zwischen

**Berufsgenossenschaft**

**Rohstoffe und chemische Industrie (BG RCI)**

Kurfürsten-Anlage 62

D-69115 Heidelberg

- nachfolgend **„Auftraggeberin“** genannt -

und

*(Bitte ausfüllen)*

- nachfolgend **„Auftragnehmer“** genannt -

1. **Präambel**

Diese Vereinbarung konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus dem Vertrag (bitte ausfüllen)       samt Anhängen vom (bitte ausfüllen)       (nachfolgend „Hauptvertrag“ genannt) ergeben. Die Vereinbarung regelt eine Auftragsverarbeitung im Sinne des Artikel 28 der Europäischen Datenschutzgrundverordnung (DS-GVO) beziehungsweise § 80 Sozialgesetzbuch Zehntes Buch (SGB X). Sie findet Anwendung auf alle Tätigkeiten, die nach Weisung der Auftraggeberin mit dem Hauptvertrag im Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte Personen Sozialdaten beziehungsweise personenbezogene Daten der Auftraggeberin (nachfolgend auch „Daten“ genannt) verarbeiten.

Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen Vertrages über die Auftragsverarbeitung, diese nicht durchgeführt werden darf.

Die Vereinbarung gilt entsprechend für (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf Daten nicht ausgeschlossen werden kann.

1. **Gegenstand, Dauer und Spezifizierung der Vereinbarung**
2. **Der Gegenstand des Auftrages** ist im Hauptvertrag konkretisiert.
3. *Der Auftragnehmer erbringt folgende* ***Prüf- bzw. Wartungstätigkeiten****:*

*(Bei (Fern-) Prüfung und Wartung automatisierter Verfahren bitte ausfüllen)*

1. Die **Dauer des Auftrages** richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht etwas anderes ergibt.
2. Aus dem Hauptvertrag ergeben sich **Umfang und** **Art der Datenverarbeitung.**

Es werden von dem Auftragnehmer Daten

erhoben/  gespeichert  verwendet  ausgelesen/  
 erfasst abgefragt

verändert/  organisiert/  eingeschränkt/  abgeglichen/

angepasst geordnet gelöscht/ vernichtet verknüpft

übermittelt/ offengelegt/ verbreitet/ bereitgestellt

*(Zutreffendes bitte ankreuzen)*

1. Im Einzelnen sind insbesondere die folgenden **Datenarten** und **Kategorien betroffener Personen** Bestandteil der **zweckgebundenen** Datenverarbeitung

*(Bitte die Tabelle ausfüllen beziehungsweise Unzutreffendes streichen)*

|  |  |  |
| --- | --- | --- |
| **Art der Daten,** siehe untenstehende Beispiele | **Zweck der Datenverarbeitung** (zum Beispiel Gewährleistung der Funktionsfähigkeit der IT-Systeme) | **Kategorien betroffener Personen** |
|  |  | **Versicherte** |
|  |  | **Mitgliedsunternehmen** |
|  |  | **Mitarbeiter/Bewerber** |
|  |  | **Leistungserbringer im Aufgabenbereich der Auftraggeberin** |
|  |  | **Lieferanten/Dienstleister** |
|  |  | **Behörden** |

**Stammdaten**

(Name, Anschrift, Firmenbezeichnung, Gesellschaftsform, Telefon, Fax, Email, Geburtsdatum, -ort, Bankverbindungsdaten, Staatsangehörigkeit, Geschlecht, gesetzlicher Vertreter, dienstliche Kontaktdaten)

**Ordnungsmerkmale**

(Aktenzeichen, Mitgliedsnummer, Unternehmensnummer, Institutionskennzeichen)

**Unfalldaten/Berufskrankheiten**

(Unfallart, -tag, -zeit, Unfallnummer, Meldedatum, Kassenzugehörigkeit, Mitgliedsart, Diagnose, Krankheitstage, Berufskrankheitennummer, Zusatzversicherung, Jahresarbeitsverdienst, Daten zum Unternehmen)

**Gesundheitsdaten**

(Diagnose, Gutachtendaten)

**Leistungsdaten**

(Art der Leistung, Leistungszeitraum, -höhe, -erbringer, Daten über andere Leistungsträger, Daten zu Ersatzkräften, Daten über Erstattungs- und Ersatzansprüche)

**Beitragsdaten**

(Beitrags-Soll, Beitrags-Ist, Zahlungspflichtige, Daten für Beitragseinzug, Daten zum Mahn- bzw. Vollstreckungsverfahren, Beitragsberechnungsdaten)

**Katasterdaten**

(Anzahl der Arbeitstage; Anzahl der Beschäftigten bzw. Versicherten)

**Präventionsdaten**

(Daten über Betriebsprüfungen und deren Feststellungen, Daten zu Sicherheitsfachkräften, Betriebsärzten, Fachkräften für Arbeitssicherheit, Daten über Ordnungswidrigkeiten, Daten über Bußgeldbescheid, Art des Verstoßes)

**Vertrags-/Abrechnungs-/Zahlungsdaten**

(Eingruppierung, Gehalt, Zeiterfassung, Sozialversicherungsdaten, Steuerdaten, Zeiträume, Zahlsätze, Wert der Leistung, Art der Tätigkeit, Art der Leistung/des Vertrages, Rechnungsdaten)

Sofern nicht hier beschrieben, ergibt sich eine genaue Beschreibung des **Zwecks der Datenverarbeitung** aus dem Hauptvertrag.

1. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
2. Die Auftraggeberin und der Auftragnehmer sind bezüglich der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.
3. Sofern bei der Auftragsverarbeitung **Sozialdaten** der Auftraggeberin verarbeitet werden, ist den Parteien bewusst, dass die Auftragsverarbeitung ohne Beachtung der Vorgaben des   
   **§ 80 SGB X** – insbesondere der vorvertraglichen Anzeige- und Rechtfertigungspflichten – nicht zulässig ist. Bei der Verarbeitung von Sozialdaten im Auftrag hat die zuständige Datenschutz-Aufsichtsbehörde auch gegenüber dem Auftragnehmer sämtliche Rechte und Befugnisse.
4. **Verantwortlichkeit und Weisungsbefugnis der Auftraggeberin**
5. Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein die Auftraggeberin verantwortlich (Verantwortlicher entsprechend Art. 4 Nr. 7 DS-GVO). Die Auftraggeberin wird in ihrem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (zum Beispiel durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.
6. Die Auftraggeberin behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Die Weisungen der Auftraggeberin werden anfänglich durch den Hauptvertrag festgelegt und können von der Auftraggeberin danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind von der Weisungsbefugnis der Auftraggeberin gedeckt, sofern diese aufgrund von Änderungen der gesetzlichen Regelungen bzgl. der Verarbeitung der Daten erfolgen. Solche Änderungen sind von den Parteien entsprechend zu dokumentieren.

Weisungen, die im Hauptvertrag nicht vorgesehen sind, werden ansonsten als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

1. Weisungsberechtigte Personen der Auftraggeberin sind:

*(Bitte ausfüllen: Name, Organisationseinheit, Funktion, E-Mail, Telefon)*

Weisungsempfänger bei dem Auftragnehmer sind:

*(Bitte ausfüllen: Name, Funktion, E-Mail, Telefon)*

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind der Auftraggeberin unverzüglich schriftlich die Nachfolger beziehungsweise Vertreter mitzuteilen.

Gleiches gilt für einen Inhaberwechsel, Änderung der Rechtsform sowie andere relevante Änderungen bei dem Auftragnehmer.

1. **Pflichten der Auftraggeberin**

* 1. Die Auftraggeberininformiert den Auftragnehmer unverzüglich und vollständig, wenn Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse bezüglich datenschutzrechtlicher Bestimmungen festgestellt werden.
  2. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichtet sich die Auftraggeberin, den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
  3. Der Auftraggeberin obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde beziehungsweise gegenüber den von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen.
  4. Datenschutzbeauftragter der Auftraggeberin und Ansprechpartner in Datenschutzfragen ist

**Herr Claus Diesing (Claus.Diesing@bgrci.de)**.

* 1. Die Auftraggeberin ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Dies gilt auch nach Beendigung dieses Vertragsverhältnisses fort.

1. **Kontrollrechte der Auftraggeberin**
2. Der Auftragnehmer räumt der Auftraggeberin, den zuständigen Aufsichtsbehörden sowie den Prüfeinrichtungen der Auftraggeberin das Recht ein, vor Beginn der Datenverarbeitung und sodann regelmäßig insbesondere

* Auskünfte bei ihm einzuholen,
* während der allgemeinen Betriebs- oder Geschäftszeiten des Auftragnehmers seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen und Prüfungen vorzunehmen,
* geschäftliche Unterlagen, Datenverarbeitungsprogramme des Auftragnehmers sowie die gespeicherten personenbezogenen Daten bzw. Sozialdaten der Auftraggeberin beim Auftragnehmer einzusehen,

soweit es im Rahmen des Auftrages für die Überwachung des Datenschutzes erforderlich ist. Der Auftragnehmer gewährt die notwendige personelle und sachliche Unterstützung.

1. Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebes zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und unter Berücksichtigung der Interessen des Auftragnehmers an einem ungestörten Betriebsablauf statt.
2. Die Kontrolle sowie der Nachweis der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO sowie der Einhaltung ausreichender technischer und organisatorischer Sicherheitsmaßnahmen, kann ebenfalls durch Vorlage aussagekräftiger Unterlagen über
3. die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
4. die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
5. aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (zum Beispiel Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
6. eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (zum Beispiel nach BSI-Grundschutz);
7. schriftliche Selbstauskünfte des Auftragnehmers entsprechend der Vorgaben der Auftraggeberin (Checklisten) erfolgen.
8. **Pflichten des Auftragnehmers**
9. Der Auftragnehmer darf Daten der Auftraggeberin nur im Rahmen des Auftrages und der Weisungen der Auftraggeberin verarbeiten. Der Auftragnehmer verpflichtet sich, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihm überlassen wurden. Eine Datenverarbeitung zu anderen, insbesondere eigenen Zwecken ist unzulässig.
10. Der Auftragnehmer darf die Daten der Auftraggeberin ausschließlich in der Art, in dem Umfang und zu dem Zweck verarbeiten, wie im Hauptvertrag beziehungsweise in dieser Vereinbarung abschließend festgelegt. Die Datenverarbeitung durch den Auftragnehmer betrifft ausschließlich die hier abschließend festgelegten Datenarten und den bestimmten Kreis der Betroffenen. Jede davon abweichende oder darüberhinausgehende Verarbeitung dieser Daten ist dem Auftragnehmer untersagt.
11. Der Auftragnehmer informiert die Auftraggeberin unverzüglich, sofern er durch das Recht der Union oder der Mitgliedsstaaten zu einer von dieser Vereinbarung abweichenden Verarbeitung der Daten der Auftraggeberin verpflichtet ist.
12. Der Auftragnehmer informiert die Auftraggeberin unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Sofern nach Zugang einer schriftlichen Anzeige der vertrags- oder rechtswidrigen Weisung keine Prüfung und schriftliche Rückmeldung des Prüfungsergebnisses durch die Auftraggeberin erfolgt, ist der Auftragnehmer berechtigt, die als vertrags- beziehungsweise rechtswidrig erachtete Verwendung auszusetzen.
13. Der Auftragnehmer informiert die Auftraggeberin unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.
14. Der Auftragnehmer unterstützt die Auftraggeberin bei der Einhaltung der in den Art. 32 bis 36 der DS-GVO genannten Pflichten.

Hierzu gehören unter anderem:

1. Die Sicherstellung eines angemessenen Schutzniveaus und eines Verfahrens zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, 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,
2. die Verpflichtung, die Auftraggeberin unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten zu unterrichten. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit der Auftraggeberin ab. Der Auftragnehmer unterstützt die Auftraggeberin bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde beziehungsweise den von einer Verletzung betroffenen Personen. Die Mitteilung hat mindestens die Angaben nach Art. 33 Abs. 3 DS-GVO zu enthalten,
3. die Verpflichtung, die Auftraggeberin im Rahmen ihrer Informationspflicht gegenüber den Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,
4. die Unterstützung der Auftraggeberin bei Datenschutz-Folgenabschätzungen,
5. die Unterstützung der Auftraggeberin im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.
6. Der Auftragnehmer unterstützt die Auftraggeberin im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO.
7. Im Falle einer Inanspruchnahme der Auftraggeberin durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO verpflichtet sich der Auftragnehmer, die Auftraggeberin bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
8. An der Ergänzung des Verfahrensverzeichnisses nach Art. 30 DS-GVO der Auftraggeberin hat der Auftragnehmer mitzuwirken, indem er die erforderlichen Angaben der Auftraggeberin zuleitet.
9. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrages vertraut gemacht wurden sowie laufend angemessen überwacht und angeleitet werden. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten der Auftraggeberin befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit und zur Verschwiegenheit verpflichtet sind. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
10. Der Auftragnehmer übergibt der Auftraggeberin auf Verlangen eine Aufstellung derjenigen Personen, die Zugriff auf die zu verarbeitenden Daten haben.
11. Die Verarbeitung der Daten der Auftraggeberin in Telearbeit beziehungsweise in Privatwohnungen ist den Beschäftigten des Auftragnehmers untersagt, sofern im Rahmen der Telearbeit Sozialdaten der Auftraggeberin verarbeitet werden sollen.

1. Überlassene Dateien und/oder Datenträger sowie sämtliche hiervon gefertigte Kopien oder Reproduktionen werden besonders gekennzeichnet und verbleiben im Eigentum der Auftraggeberin. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, der Auftraggeberin jederzeit und auf erstes Verlangen Daten in einer lesbaren beziehungsweise in einer weiterverarbeitbaren Form herauszugeben und Auskünfte zu erteilen, soweit Daten der Auftraggeberin betroffen sind.
2. Sollten die Daten der Auftraggeberin beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so informiert der Auftragnehmer die Auftraggeberin unverzüglich darüber. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei der Auftraggeberin als „Verantwortlichen“ im Sinne der DS-GVO liegen.

Der Auftragnehmer erwirbt keine eigenen Rechte an den zu verarbeitenden Daten der Auftraggeberin. Es besteht kein Zurückbehaltungsrecht an den o.g. Daten, Dateien, Dokumenten oder Datenträgern, gleich aus welchem Rechtsgrund.

1. Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftraggeberin vertraulich zu behandeln. Dies gilt auch nach Beendigung dieses Vertragsverhältnisses fort.
2. Der Beauftragte für den Datenschutz bei dem Auftragnehmer ist

*(Bitte ausfüllen: Name, Adresse/Organisation- falls abweichend, E-Mail, Telefon)*

Ein Wechsel des Beauftragten für den Datenschutz ist der Auftraggeberin unverzüglich mitzuteilen.

1. **Subunternehmer (weitere Auftragsverarbeiter)**
2. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeitern ist – sofern nicht bereits im Hauptvertrag vereinbart - nur zulässig, wenn die Auftraggeberin vorher zugestimmt hat. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer Namen und Anschrift des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer versichern, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeberin und Auftragnehmer auch gegenüber Subunternehmern gelten. Hierzu gehören auch Kontrollen durch die Auftraggeberin. Eine Kopie des unterzeichneten Vertrages mit dem Subunternehmer ist der Auftraggeberin auf Wunsch vorzulegen.
3. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Hauptvertrag vereinbarten Leistung beauftragt.
4. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber der Auftraggeberin.
5. **Technische und organisatorische Maßnahmen**
6. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten der Auftraggeberin treffen, die den Anforderungen gem. Art. 28 Abs. 3 c), Art. 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO genügen. 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.
7. Der Auftragnehmer dokumentiert seine technischen und organisatorischen Maßnahmen mit folgenden Anlagen:

*(Bitte ausfüllen: Datenschutz-/IT-Sicherheitskonzept, Zertifikat und/oder Checkliste benennen)*

Die beigefügten Anlagen werden Bestandteil dieser Vereinbarung**.**

1. Der Auftragnehmer sichert zu, dass die verarbeiteten Daten des Auftraggebers von sonstigen Datenbeständen getrennt werden.
2. 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 sind zu dokumentieren und der Auftraggeberin mitzuteilen.
3. Soweit die bei dem Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen der Auftraggeberin nicht genügen, benachrichtigt er die Auftraggeberin unverzüglich.
4. **Berichtigung, Einschränkung der Verarbeitung, Löschung und Rückgabe von Daten**
5. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggeberin berichtigen, löschen oder deren Verarbeitung einschränken
6. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Einschränkung der Verarbeitung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an die Auftraggeberin verweisen, sofern eine Zuordnung an die Auftraggeberin nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an die Auftraggeberin weiter. Der Auftragnehmer unterstützt die Auftraggeberin im Rahmen seiner Möglichkeiten soweit vereinbart.
7. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenübertragbarkeit und Auskunft nach dokumentierter Weisung der Auftraggeberin unmittelbar durch den Auftragnehmer sicherzustellen.
8. Kopien oder Duplikate der Daten werden ohne Wissen der Auftraggeberin 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.
9. Die Daten dürfen nur so lange gespeichert werden, wie sie zur ordnungsgemäßen Durchführung des Vertrages benötigt werden. Nach Abschluss der vertraglich vereinbarten Arbeiten beziehungsweise spätestens mit Beendigung des Hauptvertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltendem nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für Testmaterial.

Ein Protokoll der Löschung ist auf Anforderung vorzulegen.

1. Es ist der **Anhang**  mit Hinweisen zur Vernichtung und Löschung von Daten für Auftragnehmer zu beachten. Ferner wird auf die Regelung DIN 66399 zur Vernichtung von Datenträgern hingewiesen.
2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende der Auftraggeberin übergeben.
3. ***Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen gelten ergänzend folgende Regelungen:***
4. *Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch die jeweiligen Berechtigten der Auftraggeberin durchgeführt.*
5. *Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung der Auftraggeberin ausgeführt.*
6. *Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.*
7. *Vor Durchführung von Fernzugriffen zu Zwecken von Prüfungs- und/oder Wartungsarbeiten werden sich die Auftraggeberin und der Auftragnehmer über etwaige notwendige Datensicherungsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.*
8. *Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Die Auftraggeberin ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist die Auftraggeberin - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen.*
9. *Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) der Auftraggeberin nur in dem Umfange – auch in zeitlicher Hinsicht - Gebrauch machen, als dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.*
10. *Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) der Auftraggeberin notwendig ist, wird der Auftragnehmer die vorherige Einwilligung der Auftraggeberin einholen.*
11. *Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung der Auftraggeberin. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment der Auftraggeberin oder auf solchen des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung der Auftraggeberin vorliegt. Wirkdaten dürfen nicht ohne Zustimmung der Auftraggeberin auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.*
12. *Fernzugriffe zu Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz der Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen, wie im Datenschutz- und Sicherheitskonzept beschrieben, ergreifen.*
13. **Freistellung von der Haftung, Vertragsstrafe und Kündigungsrecht**
    1. Für den Ersatz von Schäden, die Betroffene wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleiden, ist die Auftraggeberin gegenüber den Betroffenen entsprechend Art. 82 Abs. 2 DS-GVO verantwortlich. Auftraggeberin und Auftragnehmer haften als Gesamtschuldner. Soweit die Auftraggeberin vollständigen Schadenersatz für den erlittenen Schaden gezahlt hat, so ist sie berechtigt, von dem Auftragnehmer entsprechend Art. 82 Abs. 5 DS-GVO einen Teil des Schadenersatzes zurückzufordern.

Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenen Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer die Auftraggeberin auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen die Auftraggeberin erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer der Auftraggeberin ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

* 1. Sofern der Auftragnehmer die Daten verarbeitet, obwohl die Verarbeitung den Weisungen, Zweckbestimmungen und Vorgaben zu Mitteln der Verarbeitung der Auftraggeberin widerspricht, so macht ihn dies zum Verantwortlichen für die entsprechende Verarbeitung. Er haftet gegenüber den Betroffenen unmittelbar nach den Vorschriften der Art. 82, 83 u. 84 DS-GVO wie ein Verantwortlicher.
  2. Bei einem Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des gesetzlichen Datenschutzes, wird eine Vertragsstrafe vereinbart. Diese beträgt 20 Prozent der vertragsgemäßen Vergütung für diesen Auftrag.
  3. Die Auftraggeberin kann den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des Datenschutzes oder dieses Vertrages vorliegt, insbesondere wenn der Auftragnehmer ohne berechtigten Grund weisungswidrig handelt, den Zutritt der Auftraggeberin oder Auskünfte an die Auftraggeberin vertragswidrig verweigert.

1. **Schlussbestimmungen**
   1. Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
   2. Sollte eine Bestimmung dieser Vereinbarung unwirksam sein bzw. werden oder sollte diese Vereinbarung eine Regelungslücke enthalten, so soll davon die Wirksamkeit der Vereinbarung im Übrigen nicht berührt werden.
   3. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.
   4. Gerichtsstand ist der Sitz der Auftraggeberin.

**Ort/Datum**

**(Auftragnehmer)**

**Ort/Datum**

**(Auftraggeberin)**