

***Vertrag zur Auftragsverarbeitung
gemäß Art. 28 EU-DSGVO***

Vereinbarung

zwischen dem/der

Kreis Lippe,

- Verantwortlicher - nachstehend Kreis genannt –

und der

Stadt Bielefeld

- Auftragsverarbeiter - nachstehend Auftragsverarbeiter genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der öffentlich-rechtlichen Vereinbarung vom 16.01.2019 auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Kreis sind konkret beschrieben in der Leistungsvereinbarung vom 16.01.2019.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Kreises und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Kunden, Interessenten, Beschäftigte, Lieferanten, Handelsvertreter und Ansprechpartner

(4) Weitere Leistungen

Die Bereitstellung der in § 3 Abs. 2 der Leistungsvereinbarung genannten Statistiken wird geschuldet.

3. Weisungen des Kreises

(1) Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kreises verarbeiten. Der Kreis entscheidet allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten. Eine Verarbeitung für andere Zwecke, insbesondere für eigene Zwecke des Auftragsverarbeiters, ist nicht zulässig. Weisungen werden nur vom Kreis und von keinem Dritten erteilt, auch wenn die Datenverarbeitung im Interesse oder Auftrag dieses Dritten erfolgt und/oder dieser seinerseits Auftraggeber der Kreis ist.

(2) Dies gilt nicht, wenn der Auftragsverarbeiter nach dem Recht der EU oder des Mitgliedsstaats der EU, dessen Recht für ihn gilt, zu einer Datenverarbeitung verpflichtet ist. Liegt ein solcher Fall einer von Weisungen unabhängigen und/oder ihnen widersprechenden Verarbeitung personenbezogener Daten vor, wird der Auftragsverarbeiter dem Kreis diese rechtlichen Anforderungen vor der Verarbeitung mitteilen, es sei denn, eine solche Mitteilung ist ebenfalls verboten.

(3) Mündliche Weisungen bestätigt der Kreis unverzüglich dokumentierbar (mind. Textform). Der Auftragsverarbeiter dokumentiert die Weisungen.

(4) Der Auftragsverarbeiter hat den Kreis unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Kreis bestätigt oder geändert wird.

Weisungsberechtigte Personen des Kreises sind:

- (Team-)Leitung des Bürgerservice
- Leitung des Fachbereichs 1 Service und Wirtschaftsförderung
- Verwaltungsvorstand II/allgemeiner Vertreter

Weisungsempfänger beim Auftragsverarbeiter sind:

- Geschäftsbereichsleitung des BürgerServiceCenters
- Stellv. Geschäftsbereichsleitung des BürgerServiceCenters
- Abteilungsleitung des BürgerServiceCenters

Technisch-organisatorische Maßnahmen

(1) Ein Sicherheitskonzept nach Art. 32 DSGVO ist in Vorbereitung. Bei der Stadt Bielefeld bestehen bereits IT-Richtlinien und Dienstanweisungen, die grundlegende Vorgaben für die Benutzung von IT-Systemen und Applikationen enthalten und die sich als Vorgaben an die Mitarbeiter/-innen richten. Der für die IT-Infrastruktur zuständige Auftragsverarbeiter, die Stadtwerke Bielefeld GmbH, hat ein Sicherheitskonzept für den Netz-Betrieb, welches in Teilen auch Infrastrukturelemente beinhaltet, die von der Stadt Bielefeld mitgenutzt werden (z. B. Zugangskontrollen zum Maschinenraum, Kontrolle des Zugangs zum Betriebsgelände).

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Darüber hinaus beobachtet der Auftragnehmer die technische Entwicklung und schlägt ggf. notwendige Anpassungen der technisch-organisatorischen Maßnahmen vor.

4. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Der Auftragsverarbeiter wird schriftlich einen Datenschutzbeauftragten bestellen, der seine Tätigkeit gemäß Art. 38 und 39 EU-DSGVO ausübt. Die jeweils aktuellen Kontaktdaten des Datenschutzbeauftragten sind auf der Homepage des Auftragsverarbeiters leicht zugänglich hinterlegt.
- b) Der Auftragsverarbeiter verpflichtet sich, die ihm im Rahmen des Auftragsverhältnisses zur Verfügung gestellten oder erarbeiteten Unterlagen und Daten sowie ihm sonst bekannt gewordene Informationen vertraulich zu behandeln und nur im Rahmen der Tätigkeit für dieses Vertragsverhältnis zu nutzen. Diese Verpflichtung gilt auch nach Ende des Vertragsverhältnisses. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer belehrt die bei der Durchführung der Arbeiten eingesetzten Personen insbesondere darüber, dass sie Daten nur auf Weisung des Kreises verarbeiten dürfen, wenn sie gesetzlich nicht zu einer anderen Verarbeitung verpflichtet sind. Er überwacht durch regelmäßige Kontrollen, dass sie diese Verpflichtung einhalten. Er unterrichtet sie regelmäßig über ihre datenschutzrechtlichen Verpflichtungen.
- c) Der Auftragsverarbeiter setzt alle für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO um und hält sie ein. Beispielhafte Maßnahmen werden in Anlage 1 aufgeführt.
- d) Der Kreis und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Der Auftragsverarbeiter informiert den Kreis unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
- f) Soweit der Kreis seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
- g) Der Auftragsverarbeiter weist die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Kreis im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages nach.
- h) Der Auftragsverarbeiter unterstützt den Kreis durch geeignete technische und organisatorische Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der Betroffenen.

5. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern

sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kreises auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet; sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem Unterauftragnehmer aufzuerlegen.

6. Kontrollrechte des Kreises

(1) Der Kreis hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch von ihm beauftragte Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung, der Vorschriften der DSGVO und weiterer evtl. einschlägiger datenschutzrechtlicher Vorschriften durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Der Auftragsverarbeiter unterstützt den Kreis bei diesen Prüfungen. Ggf. sorgt er auch dafür, dass der Kreis oder von ihm beauftragte Prüfer Prüfungen auch bei Unterauftragnehmer durchführen können und auch diese den Kreis bzw. dessen Prüfer unterstützen.

(2) Der Auftragsverarbeiter stellt sicher, dass sich der Kreis von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 EU-DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Kreis auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO.

7. Mitwirkung des Auftragsverarbeiters bei der Erfüllung der Pflichten nach Art. 33 ff. DSGVO

(1) Der Auftragsverarbeiter unterstützt den Kreis bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Kreis zu melden
- b) die Verpflichtung, den Kreis im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

- c) die Unterstützung des Kreises für dessen Datenschutz-Folgenabschätzung
 - d) die Unterstützung des Kreises im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde
- (2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

8. Löschung und Rückgabe von personenbezogenen Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Kreises nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Kreis – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kreis auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Kreis übergeben.
- (4) Gerichtsstand ist, soweit nicht in einer Leistungsvereinbarung Abweichendes geregelt ist, Bielefeld.

9. Außerordentliche Kündigung

Unabhängig von den Regelungen über die oben getroffenen Laufzeiten bzw. die Dauer der Vereinbarung steht dem Kreis ein Recht auf fristlose Kündigung bei schwerwiegenden Vertragsverletzungen des Auftragsverarbeiters zu. Dies kommt insbesondere in Betracht bei Verstoß gegen datenschutzrechtliche Vorschriften, Datenschutz- und Datensicherheitsvereinbarungen, wenn der Auftragsverarbeiter eine Weisung des Kreises nicht ausführen kann oder will oder der Auftragsverarbeiter eine Kontrolle des Kreises oder der nordrhein-westfälischen Datenschutzbeauftragten vertragswidrig verweigert.

10. Haftung

- (1) Der Auftragsverarbeiter haftet dem Kreis für Schäden, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder seine Subunternehmer bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.
- (2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach der EU-DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Kreis gegenüber den Betroffenen verantwortlich. Soweit der Kreis zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragsverarbeiter vorbehalten.

(3) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

11. Sonstiges

(1) Es besteht bei den Vertragsparteien Einigkeit darüber, dass die „Allgemeinen Geschäftsbedingungen“ des Auftragsverarbeiters auf diese Vereinbarung keine Anwendung finden.

Diese Vereinbarung sowie ihre Anlagen enthalten alle vertraglichen Regelungen zwischen den Parteien. Nebenabreden bestehen nicht.

(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich des Anspruchs auf Rückgabe der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

12. Wirksamkeit der Vereinbarung

Diese Vereinbarung bleibt auch bei rechtlicher Unwirksamkeit einzelner Punkte in seinen übrigen Teilen verbindlich. Unwirksame Bestimmungen sind von den Parteien durch wirksame zu ersetzen, die dem gewollten Zweck möglichst nahe kommen. Entsprechendes gilt im Falle einer Vertragslücke.

Detmold, den 07.01.2019

Bielefeld, den 16.01.2019

Lehmann

Clausen

Auftraggeber

Auftragnehmer