

**automadeit GmbH**

Im Mediapark 4e | 50670 Köln // DE

E-Mail: office@automadeit.com

Amtsgericht Köln | HR-Nr.: HRB 116038 | Geschäftsführung: Tim Schröder

**§1****Allgemeines**

1. Diese Geschäftsbedingungen gelten nur gegenüber Unternehmern im Sinne von § 14 BGB, juristischen Personen des öffentlichen Rechts oder öffentlich-rechtlichen Sondervermögen. Sie gelten nicht nur für das Vertragsverhältnis, in das sie einbezogen wurden, sondern auch für alle zukünftigen Geschäftsbeziehungen, wenn wir auf keine anderen Geschäftsbedingungen verweisen. Wir lehnen den Vertragsschluss mit Verbrauchern ab.

2. Abweichende, entgegenstehende oder ergänzende Geschäftsbedingungen des Kunden werden, selbst bei unserer Kenntnis, nicht Vertragsbestandteil, es sei denn, ihrer Geltung wird ausdrücklich zugestimmt. Diese Geschäftsbedingungen gelten auch, wenn wir in Kenntnis entgegenstehender oder von unseren Bedingungen abweichender oder zusätzlicher Bedingungen des Kunden den Vertrag vorbehaltlos durchführen.

**§2****Vertragsschluss**

1. Unsere Angebote sind freibleibend. Mit der Annahme eines Angebotes erklärt der Kunde verbindlich, die ausgewiesenen Leistungen bestellen zu wollen. Wir sind berechtigt, das mit der Bestellung des Kunden vorliegende Vertragsangebot innerhalb einer Woche nach Zugang anzunehmen. Die Annahme kann entweder ausdrücklich oder durch den Beginn der Bearbeitung der Bestellung erklärt werden.

2. Soweit Gegenstand des Angebotes Leistungen Dritter sind (z. B. Software oder Hardware von Drittanbietern) stehen diese unter dem Vorbehalt der Selbstbelieferung. Sollte die Leistungen aus Gründen nicht verfügbar sein, die für uns bei Vertragsschluss nicht vorhersehbar waren, oder sollten wir unverschuldet von einem Lieferanten nicht beliefert werden, haben wir das Recht, uns insoweit von dem Vertrag zu lösen. In diesem Fall werden wir den Kunden unverzüglich darüber informieren, dass eine Lieferung nicht möglich ist und auf seinen Wunsch den gesamten Vertrag aufheben, wenn dieser aufgrund der ausbleibenden Leistung für den Kunden nicht mehr von Interesse ist und wir keinen gleichwertigen Ersatz anbieten können, der dem Kunden zumutbar ist.

3. Als Beschaffenheit der Leistung gelten nur die Angaben in unserem Angebot als vereinbart. Davon abweichende öffentliche Äußerungen, Anpreisungen oder Werbung stellen keine vertragsgemäße Beschaffenheitsangabe der Leistung dar.

4. Durch Überlassung von Mustern vor oder aus Anlass des Vertragsabschlusses wird kein »Kauf nach Muster« vereinbart. Die Muster sind lediglich Anschauungsmuster, die den ungefähren Charakter der Ware zeigen. Bestimmte Eigenschaften werden hierdurch nicht vereinbart. Dies gilt nicht, wenn ausdrücklich vereinbart wird, dass Lieferung gemäß dem Muster erfolgen soll.

## §3

### Unsere Leistungen

1. Zu den von uns geschuldeten Leistungen gehört je nach Auftragsumfang insbesondere
  - 1.1. Strategische Beratung hinsichtlich der Gestaltung und Positionierung der Produkte des Kunden;
  - 1.2. Entwicklung und Optimierung der Markenbotschaft, Markenstrategie, Positionierung der Marke sowie Unternehmenskommunikation;
  - 1.3. Social-Media-Marketing;
  - 1.4. Entwicklung, Durchführung, Kontrolle und Optimierung von Werbestrategien und -maßnahmen;
  - 1.5. Aufsetzen der für die Umsetzung von Werbestrategien und -maßnahmen erforderlichen technischen Mittel;
  - 1.6. Entwicklung und Erstellung von Werbemitteln und anderem Content für die Zwecke dieses Vertrages;
2. Wir werden mit dem Kunden die zu erbringenden Leistungen im erforderlichen Umfang von Fall zu Fall abstimmen und konkretisieren, wobei das Leistungsbestimmungsrecht nach § 315 BGB uns zusteht.
3. Wir schulden nicht das Erreichen eines bestimmten Unternehmenserfolges. Sofern wir mit dem Kunden als Ziel unserer Tätigkeit einen konkreten Erfolg beschreiben sollten, schulden wir nur ein Bemühen, dieses Ziel durch eine ordnungsgemäße Tätigkeit zu erreichen und nicht die Erreichung des Ziels im Sinne Versprechens, dieses Ziel zu erreichen. Dies gilt nicht, wenn die entsprechende Leistung ausdrücklich aus geschuldeter Leistungserfolg vereinbart wurde.
4. Wir erbringen unsere Leistungen nach dem bewährten Stand der Tätigkeit der Technik und eines Unternehmensberaters. Wir sind nicht fest in die Organisation des Anbieters eingebunden. Wir können innerhalb des Vereinbarten die Art und Weise der Leistungserbringung frei bestimmen und sind insoweit keinen Weisungen des Kunden unterworfen.

## §4

### Werbemaßnahmen

1. Sofern wir dem Kunden die Planung und Umsetzung von Werbemaßnahmen (z. B. Schaltung von Werbung, Produktion von Content durch Dritte) schulden, stellt uns der Kunden hierfür ein Budget zur Verfügung, über dessen Höhe und Verwendung wir uns von Fall zu Fall mit dem Kunden verständigen werden. Das Budget ist ausschließlich für Fremdkosten zu verwenden (z. B. Schaltung von Anzeigen) und dient nicht der Vergütung unserer Leistungen. Der Kunde stellt für die Abrechnung dieser Kosten die entsprechenden Online-Zugänge oder eine Kreditkarte o. Ä. zur Verfügung.
2. Werbestrategien und Werbemittel wie Anzeigen, Landingpages, Funnel etc. (zusammen die „Werbemittel“), die für den Kunden entwickelt und produziert werden, werden im Außenverhältnis, sofern nicht anders vereinbart, stets vom Kunden als rechtlich Verantwortlichen genutzt und betrieben. Soweit für die Umsetzung von Werbemittel technische Hilfsmittel erforderlich sind (z. B. das Hosting von Landingpages oder Funnel) erfolgt dies im Namen und auf Rechnung des Kunden.
3. Für Werbemaßnahmen auf Webseiten und in Apps geltend ergänzend die entsprechenden Bedingungen des jeweiligen Anbieters, z. B. Facebook, LinkedIn etc.

4. Werbemittel werden erst mit entsprechender Freigabe des Anbieters genutzt und veröffentlicht werden. Der Anbieter wird die Freigabe nicht unbillig verweigern.
5. Der Kunde wird alle für Werbemittel erforderlichen Inhalte (Logos, Bilder, Links etc.), soweit diese aus seiner Sphäre stammen, im erforderlichen Format zur Verfügung stellen bzw. an deren Erstellung mitwirken (z. B. Produktion von Bildern oder Videos) und überträgt uns für die Laufzeit dieses Vertrages alle Rechte, die für deren vertragsgemäße Nutzung erforderlich sind.
6. Die rechtliche Prüfung der Zulässigkeit der Werbestrategie bzw. -mittel obliegt dem Kunden.

## **§5**

### **Onlinekurse, Webinare o. Ä.**

1. Zugangsdaten, die wir dem Kunden für Onlinekurse, Webinare o. Ä. zur Verfügung stellen, dürfen nur für und von den Mitarbeitern des Kunden genutzt werden, für die wir diese zur Verfügung stellen. Eine Überlassung an Dritte oder das Teilen von Zugangsdaten für mehrere Nutzer ist unzulässig. Sie sind von diesen im erforderlichen Umfang vor unberechtigter Kenntnisnahme durch Dritte zu schützen. Sofern der Verdacht besteht, dass unberechtigte Dritte von diesen Kenntnis erlangt haben, hat uns der Kunde unverzüglich zu informieren und wir sind berechtigt, diese Zugangsdaten zu ändern.
2. Das Herunterladen der Onlinekurse, Webinare o. Ä. oder eine anderweitige Vervielfältigung sind nicht gestattet, sofern und soweit dies nicht für die bestimmungsgemäße Nutzung erforderlich ist.
3. Es ist Kunden nicht gestattet, in den von uns angebotenen Kursen, Webinaren gegenüber anderen Kunden Werbung zu betreiben und insbesondere ihnen Waren oder Dienstleistungen anzubieten.

## **§6**

### **Entgelt**

1. Für unsere Leistungen fallen die mit dem Kunden vereinbarten Entgelte an. Sofern für eine mit dem Kunden vereinbarte Leistungen kein Entgelt vereinbart wurde, gilt unsere aktuelle Preisliste, hilfsweise gilt eine übliche Vergütung als vereinbart.
2. Alle von uns angegebenen Preise sind Nettopreise und verstehen sich in Euro.
3. Unsere Entgelte werden wie im Angebot ausgewiesen vorab in Rechnung gestellt. Monatliche Entgelte werden jeweils zu Beginn eines Monats abgerechnet.
4. Wir sind berechtigt, Rechnungen in digitaler Form an den Kunden zu versenden.

## **§7**

### **Laufzeit des Vertrages**

1. Sofern nicht anders vereinbart, werden Verträge über den jeweils vereinbarten Zeitraum fest abgeschlossen und verlängern sich mangels Kündigung wiederholt um die jeweils

vereinbarte initiale Laufzeit. Die Kündigungsfristen sind wie folgt: Verträge mit einer Laufzeit von einem Jahr, 3 Monate, von sechs Monaten, 2 Monate, und von drei Monaten, ein Monat.

2. Die Kündigung nach § 627 BGB ist ausgeschlossen. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Als wichtiger Grund gelten insbesondere die folgenden Gründe, wenn sie für die andere Partei vorliegen:

2.1. die Verletzung wesentlicher Vertragspflichten durch die andere Partei, wenn die Verletzung trotz Mahnung und Setzung einer angemessenen Frist nicht beseitigt wird. Die Mahnung und Fristsetzung ist bei Unzumutbarkeit nicht erforderlich;

2.2. Der Zahlungsverzug mit einem Betrag von mehr als 5.000 EUR um mehr als 30 Tage;

2.3. der Eigenantrag auf Eröffnung des Insolvenzverfahrens, die Eröffnung des Insolvenzverfahrens sowie die Ablehnung der Eröffnung mangels Masse;

3. Kündigungen haben in Textform zu erfolgen.

## §8

### **Pflichten des Kunden**

1. Der Kunde verpflichtet sich, unsere Tätigkeit im erforderlichen Umfang zu unterstützen. Insbesondere schafft er unentgeltlich alle ihm obliegenden technischen, personellen und räumlichen Voraussetzungen, die zur ordnungsgemäßen Durchführung des Vertrages erforderlich sind. Er stellt uns auf unseren Wunsch alle Daten und Informationen aus seiner Sphäre zur Verfügung, die wir für den Vertragszweck von ihm benötigen.

1.1. Während der Vertragsdauer wird der Kunde einen informierten und kompetenten Ansprechpartner benennen.

1.2. Besteht unsere Leistung aus Lieferung, Installation oder Anpassung von Software, Webseiten o. Ä., wird der Kunde

1.3. uns bei Arbeitsaufnahme ohne Wartezeit ungehinderten Zugang zu den entsprechenden IT-Systemen verschaffen;

2. uns vorab in angemessener Frist informieren, wenn wir unsere Tätigkeit nicht an einem Test/Staging-, sondern an einem Produktiv-System erbringen sollen. In diesem Fall wird er in Abstimmung mit uns geeignete Maßnahmen für den Fall treffen, dass unsere Leistung nicht vertragsgemäß erbracht wird, um Auswirkungen auf die Geschäftstätigkeit des Kunden möglichst zu minimieren, z. B. Spiegelung von Systemen, Datensicherung, fortlaufende Überprüfung der Ergebnisse der Datenverarbeitung;

3. von den von unseren Leistungen betroffenen IT-Systemen eine aktuelle, rücksicherbare Datensicherung anlegen, bevor er uns Zugriff auf diese gewährt. Er hat uns in Textform gegen Bestätigung darauf hinzuweisen, wenn von den Systemen keine rücksicherbare Sicherung vorhanden sein sollte. Dies gilt nicht, wenn wir mit der Datensicherung beauftragt sind;

4. Mit dem Kunden vereinbarte Fälligkeiten und Fristen verlängern sich um die Zeit, in welcher er trotz Mahnung eine ihm obliegende Mitwirkungshandlung verzögert oder sonst die Behinderung zu vertreten hat und dies unsere Leistungserfüllung behindert. Eine Mahnung ist entbehrlich, wenn wir bei unserem Mitwirkungsverlangen bereits eine angemessene Frist gesetzt haben oder ein Termin für die Erbringung der Leistung vereinbart wurde.

5. Der Kunde wird uns über Störungen oder Mängel unserer Leistung unverzüglich informieren und in diesem Rahmen die Störung bzw. den Mangel so präzise wie ihm möglich unter Angabe der ihm bekannten und zweckdienlichen Informationen beschreiben. Soweit

der Kunde vernünftigerweise nicht in der Lage ist, uns diese Informationen zu überlassen, ist dies für unsere Leistungsverpflichtung unbeachtlich.

6. Der Kunde gewährleistet, dass er an allen uns übergebenen Daten, Informationen, Dokumenten, Grafiken etc. die notwendigen Rechte hat und deren vertragsgemäßer Nutzung keine Rechte Dritter oder Gesetze entgegenstehen. Er stellt uns von allen Ansprüchen Dritter frei, die diese gegen uns wegen eines Verstoßes gegen Satz 1 geltend machen.

7. Der Kunde trägt den Aufwand, der dadurch entsteht, dass Arbeiten infolge seiner unrichtigen, nachträglich berichtigten oder lückenhaften Angaben von uns wiederholt werden müssen oder verzögert werden.

## **§9**

### **Termine**

1. Angegebene Liefer- oder Leistungstermine sind unverbindlich, sofern sie nicht ausdrücklich von uns als verbindlich bezeichnet werden.

## **§10**

### **Rechteübertragung, Übergabe der Leistung**

1. Der Kunde erwirbt an unseren Leistungen die Rechte, wie sie im Angebot, das unserer Beauftragung zugrunde liegt, ausgewiesen sind. Wurde mit dem Kunden keine Regelung zum Umfang der Rechteübertragung vereinbart, erwirbt er an unseren Leistungen die für die Vertragserfüllung erforderlichen Rechte.

2. Es besteht keine Verpflichtung auf die Nennung des Urhebers der Leistung.

3. Sofern nicht anders vereinbart, bekommt der Kunde unsere Leistungen nicht in einem bearbeitbaren Format ausgeliefert.

4. An Webseiten oder Inhalten für die Nutzung in Cloud Diensten, z. B. Funnel, erwirbt der Kunde auch Bearbeitungsrechte an unseren Leistungen.

5. Der Kunde erwirbt die ihm vertraglichen zustehenden Rechte Zug-um-Zug gegen Zahlung der für die entsprechenden Leistungen vereinbarten Entgelte. Sofern wir dem Kunden bereits vorab eine Nutzung unserer Leistungen ermöglichen, ist diese temporäre Rechteübertragung jederzeit widerruflich; insbesondere, wenn sich der Kunde im Zahlungsverzug befindet.

## **§11**

### **Datenschutz**

1. Für eine Verarbeitung personenbezogener Daten, die Art. 28 DSGVO unterfällt, gilt der anliegende Auftragsverarbeitungsvertrag. Im Übrigen verpflichten wir uns hinsichtlich personenbezogener Daten, welche uns der Kunde zur Verarbeitung überlässt, die insoweit bestehenden gesetzlichen Vorgaben zu beachten.

## **§12**

### **Mängel**

1. Für etwaige Mängel der Leistungen gelten die gesetzlichen Bestimmungen, sofern nicht nachfolgend etwas Abweichendes vereinbart wird.
2. Mängel sind, soweit es dem Kunden möglich ist, durch eine nachvollziehbare Schilderung der Fehlersymptome und die Mängel veranschaulichende Unterlagen zu rügen. Gesetzliche Untersuchungs- und Rügepflichten des Kunden bleiben unberührt.
3. Die Behebung von Mängeln erfolgt nach unserer Wahl durch Nachbesserung oder Ersatzlieferung. Soweit es dem Kunden zumutbar ist, kann die Behebung eines Mangels auch durch Bereitstellung eines sog. workarounds (Umgehung eines Mangels) erfolgen.
4. Wenn wir auf eine Mängelrüge des Kunden Leistungen für Mangelsuche oder -beseitigung erbringt, so können wir hierfür eine Vergütung nach unseren üblichen und angemessenen Sätzen verlangen, sofern kein Mangel vorliegt, für den wir einstandspflichtig sind, und dies im Zeitpunkt der Mängelrüge dem Kunden erkennbar war.
5. Sollte sich der Kunde im Zeitpunkt der Mängelrüge mit der Entrichtung des vereinbarten Entgelts im Verzug befinden, können wir die Nacherfüllung verweigern, bis der Kunde die fällige Vergütung abzüglich eines Betrages, der der wirtschaftlichen Bedeutung des Mangels entspricht, an uns entrichtet hat.
6. Die Rechte des Kunden wegen Mängeln sind ausgeschlossen, soweit er Änderungen an der betroffenen Leistung vorgenommen hat oder von Dritten hat vornehmen lassen, es sei denn, er weist nach, dass die Änderungen keine für uns unzumutbaren Auswirkungen auf Analyse und Beseitigung des jeweiligen Mangels haben. Die Rechte des Auftraggebers bleiben unberührt, sofern er zur Vornahme von Änderungen, insbesondere im Rahmen der Ausübung des Selbstbeseitigungsrechts berechtigt ist und diese fachgerecht ausgeführt sowie nachvollziehbar dokumentiert wurden.
7. Eine Kündigung des Kunden gemäß § 543 Abs. 2 Satz 1 Nr. 1 BGB wegen Nichtgewährung der vertragsgemäßen Nutzung ist erst zulässig, wenn er uns eine angemessene Gelegenheit zur Mängelbeseitigung gewährt hat und diese fehlgeschlagen ist.
8. Unsere verschuldensunabhängige Haftung auf Schadensersatz (§ 536a BGB) für bei Vertragsschluss vorhandene Mängel ist ausgeschlossen, soweit es sich nicht um eine von uns zugesicherte Eigenschaft (Garantie, § 276 Abs. 1 BGB) handelt.
9. Für Mängelansprüche ist eine Verjährungsfrist von einem Jahr vereinbart. Dies gilt nicht für die Haftung für Schäden wegen Mängeln, insoweit gelten die Regelung zur Haftung. Für Schadensersatzansprüche, die auf einer verweigerter Nacherfüllung beruhen, gelten die gesetzlichen Verjährungsfristen nur dann, wenn die Nacherfüllung innerhalb der auf ein Jahr verkürzten Frist für Mängelansprüche verlangt worden ist.

## **§13**

### **Haftung**

1. Die Haftung für Vorsatz und grobe Fahrlässigkeit ist unbeschränkt.
2. Bei einfach fahrlässiger Verletzung wesentlicher Vertragspflichten ist die Haftung der Höhe nach beschränkt auf vorhersehbare und vertragstypische Schäden. Wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung die verletzte Partei regelmäßig vertrauen darf. Die Verjährungsfrist für Ansprüche nach diesem Absatz beträgt ein Jahr.

3. Absatz 2 gilt nicht für Ansprüche aus der Verletzung des Lebens, des Körpers oder der Gesundheit, bei arglistigem Handeln, bei Übernahme einer Garantie, bei Haftung für anfängliches Unvermögen oder zu vertretender Unmöglichkeit sowie für Ansprüche nach dem Produkthaftungsgesetz.

4. Im Übrigen ist die Haftung — gleich aus welchem Rechtsgrund — ausgeschlossen.

## **§14**

### **Höhere Gewalt**

1. Jede Partei wird von ihrer Leistungspflicht temporär befreit, solange sie an der Erbringung der Leistung aus höherer Gewalt gehindert ist. Das gilt auch für den Fall, dass die Partei sich bereits im Verzug befindet. In diesem Fall wird auch die andere Partei temporär von den von ihr insoweit geschuldeten Gegenleistungen frei.

2. Höhere Gewalt sind entsprechende Ereignisse im Sinne des § 206 BGB sowie ein sonst ungewöhnliches und unvorhergesehenes Ereignis, wenn diejenige Partei, die sich hierauf beruft, das Ereignis nicht verursacht hat, nicht mit dem Ereignis rechnen, dessen Eintritt nicht beeinflussen, dessen Folge trotz Anwendung der gebotenen Sorgfalt nicht verhindern konnte und aus dem Grund an der Leistungserbringung gehindert ist. Dies gilt insbesondere für Krieg, Terrorismus, Aufruhr, Pandemien, Unwettern, Umweltkatastrophen oder wenn die Leistungsverhinderung sonst auf staatliche Anordnung beruht.

3. Die Partei, die sich auf das Vorliegen höherer Gewalt beruft, hat

4. die andere Partei unverzüglich in Textform über die Tatsache und die Gründe hierfür zu informieren;

5. mit der Sorgfalt eines ordentlichen Kaufmanns die Maßnahmen zu ergreifen, die erforderlich sind, um die vollständige Erfüllung ihrer Verpflichtungen möglichst unverzüglich wieder aufnehmen zu können;

6. angemessene Anstrengungen zu unternehmen, die negativen Auswirkungen auf die Erfüllung des Vertrages möglichst zu minimieren;

## **§15**

### **Schlussbestimmungen**

1. Dieser Vertrag enthält alle Vereinbarungen der Parteien zum Vertragsgegenstand. Eventuell abweichende Nebenabreden und frühere Vereinbarungen zum Vertragsgegenstand werden hiermit unwirksam.

2. Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform, soweit nicht gesetzlich eine strengere Form vorgeschrieben ist. Dies gilt auch für jeden Verzicht auf das Formerfordernis.

3. Andere allgemeine Geschäftsbedingungen der Parteien finden keine Anwendung. Dies gilt auch dann, wenn auf deren Einbeziehung in späteren Dokumenten, die im Zusammenhang mit diesem Vertrag stehen (z. B. Abruf von Leistungen), unwidersprochen hingewiesen wurde.

4. Sollte eine Bestimmung des Vertrages ganz oder teilweise nichtig, unwirksam oder nicht durchsetzbar sein oder werden, oder sollte eine an sich notwendige Regelung nicht enthalten sein, bleibt die Wirksamkeit und die Durchsetzbarkeit aller übrigen Bestimmungen dieses Vertrages unberührt. Es ist der ausdrückliche Wille der Parteien, dass diese

salvatorische Klausel keine bloße Beweislastumkehr zur Folge hat, sondern § 139 BGB insgesamt abbedungen ist.

5. Der Vertrag unterliegt allein dem Recht der Bundesrepublik Deutschland. Das internationale Privatrecht findet keine Anwendung, soweit es abdingbar ist.

6. Alleiniger Gerichtsstand für alle Streitigkeiten im Zusammenhang mit diesem Vertrag ist an unserem Sitz. Wir sind berechtigt, den Kunden auch an einem seiner gesetzlichen Gerichtsstände in Anspruch zu nehmen.

**automadeit GmbH**

Im Mediapark 4e | 50670 Köln // DE

E-Mail: office@automadeit.com

Amtsgericht Köln | HR-Nr.: HRB 116038

## **Anlage Auftragsverarbeitungsvertrag**

### **Gegenstand der Beauftragung**

1. Der Auftraggeber lässt durch den Auftragnehmer auf Grundlage des Vertrages, zu dem dieser Auftragsverarbeitungsvertrag Anlage ist (der „Hauptvertrag“) personenbezogenen Daten im Auftrag verarbeiten. Zur Durchführung des Hauptvertrages beauftragt der Auftraggeber den Auftragnehmer mit einer Auftragsverarbeitung gem. Art. 28 DSGVO. Dieser Auftragsverarbeitungsvertrag geht im Fall von Widersprüchen dem Hauptvertrag vor.
2. Ziel der Verarbeitung personenbezogener Daten durch den Auftragnehmer ist die Erbringung der im Hauptvertrag vereinbarten Leistungen. Die Kategorien der von der Verarbeitung Betroffenen und personenbezogener Daten sind in der Anlage 1 wiedergegeben. Von der Verarbeitung erfasst sind keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO.

### **Ort der Auftragsverarbeitung**

Eine Verlagerung der Auftragsverarbeitung in ein Drittland darf nur erfolgen, wenn die Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

### **Verantwortlichkeit und Weisungsrecht des Auftraggebers**

1. Der Auftraggeber ist für die Zwecke der Auftragsverarbeitung der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Übermittlung der Daten an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung durch diesen, verantwortlich.
2. Der Auftraggeber hat jederzeit das Recht, den Hauptvertrag ergänzende Weisungen über Art, Umfang und Verfahren der Verarbeitung der personenbezogenen Daten zu erteilen. Weisungen können mündlich oder in Textform erfolgen. Mündliche Weisungen des Auftraggebers sind durch diesen unverzüglich in Textform zu bestätigen.
3. Der Auftragnehmer wird den Auftraggeber unverzüglich in Textform informieren, wenn nach seiner Auffassung eine vom Auftraggeber erteilte Weisung gegen gesetzliche Regelungen verstößt. Solange die Parteien die Bedenken des Auftragnehmers nicht ausgepäumt haben, ist der Auftragnehmer berechtigt, die Durchführung der betreffenden Weisung auszusetzen.
4. Sofern der Auftragnehmer der Auffassung sein sollte, eine Weisung des Auftraggebers aus technischen Gründen nicht befolgen zu können, wird er den Auftraggeber hierüber in Textform informieren und sich zum weiteren Vorgehen mit diesem abstimmen.

### **Pflichten des Auftragnehmers**

1. Jegliche Verarbeitung der personenbezogenen Daten erfolgt ausschließlich entsprechend den Vorgaben des Hauptvertrages sowie den ggf. vom Auftraggeber erteilten Weisungen. Dies gilt auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Dieser Absatz 1 gilt nicht, wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, verpflichtet ist; 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.
2. Der Auftragnehmer bestätigt, dass er gesetzlich nicht verpflichtet ist, einen betrieblichen Datenschutzbeauftragten zu bestellen. Er benennt dem Auftraggeber an dessen Stelle einen Ansprechpartner für alle Belange des Datenschutzes und der Durchführung dieses Vertrages.
3. Der Auftragnehmer hat die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
4. Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten unterstützen. Hierfür wird er insbesondere die in diesem Vertrag vorgesehenen Leistungen erbringen.
5. Soweit erforderlich, unterstützt der Auftragnehmer den Auftraggeber bei der Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und wird ihm alle hierfür aus seiner Sphäre erforderlichen Informationen und Nachweise überlassen. Er ist entsprechend verpflichtet, wenn der Auftraggeber eine vorherige Konsultation nach Art. 36 DSGVO mit einer Aufsichtsbehörde durchführen muss. Für die unter diesem Absatz zu erbringenden Leistungen steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu. Der Auftragnehmer darf die Erbringung der von ihm geschuldeten Leistungen nicht davon abhängig machen, dass der Auftraggeber eine bestimmte Vergütung anerkennt und/oder vorab leistet.
6. Auf berechtigten Wunsch des Auftraggebers wird der Auftragnehmer diesem alle erforderlichen Informationen zum Nachweis der Einhaltung der dem Auftragnehmer nach Artikel 28 DSGVO obliegenden Pflichten zur Verfügung stellen.
7. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden oder ist es zu entsprechenden Maßnahmen gekommen, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber umfassend zu informieren, es sei denn, dies ist ihm gesetzlich nicht gestattet. Ferner ist der Auftragnehmer verpflichtet, alle insoweit relevanten Dritten darauf hinweisen, dass es sich bei den Daten um personenbezogene Daten handelt, für die der Auftraggeber Verantwortlicher ist und er selbst nur als Auftragsverarbeiter tätig wird.

### **Pflichten des Auftraggebers**

Der Auftraggeber hat den Auftragnehmer unverzüglich unter Angabe der Gründe zu informieren, wenn er in den Auftragsergebnissen oder hinsichtlich der Tätigkeit des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich der Vorgaben dieses Vertrages oder der DSGVO feststellt.

## **Sicherheit der Verarbeitung**

1. Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen, insbesondere geeignete technische und organisatorische Maßnahmen, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten. Zum Zeitpunkt des Vertragsschlusses sind dies die in der Anlage 2 beschriebenen Maßnahmen. Er hat die Einhaltung dieser Vorgaben dem Auftraggeber auf dessen Verlangen mit geeigneten Mitteln nachzuweisen.
2. Der Auftragnehmer ist zur Anpassung an geänderte technische oder rechtliche Gegebenheiten berechtigt, Änderungen an den in Anlage 2 beschriebenen Maßnahmen vorzunehmen. Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen, eine Erhöhung der Risiken für die Rechte und Freiheiten der von der Verarbeitung Betroffenen oder generell eine Reduktion des vereinbarten Schutzniveaus mit sich bringen könnten, bedürfen der Zustimmung des Auftraggebers. Andere Änderungen, insbesondere eine Verbesserung der ergriffenen Maßnahmen, können vom Auftragnehmer ohne Zustimmung des Auftraggebers umgesetzt werden. Nach Vornahme solcher Änderungen passt der Auftragnehmer die Anlage 2 entsprechend an und übermittelt die jeweils aktuelle Version der Anlage 2 unverzüglich dem Auftraggeber bzw. weist diesen darauf hin, wo die neue Version auf der Webseite des Auftragnehmers zur Verfügung gestellt wird.

## **Betroffenenrechte**

1. Der Auftragnehmer wird, soweit es ihm möglich und zumutbar ist, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 der DSGVO genannten Rechte der betroffenen Personen nachzukommen. Hierfür hat der Auftraggeber den Auftragnehmer in Textform zu informieren, welche Unterstützungshandlung des Auftragnehmers er benötigt und diesem insoweit die Daten zu überlassen, die zur Erfüllung der Anfrage erforderlich sind. Soweit eine Partei weitere Informationen von der anderen Partei benötigt, wird sie diese unverzüglich in Textform darauf hinweisen. Der Auftragnehmer erbringt seine Unterstützungshandlung in angemessener Frist, so dass der Auftraggeber die ihm obliegenden Fristen wahren kann. Er hat den Auftraggeber unverzüglich unter Angabe der Gründe zu informieren, wenn er sich nicht in der Lage sieht, die verlangte Unterstützungshandlung zu erbringen.
2. Wenn ein Betroffener sich zur Ausübung der diesem aus Kapitel 3 der DSGVO zustehenden Rechte unmittelbar an den Auftragnehmer wenden sollte, wird der Auftragnehmer diesen an den Auftraggeber verweisen, soweit ihm die Zuordnung zu diesem möglich ist. Sollte ihm eine Zuordnung nicht möglich und der Auftragnehmer auch nicht als Verantwortlicher unmittelbar gegenüber dem Betroffenen aus Kapitel 3 der DSGVO verpflichtet sein, wird er ihn darüber informieren, dass er als Auftragsverarbeiter für Dritte tätig ist und er den Dritten hinsichtlich des Betroffenen nicht identifizieren kann. Sofern und soweit der Auftragnehmer gegenüber dem Betroffenen selbst als Verantwortlicher nach Kapitel 3 der DSGVO verpflichtet ist, obliegt die Erfüllung der entsprechenden Verpflichtungen alleine dem Auftragnehmer als Verantwortlichen.
3. Für die unter dieser Ziffer für den Auftraggeber zu erbringenden Leistungen steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu. Der Auftragnehmer darf die Erbringung der von ihm geschuldeten Leistungen nicht davon abhängig machen, dass der Auftraggeber eine bestimmte Vergütung anerkennt und/oder vorab leistet.

### **Kontrollrechte des Auftraggebers**

1. Dem Auftraggeber stehen alle Kontrollrechte, insbesondere Inspektionen, zu, die zur Wahrung der ihm nach den Vorgaben der DSGVO obliegenden Pflichten erforderlich sind. Das Kontrollrecht ist mit einer angemessenen Ankündigungsfrist und zu den üblichen Geschäftszeiten des Auftragnehmers auszuüben. Der Auftragnehmer ist zur Reduktion der Auswirkungen von Inspektionen auf seinen Geschäftsbetrieb berechtigt, diese mit denen anderer Auftraggeber zu verbinden, soweit dies dem Auftraggeber zumutbar ist (z. B. gemeinsame Inspektionstermine, die in angemessener Frist durchgeführt werden). Der Auftraggeber wird Sorge dafür tragen, dass Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers nicht unverhältnismäßig zu stören.
2. Der Auftraggeber ist berechtigt, die Ausübung der Kontrollrechte auf einen von diesem beauftragten Dritten zu übertragen. Sollte der Dritte in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, hat dieser gegen dessen Tätigkeit ein Einspruchsrecht.
3. Der Auftragnehmer hat an der Ausübung der Kontrollrechte im erforderlichen Umfang mitzuwirken. Er darf Kontrollen durch den Auftraggeber von der Unterzeichnung einer üblichen und angemessenen Verschwiegenheitserklärung abhängig machen, soweit dies zum Schutz seiner Geschäftsgeheimnisse nach den gesetzlichen Vorgaben erforderlich ist.
4. Für die unter dieser Ziffer zu erbringenden Leistungen steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu. Der Auftragnehmer darf die Erbringung der von ihm geschuldeten Leistungen nicht davon abhängig machen, dass der Auftraggeber eine bestimmte Vergütung anerkennt und/oder vorab leistet.

### **Maßnahmen von Aufsichtsbehörden**

1. Der Auftragnehmer informiert, soweit zulässig, den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen einer (Aufsichts-)Behörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt insbesondere, soweit eine Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Auftragsverarbeitung beim Auftragnehmer ermittelt.
2. Soweit der Auftraggeber seinerseits einer Kontrolle der (Aufsichts-)Behörde, 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 im erforderlichen Umfang zu unterstützen. Für die insoweit zu erbringenden Leistungen steht dem Auftragnehmer ein angemessenes, am Zeitaufwand orientiertes Entgelt zu, sofern und soweit er die entsprechende Kontrolle etc. nicht zu vertreten hat. Der Auftragnehmer darf die Erbringung der von ihm geschuldeten Leistungen nicht davon abhängig machen, dass der Auftraggeber eine bestimmte Vergütung anerkennt und/oder vorab leistet.

### **Unterauftragsverarbeiter**

1. Der Auftragnehmer setzt für die Verarbeitung die in der Anlage 3 benannten Unterauftragsverarbeiter ein.
2. Der Auftragnehmer wird den Auftraggeber in Textform über Änderungen an der Beauftragung von Unterauftragsverarbeitern informieren. Der Auftraggeber kann innerhalb einer Frist von zwei Wochen seit Zugang der Information der Änderung widersprechen. Der Widerspruch darf jedoch nicht willkürlich erfolgen. Der Auftragnehmer setzt die Änderung nicht vor Ablauf der Widerspruchsfrist um. Im Falle eines Widerspruchs ist der Auftragnehmer berechtigt, den Auftragsverarbeitungsvertrag mit einer Frist von mindestens

einem Monat zu kündigen, sofern die Änderung dem Auftraggeber zumutbar gewesen wäre und der Widerspruch dem Auftragnehmer unzumutbar ist. Zumutbarkeit für den Auftraggeber ist gegeben, wenn mit der Änderung keine Nachteile für ihn zu befürchten gewesen wären und insbesondere sichergestellt gewesen wäre, dass die Vorgaben dieses Vertrages und der DSGVO bei Umsetzung der Änderung weiter eingehalten worden wären.

3. Der Auftragnehmer wird für eventuelle Unterauftragsverarbeiter die in den Absätzen 2 und 4 des Art. 28 DSGVO genannten Bedingungen einhalten. Er hat ferner sicherzustellen, dass die sonst mit dem Auftraggeber insoweit getroffenen vertraglichen Vereinbarungen sowie die ggf. ergänzende Weisungen des Auftraggebers auch von den Auftragsverarbeitern eingehalten werden. Er hat dies dem Auftraggeber auf dessen Wunsch nachzuweisen.

### **Verstoß gegen datenschutzrechtliche Vorschriften, Vereinbarungen oder Weisungen**

1. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften, gegen die getroffenen Vereinbarungen und/oder die erteilten Weisungen unverzüglich, spätestens 24 Stunden nach erster Kenntnis, in Textform mitzuteilen.

2. Jegliche, etwaige erforderliche Meldung an eine Aufsichtsbehörde oder Information von Betroffenen obliegt allein dem Auftraggeber. Der Auftragnehmer wird hieran im erforderlichen Umfang mitwirken.

3. Der Auftragnehmer ist weiter verpflichtet, den Verstoß im erforderlichen Umfang unverzüglich aufzuklären und dem Auftraggeber eine entsprechende Dokumentation zu überlassen. Die Dokumentation hat eine Darstellung zu umfassen, welche Maßnahmen der Auftragnehmer ergriffen hat, um weitere Verstöße zu unterbinden und warum er der Auffassung ist, dass die ergriffenen Maßnahmen ausreichend sind, um den Vorgaben dieses Vertrages und der gesetzlichen Vorschriften zu genügen.

### **Vergütung des Auftragnehmers**

Dem Auftragnehmer steht für die von ihm unter diesem Vertrag erbrachten Leistungen kein gesondertes Entgelt zu, sofern nicht anders in diesem Vertrag vereinbart.

### **Haftung**

Die Haftung der Parteien richtet sich nach den Vereinbarungen des Hauptvertrages. Die unmittelbare Haftung der Parteien gegenüber einem Betroffenen aus gesetzlichen Bestimmungen des Datenschutzes bleibt unberührt.

### **Dauer des Vertrages**

Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages. Er kann isoliert vom Hauptvertrag nur aus wichtigem Grund gekündigt werden, es sei denn, dieser Vertrag oder zwingende gesetzliche Vorschriften bestimmt etwas Anderes.

### **Folgen der Vertragsbeendigung**

1. Der Auftragnehmer wird nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder einem strukturierten, gängigen und maschinenlesbaren Format zurückgeben und die vorhandenen Kopien löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Auftragnehmer unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Der Auftragnehmer hat die Durchführung der Löschung entsprechend den Vorgaben des Auftraggebers diesem zu bestätigen.
2. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren.
3. Jegliches Zurückbehaltungsrecht Auftragnehmers hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ist im Übrigen ausgeschlossen.

## **Anlage 1 – Kategorien personenbezogener Daten und Betroffener**

### **A. Stammdaten**

- Vor- und Nachname
- Anrede, Titel
- Geburtsdatum
- Geschlecht
- Staatsangehörigkeit
- Kundennummer / interne ID

### **B. Adress- und Kontaktdaten**

- Wohnadresse (Straße, Hausnummer, PLZ, Ort, Land)
- E-Mail-Adresse(n)
- Telefonnummer(n) (Festnetz, Mobil)
- ggf. Lieferadresse / Rechnungsadresse (falls abweichend)

### **C. Vertragsdaten**

- Vertragsnummer
- Vertragslaufzeit, Vertragsbeginn, Vertragsende
- Vertragsgegenstand
- Art der vertraglichen Leistung oder Dienstleistung
- Kommunikationsverlauf im Rahmen der Vertragserfüllung
- Kündigungsdaten oder -gründe

### **D. Zahlungs- und Abrechnungsdaten**

- Bankverbindung (IBAN, BIC, Kontoinhaber)
- Kreditkartendaten (soweit erforderlich und gespeichert)
- Rechnungsinformationen (Rechnungsnummern, Beträge, Fälligkeiten)
- Zahlungseingänge, Mahnstufen, Zahlungsverhalten
- ggf. SEPA-Mandatsinformationen

### **E. Nutzungsdaten (bei Online-Diensten oder IT-Systemen)**

- Logins, Nutzerkennungen, Passworthashes
- IP-Adressen, Gerätekennungen (z. B. MAC-Adresse)
- Zugriffsprotokolle, Logfiles
- Nutzungsverhalten auf Webseiten oder Plattformen
- Cookie-Informationen
- Standortdaten (sofern relevant und zulässig)

### **F. Kommunikationsdaten**

- E-Mail-Verkehr (soweit geschäftsrelevant)

- Telefonnotizen, Gesprächsprotokolle
- Inhalte von Kontaktformularen oder Supportanfragen
- Chatverläufe (z. B. in Kundenportalen oder Apps)

#### **G. Sonstige relevante Daten (je nach Verarbeitungskontext)**

- Beschwerdedaten, Feedback, Bewertungen
- Foto-/Videoaufnahmen (z. B. bei Veranstaltungen, mit Einwilligung)
- Mitarbeiterdaten (falls Personalverarbeitung erfolgt, siehe unten)

#### **2. Kategorien betroffener Personen**

Die personenbezogenen Daten betreffen insbesondere folgende Kategorien von Personen:

- Kunden (natürliche Personen)
- Mitarbeiter von Kunden oder Geschäftspartnern
- Interessenten und Leads
- Nutzer von Online-Diensten oder Plattformen
- Lieferanten und Dienstleister (sofern natürliche Personen oder Einzelunternehmer)
- Beschäftigte des Auftraggebers (nur falls Gegenstand der Verarbeitung)
- ggf. Teilnehmer an Veranstaltungen, Webinaren, Gewinnspielen etc.

## **Anlage 2 – Technische und organisatorische Maßnahmen**

### **Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

#### **1. Zutrittskontrolle**

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- Sicherheitstüren / -fenster
- Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- Alarmanlage
- Absicherung von Gebäudeschächten
- Videoüberwachung
- Mitarbeiter- und Berechtigungsausweise
- Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

#### **2. Zugangskontrolle**

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Autorisierungsprozess für Zugangsberechtigungen
- Begrenzung der befugten Benutzer
- BIOS-Passwörter
- Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- Personalisierte Chipkarten, Token, PIN-/TAN, etc.
- Protokollierung des Zugangs
- Zusätzlicher System-Log-In für bestimmte Anwendungen
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (z.B. passwortgeschützter Bildschirmschoner)

#### **3. Zugriffskontrolle**

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Verwaltung und Dokumentation von differenzierten Berechtigungen
- Abschluss von Verträgen zur Auftragsdatenverarbeitung für externe Wartung und Reparatur
- Auswertungen/Protokollierungen von Datenverarbeitungen
- Autorisierungsprozess für Berechtigungen
- Genehmigungsroutinen
- Profile/Rollen

- Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops
- Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger
- Mobile Device Management-System
- Vier-Augen-Prinzip
- Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- Nicht-reversible Löschung von Datenträgern
- Sichtschutzfolien für mobile Datenverarbeitungssysteme

#### **4. Trennungskontrolle**

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Speicherung der Datensätze in physikalisch getrennten Datenbanken
- Verarbeitung auf getrennten Systemen
- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- Mandantenfähigkeit von IT-Systemen
- Verwendung von Testdaten
- Trennung von Entwicklungs- und Produktionsumgebung

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

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

#### **Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

##### **1. Weitergabekontrolle**

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Verschlüsselung von Email bzw. Email-Anhängen
- Verschlüsselung des Speichermediums von Laptops
- Gesicherter File Transfer (z.B. sftp)
- Gesicherter Datentransport (z.B. SSL, ftps, TLS)
- Verschlüsselung von CD/DVD-ROM, externen Festplatten oder USB-Sticks
- Physikalische Transportsicherung
- Verpackungs- und Versandvorschriften
- Elektronische Signatur
- Gesichertes WLAN
- Fernwartungskonzept
- Mobile Device Management-System
- Data Loss Prevention (DLP)-System

- Regelung zum Umgang mit mobilen Speichermedien
- Protokollierung von Datenübertragung oder Datentransport
- Getunnelte Datenfernverbindungen (VPN)

## **2. Eingabekontrolle**

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Zugriffsrechte
- Systemseitige Protokollierungen
- Dokumenten Management System (DMS) mit Änderungshistorie
- Sicherheits-/Protokollierungssoftware
- Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- Mehraugenprinzip
- Data Loss Prevention (DLP)-System

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

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und stets verfügbar sind:

1. Sicherheitskonzept für Software- und IT-Anwendungen
2. Back-Up Verfahren
3. Aufbewahrungsprozess für Back-Ups
4. Gewährleistung der Datenspeicherung im gesicherten Netzwerk
5. Bedarfsgerechtes Einspielen von Sicherheits-Updates
6. Spiegeln von Festplatten
7. Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
8. Geeignete Archivierungsräumlichkeiten für Papierdokumente
9. Virenschutz
10. Notfallplan
11. Erfolgreiche Notfallübungen
12. Redundante, örtlich getrennte Datenaufbewahrung

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

### **1. Datenschutz-Management**

Folgende Maßnahmen sollen gewährleisten, dass eine datenschutzkonforme Organisation vorhanden ist:

- Interne Datenschutz-Richtlinie
- Richtlinien/Anweisungen zur Datensicherheit
- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten

- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich
- Externe Prüfung/Auditierung der Informationssicherheit

## **2. Incident-Response-Management**

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Meldeprozess für Datenschutzverletzungen gegenüber den Betroffenen (Art. 34 DSGVO)

### **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**

Die Default-Einstellungen sind bei den standardisierten Voreinstellungen von Systemen und Apps sowie bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen.

- Beispiele: Kennzeichnung von Eingabefeldern in Onlineformularen als Pflichtfelder, obwohl die Inhalte nicht notwendig sind.

### **Auftragskontrolle**

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur gemäß Weisungen verarbeitet werden:

1. Vereinbarung zur Auftragsverarbeitung mit Regelungen zu Rechten und Pflichten
2. Prozess zur Erteilung und/oder Befolgung von Weisungen
3. Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
4. Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
5. Schulungen aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
6. Unabhängige Auditierung der Weisungsgebundenheit
7. Verpflichtung der Mitarbeiter auf das Datengeheimnis
8. Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
9. Formalisiertes Auftragsmanagement
10. Dokumentiertes Verfahren zur Auswahl von Dienstleistern
11. Standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister

### **Anlage 3 – Unterauftragsverarbeiter**

Keine Vorhanden