

## Auftragsverarbeitungsvertrag

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen

**Berliner Stadtgüter GmbH**, Karl-Liebknecht-Straße 33, 10178 Berlin, vertreten durch die Geschäftsführung [vollständige Namen]

- nachfolgend „**Auftraggeber**“ genannt –

und

[Bieter], Adresse, vertreten durch die Geschäftsführung [vollständige Namen]

- nachfolgend „**Auftragnehmer**“ genannt –

### 1. Vertragsgegenstand

Im Rahmen der Leistungserbringung nach dem Vertrag vom [Datum] (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Auftraggeber-Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrags.

### 2. Gegenstand und Umfang der Beauftragung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie in **Anlage 1** zu diesem Vertrag spezifiziert; die Verarbeitung betrifft ausschließlich die darin bezeichneten Kategorien personenbezogener Daten und Kategorien betroffener Personen. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages. Der Auftragnehmer ist verpflichtet, auf Verlangen des Auftraggebers, Änderungen der Festlegungen in **Anlage 1** dieses Vertrags zuzustimmen, soweit er keinen sachlichen Grund zur Verweigerung dieser Zustimmung hat. Die Änderungen sind in Textform festzulegen.

2.3 Jede von den Festlegungen in **Anlage 1** abweichende oder darüber hinausgehende Verarbeitung von Auftraggeber-Daten ist dem Auftragnehmer untersagt, insbesondere eine Verarbeitung der Auftraggeber-Daten zu eigenen Zwecken. Das gilt auch für eine Anonymisierung der Auftraggeber-Daten und für jegliche Verwendung anonymisierter Auftraggeber-Daten.

2.4 Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Eine Datenverarbeitung außerhalb Deutschlands, auch im Wege der Gewährung des Zugriffs auf Auftraggeber-Daten an Personen außerhalb Deutschlands, bedarf der vorherigen Zustimmung des Auftraggebers in Textform. Datenverarbeitungen in Ländern, die weder Mitgliedstaat der Europäischen Union noch Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, sind ausdrücklich untersagt.

2.5 Sofern der Auftragnehmer Auftraggeber-Daten außerhalb seiner Hauptniederlassung verarbeitet, informiert er den Auftraggeber über alle sonstigen Orte, an denen er Auftraggeber-Daten verarbeitet. Der Auftraggeber ist berechtigt, nach billigem Ermessen der Verarbeitung von Auftraggeber-Daten außerhalb der Hauptniederlassung des Auftragnehmers zu widersprechen.

2.6 Der Auftragnehmer erwirbt an den Auftraggeber-Daten keine Rechte und ist auf Verlangen des Auftraggebers jederzeit auf erstes Anfordern zur Herausgabe der Auftraggeber-Daten in einer für den Auftraggeber lesbaren und weiterverarbeitbaren Form verpflichtet. Zurückbehaltungsrechte in Bezug auf die Auftraggeber-Daten und die dazugehörigen Datenträger sind ausgeschlossen.

### 3. Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer darf die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht durch das Recht der Europäischen Union oder ihrer Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen rechtzeitig vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Der Auftraggeber besitzt insoweit gegenüber dem Auftragnehmer ein umfassendes Weisungsrecht über Art, Umfang, Zweck und Verfahren der Verarbeitung von Auftraggeber-Daten. Die Weisungen des Auftraggebers sollen grundsätzlich in Textform erfolgen. Bei Bedarf kann der Auftraggeber Weisungen auch mündlich oder telefonisch erteilen. Mündlich oder telefonisch erteilte Weisungen bedürfen jedoch einer unverzüglichen Bestätigung durch den in Ziffer 3.3 genannten Weisungsberechtigten des Auftraggebers in Textform. Der Auftragnehmer ist verpflichtet, sämtliche Weisungen des Auftraggebers zu dokumentieren.

3.3 Weisungen sollen im Regelfall von dem Weisungsberechtigten des Auftraggebers oder dessen Stellvertreter erteilt werden. Derzeit fungieren auf Seiten des Auftraggebers folgende Personen als Weisungsberechtigter und als dessen Stellvertreter:

*Weisungsberechtigter:* **[von BSG zu benennen]**

*Stellvertreter:* **[von BSG zu benennen]**

3.4 Der Auftraggeber wird dem Auftragnehmer einen Wechsel in der Person des Weisungsberechtigten oder des Stellvertreters möglichst frühzeitig anzeigen.

3.5 Die Parteien vereinbaren als Empfangsberechtigten für Weisungen auf Seiten des Auftragnehmers folgende Person:

*Empfangsberechtigter:* **[von Bieter zu benennen]**

*Stellvertreter:* **[von Bieter zu benennen]**

In dringenden Fällen darf der Auftraggeber aber auch jedem anderen Beschäftigten des Auftragnehmers entsprechende Weisungen erteilen, sofern weder der Empfangsberechtigte noch sein Stellvertreter für den Auftraggeber erreichbar waren.

3.6 Ein Wechsel in der Person des Empfangsberechtigten oder des Stellvertreters bzw. deren dauerhafte Verhinderung hat der Auftragnehmer dem Auftraggeber möglichst frühzeitig in Textform unter Benennung eines Vertreters mitzuteilen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt für Weisungen des Auftraggebers.

3.7 Der Auftragnehmer ist verpflichtet, die Weisungen des Auftraggebers unverzüglich auszuführen. Der Auftraggeber ist berechtigt, dem Auftragnehmer hierfür im Einzelfall eine jeweils angemessene Frist zu setzen, die der Auftragnehmer einzuhalten hat.

3.8 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Bestimmungen dieses Vertrags und den Weisungen des Auftraggebers verarbeitet. Der Auftragnehmer bestätigt, dass ihm und seinen Mitarbeitern, die mit Auftraggeber-Daten umgehen, die Vorschriften der DSGVO und die sonstigen einschlägigen Datenschutzvorschriften bekannt sind. Ist der Auftragnehmer der begründeten Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber mit mindestens 14-tägiger Frist berechtigt, die Ausführung der Weisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. Bestätigt der Auftraggeber die Weisung, ist der Auftragnehmer verpflichtet, sie zu befolgen.

3.9 Falls eine Weisung die gemäß Ziffer 2.2 und **Anlage 1** dieses Vertrags getroffenen Festlegungen ändert oder aufhebt, ist sie nur zulässig, wenn hierbei eine entsprechende neue Festlegung in Textform nach Ziffer 2.2 erfolgt.

## 4. Rechtsstellung des Auftraggebers

Der Auftraggeber ist Eigentümer der Auftraggeber-Daten und im Verhältnis der Parteien zueinander Inhaber aller etwaigen Rechte an den Auftraggeber-Daten.

## 5. Anforderungen an Personal und Systeme

5.1 Der Auftragnehmer gewährt Personen Zugriff auf Auftraggeber-Daten nur, soweit dies unmittelbar für die Erfüllung einer konkreten Aufgabe durch diese Person notwendig ist

(Need-to-know-Prinzip). Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten in Textform zur Vertraulichkeit zu verpflichten und die Verpflichtung dem Auftraggeber auf erstes Anfordern nachzuweisen.

5.2 Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeber-Daten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

5.3 Der Auftragnehmer gewährleistet, dass er nur solche Systeme für die Verarbeitung von Auftraggeber-Daten einsetzt, die dafür ausgelegt sind, den Datenschutz durch eine der Verarbeitungssituation angemessene technische Systemgestaltung zu unterstützen.

## 6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zu ergreifen und während der Dauer der Verarbeitung von Auftraggeber-Daten aufrecht zu erhalten, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

6.2 Der Auftragnehmer garantiert, vor dem Beginn der Verarbeitung der Auftraggeber-Daten insbesondere die in **Anlage 2** zu diesem Vertrag spezifizierten technischen und organisatorischen Maßnahmen zu ergreifen und sicherzustellen, dass die Verarbeitung von Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.

6.3 Dem Auftragnehmer ist es gestattet, nach vorheriger Zustimmung des Auftraggebers in Textform alternative adäquate technische und organisatorische Maßnahmen umzusetzen, sofern das Sicherheitsniveau der in **Anlage 2** festgelegten technischen und organisatorischen Maßnahmen nicht unterschritten wird.

6.4 Auf Weisung des Auftraggebers wird der Auftragnehmer darüber hinausgehende wirksame technische und organisatorische Maßnahmen umsetzen, wenn sich die in **Anlage 2** des Vertrags bestimmten Maßnahmen als nicht ausreichend erwiesen haben oder wenn der technische Fortschritt dies erfordert. Der Auftragnehmer hat den Auftraggeber unverzüglich in Textform zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß **Anlage 2** nicht (mehr) ausreichend sind oder der technische Fortschritt weitere Maßnahmen erfordert.

6.5 Für die Sicherheit der Auftraggeber-Daten relevante Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind in jedem Fall vom Auftragnehmer im Voraus mit dem Auftraggeber abzustimmen, auch wenn hierdurch keine Abweichung von den Maßnahmen nach **Anlage 2** erfolgt.

6.6 Auf Verlangen weist der Auftragnehmer dem Auftraggeber die Einhaltung der in **Anlage 2** festgelegten technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis nach Verlangen des Auftraggebers durch die Vorlage eines aktuellen Testats oder Berichts einer unabhängigen Instanz (wie z.B. eines Wirtschaftsprüfers, Revisors, dem betrieblichen Datenschutzbeauftragten oder einem externen Datenschutzauditor etc.) oder einer geeigneten Zertifizierung (z.B. nach BSI-Grundschutz) erbracht werden. Die Kontrollrechte des Auftraggebers nach Ziffer 10 bleiben davon unberührt.

6.7 Der Auftragnehmer ist verpflichtet, die Grundsätze der ordnungsmäßigen automatisierten Verarbeitung personenbezogener Daten einzuhalten und insbesondere jeweils aktuelle Dokumentationen aller automatisierten Verfahren zur Verarbeitung von Auftraggeber-Daten vorzuhalten sowie definierte und dokumentierte Test- und Freigabeverfahren für diese automatisierten Verfahren einzuhalten.

6.8 Auf Verlangen stellt der Auftragnehmer dem Auftraggeber ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung nach diesem Vertrag zur Verfügung.

## 7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1 Der Auftragnehmer darf weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten nur nach vorheriger Zustimmung des Auftraggebers in Textform hinzuziehen. Der Zustimmungspflicht unterliegen auch Vertragsverhältnisse, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, sofern dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann.

7.3 Der Auftragnehmer hat den weiteren Auftragsverarbeiter in dem Unterauftragsverarbeitungsvertrag in Textform ebenso zu verpflichten, wie auch der Auftragnehmer aufgrund dieses Vertrags gegenüber dem Auftraggeber verpflichtet ist. Dem Auftraggeber sind im Unterauftragsverarbeitungsvertrag gegenüber dem weiteren Auftragsverarbeiter unmittelbar sämtliche Kontrollrechte gemäß Ziffer 9 dieses Vertrags einzuräumen (echter Vertrag zugunsten Dritter). In dem Unterauftragsverarbeitungsvertrag sind die Verantwortlichkeitssphären des Auftragnehmers und des weiteren Auftragsverarbeiters klar voneinander abzugrenzen. Der Auftragnehmer haftet für ein Verschulden jedes weiteren Auftragsverarbeiters wie für eigenes Verschulden.

7.5 Der Auftraggeber stimmt hiermit der Inanspruchnahme der weiteren Auftragsverarbeiter gemäß **Anlage 3** zu.

7.6 Der Auftragnehmer hat abgeleitete Kontrollpflichten gegenüber den weiteren Auftragsverarbeitern und kann und muss hierfür die in diesem Vertrag beschriebenen und in dem Unterauftragsverarbeitungsvertrag zu spiegelnden Kontrollbefugnisse des Auftraggebers wahrnehmen. Der Auftragnehmer hat die Einhaltung der vertraglichen Verpflichtungen des weiteren Auftragsverarbeiters regelmäßig (d.h. mindestens einmal jährlich) in geeigneter Form zu überprüfen, das Ergebnis der Prüfung zu dokumentieren und den entsprechenden Prüfbericht dem Auftraggeber innerhalb von sechs Wochen nach

Durchführung der Prüfung unaufgefordert zur Verfügung zu stellen. Der Auftraggeber bleibt berechtigt, die Ausübung der Kontrollbefugnisse durch den Auftragnehmer uneingeschränkt zu überwachen und kann jederzeit auch selbst diese Kontrolle gegenüber dem weiteren Auftragsverarbeiter ausüben.

## 8. Rechte der betroffenen Personen

8.1 Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich, spätestens aber innerhalb von 3 Tagen an den Auftraggeber weiterleiten und ohne entsprechende Einzelweisung des Auftraggebers nicht mit der betroffenen Person in Kontakt treten.

8.3 Der Auftragnehmer wird dem Auftraggeber unverzüglich, längstens aber innerhalb von fünf Werktagen Informationen über die gespeicherten Auftraggeber-Daten (auch soweit sie sich auf den Speicherungszweck beziehen), die Empfänger von Auftraggeber-Daten, an die der Auftragnehmer sie auftragsgemäß weitergibt und den Zweck der Speicherung mitteilen, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen.

8.4 Der Auftragnehmer ist verpflichtet, Auftraggeber-Daten auf Weisung des Auftraggebers unverzüglich, spätestens aber innerhalb einer Frist von fünf Werktagen, zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken. Der Auftragnehmer wird dem Auftraggeber die weisungsgemäße Berichtigung oder Löschung der Daten bzw. die Einschränkung von deren Verarbeitung jeweils auf Verlangen in Textform bestätigen.

8.5 Der Auftragnehmer stellt sicher, dass er auf Einzelweisung des Auftraggebers den gesamten zu einer betroffenen Person gespeicherten Datensatz in einem vom Auftraggeber im Einzelfall festzulegenden, strukturierten, gängigen und maschinenlesbaren Format an den Auftraggeber übergeben kann.

## 9. Mitteilungs- und Unterstützungspflichten bei Verletzungen des Schutzes von Auftraggeber-Daten

9.1 Der Auftragnehmer meldet dem Auftraggeber unverzüglich – spätestens aber innerhalb von 24 Stunden – nachdem ihm eine solche bekannt geworden ist, jede potentielle Verletzung des Schutzes von Auftraggeber-Daten, insbesondere Vorkommnisse, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Auftraggeber-Daten führen können („Datensicherheitsvorfall“). Die Meldung enthält mindestens eine Beschreibung:

- der Art der Verletzung des Schutzes der Auftraggeber-Daten mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen



Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- der möglichen Folgen der Verletzung des Schutzes der Auftraggeber-Daten;
- der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

9.2 Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfe- und Informationsmaßnahmen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen (etwa nach Art. 33 oder Art. 34 DSGVO) auf erstes Anfordern im Rahmen des Zumutbaren zu unterstützen. Der Auftragnehmer wird insbesondere unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftraggeber-Daten zu minimieren und zu beseitigen, die Auftraggeber-Daten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.

9.3 Der Auftragnehmer ist verpflichtet, ein Verzeichnis über alle sich während der Vertragslaufzeit bei ihm ereignenden Datensicherheitsvorfälle zu führen, in das Informationen aufzunehmen sind über (1) sämtliche Umstände und Fakten im Zusammenhang mit dem Datensicherheitsvorfall, (2) dessen Auswirkungen und (3) den jeweils ergriffenen Abhilfemaßnahmen. Auf Verlangen des Auftraggebers hat der Auftragnehmer ihm dieses Verzeichnis vorzulegen.

## 10. Sonstige Unterstützungspflichten des Auftragnehmers

10.1 Der Auftragnehmer hat den Auftraggeber unverzüglich darüber zu informieren, wenn das Eigentum des Auftraggebers oder seine sonstigen Rechte an den Auftraggeber-Daten beim Auftragnehmer durch Maßnahmen Dritter, z.B. durch Pfändung, Beschlagnahme, Insolvenz oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet wird. Ferner wird der Auftragnehmer alle jeweils beteiligten Dritten darüber informieren, dass die Auftraggeber-Daten im Eigentum des Auftraggebers stehen.

10.2 Ist der Auftraggeber gegenüber einer staatlichen Stelle oder einem Dritten verpflichtet, Auskünfte über die Auftraggeber-Daten oder deren Verarbeitung zu erteilen, so ist der Auftragnehmer verpflichtet, den Auftraggeber bei der Erteilung solcher Auskünfte auf erstes Anfordern zu unterstützen, insbesondere durch unverzügliches Zurverfügungstellen sämtlicher Informationen und Dokumente über die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten einschließlich den vom Auftragnehmer ergriffenen technisch-organisatorischen Maßnahmen, über den technischen Ablauf und die Orte der Verarbeitung von Auftraggeber-Daten und über die an der Verarbeitung beteiligten Personen.

10.3 Der Auftragnehmer hat dem Auftraggeber auf Verlangen unverzüglich eine jeweils aktuelle Aufstellung der Angaben nach Art. 30 Abs. 2 DSGVO sowie der beim

Auftragnehmer zugriffsberechtigten Personen jeweils in Bezug auf die Auftraggeber-Daten zur Verfügung zu stellen.

10.4 Der Auftragnehmer bestätigt, dass er einen fachkundigen und zuverlässigen Datenschutzbeauftragten nach Art. 37 DSGVO bestellt hat und verpflichtet sich, die Bestellung eines Datenschutzbeauftragten während der Dauer der Verarbeitung von Auftraggeber-Daten aufrechtzuerhalten, auch wenn die gesetzlichen Voraussetzungen für eine Bestellpflicht entfallen sollten. Die Kontaktdaten des Datenschutzbeauftragten sind wie folgt: **[vom Bieter anzugeben]**. Einen Wechsel in der Person des Datenschutzbeauftragten hat der Auftragnehmer dem Auftraggeber unverzüglich in Textform mitzuteilen.

10.5 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren bei etwa von ihm durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

## 11. Datenlöschung und -rückgabe

11.1 Der Auftragnehmer wird nach Wahl des Auftraggebers nach Abschluss der Erbringung der Verarbeitungsleistungen alle Auftraggeber-Daten entweder vollständig und unwiderruflich löschen oder die vorhandenen Kopien löschen und die Auftraggeber-Daten an den Auftraggeber zurückgeben, sofern nicht nach dem Recht der Europäischen Union oder ihrer Mitgliedstaaten, dem der Auftragnehmer unterliegt, eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

11.2 Der Auftragnehmer stellt darüber hinaus sicher, dass er Auftraggeber-Daten auf Einzelweisung des Auftraggebers jederzeit löschen kann; etwa, wenn ihre Kenntnis für die Erfüllung des Zwecks der jeweiligen Verarbeitung nicht mehr erforderlich ist.

11.3 Mindestens 1 Monat vor Beendigung des Hauptvertrages hat der Auftragnehmer beim Auftraggeber unter detaillierter Angabe der betroffenen Auftraggeber-Daten eine Entscheidung darüber abzufragen, ob die Auftraggeber-Daten mit Vertragsbeendigung von ihm gelöscht oder die vorhandenen Kopien gelöscht und die Auftraggeber-Daten zurückgegeben werden sollen. Erteilt der Auftraggeber ihm hierauf keine anderweitige Einzelweisung, wird der Auftragnehmer die vorhandenen Kopien der Auftraggeber-Daten löschen und die Auftraggeber-Daten dem Auftraggeber zurückgeben.

11.4 Die Bestimmungen der Ziffern 11.1–11.3 gelten auch für Vervielfältigungen der Auftraggeber-Daten (insbesondere Archivierungs- und Sicherungsdateien) in allen Systemen des Auftragnehmers sowie für Test- und Ausschussdaten.

11.5 Über jede Löschung und Vernichtung von Auftraggeber-Daten und Kopien von Auftraggeber-Daten hat der Auftragnehmer ein Protokoll in Textform zu erstellen, das dem Auftraggeber auf Verlangen unverzüglich vorzulegen ist.

11.6 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, sind durch den Auftragnehmer für eine Dauer



von zehn Jahren nach Vertragsende aufzubewahren und dem Auftraggeber auch nach Vertragsende auf Verlangen in Kopie herauszugeben.

## 12. Nachweise und Überprüfungen

12.1 Der Auftragnehmer hat sicherzustellen und regelmäßig (mindestens einmal pro Jahr) zu kontrollieren, dass die Verarbeitung der Auftraggeber-Daten mit diesem Vertrag sowie den Weisungen des Auftraggebers in Einklang steht.

12.2 Der Auftragnehmer wird die Umsetzung der Pflichten nach diesem Vertrag in geeigneter Weise dokumentieren und dem Auftraggeber entsprechende Nachweise auf dessen Verlangen vorlegen. Der Auftragnehmer wird insbesondere dokumentieren:

- alle Eigenkontrollen gemäß Ziffer 12.1;
- alle Vertraulichkeitsverpflichtungen von Personen, die Auftraggeber-Daten verarbeiten;
- alle Verträge über die Inanspruchnahme weiterer Auftragsverarbeiter und alle Prüfungen weiterer Auftragsverarbeiter im Sinne von Ziffer 7;
- alle auf Weisung des Auftraggebers erfolgten Löschungen von Auftraggeber-Daten.

12.3 Der Auftraggeber ist berechtigt, den Auftragnehmer regelmäßig während der Verarbeitung von Auftraggeber-Daten bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen gemäß **Anhang 2**, zu überprüfen, einschließlich durch Vor-Ort-Kontrollen.

12.4 Zur Durchführung von Kontrollen nach Ziffer 12.3 ist der Auftraggeber berechtigt, jederzeit sämtliche Geschäftsräume des Auftragnehmers zu betreten und dort Vor-Ort-Kontrollen durchzuführen. Soweit möglich, wird der Auftraggeber dem Auftragnehmer solche Vor-Ort-Kontrollen rechtzeitig vorher ankündigen. Der Auftragnehmer gewährt dem Auftraggeber sämtliche für die Durchführung der Kontrolle benötigten Zugangs-, Auskunfts- und Einsichtsrechte. Der Auftragnehmer verpflichtet sich insbesondere, dem Auftraggeber Zugang zu den Datenverarbeitungseinrichtungen, Dateien und anderen Dokumenten zu gewähren, um die Kontrolle und Überprüfung der relevanten Datenverarbeitungseinrichtungen, Dateien und anderer Dokumentationen zu ermöglichen, die mit der Verarbeitung von Auftraggeber-Daten im Zusammenhang stehen. Der Auftraggeber nimmt hierbei angemessene Rücksicht auf die Betriebsabläufe und berechnigte Geheimhaltungsinteressen des Auftragnehmers.

12.5 Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei, unter anderem durch die Bereitstellung aller notwendigen Informationen einschließlich aller Zertifikate, Auditberichte und sonstigen Ergebnisse von Überprüfungen im Hinblick auf die Verarbeitung von Auftraggeber-Daten.

12.6 Der Auftraggeber ist berechtigt, von dem Datenschutzbeauftragten des Auftragnehmers Auskunft über sämtliche Aspekte der Verarbeitung von Auftraggeber-Daten, einschließlich der getroffenen technisch-organisatorischen Maßnahmen, zu erhalten und von ihm regelmäßig eine Bestätigung der Einhaltung der technischen und organisatorischen Maßnahmen gemäß **Anlage 2** zu verlangen. Der Auftragnehmer wird unter Beachtung von dessen Weisungsfreiheit dafür sorgen, dass der Datenschutzbeauftragte auf Verlangen des Auftraggebers Auskünfte und Bestätigungen zeitnah erteilt.

12.7 Der Auftraggeber ist berechtigt, die Kontrollhandlungen nach dieser Ziffer 12 selbst oder durch einen zur Geheimhaltung verpflichteten Bevollmächtigten vorzunehmen. Der Auftragnehmer ist verpflichtet, die Kontrollhandlungen eines solchen Bevollmächtigten in derselben Weise zu dulden und zu unterstützen wie Kontrollen durch den Auftraggeber.

12.8 Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen des Auftraggebers wird der Auftragnehmer den Auftraggeber im Rahmen von behördlichen Aufsichtsverfahren nach Kräften unterstützen, wenn und soweit die vertragsgegenständliche Verarbeitung von Auftraggeber-Daten Gegenstand des Aufsichtsverfahrens ist. Der Auftragnehmer wird insbesondere auf Verlangen des Auftraggebers ihm selbst oder der Aufsichtsbehörde unmittelbar alle Informationen im Zusammenhang mit diesem Vertrag geben und entsprechende Auskünfte erteilen und der Aufsichtsbehörde die Möglichkeit einräumen, Prüfungen in demselben Umfang durchzuführen, wie sie die Aufsichtsbehörde beim Auftraggeber durchführen darf. Der Auftragnehmer verpflichtet sich, der zuständigen Aufsichtsbehörde auch in diesem Rahmen alle erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte zu gewähren. Falls die Aufsichtsbehörde beim Auftragnehmer Kontrollhandlungen, Ermittlungen oder Maßnahmen durchführt, die Auftraggeber-Daten betreffen, hat der Auftragnehmer den Auftraggeber darüber so früh wie möglich und in der Regel unverzüglich nach Erhalt der Ankündigung der Aufsichtsmaßnahme durch die Behörde zu informieren.

### **13. Vertragsdauer und Kündigung**

13.1 Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Die Regelungen zur ordentlichen Kündigung des Hauptvertrags gelten entsprechend.

13.2 Der Auftraggeber ist zu einer jederzeitigen außerordentlichen Kündigung dieses Vertrags sowie des Hauptvertrags aus wichtigem Grund berechtigt. Ein wichtiger Grund liegt für den Auftraggeber insbesondere vor, wenn – der Auftragnehmer gegen eine wesentliche Pflicht aus diesem Vertrag verstößt, – der Auftragnehmer die Auftraggeber-Daten für andere als nach Ziffer 2.2 zugelassene Zwecke verwendet, – der Auftragnehmer eine Weisung des Auftraggebers nach Ziffer 3 dieses Vertrags nicht ausführt, – der Auftragnehmer einer Meldepflicht nach Ziffer 9.1 nicht nachkommt, – der Auftragnehmer die Ausübung der Kontrollrechte des Auftraggebers nach Ziffer 9 dieses Vertrags verweigert oder nicht nur unerheblich behindert oder – der Auftragnehmer einen weiteren

Auftragsverarbeiter entgegen Ziffer 7.1 ohne vorherige Zustimmung des Auftraggebers in Textform einschaltet.

13.3 Der Hauptvertrag darf im Falle einer Beendigung dieses Vertrags nur fortgeführt werden, wenn ausgeschlossen ist, dass der Auftragnehmer Auftraggeber-Daten verarbeitet. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als eine Kündigung dieses Vertrags und gilt eine Kündigung dieses Vertrags auch als Kündigung des Hauptvertrags.

#### **14. Haftung und Vertragsstrafe**

14.1 Für Schäden des Auftraggebers durch schuldhafte Verstöße des Auftragnehmers gegen diesen Vertrag sowie gegen die ihn unmittelbar treffenden gesetzlichen Datenschutzverpflichtungen haftet der Auftragnehmer entsprechend den gesetzlichen Haftungsregelungen. Etwaige anderweitig zwischen den Parteien vereinbarte Haftungsbegrenzungen (z.B. aus dem Hauptvertrag) finden diesbezüglich keine Anwendung. Soweit Dritte Ansprüche gegen den Auftraggeber geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftragnehmers gegen diesen Vertrag oder gegen eine ihn unmittelbar treffende gesetzliche Datenschutzverpflichtung haben, stellt der Auftragnehmer den Auftraggeber von diesen Ansprüchen auf erstes Anfordern frei.

14.2 Der Auftragnehmer verpflichtet sich, den Auftraggeber auch von allen etwaigen Geldbußen, die gegen den Auftraggeber verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftragnehmer Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

14.3 Der Auftragnehmer trägt die Beweislast dafür, dass etwaige Schäden und Geldbußen nicht auf einem von ihm zu vertretenden Umstand beruhen, soweit die jeweilige Ursache in der Verarbeitung von Auftraggeber-Daten in der Zuständigkeitssphäre des Auftragnehmers liegt.

#### **15. Schlussbestimmungen**

15.1 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.

15.2 Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

15.3 Jede Änderung dieses Vertrages bedarf einer ausdrücklichen Vereinbarung zwischen den Parteien.

informativ

**Anlagen:**

- **Anlage AVV 1:** Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen
- **Anlage AVV 2:** Technische und organisatorische Maßnahmen
- **Anlage AVV 3:** Weitere Auftragsverarbeiter

informativ

**Anlage AVV 1: Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen**

**Zweck der Datenverarbeitung**

**Art und Umfang der Datenverarbeitung**

**Art der Daten**

**Kategorien betroffener Personen**

**Dauer der Verarbeitung**

Die Dauer entspricht der Laufzeit des Hauptvertrags vom [Datum].



## **Anlage AVV 2: Technische und organisatorische Maßnahmen**

Der Auftragnehmer verpflichtet sich, die folgenden technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO umzusetzen und während der gesamten Vertragslaufzeit aufrechtzuerhalten. Die Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen auszugestalten.

### **1. Zutrittskontrolle**

Maßnahmen zur Verhinderung des unbefugten Zutritts zu Datenverarbeitungsanlagen. **[Vom Auftragnehmer zu konkretisieren, z.B. Zutrittskontrollsysteme, Besucherregelungen, Alarmanlagen.]**

### **2. Zugangskontrolle**

Maßnahmen zur Verhinderung der unbefugten Nutzung von Datenverarbeitungssystemen. **[Vom Auftragnehmer zu konkretisieren, z.B. Passwortpolicies, Zwei-Faktor-Authentifizierung, VPN-Zugang, automatische Sperrung.]**

### **3. Zugriffskontrolle**

Maßnahmen zur Gewährleistung, dass nur befugte Personen auf Auftraggeber-Daten zugreifen können. **[Vom Auftragnehmer zu konkretisieren, z.B. Berechtigungskonzepte, Need-to-know-Prinzip, Rollenmodelle gemäß Projektanforderung: Admin, Hausverwalter, Nur-Lese-Zugriff.]**

### **4. Weitergabekontrolle**

Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens bei der Übertragung von Auftraggeber-Daten. **[Vom Auftragnehmer zu konkretisieren, z.B. Verschlüsselung der EBICS-Kommunikation, TLS-Verschlüsselung für alle Datenübertragungen.]**

### **5. Eingabekontrolle**

Maßnahmen zur Gewährleistung der Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen. **[Vom Auftragnehmer zu konkretisieren, z.B. vollständiges Audit-Log mit Zeitstempel und Benutzeridentität gem. AC-09 des Proposals.]**

### **6. Auftragskontrolle**

Maßnahmen zur Gewährleistung, dass Auftraggeber-Daten nur entsprechend den Weisungen verarbeitet werden. **[Vom Auftragnehmer zu konkretisieren, z.B. Weisungsdokumentation in Textform, Weisungsempfänger gem. Ziffer 3 dieses Vertrags.]**

## **7. Verfügbarkeitskontrolle**

Maßnahmen zum Schutz vor zufälliger Zerstörung oder Verlust. **[Vom Auftragnehmer zu konkretisieren, z.B. Backup-Konzepte, Monitoring-Dashboard, Wiederherstellungsverfahren.]**

## **8. Trennungskontrolle**

Maßnahmen zur getrennten Verarbeitung von Daten verschiedener Auftraggeber oder Zwecke. **[Vom Auftragnehmer zu konkretisieren, z.B. logische Mandantentrennung, separate Test- und Produktionsumgebungen.]**

**[Hinweis: Die konkreten TOMs sind vom Auftragnehmer vor Beginn der Datenverarbeitung in Textform zu dokumentieren und dem Auftraggeber vorzulegen.]**

**Anlage AVV 3: Weitere Auftragsverarbeiter**

**[Hinweis: Die konkreten Unterauftragsverarbeiter sind vom Auftragnehmer vor Beginn der Datenverarbeitung in Textform zu dokumentieren und dem Auftraggeber vorzulegen.]**

Firma, Anschrift	Art der Verarbeitung	Zweck	Art der Daten	Kategorien der betroffenen Personen