**Vereinbarung über Auftragsverarbeitung zwischen**

**Karl Wörwag Lack- und Farbenfabrik GmbH & Co. KG**
**Strohgäustraße 28, 70435 Stuttgart**

- Auftraggeber -

**und**

**LIEFERANT**

- Auftragsverarbeiter -

## Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsdatenverarbeitungsverhältnis gemäß Art. 28 EU-DSGVO eingegangen bzw. erfolgt die in der Leistungsvereinbarung niedergelegte Verarbeitung der Daten im Auftrag des Verantwortlichen (sog. Auftragsverarbeitung). Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

## 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Verantwortliche (Art. 4 Nr. 7 DSGVO) zuständig ist.

## 2 Begriffsbestimmung

2.1 Diese Vereinbarung bezieht sich nur auf die Verarbeitung personenbezogener Daten nach den vom Verantwortlichen vorgegebenen Weisungen.

2.2 Verarbeitung meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

2.3 Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung

wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2.4 Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

2.5 Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (z.B. Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragsverarbeiters mit personenbezogenen Daten gerichtete Anordnung des Verantwortlichen. Bestehende Weisungen (z.B. durch diese Vertragsergänzung) können vom Verantwortlichen danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

## 3 Konkretisierung des Auftragsinhalts

3.1 Der Gegenstand und die Dauer der Auftragsdatenverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten sind in der Leistungsvereinbarung niedergelegt.

3.2 Die Art der verwendeten personenbezogenen Daten ist im **Anhang 2** („Konkretisierung der Datenkategorien“) konkret beschrieben.

3.3 Der Kreis der durch den Umgang mit den personenbezogenen Daten Betroffenen ist im **Anhang 3** („Genehmigte Subunternehmer“) konkret beschrieben.

## 4 Verantwortlichkeit und Weisungsbefugnis

4.1 Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen (Art. 28 Abs. 3 lit. g DSGVO) soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Soweit ein Betroffener sich zwecks Löschung oder Berichtigung seiner Daten unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortliche weiterleiten und anhand der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Erfüllung unterstützen (Art. 28 Abs. 3 lit. f DSGVO).

4.2 Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der dokumentierten Weisungen des Verantwortlichen verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen unverzüglich diese rechtlichen Anforderungen vor der Verarbeitung mit. Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit personenbezogenen Daten gerichtete schriftliche Anordnung des Verantwortlichen. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortliche danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Art. 28 Abs. 3 lit. a DSGVO).

4.3 Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich entsprechend Art. 28 Abs. 3 DSGVO zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche

Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Verantwortlichen bestätigt oder geändert wird.

4.4 Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Etwas anderes gilt nur bei Regelung im Vertrag oder in den in Ziffer 4.2 dieser Vereinbarung genannten Fällen.

4.5 Der Verantwortliche führt das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten zur Verfügung.

4.6 Die Verarbeitung und Nutzung der Daten im Auftrag des Verantwortlichen findet ausschließlich innerhalb der Europäischen Union oder dem Europäischen Wirtschaftraum statt. Eine Verlagerung in einen Staat außerhalb des Hoheitsgebiets der Bundesrepublik Deutschland bedarf der vorherigen Zustimmung des Verantwortlichen. Dies gilt nicht für mit dem Auftragsverarbeiter gemäß § 15 des deutschen Aktiengesetzes verbundene Unternehmen, sofern Binding Corporate Rules oder EU-Standardvertragsklauseln mit diesen Unternehmen vereinbart wurden. Die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO bleiben auch für andere Fälle unberührt.

4.7 Eine Verarbeitung von personenbezogenen Daten in Privatwohnungen der Mitarbeiter des Auftragsverarbeiters (Telearbeitsplätze, Heimarbeitsplätze) ist nur unter folgenden Voraussetzungen zulässig: Es handelt sich um Hardware des Auftragsverarbeiters, die den Mitarbeitern für dienstliche Zwecke überlassen worden ist und hinter einer Firewall betrieben wird sowie mit einem VPN-Client-Zertifikat gesichert ist. Zugriffe von eigener Hardware der Mitarbeiter sind in keinem Fall gestattet.

## 5 Verantwortliche Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

5.1 Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragsverarbeiter gemäß Art 28 Abs. 3, Art. 30 DSGVO die nachfolgenden gesetzlichen Pflichten.

5.2 Der Auftragsverarbeiter stellt sicher, dass die mit der Verarbeitung der Daten des Verantwortlichen befassten Mitarbeiter gemäß Art. 5 I c) DSGVO verpflichtet und in die Schutzbestimmungen des Datenschutzrechts eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

5.3 Der Auftragsverarbeiter hat nach Maßgabe des Art. 37 DSGVO einen betrieblichen Datenschutzbeauftragten bestellt, der seine Tätigkeit gemäß §§ Art. 38 und Art 39 DSGVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

5.4 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden nach Art. 58 DSGVO oder falls eine Aufsichtsbehörde nach Art. 83 DSGVO bei dem Auftragsverarbeiter ermittelt. Darüber hinaus teilt der Auftragsverarbeiter dem Verantwortlichen unverzüglich mit, wenn er wegen eines Verstoßes gegen die DSGVO auf Schadensersatz verklagt wird und informiert ihn sodann in regelmäßigen Abständen über das laufende Verfahren.

5.5 Der Auftragsverarbeiter verpflichtet sich mit Inkrafttreten der DSGVO zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten, die alle Kategorien zu den im Auftrag durchgeführten Tätigkeiten der Verarbeitung (Art. 30 Abs. 2 DSGVO) beinhaltet. Dieses Verzeichnis enthält mindestens

(a) den Namen und die Kontaktdaten des Auftragsverarbeiters und jedes verantwortlichen Mitarbeiters des Verantwortlichen in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

(b) die Kategorien von Verarbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden;

(c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

(d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO.

Der Auftragsverarbeiter gewährt dem Verantwortlichen auf Anfrage binnen 14 Tagen nach schriftlicher Aufforderung Einsicht in die diese Verarbeitung betreffenden Informationen des Verzeichnisses.

## 6 Sicherheit der Verarbeitung und deren Kontrolle

6.1 Die Vertragsparteien vereinbaren die in dem **Anhang 1** „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO bzw. § 22 BDSG 2018, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Der Anhang ist Gegenstand dieser Vereinbarung.

6.2 Technische und organisatorische Maßnahmen berücksichtigen zum Zeitpunkt des Abschlusses dieser Vereinbarung den Stand der Technik und unterliegen jeweils dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technische und organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6.3 Der Auftragsverarbeiter verpflichtet sich, die konkreten technischen und organisatorischen Maßnahmen auf deren Wirksamkeit im Hinblick auf die Sicherheit der Verarbeitung in regelmäßigen Abständen zu überprüfen, zu bewerten und diese Risikobewertung zu dokumentieren.

6.4 Der Auftragsverarbeiter wird dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Aufgrund der Kontrollverpflichtung des Verantwortlichen gemäß Art. 28 Abs. 1, Abs. 3 DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragsverarbeiter sicher, dass sich der Verantwortliche von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragsverarbeiter dem Verantwortlichen auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art: 32 Abs. 1 sowie die Durchführung der regelmäßig durchgeführten Risikobewertung gemäß Ziffer 6.3 nach. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats oder von Berichten unabhängiger

Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz, ISO 27001) erbracht werden.

6.5 Der Verantwortliche kann sich zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen (Art. 28 Abs.3 lit. h DSGVO).

## 7 Mitteilung bei Verstößen durch den Auftragsverarbeiter

7.1 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich nach Feststellung schwerwiegender Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen (Art. 28 Abs. 3 Satz 3, Art. 33, Art 34 DSGVO). Dabei hat die Unterrichtung mindestens folgenden Inhalt:

(a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

(b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

(c) eine Beschreibung der bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Können nicht alle in Ziffer 7.1. lit. a – lit. c genannten Informationen zum Zeitpunkt der Unterrichtung zur Verfügung gestellt werden, so sind die Informationen unverzüglich nach Kenntnis, ggf. schrittweise zur Verfügung zu stellen.

7.2 Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

## 8 Löschung und Rückgabe von Daten

8.1 Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

8.2 Nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Verjährung der Ansprüche aus der zugrundeliegenden Leistungsvereinbarung hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten (Art. 28 Abs. 3 lit. g DSGVO ). Gleiches gilt für Test- und Ausschussmaterial. Eine Dokumentation über die Sicherstellung ordnungsgemäßer Löschung sowie ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

8.3 Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Verjährungs- bzw. Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

## 9 Subunternehmer

9.1 Der Auftragsverarbeiter beauftragt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte schriftliche Genehmigung des Verantwortlichen und verpflichtet sich nur Subunternehmer unter Beachtung der nachstehenden Voraussetzungen einzusetzen:

(a) Der Auftragsverarbeiter wählt den Subunternehmer sorgfältig aus und prüft vor der Beauftragung, dass dieser die zwischen Verantwortlichem und Auftragsverarbeiter getroffenen Vereinbarungen einhalten kann. Der Auftragsverarbeiter hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach Art. 32 Abs. 1 DSGVO geeigneten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragsverarbeiter zu dokumentieren. Der Auftragsverarbeiter ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser, sofern gesetzlich gefordert, einen betrieblichen Datenschutzbeauftragten i.S.d. Art. 37 DSGVO bestellt hat.

(b) Der Auftragsverarbeiter gestaltet die vertraglichen Vereinbarungen mit dem / den Subunternehmer/n so, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Verantwortlichem und Auftragsverarbeiter entsprechen.

9.2 Nicht als Subunternehmer im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

9.3 Zum Zeitpunkt der Vertragsunterzeichnung beauftragte Subunternehmer werden in **Anhang 3** („Genehmigte Subunternehmer“) einschließlich der Verarbeitungsstandorte und der Art der Dienstleistung dokumentiert. Die in dieser Liste genannten Subunternehmer gelten als von Anfang an rechtmäßig beauftragt im Sinne von Ziffer 9 Abs. 1, sofern die Umsetzung der dort genannten Voraussetzungen durch den Auftragsverarbeiter gewährleistet wird.

9.4 Ein Zugriff auf Daten darf durch den Subunternehmer erst dann erfolgen, wenn auch der Subunternehmer die Pflichten des Auftragsverarbeiters aus diesem Vertrag erfüllt bzw. dies gegenüber dem Auftragsverarbeiter zugesichert hat und der Auftragsverarbeiter die Einhaltung dieser Pflichten durch den Subunternehmer regelmäßig überprüft.

## 10 Nebenleistungen

Die Ziffern 1 bis 8 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

## 11 Vertraulichkeit und Datenschutzkontrolle

11.1Der Verantwortliche und der Auftragsverarbeiter verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen vertraulich zu behandeln. Dies gilt für den in der Leistungsvereinbarung vereinbarten Zeitraum und auch über die Beendigung der Einzelaufträge bzw. der Geschäftsbeziehung hinaus.

11.2Der Auftragsverarbeiter verpflichtet sich, dem betrieblichen Datenschutzbeauftragten des Verantwortlichen zur Erfüllung seiner jeweiligen gesetzlichen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren.

## 12 Schlussbestimmungen

12.1Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Das Schriftformerfordernis gilt nicht, soweit dieses zwischen den Vertragsparteien aufgrund einer ausdrücklichen und individuellen Vereinbarung aufgehoben wird.

12.2Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

**Anhang 1** „Technische und organisatorische Maßnahmen“

**Anhang 2** „Konkretisierung Datenarten, Datenkategorien

**Anhang 3** „Genehmigte Subunternehmer“

**Anhang 1 zur Vereinbarung über Auftragsverarbeitung**

A. Technisch-Organisatorische Maßnahmen nach Art. 32 Abs. 1 a-d EU-DSGVO

1. Pseudonymisierung (Art. 32 Abs. 1 lit. a EU-DSGVO)
Daten, die nur zu statistischen Zwecken ausgewertet werden sollen, werden pseudonymisiert und ohne Personenbezug gespeichert. Daten, die an Subunternehmer weitergegeben werden sollen, werden, soweit möglich, pseudonymisiert und sind dann für den Subunternehmer gemäß EuGH-Urteil vom 19.10.2016 (C 582/2014) keine personenbezogenen Daten.

2. Verschlüsselung (Art. 32 Abs. 1 lit. a EU-DSGVO)
Personenbezogene Daten werden auf mobilen Datenträgern und mobilen Geräten ausschließlich verschlüsselt gespeichert. Ein Zugriff auf die im Rechenzentrum gespeicherten Daten ist ausschließlich über verschlüsselte Verbindungen möglich. Daten werden ausschließlich stark verschlüsselt nach der BSI-Richtlinie TR-2102 übertragen.

3. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)
Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern. Die Berechtigungen werden über ein rollenbasiertes Rechtekonzept verwaltet. Jeder Mitarbeiter hat einen eigenen Zugang zu den DV-Systeme der mit Kennwortschutz abgesichert ist. Das Kennwort muss zwingend aus einer Mischung von Zahlen, Buchstaben und Sonderzeichen bestehen sowie eine Mindestlänge von acht Zeichen aufweisen. Die einzelnen DV-Systeme werden in Pausenzeiten gesperrt. Die Sperrung ist nur mit Kennwort wiederaufhebbar. Berechtigungen werden regelmäßig auf Aktualität überprüft. Es wird durch zahlreiche Maßnahmen sichergestellt, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (z.B. durch Mandantenfähigkeit und Berechtigungskonzept). Der Zutritt zu Räumen, in denen Datenverarbeitung stattfindet, wird kontrolliert und Unbefugten verwehrt. Die Büroräume sind durch ein Schließsystem gesichert, Besucher müssen sich mit Anwesenheitszeiten in eine Liste eintragen. Die Räume des Rechenzentrums werden durch ein elektronisches Zugangssystem mit dokumentierten Berechtigungen gesichert, ein Aufenthalt von nicht autorisierten Personen im Rechenzentrum ist nur für Fälle der Wartung und nur in Begleitung einer autorisierten Person zulässig. Die Anwesenheitszeiten im Rechenzentrum werden elektronisch protokolliert. Auftragsverarbeiter werden nur dann mit der Verarbeitung von personenbezogenen Daten beauftragt, wenn gleichwertige technisch-organisatorische Maßnahmen gewährleistet sind. Personenbezogene Daten werden, soweit es sich nicht um Auftragsverarbeiter handelt, nur nach Weisung des Verantwortlichen oder auf gesetzlicher Grundlage weitergegeben.

4. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b EU-DSGVO)
Es werden nur eingeschränkte Schreibberechtigungen auf Daten eingeräumt, es finden regelmäßig Integritätsprüfungen statt. Es werden regelmäßig Sicherheitsprüfungen wie z.B. Penetrationstests statt.

5. Gewährleistung der Verfügbarkeit (Art. 32 Abs. 1 lit. b EU-DSGVO)
Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Grundsätzlich werden alle Daten redundant gespeichert (mindestens über ausfallsichere RAID-Systeme Level 5 oder 6). Es werden vollständige mehrfach redundante Datensicherungen und/oder Replikationen erstellt, die außerhalb des Gebäudes der Originaldaten gespeichert werden. Es existieren zur Sicherung der Verfügbarkeit eine unterbrechungsfreie Stromversorgung, eine Firewall und aktueller Virenschutz.

6. Gewährleistung der Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b EU-DSGVO)
Die Belastbarkeit der Kommunikationsverbindungen und der Rechenkapazität wird durch laufende Überwachung der Auslastung sichergestellt.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall (Art. 32 Abs. 1 lit. c EU-DSGVO)
Es finden regelmäßig Tests zur Rücksicherung von Backup-Daten statt, durch redundante Speicherung an verschiedenen Standorten wird versucht, Ausfallzeiten zu minimieren

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d EU-DSGVO)
Es besteht ein IT-Sicherheits- und Datenschutzkonzept, das laufend auf Anpassungsbedarf überprüft wird. Änderungen werden dokumentiert und in regelmäßigen Abständen auf ihre Wirksamkeit überprüft

B. Zusätzliche technisch-organisatorische Maßnahmen für den Fall der Verarbeitung sensibler Daten nach § 22 Abs. 2 BDSG 2018:

Die Mitarbeiter werden regelmäßig im Bereich des Datenschutzes über den aktuellen Stand unterrichtet. Es ist ein Datenschutzbeauftragter bestellt.

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen werden bei der Verarbeitung sensibler Daten nach Art. 9 Abs. 1 der EU-DSGVO folgende weitere Sicherheitsmaßnahmen im Rahmen der Verhältnismäßigkeit umgesetzt:

S1. Eingabekontrolle (§ 22 Abs. 2 Nr. 2 BDSG 2018)

Die Eingabe, Veränderung und Löschung von sensiblen personenbezogenen Daten wird mit Angabe einer individualisierbaren Bearbeiterkennung protokolliert.

S2. Beschränkung des Zugangs zu personenbezogenen Daten (§ 22 Abs. 2 Nr. 5 BDSG 2018)

Personenbezogene Daten sind gegen Zugriffe von Mitarbeitern des Verantwortlichen bzw. des Auftragsverarbeiters gesperrt, die nach dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) der EU-DSGVO für die rechtmäßige Verarbeitung der Daten keinen Zugriff benötigen. Dafür wird ein rollen- und gruppenbasiertes Berechtigungskonzept eingesetzt (vgl. oben auch A Nr. 3 und Nr. 8)

S3. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen

Bei besonderen Datenschutzanforderungen durch branchenspezifische gesetzliche, satzungsmäßige oder vertragliche Regelungen werden die Schutzmaßnahmen mit dem Verantwortlichen im Einzelfall besprochen und an das jeweils notwendige Schutzniveau angepasst. Dazu kann auch die Einhaltung von bestimmten Datenschutz- und Datensicherheitsnormen und -standards gehören (ISO 27001, BSI Grundschutzstandards 200-1 bis 200-3, Sicherheitsüberprüfungsgesetz, Schutzklasseneinteilungen von Dokumenten im öffentlichen Dienst etc.)

Die übrigen Punkte des § 22 Abs. 2 BDSG werden bereits durch die Vorschriften der Verordnung (siehe oben A Nr. 1 bis 8) abgedeckt.

**Anhang 2 zur Vereinbarung über Auftragsverarbeitung**

Konkretisierung der Datenarten, der Datenkategorien und der von der Verarbeitung Betroffenen

1. Konkretisierung der Datenarten und Datenkategorien:
- Kundenstammdaten (z.B. Kundenkontaktdaten, Anschriften, etc.)
- Referenzdaten (z.B. Zahlungs- und Lieferbedingungen, Bankverbindungen, etc.)
- Unternehmensweite Strukturdaten (z.B. Produkte, Services, Zuständigkeiten der Mitarbeiter, etc.)
- Transaktionsdaten (z.B. Geschäftsaktivität, etc.)

2. Konkretisierung der von der Verarbeitung Betroffenen:
- Kunden und deren Mitarbeiter (Ansprechpartner)

**Anhang 3 zur Vereinbarung über Auftragsverarbeitung**

Genehmigte Subunternehmer