VEREINBARUNG ZUR AUFTRAGSDATENVERARBEITUNG (ADV)

nach Art. 28 EU DS-GVO (EU-Datenschutz-Grundverordnung)

AUFTRAGSPARTNERDATEN

Auftraggeber:

Unternehmen _____

Straße / Nr. _____

PLZ / Ort _____ _____

HR-Nr. / Gericht _____ _____

Auftragnehmer:

GELO GmbH
Königsbrücker Landstraße 5
01109 Dresden

Präambel

Der Auftragnehmer verarbeitet personenbezogene Daten des Auftraggebers im Rahmen der Durchführung des zwischen den Parteien geschlossenen Dienstleistungsvertrages in Verbindung mit den Allgemeinen Geschäftsbedingungen des Auftragnehmers (im Folgenden auch „Hauptvertrag"). Die Verarbeitung der personenbezogenen Daten durch den Auftragnehmer findet derzeit ausschließlich in der Europäischen Union statt. Die Parteien wollen ihren wechselseitigen datenschutzrechtlichen Verpflichtungen insbesondere nach Art. 28 DS-GVO im Rahmen ihres Vertragsverhältnisses Rechnung tragen und schließen deswegen die nachstehende Vereinbarung zur Auftragsdatenverarbeitung (ADV).

§ 1 Gegenstand, Dauer und Kündigung der Vereinbarung

1. Gegenstand des Vertragsverhältnisses ist die Erbringung von Dienstleistungen im Bereich der Lohnbuchhaltung sowie ggf. damit im Zusammenhang stehende Dienstleistungen, wie z. B. Personalcontrolling.
2. Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieser Vereinbarung.
3. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
4. Diese Vereinbarung tritt mit ihrer Unterzeichnung durch beide Parteien in Kraft und endet mit der Beendigung des Hauptvertrages.
5. Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in dieser Vereinbarung vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen Verstoß dar.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

1. Die vertragsgegenständlichen Leistungen beziehen sich auf die folgenden Arten der Datenverarbeitung:

   Das Erheben, das Erfassen, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung und die Übermittlung von personenbezogenen Daten.
2. Der Zweck der Verarbeitung besteht in der Lohnbuchhaltung für den Auftraggeber gem. § 6 Ziffer 4 StBerG sowie ggf. der Erbringung von damit im Zusammenhang stehenden Dienstleistungen, wie z. B. Personalcontrolling.

3. Folgende Arten von personenbezogenen Daten sind von der Auftragsverarbeitung umfasst: Firmen- und Personalstammdaten einschließlich der Kommunikations- und Vertragsdaten.

4. Von der Verarbeitung sind folgende Personen betroffen: Beschäftigte des Auftraggebers.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

3. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

4. Der Auftraggeber ist berechtigt, sich wie unter § 4 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen.

5. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

6. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

§ 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber 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) DS-GVO).

2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

3. Der Auftragnehmer wird im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen vornehmen. Er ist dafür verantwortlich, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

4. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

5. Der Auftragnehmer wird seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachkommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einsetzen. Das Ergebnis der Kontrollen ist zu dokumentieren.

6. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e) und f) DS-GVO).

7. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

8. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

9. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

10. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h) DS-GVO).

11. Der Auftragnehmer wird, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirken.

12. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

13. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung dieser Vereinbarung fort.

14. Der Auftragnehmer wird die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut machen und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichten (Art. 28 Abs. 3 Satz 2 lit. b) und Art. 29 DS-GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

15. Ein betrieblicher Datenschutzbeauftragter muss beim Auftragnehmer nicht bestellt werden, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt. Der Ansprechpartner für den Datenschutz ist in der Anlage 3 geregelt.

16. Sofern einschlägig wird der Auftragnehmer den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich informieren.

§ 5 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen und Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f) DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. §§ 3 und 4 dieser Vereinbarung durchführen.

§ 6 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d) DS-GVO)

1. Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 2 genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Gleiches gilt für den Fall der Ersetzung eines Auftragsverarbeiters durch einen anderen. Der Auftragnehmer setzt den Auftraggeber hiervon unverzüglich in Kenntnis, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO). Der Auftragnehmer ist verpflichtet, den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auszuwählen. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

2. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

3. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

4. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

5. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

6. Der Auftragnehmer hat die Einhaltung der vertraglichen und gesetzlichen Pflichten des/der Subunternehmer(s) regelmäßig zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

7. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

§ 7 Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c) DS-GVO)

1. Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

2. In der Anlage 1 sind die technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dargestellt.

3. Der Auftragnehmer wird den Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln führen. Zum Nachweis kann der Auftragnehmer dem Auftraggeber nach seiner Wahl folgende Informationen zur Verfügung stellen:
   - Ergebnisbericht der Durchführung eines Datenschutzaudits
   - Zertifikat zu Datenschutz und/oder Informationssicherheit (z. B. ISO 27001)
   - genehmigte Verhaltensregeln nach Art. 40 DS-GVO
   - Zertifikate nach Art. 42 DS-GVO
4. Im Falle der Durchführung von Datenschutzaudits hat der Auftragnehmer regelmäßig eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d) DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber auf Nachfrage mitzuteilen. Im Falle von Zertifizierungen können die vollständigen Prüfunterlagen und Auditberichte vom Auftraggeber jederzeit eingesehen werden.
5. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.
6. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.
7. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

§ 8 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

(Art. 28 Abs. 3 Satz 2 lit. g) DS-GVO)

1. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
2. Der Auftragnehmer ist berechtigt, Dokumentationen, die er benötigt, um die auftrags- und ordnungsgemäße Datenverarbeitung nachweisen zu können, gem. den jeweiligen gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie dem Auftraggeber zu seiner Entlastung bei Vertragsende übergeben.

§ 9 Vergütung

Soweit der Auftraggeber Unterstützung nach § 4 Abs. 6 benötigt, hat er die hierdurch entstehenden Kosten zu erstatten. Gleiches gilt für den Fall, dass der Auftraggeber seine Kontrollrechte nach § 4 Abs. 10 persönlich ausübt. Die vorab jeweils zu vereinbarende Höhe der Vergütung orientiert sich an einem festzulegenden Stundensatz des für die Unterstützung/Betreuung vom Auftragnehmer abgestellten Personals.

§ 10 Haftung

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

§ 11 Sonstiges

1. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
2. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
3. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
4. Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
5. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
6. Vertragsgegenständliche Anlage:

   Anlage 1: Technische und Organisatorische Maßnahmen
   Anlage 2: Unterauftragsverarbeiter
   Anlage 3: Weisungsberechtigte Personen
   Anlage 4: Art der Kundendaten
   Anlage 5: Kreis der Betroffenen

AUFTRAGGEBER		GELO GMBH	
Ort, Datum		Ort, Datum	
Unterschrift gesetzl. Vertreter		Unterschrift	
Stempel		Stempel	

ANLAGEN ZUR ADV

ANLAGE 1 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Der Auftragnehmer ist verpflichtet, die folgenden technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes zu ergreifen:

Vertraulichkeit
(Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Der Auftragnehmer muss für den Zeitraum der Auftragsdatenverarbeitung angemessene Maßnahmen ergreifen, um den Zugang unautorisierter Personen zum Datenverarbeitungsequipment zu verhindern.

Dies geschieht durch:

1. Schlüsselregelung oder codierte Zugangschips;
2. Regelungen für Firmenfremde;
3. Festlegung der Personen, die zugangsberechtigt sind;
4. Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz bzw. externen Wachschutz;

Zugangskontrolle

Der Auftragnehmer sorgt dafür, dass die Personen, die berechtigt sind, das Datenverarbeitungssystem des Auftragnehmers zu nutzen, lediglich Zugang zu solchen Daten haben, die von ihrer jeweiligen Zugangsautorisierung abgedeckt sind.

Dies geschieht durch:

1. Sperrung von Terminals;
2. Zuordnung einzelner Terminals und/oder Terminalnutzer ausschließlich für spezielle Funktionen;
3. Regelungen für Benutzerberechtigung;
4. Verpflichtungen der Mitarbeiter auf das Datengeheimnis;
5. Nutzercodes für Daten und Programme;
6. Differenzierte Zugangsregelungen (z. B. durch Segmentzugriffssperren);
7. Führen eines Logbuches;
8. Kontrollierte Vernichtung von Datenträgern;
9. Arbeitsanweisungen für Datenerfassungsvorlagen;
10. Prüf-, Abstimm- und Kontrollsysteme;

Darüber hinaus erfolgt der elektronische Datenaustausch zwischen Auftraggeber und Auftragnehmer unter Einsatz von Sicherungssystemen mit mehrfachen und komplexen Prüfungsläufen. Anhand von Firewalls, Proxy-Servern, VPN-Routern und Analysesystemen erfolgt die technische Absicherung der Verbindungen. Hierzu werden für das Rechenzentrum wirtschaftlich vertretbare, geeignete Verschlüsselungstechnologien eingesetzt.

Zugriffskontrolle

Der Auftragnehmer trifft geeignete Maßnahmen, um zu verhindern, dass unautorisierte Personen auf ihre Datenverarbeitungssysteme zugreifen. Außerdem trifft der Auftragnehmer angemessene Maßnahmen, die das unautorisierte Lesen, Kopieren oder Löschen der Daten sowie die unautorisierte Speicherung oder Veränderung von gespeicherten Daten verhindern sollen.

Dies geschieht durch:

1. Autorisierungskonzepte;
2. Identifikation des Terminals/des Terminalnutzers im System des Auftragnehmers;
3. Automatische Abschaltung der User ID bei mehrmaliger fehlerhafter Eingabe des Passworts;
4. Logfiles (Überwachung von Einbruchs-Versuchen);
5. Festlegung des zugriffsberechtigten Personals;
6. Schützende Maßnahmen für die Datenspeicherung sowie für das Lesen, Sperren und die Löschung gespeicherter Daten;
7. Verschlüsselung von Sicherheitsdateien;
8. Verschließbare Einrichtungen zur Datenverarbeitung (Räume, Gebäude, Computerhardware und zugehöriges Equipment);
9. Bestimmung der Personen in solchen Bereichen, die für die Entfernung von Datenträgern autorisiert sind.
10. Kontrolle der Entfernung von Datenträgern;
11. Sicherung der Bereiche, in denen Datenträger untergebracht sind;
12. Herausgabe von Datenträgern ausschließlich an autorisierte Personen;
13. Kontrolle der Dateien, kontrollierte und dokumentierte Vernichtung von Datenträgern.

Trennungskontrolle

Der Auftragnehmer trifft geeignete Maßnahmen um sicherzustellen, dass eine getrennte Verarbeitung von Daten erfolgt, die zu unterschiedlichen Zwecken erhoben wurden.

1. Durch die Mandantenfähigkeit in den Datenverarbeitungssystemen erfolgt eine strikte Trennung von Kundendaten.
2. Trennung von Produktions- und Testumgebung für Bibliotheken und Dateien;

Weitergabekontrolle

Der Auftragnehmer ermöglicht die Überprüfung und Bestimmung der Stellen/Orte, an die die Daten der Betroffenen übermittelt werden. Die Überprüfung und Bestimmung erfolgt mittels nachfolgend aufgeführter technischer bzw. organisatorischer Einrichtungen beim Auftragnehmer.

Dies geschieht durch:

1. Bestimmung befugter Personen;
2. Interne Anforderungen zur Verifizierung (Vieraugenprinzip);
3. Kontrolle der Dateien;
4. Sicherheitsschränke;
5. Kontrollierte Vernichtung der Datenträger;
6. Dokumentation der Übermittlungsprogramme;
7. Autorisierungsrichtlinien;
8. Vollständigkeits- und Richtigkeitsprüfung des Datentransfers (End to End Check);
9. Verschlüsselung.

ANLAGEN ZUR ADV

ANLAGE 1 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Eingabekontrolle

Der Auftragnehmer sorgt dafür, dass nachträglich geprüft und festgestellt werden kann, ob und wann die vom Auftraggeber übermittelten personenbezogenen Daten von den Datenverarbeitungssystemen des Auftragnehmers empfangen worden sind.

Dies geschieht durch:

1. Elektronische Protokollierung der Datenverarbeitung, insbesondere der Nutzung der Daten.

Verfügbarkeit und Belastbarkeit
(Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

1. Unterbrechungsfreie Stromversorgung (USV)/ Überspannungseinrichtungen
2. Virenschutz/ SPAM-Filter/ Firewall/ Intrusion Detection System/ Notfallplan
3. Brand-/Wasserschutzeinrichtungen (u. a. Feuerlöschanlage, Brandschutztüren, Rauch/Brandmelder)
4. Einbruchmeldeanlagen

Maßnahmen zur schnellen Wiederherstellbarkeit (Art. 32 Abs.1 lit. c DS-GVO)

1. Backup-Verfahren (u. a. RAID-Verfahren, Bandsicherung im feuerfesten Tresor)
2. Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25. 1 DS-GVO)

Organisationskontrolle

Der Auftragnehmer führt seine interne Organisation dergestalt, dass sie den Anforderungen dieses Vertrages genügt.

Dies geschieht durch:

1. Interne Datenverarbeitungsrichtlinien und -verfahren, Arbeitsanweisungen, Prozessbeschreibungen und Regelungen für Tests und Freigabe neuer Verfahren, sofern die vom Auftraggeber übermittelten Daten betroffen sind;
2. Nutzung von branchenüblichen Standardsystemen und Programmprüfung, sowie geeigneter Individualsoftware.
3. Formulierung eines Notfallplans.
4. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Auftragskontrolle

Der Auftragnehmer gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

1. Es wird eine geeignete Auswahl von Partnerunternehmen hinsichtlich der getroffenen technisch-organisatorischen Maßnahmen getroffen.
2. Umsetzung klarer Regelungen von Verantwortlichkeiten.
3. Die Auftragserteilung erfolgt nach spezifischen Regeln.
4. Die Vertragsdurchführung erfolgt weisungsgebunden.
5. Die Vertragsdurchführung wird regelmäßig kontrolliert.

Weisungskontrolle

Die vom Auftraggeber an den Auftragnehmer übermittelten Daten dürfen ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers verarbeitet werden.

Dies geschieht durch:

1. Für die Mitarbeiter des Auftragnehmers bindende Richtlinien und Arbeitsanweisungen, die sich aus dem jeweiligen Verfahren ergeben;
2. Auskunftserteilung gegenüber dem Auftraggeber zu speziellen Verfahren oder Daten des Auftraggebers auf Anfrage.

ANLAGEN ZUR ADV

ANLAGE 2 UNTERAUFTRAGSVERARBEITER GEM. ART. 28 DS-GVO

Name	Anschrift	Auftragsinhalt
WK Software und Service	Wolters Kluwer Software und Service GmbH Stuttgarter Straße 35 71638 Ludwigsburg	• Servicedienstleistungen • Development • Support • Rechenzentrumsleistungen (Betrieb/Hosting)
Ditpro GmbH & Co. KG	Ditpro GmbH & Co. KG Würzburger Straße 14 01187 Dresden	• IT-Dienstleistungen • Support
Veolia Umweltservice Ost GmbH & Co. KG	Veolia Umweltservice Ost GmbH & Co. KG Rosenstraße 99 01159 Dresden	• Aktenvernichtung • Entsorgung

ANLAGE 3 WEISUNGSBERECHTIGTE PERSONEN

Weisungsberechtigte Anfragen im Sinne dieser ADV sind an info@gelo-lohn.de zu richten.

Verantwortlicher Ansprechpartner für Datenschutz	Sören C. Burghardt Königsbrücker Landstraße 5 01109 Dresden Telefon: +49 351 / 213 491-50 E-Mail: sb@gelo-lohn.de

ANLAGE 4 ART DER VERARBEITETEN KUNDEN UND MANDANTENDATEN

Art der Daten	
Im Bereich von Institutionen	• Meldungen für Sozialversicherungsträger • Meldungen für Berufsgenossenschaften
Beschäftigtendaten	• Name und Anschrift • Geschlecht, Familienstand, Konfession, Einkommen, Krankenkasse, Bankverbindung und Zahldaten • Arbeits-, Urlaubs-, Krankheitszeiten, u. ä.
Lieferantendaten	• Adress-/Kontaktdaten, Bankverbindung, Vertragsdaten
Kundendaten	• Adress-/Kontaktdaten, Bankverbindungen, Vertragsdaten, Kundenhistorie • Beschäftigtendaten (s. o.)
Im Bereich Steuern und Rechnungswesen	• Voranmeldungen • Anmeldungen • Lohnsteuerberechnungen • Steuererklärungen und eBilanz • Finanzbuchhaltungsdaten
Im Bereich des eBusiness-Geschäftsverkehres	• Hochgeladene Dokumente und Dateien • E-Mail-Verkehr • Bereitgestellte Auswertungen aus den Programmen • Druckdienstleistungen
Banken	• Zahldaten, Bankverbindungen, Kontoauszugsdaten

ANLAGE 5 KREIS DER BETROFFENEN

Kreis der Betroffenen	
	• Kunden / deren Mandanten • Beschäftigte • Lieferanten