(3) Gesetzliche Aufbewahrungs-, Dokumentations- und Nachweispflichten des Verantwortlichen, insbesondere aus Haushalts-, Kommunal-, Vergabe- oder sonstigem Fachrecht, bleiben unberührt.

3. Art, Zweck und Umfang der Verarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich geschuldeten Leistungen.

(2) Die Verarbeitung erfolgt nur in dem Umfang, der zur Vertragserfüllung erforderlich ist.

(3) Die Leistung kann insbesondere umfassen die Bereitstellung und den Betrieb von IT-Systemen, die Speicherung und Bereitstellung von Daten, Benutzer- und Rechteverwaltung, Support und Fehlerbehebung, Fernwartung, technische Administration, Datensicherung und Wiederherstellung sowie die Weiterentwicklung, Pflege oder Betreuung von Anwendungen.

(4) Anlage 1 beschreibt je Leistung oder System mindestens die Bezeichnung der Leistung, den Zweck der Verarbeitung, die Art der Verarbeitung, die Kategorien personenbezogener Daten, die Kategorien betroffener Personen, die eingesetzten Systeme oder Anwendungen, Empfänger oder Empfängerkategorien, Verarbeitungsorte sowie Speicher- und Löschrufen.

4. Weisungen des Verantwortlichen

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern keine gesetzliche Verpflichtung zur Verarbeitung besteht.
- (2) Weisungen erfolgen grundsätzlich in Textform, insbesondere per E-Mail, über ein Ticket-System oder über einen sonstigen dokumentierten Kommunikationsweg.
- (3) Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
- (4) Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, hat er den Verantwortlichen unverzüglich darauf hinzuweisen.
- (5) Der Auftragsverarbeiter darf die Daten nicht für eigene Zwecke verwenden. Eine Nutzung zur eigenen Produktverbesserung, Profilbildung, statistischen Auswertung oder sonstigen Eigenzwecken ist nur zulässig, wenn hierfür eine eigenständige datenschutzrechtliche Grundlage besteht und keine Verarbeitung mehr im Auftrag vorliegt.

5. Pflichten des Verantwortlichen

- (1) Der Verantwortliche bleibt für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten verantwortlich.
- (2) Er benennt die zuständigen Stellen oder Personen für fachliche Weisungen, datenschutzrechtliche Rückfragen und Sicherheitsmeldungen.
- (3) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler, Unregelmäßigkeiten oder datenschutzrechtliche Risiken im Zusammenhang mit der Auftragsverarbeitung feststellt.

6. Vertraulichkeit und berechtigter Zugriff

- (1) Der Auftragsverarbeiter stellt sicher, dass alle Personen, die unter seiner Verantwortung personenbezogene Daten verarbeiten, auf Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (2) Der Zugriff auf personenbezogene Daten ist auf diejenigen Personen zu beschränken, die ihn zur Erfüllung ihrer Aufgaben benötigen.
- (3) Der Auftragsverarbeiter hat ein Rollen- und Berechtigungskonzept vorzuhalten. Berechtigungen sind regelmäßig zu überprüfen und bei Wegfall des Bedarfs unverzüglich zu entziehen.
- (4) Privilegierte Zugriffe, insbesondere Administrations-, Wartungs- und Supportzugriffe, sind besonders abzusichern und, soweit möglich, individuell zuzuordnen und zu protokollieren.

7. Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die Maßnahmen sind in Anlage 2 konkret zu beschreiben.

(3) Die Maßnahmen müssen insbesondere folgende Bereiche abdecken: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabe- und Übermittlungskontrolle, Eingabe- und Änderungskontrolle, Verfügbarkeitskontrolle, Trennungsgebot, Protokollierung und Nachvollziehbarkeit, Datensicherung und Wiederherstellung, Schwachstellen- und Patchmanagement, Notfallmanagement sowie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

(4) Der Auftragsverarbeiter darf seine Maßnahmen weiterentwickeln, soweit das vereinbarte Schutzniveau nicht unterschritten wird.

8. Protokollierung

(1) Soweit im konkreten Verarbeitungszusammenhang erforderlich oder gesetzlich vorgegeben, hat der Auftragsverarbeiter eine angemessene Protokollierung sicherzustellen.

(2) Protokolliert werden sollen insbesondere sicherheits- und datenschutzrelevante Vorgänge, insbesondere Zugriffe, Änderungen, administrative Tätigkeiten, Übermittlungen und Löschvorgänge, soweit dies technisch möglich und sachlich erforderlich ist.

(3) Die Einzelheiten der Protokollierung, insbesondere Umfang, Schutz, Berechtigung zur Einsichtnahme, Aufbewahrung und Löschung, sind in Anlage 2 festzulegen.

(4) Protokolle dürfen nur für legitime Zwecke verwendet werden, insbesondere zur Sicherheit, Nachvollziehbarkeit, Eigenkontrolle, Fehleranalyse und zur Erfüllung rechtlicher Pflichten.

9. Unterstützung bei Betroffenenrechten und Datenschutzpflichten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Betroffenenrechten, soweit dies im Rahmen der beauftragten Leistung möglich und erforderlich ist.

(2) Dies betrifft insbesondere die Unterstützung bei Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, soweit einschlägig, Widersprüchen sowie datenschutzrechtlichen Beschwerden.

(3) Gehen entsprechende Anfragen unmittelbar beim Auftragsverarbeiter ein, leitet er diese unverzüglich an den Verantwortlichen weiter.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen außerdem bei Datenschutz-Folgenabschätzungen und erforderlichen Abstimmungen mit der Aufsichtsbehörde, soweit seine Informationen hierfür benötigt werden.

10. Meldung von Datenschutzvorfällen

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über jede Verletzung des Schutzes personenbezogener Daten, die im Zusammenhang mit der vertragsgegenständlichen Leistung steht.

(2) Die Meldung hat ohne schuldhaftes Zögern, spätestens innerhalb von [24 Stunden] nach Kenntniserlangung zu erfolgen.

(3) Die Meldung muss mindestens enthalten:

- Beschreibung des Vorfalls,
- betroffene Systeme oder Leistungen,
- betroffene Datenkategorien,
- soweit bekannt Umfang und betroffene Personengruppen,
- mögliche Auswirkungen,
- bereits getroffene oder geplante Gegenmaßnahmen,
- zuständige Ansprechstelle beim Auftragsverarbeiter.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der weiteren Aufklärung sowie bei etwaigen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

11. Einsatz von Subunternehmen

(1) Der Einsatz von Subunternehmen, die personenbezogene Daten im Auftrag verarbeiten, bedarf der vorherigen Genehmigung des Verantwortlichen.

(2) Die bei Vertragsschluss eingesetzten Subunternehmen sind in Anlage 3 aufzuführen.

(3) Die beabsichtigte Hinzunahme oder der Austausch eines Subunternehmens ist dem Verantwortlichen rechtzeitig vorab mitzuteilen.

(4) Der Auftragsverarbeiter hat sicherzustellen, dass jedes eingesetzte Subunternehmen vertraglich mindestens denselben Datenschutzpflichten unterliegt, die in diesem Vertrag festgelegt sind.

(5) Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Einhaltung der Pflichten durch seine Subunternehmen verantwortlich.

(6) Reine Nebenleistungen ohne Datenzugriff, etwa Post-, Transport-, Reinigungs- oder Bewachungsleistungen, gelten regelmäßig nicht als Subunternehmen im Sinne dieser Klausel.

12. Drittlandverarbeitung

(1) Eine Verarbeitung personenbezogener Daten in Drittländern oder ein Zugriff aus Drittländern ist nur zulässig, wenn die datenschutzrechtlichen Voraussetzungen hierfür erfüllt sind.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen vorab über jeden Drittlandbezug und weist die hierfür eingesetzten Garantien nach.

(3) Drittlandbezüge sind in Anlage 3 oder einer gesonderten Anlage vollständig darzustellen.

13. Nachweise und Auditrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrages notwendig sind.

(2) Der Verantwortliche ist berechtigt, nach angemessener Vorankündigung Auskünfte zu verlangen, Unterlagen einzusehen und Prüfungen durchzuführen oder durch unabhängige, zur Vertraulichkeit verpflichtete Dritte durchführen zu lassen.

(3) Prüfungen können als Vor-Ort-Prüfung, Dokumentenprüfung, Remote-Audit oder durch Vorlage geeigneter Nachweise erfolgen.

(4) Der Auftragsverarbeiter unterstützt solche Prüfungen in angemessenem Umfang.

(5) Geeignete Nachweise können insbesondere aktuelle Testate, Zertifizierungen, Prüfberichte oder Selbstauskünfte sein.

14. Löschung, Rückgabe und Sperrung

(1) Nach Beendigung der vertraglichen Leistungen oder auf Weisung des Verantwortlichen hat der Auftragsverarbeiter sämtliche personenbezogenen Daten nach Wahl des Verantwortlichen zurückzugeben oder datenschutzgerecht zu löschen, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

(2) Bestehen gesetzliche Aufbewahrungs- oder Nachweispflichten, sind die betreffenden Daten zu sperren und nur noch zu dem rechtlich zulässigen Zweck vorzuhalten.

(3) Die Löschung oder Rückgabe ist dem Verantwortlichen auf Verlangen nachzuweisen.

(4) Test-, Sicherungs- und sonstige Kopien sind von dieser Regelung erfasst, soweit keine zwingenden technischen oder rechtlichen Gründe entgegenstehen.

15. Kommunikation und Ansprechpartner

(1) Die Parteien benennen die für diesen Vertrag zuständigen fachlichen, technischen und datenschutzrechtlichen Ansprechpartner. Diese werden in Anlage 4 aufgeführt.

(2) Für Weisungen, Sicherheitsmeldungen, Datenschutzvorfälle, Auditankündigungen und Rückfragen sind verbindliche Kommunikationswege festzulegen.

(3) Änderungen von Ansprechpartnern oder Erreichbarkeiten sind unverzüglich mitzuteilen.

16. Laufzeit und Kündigung

(1) Dieser Vertrag tritt mit Unterzeichnung in Kraft und gilt für die Dauer des Hauptvertrages.

(2) Pflichten zur Vertraulichkeit, Löschung, Rückgabe, Nachweisführung und Unterstützung bei Vorfällen gelten über das Vertragsende hinaus fort, soweit dies erforderlich ist.

(3) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Ein wichtiger Grund liegt insbesondere vor, wenn der Auftragsverarbeiter schwerwiegend oder wiederholt gegen datenschutzrechtliche Pflichten, gegen Weisungen oder gegen vereinbarte Sicherheitsanforderungen verstößt.

17. Rangfolge und Schlussbestimmungen

(1) Im Falle von Widersprüchen gehen die datenschutzrechtlichen Regelungen dieses Vertrages den datenschutzbezogenen Bestimmungen des Hauptvertrages vor.

(2) Die Anlagen 1 bis 4 sind Bestandteil dieses Vertrages.

(3) Änderungen und Ergänzungen dieses Vertrages bedürfen mindestens der Textform.

(4) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

18. Unterschriften

Ort, Datum: _____

Für den Verantwortlichen

Stadtverwaltung Worms

vertreten durch den Oberbürgermeister

Name: _____

Funktion: _____

Unterschrift: _____

Für den Auftragsverarbeiter

Name: _____

Funktion: _____

Unterschrift: _____

Anlage 1 – Leistungs- und Datenbeschreibung

Für jede Leistung oder jedes System sind mindestens aufzunehmen:

- Bezeichnung der Leistung
- Zweck der Verarbeitung
- Art der Verarbeitung
- Kategorien personenbezogener Daten
- Kategorien betroffener Personen
- Systeme / Anwendungen
- Empfänger / Empfängerkategorien
- Verarbeitungsorte
- Speicher- und Löschfristen
- Besondere Schutzbedarfe

Anlage 2 – Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter beschreibt mindestens:

- Organisation und Zuständigkeiten
- Berechtigungskonzept
- Authentisierung
- Verschlüsselung
- Protokollierung
- Datensicherung / Wiederherstellung
- Schwachstellen- und Patchmanagement
- Notfallmanagement
- Trennung von Daten / Mandanten
- Löschkonzept
- Datenschutz durch Technikgestaltung

Anlage 3 – Eingesetzte Subunternehmen

Je Subunternehmen sind mindestens anzugeben:

- Name
- Anschrift
- Leistungsbereich
- Datenbezug
- Verarbeitungsort
- Drittlandbezug ja/nein
- eingesetzte Garantien bei Drittlandbezug
- Genehmigungsstatus
- Bemerkungen

Anlage 4 – Kommunikationswege und Fristen

Mindestens festzulegen sind:

- Weisungen: Kommunikationsweg und zuständige Stelle
- Datenschutzvorfälle: Frist und Notfallkontakt
- Betroffenenanfragen: Weiterleitungsweg
- Auditkommunikation: Ansprechpartner
- Änderungen bei Subunternehmen: Vorlauffrist
- technische Sicherheitsmeldungen: Eskalationsweg