

## Vertrag zur Auftragsverarbeitung

### **Auftragsverarbeitungsvertrag in Bezug auf personenbezogene und nicht personenbezogene Daten**

zwischen der

Stadtwerke Verkehrsgesellschaft Frankfurt am Main mbH

- Verantwortlicher - nachstehend nachfolgend AN oder VGF genannt -

und dem/der

.....

- Auftragsverarbeiter:in - nachstehend AN genannt

[ggf.: Vertreter:in gemäß Art. 27 DS-GVO

.....]

## 1. Gegenstand und Dauer des Auftrags

### (1) Gegenstand

- ☒ Der Gegenstand des Auftrags ergibt sich aus dem Vertrag und seinen Anlagen, insbesondere den **Anlagen 2 und 3 des Vertrages**, auf die hier verwiesen wird (im Folgenden **Leistungsvereinbarung**).

oder

- ☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den AN: ..... (Definition der Aufgaben)

### (2) Dauer

- ☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

- ☐ Der Auftrag wird zur einmaligen Ausführung erteilt. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum ..... Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Der AG kann den Auftrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des AN gegen Datenschutzvorschriften oder die Bestimmungen dieses Auftrags vorliegt, der AN eine Weisung des AGs nicht ausführen kann oder will oder der AN Kontrollrechte des AG vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Auftrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

## 2. Konkretisierung des Auftragsinhalts

(1) Der AN verarbeitet personenbezogene und für Zwecke der Informationssicherheit auch nicht personenbezogene Daten ausschließlich im Rahmen dieser getroffenen Vereinbarungen und nach Weisungen des AG, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der AN unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der AN dem AG diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

(2) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Art und Zweck der Verarbeitung personenbezogener und nicht personenbezogener Daten durch den AN für den AG sind konkret beschrieben in der Leistungsvereinbarung

oder

☐ Nähere Beschreibung des Auftragsgegenstands im Hinblick auf Art und Zweck der Aufgaben des AN: .....

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 AG und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Nachfolgendes ist nur auszufüllen, sofern die Verarbeitung nicht in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgt.

Das angemessene Schutzniveau in .....

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: ..... (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

Details zur Feststellung/Herstellung des Schutzniveaus sind/werden in den technisch organisatorischen Maßnahmen der VGF (**Anlage 1 zu diesem Auftrag**) dargestellt.

### (3) Art der Daten

- ☒ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben in: Anlage 2 Nr. 13 Satz 1;

zusätzlich sind folgende Datenarten/-kategorien betroffen

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

### (4) Kategorien betroffener Personen

- ☒ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben in Anlage 2 Nr. 13 Satz 1;

zusätzlich sind folgende Kategorien betroffener Personen betroffen

- ☒ Kund:innen
- ☒ Interessent:innen
- ☒ Dritte
- ☒ Beschäftigte
- ☒ Ansprechpartner:innen

(5) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen AG und AN abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

### 3. Technisch-organisatorische Maßnahmen

(1) Der AN hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen, auf die im Wesentlichen auch Subunternehmer zu verpflichten sind, vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem AG zur Prüfung zu übergeben. Bei Akzeptanz durch den AG werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des AG einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der AN hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in **Anlage 1 zu diesem Auftrag**].

(3) Die Maßnahmen zur Datensicherheit müssen qualitativ mindestens denen zur Veranschaulichung beigelegten der AG entsprechen und weisen eine ISO-27001-Zertifizierung auf.

(4) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und die **Anlage 1 zu diesem Auftrag** ist entsprechend zu aktualisieren.

### 4. Betroffenenrechte

(1) Der AN darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des AG berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person im Sinne der DS-GVO sich diesbezüglich unmittelbar an den AN wendet, wird der AN dieses Ersuchen unverzüglich an den AG weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des AG unmittelbar durch den AN sicherzustellen.

### 5. Qualitätssicherung und sonstige Pflichten des AN

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

- a) ☐ Schriftliche Bestellung eines/einer Datenschutzbeauftragte/n, der/die seine/ihre Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- ☐ Dessen/Deren Kontaktdaten werden dem AG zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem AG unverzüglich mitgeteilt.
  - ☐ Als Datenschutzbeauftragte/r ist beim AN Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem AG unverzüglich mitzuteilen.
  - ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des ANs leicht zugänglich hinterlegt.
- b) ☐ Der AN ist nicht zur Bestellung eines/einer Datenschutzbeauftragten verpflichtet. Als Ansprechpartner/in beim AN wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.
- c) ☐ Da der AN seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].
- d) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der AN 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 AN und jede dem AN unterstellte Person, die Zugang zu personenbezogenen und nicht personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des AGs verarbeiten einschließlich der in diesem Auftrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. In einem solchen Fall teilt der AN dem AG diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
- e) Der AN wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den AG bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten unterstützen.
- f) Der AN verpflichtet sich zur Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in **Anlage 1 zu diesem Auftrag**].
- g) Der AG und der AN arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- h) Der AN informiert den AG 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 AN ermittelt.

- i) Soweit der AG 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 AN ausgesetzt ist, hat ihn der AN nach besten Kräften zu unterstützen.
- j) Der AN kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- k) Der AN verpflichtet sich, auf Anforderung die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem AG im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Auftrags nachzuweisen.

## 6. 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 AN 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 AN ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Daten- und Informationssicherheit der Daten des AG auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Vertrag mit dem Subunternehmenden muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

(3) Der AN darf Subunternehmende (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher, schriftlicher oder dokumentierter elektronischer Zustimmung des AG beauftragen.

- a) ☐ Der AG stimmt der Beauftragung der nachfolgenden Subunternehmenden zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Subunternehmender	Anschrift/Land	Leistung

- b) ☐ Eine nachträgliche Unterbeauftragung ist unzulässig.
- c) ☒ Die Auslagerung auf Unterauftragnehmende oder
- ☒ der Wechsel bestehender Unterbeauftragungen

sind zulässig, soweit:

- der AN eine solche Auslagerung auf Unterauftragnehmenden dem AG unter Beachtung der unten genannten Frist vorher schriftlich oder in Textform anzeigt und
- der AG nicht bis zum Zeitpunkt der Unterbeauftragung gegenüber dem AN schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.
- Die Auslagerung der Daten darf erst nach Ablauf der Einspruchsfrist erfolgen.
- Kumulativ gilt: Die Inanspruchnahme oder Änderung von Subunternehmenden setzt voraus, dass dies zur Anpassung an Entwicklungen erforderlich ist, die bei Vertragsschluss nicht vorhersehbar waren und die der AN nicht veranlasst hat oder beeinflussen kann und deren Nichtberücksichtigung die Ausgewogenheit des Vertrages in bedeutendem Maß stören würde und hierdurch wesentliche Regelungen des Vertrages nicht geändert werden. Die Inanspruchnahme oder Änderung von Subunternehmenden erfordert, dass dies aus triftigem Grund erforderlich ist und die Änderung für den AG zumutbar ist. Ein triftiger Grund liegt vor, wenn die Änderung zur Anpassung an technische Entwicklungen (z.B. Änderung von technischen Plattformen und Systemen) oder aufgrund gesetzlicher oder behördlicher Vorgaben erforderlich ist und dies bei Vertragsschluss nicht vorhersehbar war. Kein triftiger Grund liegt regelmäßig vor, wenn eine Datenverarbeitung infolge der avisierten Änderung in Drittländer außerhalb der EU/des EWR verlagert würde oder durch Subunternehmende erfolgen würde, die selbst oder deren direkte oder indirekte Gesellschafterin in solchen Drittländern ihren rechtlichen Sitz unterhalten oder wenn dies in einem der genannten Sinne auf den AN selbst zutrifft. Direkte oder indirekte Gesellschafter in Drittländern in diesem Sinne liegen vor, wenn einzeln oder gemeinsam über 50 Prozent der Anteile oder Stimmrechte, jeweils direkt oder indirekt, von drittländischen Personen gehalten werden. Der AN hat die Zulässigkeit eines geplanten oder beauftragten Subunternehmernden im genannten Sinne auf Anfrage des AG nachzuweisen. Negativbeispiele sind insbesondere Cloud- und CDN-Dienste folgender Unternehmensgruppen: AWS, Microsoft Azure, Akamai, Google Cloud, Alibaba, IBM, Salesforce, Oracle, Tencent, Huawei, Dell, Cloudflare, Digital Ocean; dies gilt ausnahmsweise nicht, soweit einer der genannten Subunternehmer die in dieser Vereinbarung genannten Anforderungen nachweislich erfüllt.
- Änderungen von Subunternehmenden wird der AN dem AG drei Monate vor ihrem geplanten Wirksamwerden in Textform mitteilen. Dem AG steht wahlweise das Recht zu, Erfüllung des bisherigen Vertrags bis zum Ende der ordentlichen Vertragslaufzeit zu verlangen oder den Vertrag ohne Einhaltung einer Kündigungsfrist und ohne Kosten zum Zeitpunkt des Wirksamwerdens der Änderungen in Textform zu kündigen. Der AG kann die außerordentliche Kündigung erklären. Auf den Inhalt und den Zeitpunkt der Vertragsänderung sowie ein bestehendes Kündigungsrecht wird der AN den AN in der Änderungsmitteilung besonders hinweisen. Ein Kündigungs- oder Erfüllungsrecht steht dem AG nicht zu, wenn die Änderungen unmitteilbar durch Unionsrecht oder innerstaatlich geltendes Recht vorgeschrieben sind.

(4) Die Weitergabe von personenbezogenen und nicht personenbezogenen Daten des AG an den Subunternehmenden und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Subunternehmende die vereinbarte Leistung außerhalb der EU/des EWR stellt der AN die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleistende im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(6) Eine weitere Auslagerung durch den Subunternehmenden

- ☐ ist nicht gestattet;
- ☒ bedarf der ausdrücklichen Zustimmung des AG (mind. Textform);
- ☐ bedarf der ausdrücklichen Zustimmung des AN (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmenden aufzuerlegen.

## 7. Cloud- und KI-Verarbeitung

(1) Soweit Datenverarbeitungen, auch im Rahmen von Auslagerungen oder Subunternehmenden, in der Cloud erfolgen, wird keine public cloud genutzt. Eine public cloud im genannten Sinne liegt vor, wenn die Services von beliebigen Personen oder Organisationen mitgenutzt werden und im Wesentlichen nur eine logische Datentrennung vorliegt. Die Verarbeitung findet auf dedizierten physischen Servern (insbesondere bezüglich CPU, Arbeitsspeicher und Festplatte) statt.

(2) Soweit die Vertragserfüllung durch KI im Sinne der KI-Verordnung (EU) 2024/1689 erfolgt, ist diese Verordnung einzuhalten. Die Vertragsparteien unterstützen einander hierbei, etwa im Hinblick auf Art. 50 KI-VO (Transparenz). Die Datenverarbeitung erfolgt in einer dedizierten KI-Instanz, deren ein- und ausgehende Daten nicht mit jenen fremder KI-Instanzen vermischt werden; ein Import fremder Trainingsdaten ist möglich, nicht jedoch ein Export eigener Daten. Unzulässig sind insbesondere Praktiken im Sinne von Art. 5 KI-VO (verbotene Praktiken) und Hochrisiko-KI-Systeme im Sinne der Art. 6, 7 KI-VO (Hochrisiko-KI). Im Fall von KI-Modellen gemäß Art. 51 KI-VO (KI-Modelle mit allgemeinem Verwendungszweck) wird der AN den AG rechtzeitig hierauf hinweisen.

## 8. Kontrollrechte des AG

(1) Der AG hat das Recht, im Benehmen mit dem AN Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfende durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den AN in dessen Geschäftsbetrieb zu überzeugen.

(2) Der AN stellt sicher, dass sich der AG von der Einhaltung der Pflichten des AN nach Art. 28 DS-GVO überzeugen kann. Der AN verpflichtet sich, dem AG auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen und der in diesem Auftrag festgelegten Verpflichtungen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann nach billigem Ermessen des AG auch erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## 9. Mitteilung bei Verstößen des AN

Der AN unterstützt den AG bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den AG zu melden
- c) die Verpflichtung, dem AG im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des AG für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des AG im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

## 10. Weisungsbefugnis des AG

(1) Der AG erteilt alle Aufträge, Teilaufträge und Weisungen, die sich vorbehaltlich etwaiger Regelungen in anderen Bestandteilen des Auftrags jedoch auf Datenverarbeitungen beschränken, in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

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

(3) Weisungsberechtigte Personen des AG sind:

werden im Projektverlauf genannt..... (Vor-/Nachname, Tel., E-Mail)

Weisungsempfänger:innen beim AN sind:

..... (Vor-/Nachname, Tel., E-Mail)

Bei einem Wechsel oder einer längerfristigen Verhinderung des Weisungsberechtigten oder des Weisungsempfängers/der Weisungsempfängerin ist dem jeweiligen Vertragspartner unverzüglich schriftlich der Nachfolger/die Nachfolgerin bzw. der Vertreter/die Vertreterin mitzuteilen. Falls Weisungen die unter 1. und 2. dieses Auftrags getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

## 11. Löschung und Rückgabe von Daten

(1) Kopien oder Duplikate der personenbezogenen und nicht personenbezogenen Daten werden ohne Wissen des AG 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 AG – spätestens mit Beendigung der Leistungsvereinbarung – hat der AN sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhandigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung bzw. Vernichtung ist dem AG mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den AN entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem AG übergeben.

## 12. Geheimhaltung

(1) Die Vertragsparteien sind verpflichtet, die ihnen unter diesem Vertrag von der jeweils anderen Partei zugänglich gemachten Informationen sowie Kenntnisse, die sie bei dieser Zusammenarbeit über Angelegenheiten – etwa technischer, kommerzieller oder organisatorischer Art – von der jeweils anderen Vertragspartei erlangen, vertraulich zu behandeln und während der Dauer sowie nach Beendigung dieser Vereinbarung ohne die vorherige schriftliche Einwilligung der betroffenen Partei nicht für andere Zwecke als die Durchführung dieses Vertrags zu verwerten oder zu nutzen oder Dritten zugänglich zu machen. Eine Nutzung dieser Informationen ist allein auf den Gebrauch zur Durchführung dieses Vertrages beschränkt.

(2) Diese Vertraulichkeitsverpflichtung gilt nicht für Informationen, die

- bei Vertragsabschluss bereits allgemein bekannt waren oder

- nachträglich ohne Verstoß gegen die in diesem Vertrag enthaltenen Verpflichtungen allgemein bekannt wurden oder
- Gegenstand von Ermittlungen durch Behörden oder Gerichte sind und im Zuge dieser Ermittlungen aufgrund einer Verfügung oder eines Beschlusses herauszugeben sind.

(3) Die Vertragspartner legen die von ihnen eingegangenen Verpflichtungen zur Geheimhaltung und zum Datenschutz auch allen Personen oder Gesellschaften auf, die von ihnen im Rahmen der Zusammenarbeit beauftragt werden.

(4) Im Fall des kumulativen Abschlusses einer anderen Geheimhaltungsverpflichtung gilt im Kollisionsfall die andere Geheimhaltungsverpflichtung vorrangig.

### 13. Haftung

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder dieser Datenschutzvereinbarung gelten die gesetzlichen Vorschriften, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

### 14. Sonstiges

(1) Soweit in diesem Auftrag nicht anders vereinbart, bedürfen Änderungen und Ergänzungen dieses AVV einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Der Gerichtsstand für beide Parteien ist Frankfurt am Main.

(3) Sollten einzelne Teile dieses Auftrags unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Frankfurt, \_\_\_\_\_

Stadtwerke Verkehrsgesellschaft  
Frankfurt am Main mbH

Auftragnehmer:in

\_\_\_\_\_

\_\_\_\_\_

Anlagen:

1. Darstellung der technischen und organisatorischen Maßnahmen des AN