# Auftragsverarbeitungsvertrag gem. Artt. 28, 29 DS-GVO

(entspricht auch den Bedingungen gem. § 80 SGB X, § 29 KDG, § 29 KDR-OG und §30 DSG-EKD)

zwischen der

opta data motion GmbH
Wilhelmshöher Allee 273
34131 Kassel
Telefon: +49 201 695049 00
Telefax: +49 201 695049 35
motion@optadata-gruppe.de

(Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend „Auftragnehmer" genannt)

und

Firmenname

Name | Vorname

Straße, Hausnummer

PLZ | Ort

E-Mail-Adresse

Kundennummer

Verbandsmitglied bei | Institutionskennzeichen/gültig ab

Umsatzsteuerpflichtig: ◯ ja ◯ nein | wenn ja, Steuernummer/Umsatzsteuer-ID (bei Privatabrechnung Pflichtangabe)

(Im Folgenden **Auftraggeber** genannt)

## Präambel

Diese Vereinbarung regelt die Maßnahmen zum Schutz von personenbezogenen Daten gem. Art. 4 Nr. 1 DS-GVO, Gesundheitsdaten gem. Art. 4 Nr. 15 DS-GVO und Sozialdaten im Sinne des § 67 Abs. 2 SGB X bei der Datenverarbeitung im Auftrag unter Berücksichtigung der Art. 28, 29 DS-GVO und der § 80 SGB X sowie § 29 KDG, § 29 KDR-OG und §30 DSG-EKD.

## § 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages bis zur vollständigen Erfüllung und Abwicklung der vereinbarten Leistungen. Die Geheimhaltungspflicht gilt darüber hinaus unbegrenzt.

Der Auftraggeber kann den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a) ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen des Vertrages vorliegt oder
b) der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder
c) der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert oder
d) die Grundlage der Vertragserfüllung wesentlich verändert wird oder ganz entfällt aufgrund einer Änderung der Rechts- oder Gesetzeslage oder wegen aufsichtsrechtlicher Maßnahmen.

Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

## § 2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

- Der Umfang der Tätigkeiten des Auftragnehmers richtet sich nach den Anforderungen des Auftraggebers. Die gesetzliche Grundlage für die Abwicklung des Genehmigungs-verfahrens ist dieser Vertrag gem. Art. 28 DS-GVO.
- Der Auftragnehmer übernimmt für den Auftraggeber folgende Tätigkeiten:
  - ◯ Die Konkretisierung des Auftragsinhalts ergibt sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag
  - ◯ Der Auftragsinhalt ist nicht abschließend. Je nach Wahl von Zusatzdienstleistungen durch den Auftraggeber bei dem Auftragnehmer, kann der Auftragsinhalt über die unter § 2 geregelten Inhalte hinausgehen. In diesem Fall ergibt sich die Konkretisierung aus der Leistungsvereinbarung.

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 oder der Schweiz statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn ein Angemessenheitsbeschluss nach Art. 45 DS-GVO vorliegt bzw. der Auftragnehmer durch vertragliche Maßnahmen wie. z. B. EU-Standardvertragsklauseln sicherstellen kann, dass die Bedingungen dieser Vereinbarung auch in einem Drittland gelten bzw. die Verarbeitung der Daten des Auftraggebers mit einem der Verarbeitung angemessenen Sicherheitsniveau stattfindet. In Anlage 3 sind die Standorte, bei denen Daten des Auftraggebers verarbeitet werden, eingetragen. Eine Veränderung der Standorte oder Räumlichkeiten, in denen Daten des Auftraggebers verarbeitet werden, oder ein Verlagern der Auftragsdurchführung an eine andere Ört-

lichkeit als die mit dem Auftraggeber vereinbarte, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

(2)

Art der Daten

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

- Die Datenarten bzw. Datenkategorien ergeben sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag.

(3)

Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffener Personen umfassen:

- Die Kategorien betroffener Personen ergeben sich aus Anlage 1 zu diesem Auftragsverarbeitungsvertrag

## § 3 Technisch-organisatorische Maßnahmen

(1)

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung schriftlich oder in Textform zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser umzusetzen.

(2)

Der Auftragnehmer 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. Die technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 2 zu diesem Auftragsverarbeitungsvertrag.

(3)

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen zu dokumentieren.

(4)

Sämtliche Dokumentationen zu den technischen und organisatorischen Maßnahmen, Dokumentationen von Regelungen zum Datenschutz und zur Informationssicherheit und Audit- bzw. Prüfberichte müssen in deutscher Sprache verfasst bzw. in deutscher Übersetzung bereitgehalten werden.

## § 4 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer 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) Die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in Anlage 4 mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

b) Die Wahrung der Vertraulichkeit und des Daten- sowie Sozialgeheimnisses gemäß Artt. 28 Abs. 3 Satz 2 lit. b, 29, 32 Abs. 4 DS-GVO, § 35 SGB I. Der Auftragnehmer setzt bei der Durch-führung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und zur Geheimhaltung unter Hinweis auf die rechtlichen Folgen einer Pflichtverletzung, insbesondere nach § 203 Abs. 4 StGB, nachweisbar verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Dies umfasst die Verpflichtung zur Geheimhaltung auch über das bestehende Dienst- oder Beschäftigungsverhältnis hinaus. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c, 32 DS-GVO (Einzelheiten in Anlage 2).

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers 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 bzw. Sozialdaten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber 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 Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer 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. Die Kontrollen, die Ergebnisse und ggf. umgesetzte Maßnahmen sind zu protokollieren und für mindestens 6 Jahre aufzubewahren.

h) Die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 6 dieses Vertrages.

i) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln. Diese Verpflichtung besteht über das Ende des Vertragsverhältnisses hinaus.

j) Personenbezogene Daten Auftraggebers dürfen nicht im öffentlichen Raum (z.B. Flughafen, Bahn etc.) verarbeitet werden. Die Verarbeitung der personenbezogenen Daten des Auftraggebers außerhalb der Geschäftsräume des Auftragnehmers ist nur im nichtöffentlichen Raum zulässig und nur mit gesicherten firmeneigenen Geräten des Auftragnehmers. Die Bestimmungen zu den technisch-organisatorischen Maßnahmen nach § 3 sind zu beachten. Die Verwendung von Privat-PC ist nicht zulässig.

k) Die Verarbeitung von personenbezogenen Daten in Privatwohnungen ist grundsätzlich nicht erlaubt, es sei denn der Auftraggeber stimmt dem zu. Dann ist sicherzustellen, dass dies unter Beachtung der technischen und organisatorischen Maßnahmen gemäß § 3 dieser Vereinbarung erfolgt.

l) Die Nutzung von Cloudcomputing durch den Auftragnehmer ist nur zulässig, wenn dieser mit dem jeweiligen Anbieter eine Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO abschließt und die technische und organisatorische Sicherstellung der Infrastruktur des Anbieters den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht und die Anforderungen des § 80 SGB X, insbesondere Abs. 2, bezüglich der räumlichen Beschränkungen der Verarbeitung eingehalten werden.

m) Der Auftragnehmer verpflichtet sich, dass die Daten des Auftraggebers von Daten anderer Auftraggeber streng getrennt werden. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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.

n) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (z.B. durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren) oder durch sonstige

Ereignisse gefährdet werden, hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer ist verpflichtet, alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber zu unterrichten, dass es sich um Daten des Auftraggebers handelt, über die er keinerlei Verfügungs- oder sonstige Bestimmungsgewalt oder Eigentumsrechte gem. § 273 BGB hat.

## § 5 Unterauftragsverhältnisse

(1)

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, und bei denen ein Zugriff auf personenbezogene Daten bzw. Sozialdaten nicht ausgeschlossen werden kann. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikations-dienstleister, dem Postgeheimnis unterliegende Post-/Transportdienstleistungen, Gebäude-reinigung sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Daten-schutzes und der Sicherheit der Daten des Auftraggebers auch bei ausgelagerten Neben-leistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2)

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragnehmer) nur nach vorheriger ausdrücklicher schriftlicher Zustimmung (ggf. auch Textform) des Auftraggebers beauftragen und soweit der Auftragnehmer mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO, die zudem die in diesem Vertrag vereinbarte Rechte und Pflichten berücksichtigt, geschlossen hat.

Der Auftraggeber stimmt der Beauftragung der in Anlage 1 aufgeführten Unterauftragnehmer zu, soweit jeweils eine vertragliche Vereinbarung nach Maßgabe von Satz 1 geschlossen wurde.

(3)

Sollen vom Auftragnehmer während der Vertragslaufzeit andere als in Anlage 1 benannte Unterauftragnehmer beauftragt oder Standorte von Unterauftragnehmern verlegt/erweitert werden, sind dem Auftraggeber rechtzeitig vor der geplanten Veränderung folgende Unterlagen zur Zustimmung vorzulegen:

a) Beschreibung der Arbeiten, die der Unterauftragnehmer ausführen soll,

b) Kopie der geplanten vertraglichen datenschutzrelevanten Regelungen (einschließlich der technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit) mit dem Unterauftragnehmer.

(4)

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller gesetzlichen und vertraglich vereinbarten Voraussetzungen insbesondere der vorliegenden schriftlichen (mindestens Textform) Zustimmung des Auftraggebers für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung im Sinne von Abs. 1 Satz 2, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(6) Eine weitere Auslagerung durch einen Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des (Haupt-)Auftraggebers mindestens in Textform bzw. werden diese dem Auftragnehmer vor Einbeziehung mitgeteilt und ihm ein 14-tägiges Vetorecht eingeräumt. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(7)

Die vertraglichen Vereinbarungen zwischen Auftragnehmer und Unterauftragnehmer sind so zu gestalten, dass sie den Bestimmungen des Vertragsverhältnisses zwischen Auftraggeber und Auftragnehmer entsprechen. Die vertraglichen Vereinbarungen sind durch den Auftragnehmer nachzuweisen und rechtzeitig vor Abschluss des Vertrages vorzulegen.

(8) Der Auftragnehmer hat den Unterauftragnehmer bezüglich der Einhaltung der vertraglichen Pflichten regelmäßig zu prüfen. Das Ergebnis ist zu dokumentieren, mindestens 6 Jahre aufzubewahren und auf Verlangen dem Auftraggeber vorzulegen.

(9)

Das Verhalten eines Unterauftragsnehmers ist dem Auftragnehmer wie eigenes Verhalten zuzurechnen.

(10)

Wird beim Auftragnehmer die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen und kann dabei der Zugriff auf personenbezogene Daten oder deren Kenntnisnahme durch diese Stellen nicht ausgeschlossen werden, sind dem Auftraggeber rechtzeitig vor der Auftragserteilung die Verträge über Wartungsarbeiten einschließlich der damit Beauftragten mitzuteilen. Sind Störungen im Betriebsablauf zu erwarten oder bereits eingetreten, ist der Vorgang dem Auftraggeber unverzüglich mitzuteilen.

(11)

Beauftragt der Auftragnehmer für den Datentransport einen Transportunternehmer, so hat er vertraglich sicherzustellen und dem Auftraggeber auf Verlangen nachzuweisen, dass der Transportunternehmer den Datenschutzbestimmungen Genüge tut. Werden Unterlagen des Auftraggebers abgeholt, stattet der Auftragnehmer den Transportunternehmer mit einem schriftlichen Berechtigungsausweis für die Entgegennahme der Unterlagen aus.

## § 6 Kontrollrechte des Auftraggebers und dessen Aufsichtsbehörden

(1)

Der Auftraggeber, dessen zuständige Aufsichtsbehörden bzw. ein von ihm beauftragter Dienstleister (im folgenden Auftraggeber) haben das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Sie haben das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2)

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3)

Das Prüfrecht umfasst insbesondere die Besichtigung von Grundstücken und Geschäfts-räumen, Auskünfte zur Vertragsausführung, Einsicht in Papierunterlagen und auch die Einsichtnahme in die beim Auftragnehmer gespeicherten personenbezogene Daten des Auftraggebers, soweit dies im Rahmen des Auftrags zur Überwachung von Datenschutz und Datensicherheit erforderlich ist. Dies gilt insbesondere für den Nachweis der Umsetzung der technischen und organisatorischen Maßnahmen.

(4)

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

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO oder

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder BSI-Standards).

(5)

Der Auftragnehmer sichert zu, dass er die notwendige personelle und sachliche Unterstützung bei den Prüfungen zur Verfügung stellt.

(6)

Aufwände und Kosten, die beim Auftragnehmer im Zuge der Prüfung durch den Auftraggeber entstehen, trägt allein der Auftragnehmer, wenn die Prüfungen in einem üblichen Umfang und nicht öfter als einmal jährlich stattfinden. Gehen Prüfungen umfänglich oder zeitlich über das übliche Maß hinaus, kann der Auftragnehmer die ihm entstehenden tatsächlichen Kosten dem Auftraggeber berechnen.

## § 7 Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO und § 83a bis 84 SGB X genannten Pflichten zur Sicherheit personen-bezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherige Konsultationen der Aufsichtsbehörde. 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 Auftraggeber zu melden. In diesem Falle hat der Auftragnehmer sofort alle erforderlichen Maßnahmen zur Sicherung der Sozialdaten zu treffen und weitere Anweisungen durch den Auftraggeber abzuwarten.

c) die Verpflichtung, dem Auftraggeber 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 Auftraggebers für dessen Datenschutz-Folgenabschätzung,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

## § 8 Weisungsbefugnis des Auftraggebers

(1)

Der Auftraggeber hat das Recht, erforderlichenfalls schriftliche Weisungen im Rahmen der Art. 28, 32 DS-GVO zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit zu erteilen.

(2)

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. in Textform).

(3)

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

## § 9 Berichtigung, Einschränkung, Löschung und Rückgabe von personenbezogenen Daten

(1)

Der Auftragnehmer darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2)

Soweit vom Leistungsumfang umfasst, ist das Löschkonzept, das Recht auf Vergessenwerden, die Berichtigung von personenbezogenen Daten, die Datenportabilität (soweit einschlägig) und Auskünfte nach schriftlicher oder nachvollziehbarer Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen und revisionssicher zu dokumentieren.

(3)

Sämtliche Daten und Unterlagen sowie Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit den im Hauptvertrag genannten Leistungen dieser Datenschutzbestimmungen in die Verfügungsgewalt des Auftragnehmers gelangt sind, hat dieser entsprechend der jeweiligen Vereinbarungen im Einzelfall bzw. nach Abschluss der vertraglichen Arbeiten dem Auftraggeber auszuhändigen bzw. zu übermitteln.

(4)

Auf Verlangen des Auftraggebers hat der Auftragnehmer in seinem Besitz befindliche Daten bzw. Datenbestände (z.B. physische Datenträger, elektronische Dateien oder Datenbanken in seinen Datenverarbeitungssystemen) nichtreproduzierbar zu löschen bzw. physisch zu vernichten. Die Vernichtung hat in Abhängigkeit von den verarbeiteten Sozialdaten nach DIN 66399 Teile 1 bis 3 bzw. ISO/IEC 21964 mindestens mit der Schutzklasse 3 mindestens mit Sicherheitsstufe 4 in der jeweils einschlägigen Materialklasse zu erfolgen. Die Datenlöschung hat nach anerkanntem BSI-Standard (Bundesamt für Sicherheit in der Informationstechnik) oder anderweitiger adäquater Regelungen für vertrauliche Daten in der jeweils aktuellen Fassung zu erfolgen. Dies gilt auch für Test- und Zwischenergebnisse.

Ist eine Löschung auf Sicherungskopien wegen der besonderen Art der Speicherung nur mit einem unverhältnismäßig hohen Aufwand möglich, sind die Daten nach Abstimmung mit dem Auftraggeber für jede weitere Verarbeitung einzuschränken.

(5)

Die Löschung und Vernichtung hat der Auftragnehmer in geeigneter Weise zu protokollieren. Im Zweifelsfall sind geeignete Maßnahmen mit dem Auftraggeber abzustimmen. Hinsichtlich sämtlicher Löschvorgänge hat der Auftragnehmer dem Auftraggeber Löschprotokolle auf Verlangen zu übergeben.

(6)

Endet das Vertragsverhältnis, hat der Auftragnehmer gegenüber dem Auftraggeber schriftlich zu erklären, dass die nicht mehr erforderlichen Daten und Datenträger ordnungsgemäß im Sinne dieses Vertrages gelöscht bzw. vernichtet wurden und welche Daten aus gesetzlichen Gründen über das Ende des Auftragsverhältnisses hinaus aufbewahrt werden müssen.

## § 10 Ansprechpartner

Ansprechpartner des Auftraggebers ergeben sich aus Anlage 4.

## § 11 Haftung

(1)

Der Auftragnehmer haftet gegenüber dem Auftraggeber im Rahmen der gesetzlichen Bestimmungen für Schäden, die infolge schuldhaften Verhaltens gegen Datenschutzbestimmungen und gegen diese Datenschutzvereinbarung entstehen. Ebenso haftet er für schuldhaftes Verhalten seiner Unterauftragnehmer sowie deren Unterauftragnehmer.

(2) A

uftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

## § 12 Sonstiges

(1)

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vereinbarungsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der wirtschaftlichen Zielsetzung am nächsten kommen, die die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

(2)

Sollten sich datenschutzrechtliche Änderungen während der Vertragslaufzeit ergeben, die zu einer Vertragsanpassung führen müssen, verpflichten sich die Vertragspartner Vertragsverhandlungen mit dem Ziel der Einigung aufzunehmen.

(3)

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

(4)

Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der personenbezogenen Daten/Sozialdaten und der zugehörigen Datenträger ausgeschlossen.

(3)

Sämtliche Kommunikation zwischen dem Auftragnehmer und dem Auftraggeber sowie zwischen dem Auftragnehmer und den Aufsichten/Prüfdiensten haben in deutscher Sprache zu erfolgen.

## § 13 Inkrafttreten

(1)

Diese Datenschutzbestimmungen treten mit Inkrafttreten des Hauptvertrages in Kraft und sind ohne Unterschrift gültig, wenn der Auftragnehmer nicht binnen einer Frist von 14 Tagen Widerspruch einlegt.

(2)

Es gilt die Gerichtsstandvereinbarung des Hauptvertrages.

## Anlagen:

Anlage 1:

Gegenstand und Konkretisierung des Auftragsinhalts, Datenarten7Datenkategorien, Kategorien betroffener Personen, Untervertragsverhältnisse

Anlage 2:

Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3:

Standorte des Auftragnehmers

Anlage 4:

Ansprechpartner