

Vereinbarung über die Verarbeitung von Daten im Auftrag

zwischen

der Deutschen Industrie- und Handelskammer (DIHK)
Haus der Deutschen Wirtschaft
Breite Straße 29
10178 Berlin

- Verantwortlicher, nachfolgend "DIHK" oder „Auftraggeber“-

und

XY

- Auftragsverarbeiter, nachfolgend ("XY") oder „Auftragnehmer“-

Präambel

Der Auftraggeber hat am xx.xx.202x den Auftragnehmer mit einem Variantenvergleich von Betriebsmodellen für Register im Kontext der Registermodernisierung beauftragt (Vergabenummer: 2026-07-11176). Auf die Vertragsinhalte wird Bezug genommen. Diese Vereinbarung legt die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Rahmen der Auftragsverarbeitung fest.

§ 1 Gegenstand und Dauer des Auftrags (Art. 28 Abs. 3)

- (1) Der Umfang der Daten und das Verarbeitungsverfahren ergeben sich aus der Beauftragung.
- (2) Bestimmt der Auftragnehmer die Zwecke und Mittel der Verarbeitung unter Verstoß gegen die DSGVO und diese Vereinbarung, ist er bezüglich der in dieser Vereinbarung geregelten Verarbeitung selbst Verantwortlicher und haftet entsprechend gemäß Art. 82 DSGVO.
- (3) Die Vereinbarung beginnt am xx.xx.202x und endet mit Beendigung des zwischen dem Auftraggeber und dem Auftragnehmer geschlossenen Vertrags. Die Frist für eine ordentliche Kündigung richtet sich nach dem zugrunde liegenden Vertrag. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.
- (4) Der Auftraggeber kann die Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen der DSGVO, des Bundesdatenschutzgesetzes bzw. des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften oder

dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollen des Auftraggebers oder des Landesdatenschutzbeauftragten/Bundesdatenschutzbeauftragten vertragswidrig verweigert.

§ 2 Umfang, Art und Zweck der Datenverarbeitung (Art. 28 Abs. 3)

- (1) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/
Datenkategorien:

(...)

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

(...)

Ergänzend wird auf Anlage 3 verwiesen.

- (2) Der Auftragnehmer verarbeitet die personenbezogenen Daten nach § 1 Abs. 1 ausschließlich im Rahmen des Auftrages gemäß § 1 und nach dokumentierten Weisungen des Auftraggebers. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.
- (3) Der Auftragnehmer führt innerhalb dieses Auftrags alle technischen Maßnahmen für die Sicherstellung des Vertragszwecks sowie die Sicherheit und/oder Verarbeitungen der Daten (z. B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Log-Files etc.) durch, soweit sie nicht zu inhaltlichen Änderungen der Daten führen und sie zur Erfüllung des Auftrags erforderlich sind.
- (4) Die Verarbeitung der Daten auch durch Unterauftragnehmer findet
- ☐ ausschließlich im Gebiet der Bundesrepublik Deutschland,
 - ☐ in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum,
 - ☐ in einem Drittstaat (Nennung des Drittstaats)

statt. In letzterem Fall weist der Auftragnehmer für die Rechtmäßigkeit entsprechende vertragliche oder sonstige, der DSGVO entsprechende Rechtsgrundlagen nach. Das angemessene Schutzniveau in _____

- ☐ ist festgestellt durch einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 Abs. 3 DSGVO);
- ☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b iVm Art. 47 DSGVO);
- ☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e iVm Art. 40 DSGVO);
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus

- (Art. 46 Abs. 2 lit. f iVm. Art. 42 DSGVO).
- ☐ wird hergestellt durch sonstige Maßnahmen: _____
(Art. 46 Abs 2 lit. a, Abs. 3 lit. a und b DSGVO).

Jede nachträgliche Verlagerung in ein Drittland bedarf der vorherigen Zustimmung.

Bei einer Datenübermittlung in die USA versichert der Auftragnehmer, dass die Übermittlung der Daten nicht auf das Privacy Shield gestützt wird. Er versichert zudem, dass er bei Anwendung der Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DSGVO eine Einzelfallanalyse seines Vertragspartners vorgenommen hat und notwendige Zusatzvereinbarungen zur Herstellung eines gleichwertigen Datenschutzniveaus geschlossen hat.

§ 3 Technische und organisatorische Maßnahmen/Sicherheit der Verarbeitung (Art. 28 Abs. 1, Abs. 3 c, Art. 32)

- (1) Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen (Art. 32 DSGVO), die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. 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, zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die technisch-organisatorischen Maßnahmen des Auftragnehmers sind in **Anlage 1** zu dieser Vereinbarung gesondert festgeschrieben und Bestandteil des Vertrages.
- (2) Der Auftragnehmer stellt sicher, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
- (3) Der Auftragnehmer verpflichtet sich, die technischen und organisatorischen Maßnahmen dem Stand der Technik anzupassen, soweit dies erforderlich und wirtschaftlich zumutbar ist (Art. 32 DSGVO). 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 DSGVO zu berücksichtigen.

Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

Der Auftraggeber ist über wesentliche Änderungen vorab zu informieren, Die Änderungen sind schriftlich festzuhalten und werden Vertragsbestandteil. Vorschläge des Auftraggebers hat der Auftragnehmer zu prüfen und den Auftraggeber über das Ergebnis zu informieren.
- (4) Der Auftragnehmer gewährleistet die im Rahmen der ordnungsgemäßen Abwicklung der Arbeiten erforderlichen technischen und organisatorischen Maßnahmen in Zusammenarbeit mit den Unterauftragnehmern. Die technisch-organisatorischen Maßnahmen der von dem Auftragnehmer beauftragten Dritten müssen dem Stand der Technik entsprechen.

§ 4 Berichtigung, Einschränkung der Verarbeitung und Löschung von Daten, Auskunft über Daten (Art. 28 Abs. 3)

Der Auftragnehmer hat nur nach dokumentierter Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken.

§ 5 Pflichten des Auftragnehmers (Art. 28 Abs. 3 h, Art. 32)

- (1) Der Auftragnehmer hat die Beachtung der datenschutzrechtlichen Vorschriften im Hinblick auf das Auftragsverhältnis sicherzustellen. Stellt der Auftragnehmer Unregelmäßigkeiten fest, wird er unverzüglich den Auftraggeber informieren. Der Auftragnehmer sichert zu, die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt zu trennen.
- (2) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung personenbezogener Daten des Auftraggebers die Vertraulichkeit sowie etwaige berufliche Verschwiegenheitsverpflichtungen (insbesondere die von § 203 StGB geschützten) zu wahren und dem Auftraggeber nachzuweisen. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere mit der gebotenen Sorgfalt darauf hinzuwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht unbefugt an Dritte weitergeben oder sonst verwerten.
- (3) Die Pflicht zur Wahrung der Vertraulichkeit besteht auch nach Beendigung der Tätigkeit. Der Auftragnehmer stellt sicher, dass die Geheimhaltungspflicht auch bei Einschaltung weiterer Subunternehmer oder Dritter eingehalten wird.
- (3) Der Auftragnehmer hat **Frau/Herrn ... (Vorname, Name, Organisationseinheit, Telefon, E-Mail)** als betrieblichen Datenschutzbeauftragten bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

Alt.: Der Auftragnehmer ist nicht verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Der Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen ist ... (Vorname, Name, Organisationseinheit, Telefon, E-Mail).

- (4) Der Auftragnehmer verpflichtet sich, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen.
- (5) Der Auftragnehmer verpflichtet sich, dem Landesdatenschutzbeauftragten/ Bundesdatenschutzbeauftragten und den von ihm eingesetzten Bediensteten Zugang

zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des Datenschutzgesetzes in seiner jeweiligen Fassung.

- (6) Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach der DSGVO, dem BDSG und LDSG zu informieren, soweit sie den Gegenstand dieses Vertrags betreffen. Dies gilt auch, soweit eine zuständige Behörde wegen Verstößen bei dem Auftragnehmer ermittelt.
- (7) Wenden sich Personen, die durch die Datenverarbeitung bei dem Auftragnehmer in ihren Rechten betroffen sind, an diesen, so hat der Auftragnehmer diese Personen unverzüglich an den Auftraggeber zu verweisen. Der Auftraggeber ist verantwortlich für die Wahrung dieser Rechte. Der Auftragnehmer hat alles zu tun, damit der Auftraggeber die Rechte der Betroffenen, insbesondere auf Benachrichtigung, Auskunftserteilung, Berichtigung, Einschränkung der Verarbeitung (Sperrung), Löschung von Daten, Einlegung des Widerspruchs und das Recht auf Datenportabilität erfüllen kann, vorausgesetzt, die für die Auskunftserteilung notwendige Mitwirkungshandlung ist dem Auftragnehmer nicht unmöglich.
- (8) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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 personenbezogener Daten unverzüglich an den Auftraggeber zu melden
 - c) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung und
 - d) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

§ 6 Unterauftragsverhältnisse (Art. 28 Abs. 2, Abs. 3 d, Abs. 4)

- (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 Auftragnehmer als Dienstleistungen (z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen) 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 Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Beauftragung der in **Anlage 2** genannten Unterauftragnehmer stimmt der Auftraggeber mit Unterzeichnung dieser Vereinbarung zu.

- (3) Der Abschluss zukünftiger Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Auftraggebers.
- (4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (5) Falls der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR erbringt, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
- (6) Eine weitere Auslagerung durch den Unterauftragnehmer
 - ☒ ist nicht gestattet;
 - ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
 - ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);
 sämtliche vertragliche Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.
- (7) Der Auftragnehmer hat dem Unterauftragnehmer dieselben Pflichten, die er selbst gegenüber dem Auftraggeber zu erfüllen hat, aufzuerlegen, soweit es für die Auftragserfüllung relevant ist. Bei Einschaltung eines Unterauftragnehmers muss garantiert sein, dass der Unterauftragnehmer sorgfältig ausgewählt und die Beachtung der Datenschutzvorschriften durch ihn gewährleistet ist, dieser die geeigneten technischen und organisatorischen Maßnahmen getroffen hat oder bis zur Aufnahme der Tätigkeit treffen wird, die Erfüllung der Pflichten des Auftragnehmers aus diesem Vertrag nicht beeinträchtigt werden und der Landesdatenschutzbeauftragte/Bundesdatenschutzbeauftragte sein Kontrollrecht auch gegenüber dem Unterauftragnehmer ausüben kann.
- (8) Der Auftragnehmer haftet gegenüber dem Auftraggeber vollumfänglich für Datenverstöße seiner Unterauftragnehmer.

§ 7 Kontrollrechte des Auftraggebers (Art. 28 Abs. 3 h)

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Hierbei wird sich der Auftraggeber regelmäßig von der Einhaltung der bei dem Auftragnehmer sowie den Unterauftragnehmern getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dokumentieren. Der Auftraggeber bestellt für diese Auftragskontrolle verantwortliche Personen und benennt diese vorab gegenüber dem Auftragnehmer. Ein Wechsel in der Person ist dem Auftragnehmer unverzüglich mitzuteilen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats oder von Berichten

oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder durch eine Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO sowie andere geeignete Zertifikate erbracht werden.

- (3) Falls der Auftragnehmer und/oder die von ihr beauftragten Unterauftragnehmer sich genehmigter Verhaltensregeln unterworfen haben oder ein genehmigtes Zertifizierungsverfahren erfolgreich durchlaufen haben, sind sie verpflichtet, dem Auftraggeber dies nachzuweisen. Zertifikate sind zu aktualisieren. Der Auftraggeber ist hierüber zu informieren.

§ 8 Mitteilung bei Verstößen (Art. 33 Abs. 2)

- (1) Der Auftragnehmer erstattet unverzüglich in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers, gegen die sich aus diesem Vertrag ergebenden Verschwiegenheitsverpflichtungen oder gegen die im Auftrag getroffenen Festlegungen verstoßen wurde.
- (2) Insbesondere bei eventuell bestehenden Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten gemäß Art. 33 DSGVO sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt insbesondere bei schwerwiegenden Störungen des Betriebsablaufs, bei IT-Sicherheitsvorfällen, bei Verdacht auf Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung bzw. zum Ausschluss möglicher nachteiliger Folgen für die Betroffenen zu ergreifen. Insbesondere soweit den Auftraggeber Pflichten aufgrund bestehender Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

§ 9 Weisungsbefugnis des Auftraggebers (Art. 28 Abs. 3)

- (1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers.
- (2) Der Auftraggeber ist berechtigt, dem Auftragnehmer jederzeit Weisungen zu erteilen, insbesondere hinsichtlich der Art, des Umfangs und des Zeitpunktes der Verarbeitung von Daten.
- (3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen das Datenschutzrecht verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Er ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen des Auftraggebers bestätigt oder geändert wird.

- (4) Die Weisungen des Auftraggebers erfolgen grundsätzlich in Textform.
- (5) Weisungsberechtigt sind für den Auftraggeber Bei dem Auftragnehmer sind für die Annahme von Weisungen ... verantwortlich. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.
- (6) Der Auftraggeber hat seinerseits bei der Feststellung von Fehlern oder Unregelmäßigkeiten, die er insbesondere bei der Prüfung von Ergebnissen feststellt, den Auftragnehmer unverzüglich zu informieren.
- (7) Werden von dem Auftragnehmer Störungen festgestellt, die eine wesentliche Änderung des Verfahrensablaufes erforderlich machen, ist die entsprechende Verfahrensänderung vor ihrer Durchführung mit dem Auftraggeber abzustimmen. Sie darf nicht ohne dessen in Textform erteilte Einwilligung vollzogen werden.
- (8) Erteilt der Auftraggeber Einzelweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z. B. Änderungen an den technischen und organisatorischen Maßnahmen, werden sie als Antrag auf Leistungsänderung behandelt.

§ 10 Löschung von Daten und Rückgabe von Datenträgern (Art. 28 Abs. 3 g)

- (1) Unverzüglich nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber, spätestens aber mit Beendigung der Zusammenarbeit hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen mit personenbezogenen Daten, erstellte Verarbeitungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Ein Zurückbehaltungsrecht ist ausgeschlossen. Ausgenommen hiervon sind Sicherungskopien. In diesem Fall hat der Auftragnehmer für eine die Vertraulichkeit sichernde Aufbewahrung zu sorgen. Die Vertragsparteien legen fest, wann die Sicherungskopien zu vernichten sind.
- (2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der für den betroffenen Dienst geltenden Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Diese kann der Auftragnehmer zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 11 Schlussbestimmungen

- (1) Sollten einzelne Bestimmungen dieser Vereinbarung 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 wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt bzw. diese Lücke ausfüllt.

- (2) Änderungen und Ergänzungen bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformklausel.
- (3) Beide Parteien verpflichten sich, über alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse, insbesondere über die bekannt gewordenen Daten, unter Beachtung des Betriebs- und Geschäftsgeheimnisses Stillschweigen zu bewahren. Diese Verpflichtung gilt auch nach Ende des Vertragsverhältnisses fort.

Ort, Datum

Unterschriften

Anlage 1

Darstellung der technischen und organisatorischen Maßnahmen bei der Auftragsverarbeitung/Sicherheit der Verarbeitung

Unternehmen	
Stand	

1. Organisatorische Maßnahmen

- ☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
- ☐ ja
Name: (...) Kontakt Daten: (...)
- ☐ nein, dann bitte den Ansprechpartner für den Datenschutz angeben (Name, Kontaktdaten)
- ☐ Die Mitarbeiter wurden nachweislich über Datenschutz und Datensicherheit geschult bzw. informiert
- ☐ Alle Mitarbeiter sind nachweislich auf die Vertraulichkeit (Datengeheimnis), ggf. auf das Fernmeldegeheimnis und die Wahrung von Berufsgeheimnissen, verpflichtet
- ☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z. B. technisch unterstützt oder durch Externe)
- ☐ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden
- ☐ Ein Datenschutzkonzept ist vorhanden
- ☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am tt.mm.jjjj und Bestätigung s. Anlage x)
- ☐ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am tt.mm.jjjj und Bestätigung s. Anlage x)

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☐ Sind schriftliche Zutrittsregelungen vorhanden?
 - ☐ ja, im Dokument (z. B. im Datenschutzhandbuch):
 - ☐ nein
- ☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
- ☐ Alarmanlage
- ☐ Automatisches Zutrittskontrollsystem, Ausweisleser
- ☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
- ☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
- ☐ Sicherheitsschlösser
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ biometrische Kontrollsysteme (Fingerabdrücke o. ä.)
- ☐ Manuelles Schließsystem
- ☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
- ☐ Magnetschleusen
- ☐ Werkschutz/Pförtner
- ☐ Empfang mit Anmeldung
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Lichtschranke/Bewegungsmelder
- ☐ Feuerfeste Türen
- ☐ Absicherung von Gebäudeschächten
- ☐ Fenstervergitterung
- ☐ Panzerglas
- ☐ Videoüberwachung der Zugänge

2.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☐ Passwortvergabe
 - ☐ Komplexität des Passworts
 - ☐ Definierte Wechselfristen
 - ☐ Anzahl der Fehleingaben beschränkt
- ☐ Chipkarte mit PIN/Passwort
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Biometrisches Merkmal mit PIN/Passwort
- ☐ Einsatz von VPN-Technologie
- ☐ Automatische Sperrung des Arbeitsplatzes

2.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass

personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☐ Schriftliches Berechtigungskonzepts vorhanden
- ☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- ☐ Verwaltung der Rechte durch System-Administrator
- ☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
- ☐ Gesicherte Nutzung von USB-Schnittstellen
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
 - ☐ Die Protokolle werden ausgewertet, zeitlicher Abstand:
- ☐ physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ ordnungsgemäße Vernichtung von Datenträgern
- ☐ Lösungskonzept für Daten
- ☐ Protokollierung der Vernichtung

2.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Trennung von Daten verschiedener Auftraggeber

2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass der Personenbezug von Daten nicht vollständig, aber immerhin so weit aufgelöst wird, dass ein Rückschluss auf eine bestimmte Person nur unter „Hinzuziehung zusätzlicher Informationen“, insbes. eines Identifizierungsschlüssels, möglich ist.

- ☐ Ja
- ☐ Nein

2.6 Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten durch kryptografische Maßnahmen so verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

- ☐ Ja
- ☐ Nein

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

Maßnahmen, die 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.

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Firewall
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen
- ☐ Protokollierung von Übermittlungen
- ☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐ Sicherung von Datenträgertransporten (verschießbarer Transportbehälter) auch für Papier

3.2 Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden

3.3 Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- ☐ Führung eines Verzeichnisses von Verarbeitungstätigkeiten
- ☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration

3.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☐ Vorhandene Vereinbarungen zur Auftragsdatenverarbeitung
- ☐ Kontrolle der Vertragsausführung
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Regelung zu Wartungen (speziell Fernwartung)

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Virenschutzsystem
- ☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ Konzept für Katastrophenfall vorhanden

4.2 Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)

Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

- ☐ Redundante Systemauslegung
- ☐ Ausfallsicherheits-/Hochverfügbarkeitskonzept
- ☐ Einsatz fehlertoleranter Software
- ☐ Schutz vor Überlast und Denial of Service-Angriffen

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- ☐ Datenschutz-Management
- ☐ Incident-Response-Management
- ☐ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Ort, Datum

Unterschrift Auftragnehmer

Anlage 2

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Beschreibung der Teilleistungen (nicht abschließend)	Name und Anschrift des Subunternehmers
Hosting	
Webseiten-Design	
Cloud-Lösung	
Entsorgung von Akten/Datenträgern	

Anlage 3

Genaue Beschreibung des Verarbeitungsprozesses

1. Datenkategorien

2. Betroffener Personenkreis

3. Wie genau werden die personenbezogenen Daten verarbeitet? Ablauf der Verarbeitungsschritte?