

Vereinbarung zur Auftragsverarbeitung

zum Vertrag / zur Leistungsbeschreibung

Vergabenummer 2026-III-01-OV	Maßnahmenummer ZVS-Soz-2026
Maßnahme Durchführung der Regie- und Beförderungsleistungen im besonderen Fahrdienst für Menschen mit Behinderung	
Leistung/CPV 60130000-8 Personensonderbeförderung (Straße)	

- nachfolgend „Leistungsvereinbarung“ –

zwischen dem

Land Berlin, vertreten durch die Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung, Oranienstr. 106, 10969 Berlin,

- nachfolgend „Verantwortlicher“ -

und

[Firma Vertragspartner, Anschrift Vertragspartner]

- nachfolgend „Auftragsverarbeiter“ -

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel

§ 1 Anwendungsbereich

§ 2 Konkretisierung des Auftragsinhalts

§ 3 Verantwortlichkeit und Weisungsbefugnis

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

§ 5 Technische und organisatorische Maßnahmen und deren Kontrolle

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

§ 7 Löschung und Rückgabe von Daten

§ 8 Subunternehmen

§ 9 Datenschutzkontrolle

§ 10 Schlussbestimmungen

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. In Erfüllung der sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO), und des Berliner Datenschutzgesetzes (BlnDSG), schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Verarbeitung aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen oder dem Auftragsverarbeiter bekannt werden. Nicht unter den Anwendungsbereich fallen Daten von Beschäftigten des Auftragsverarbeiters, soweit sie ausschließlich das Beschäftigungsverhältnis mit dem Auftragsverarbeiter betreffen.

§ 2 Konkretisierung des Auftragsinhalts

Der Inhalt der Auftragsverarbeitung ist in **Anlage 1** zu dieser Vereinbarung beschrieben. Dies betrifft Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen.

§ 3 Verantwortlichkeit und Weisungsbefugnis

- (1) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.
- (2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.
- (3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.
- (4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen 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 DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen.

Mündliche Anordnungen sind durch den Verantwortlichen unverzüglich schriftlich oder in Textform zu bestätigen. Die Anordnungen sind durch den Verantwortlichen sowie den Auftragsverarbeiter zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

- (5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird. Die weisungsberechtigten Personen auf Seiten des Verantwortlichen sowie die zum Empfang der Weisungen berechtigten Personen auf Seiten des Auftragsverarbeiters sowie die vorgesehenen Informationswege sind in **Anlage 1** festgelegt.
- (6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher oder textförmlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.
- (7) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in sein Verzeichnis von Verarbeitungstätigkeiten zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.
- (8) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet der Europäischen Union bzw. des Europäischen Wirtschaftsraums statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen ausdrücklichen schriftlichen oder textförmlichen Zustimmung des Verantwortlichen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.
- (9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

- (1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.
- (2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24

Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

- (3) Der Auftragsverarbeiter hat eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, die oder der ihre oder seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten der oder des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen. **[Kann entfallen, wenn keine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht.]**
- (4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technische und organisatorische Maßnahmen und deren Kontrolle

- (1) Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Dazu trifft er wenigstens die in Anlage 2 „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen.
- (2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in der Anlage 2 „Technische und organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftragsverarbeiter mitzuteilen.
- (3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.
- (4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

- (5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.
- (6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, spätestens 24 Stunden nach Bekanntwerden beim Auftragsverarbeiter, über Verletzungen des Schutzes von im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten sowie bei einem entsprechenden Verdacht, bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verstößen gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

- (1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen, es sei denn es ist ausdrücklich anders in der Leistungsvereinbarung vereinbart.
- (2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Ein Lösungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.
- (3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

- (1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher schriftlicher oder textförmlicher Zustimmung des Verantwortlichen in Anspruch nehmen. Die zur Erfüllung dieses Vertrages

hinzugezogenen Subunternehmen sind in der **Anlage 1** im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden.

- (2) Sofern es sich um eine allgemeine schriftliche Genehmigung handelt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
- (3) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.
- (4) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortliche berechtigt, auf schriftliche oder textförmliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.
- (5) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der oder dem Datenschutzbeauftragten des Verantwortlichen sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht (hier: die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit) und der Kontrolle durch die oder den Datenschutzbeauftragten des Verantwortlichen mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu

beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Schlussbestimmungen

- (1) Die Anlagen 1 und 2 sind Teil dieser Vereinbarung.
- (2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen oder textförmlichen Vereinbarung 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.
- (3) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.
- (4) Bei Widersprüchen zwischen der Leistungsvereinbarung und dieser Vereinbarung, gehen die Regelungen dieser Vereinbarung vor.

Datum, Ort

Unterschrift (Verantwortlicher)

Name, Vorname, Funktion

Datum, Ort

Unterschrift (Auftragsverarbeiter)

Name, Vorname, Funktion

Anlage 1 – Gegenstand der Auftragsverarbeitung

Beschreibung der Auftragsverarbeitung (Gegenstand, Umfang, Art und Zweck):

- ☒ Die Beschreibung der Auftragsverarbeitung ergibt sich aus der Leistungsvereinbarung.
- ☐ Die Auftragsverarbeitung ist wie folgt zu beschreiben: Klicken oder tippen Sie hier, um Text einzugeben.

Dauer der Auftragsverarbeitung

- ☒ Die Dauer der Auftragsverarbeitung ergibt sich aus der Leistungsvereinbarung.
- ☐ Die Auftragsverarbeitung dauert bis zur Beendigung der Leistungsvereinbarung.
- ☐ Die Auftragsverarbeitung dauert bis zum Klicken oder tippen Sie, um ein Datum einzugeben..

Kategorie von Daten, die Gegenstand der Auftragsverarbeitung sind (z.B. Name, Geburtsdatum, Informationen zum Einkommen, Versicherungsstatus etc.):

Aggregierte Daten zu den Themen Personal, Gremien, Vergaben und Zuwendungen.

Kreis der durch die Auftragsverarbeitung betroffenen Personen (z.B. Antragsteller/innen, Kläger/innen, Beschwerdeführer/innen, Petenten etc.):

Klicken oder tippen Sie hier, um Text einzugeben.

Weisungsberechtigte Personen des Verantwortlichen sind (einschließlich Kontaktinformationen):

Klicken oder tippen Sie hier, um Text einzugeben.

Weisungsempfangende Personen des Auftragsverarbeiters sind (einschließlich Kontaktinformationen):

Klicken oder tippen Sie hier, um Text einzugeben.

Subunternehmer bei Vertragsschluss (einschließlich Adresse und Kontaktinformationen):

Klicken oder tippen Sie hier, um Text einzugeben.

Anlage 2 „Technische und organisatorische Maßnahmen“

zur Vereinbarung zur Auftragsverarbeitung vom [Datum]

zwischen dem Land Berlin, vertreten durch die Senatsverwaltung für Arbeit, Soziales, Gleichstellung, Integration, Vielfalt und Antidiskriminierung

und [Firma Vertragspartner]

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technischen und organisatorischen Maßnahmen auf diese Anlage.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 § 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

- (1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung
1.	Zutrittskontrolle Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	[Ergänzen] z.B. Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Schlüsselvergabe, Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Türsicherung
2.	Zugangskontrolle Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	[Ergänzen] z.B. Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: Kennwortverfahren, Automatisches Sperren, Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern)

3.	Zugriffskontrolle Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	<i>[Ergänzen] z.B. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung)</i>
4.	Weitergabekontrolle Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	<i>[Ergänzung] z.B. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren, elektronische Signatur</i>
5.	Eingabekontrolle Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	<i>[Ergänzen] z.B. Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung gewährleisten, etwa durch Protokollierungs- und Auswertungssysteme</i>
6.	Auftragskontrolle Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können.	<i>[Ergänzen] Abgrenzen der Kompetenz zwischen Verantwortlichem und Auftragsverarbeiter (Beispiel: eindeutige Vertragsgestaltung, Kriterien zur Auswahl des Auftragsverarbeiters, Kontrolle der Vertragsausführung)</i>
7.	Verfügbarkeitskontrolle Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	<i>[Ergänzen] z.B. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen, Maßnahmen zur Datensicherung (Beispiel: Backup-Verfahren, Spiegeln von Festplatten,</i>

		<i>unterbrechungsfreie Stromversorgung, Firewall, Notfallplan)</i>
8.	Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	<i>[Ergänzen] z.B. Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten, Mandantenfähigkeit, Funktionstrennung zwischen Produktion/Test</i>

- (2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.