Vereinbarung
zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem/der

Rainer Bothe Malerbetrieb GmbH, Herrn Thilo Bothe, Radauberg 19, 38667 Bad Harzburg

- Verantwortlichen - nachstehend Auftraggeber genannt -

und dem/der

Sander + Partner GmbH, Emmericher Weg 12, 47574 Goch

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem gem. Art. 28 DS-GVO erforderlichen Mindestinhalt von Verträgen über die Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf sämtliche Tätigkeiten, bei denen der Auftragnehmer oder durch ihn beauftragte und vom Auftraggeber zuvor genehmigte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten oder mit diesen in Berührung kommen könnten.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

- ☐ Der Gegenstand des Auftrags ergibt sich aus dem Support-und Softwarepflegevertrag, sowie ggf. aus dem mobilen Zeiterfassungsvertrag auf den hier verwiesen wird.

(2) Dauer

- ☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Support-und Softwarepflegevertrages und ggf. dem mobilen Zeiterfassungsvertrag.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

- ☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Support-und Softwarepflegevertrag und ggf. dem mobilen Zeiterfassungsvertrag.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

☐ Gegenstand der Verarbeitung personenbezogener Daten können je nach Inhalt der konkreten Anfrage und je nach abgeschlossenem Vertrag folgende Datenarten/-kategorien sein:

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Zeiterfassungsdaten (bei aktivem Zeiterfassungsvertrag)
- ☐ Aktivierungsdaten
- ☐ Optional: GPS-Daten (Auf die Einstellungsmöglichkeit im WinWorker wird verwiesen) Verarbeitung erfolgt nur bei aktiver Einstellungsoption des Auftraggebers

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Ansprechpartner
- ☐ Geschäftspartner des Auftraggebers
- ☐ Mitarbeiter des Auftraggebers

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung, zu dokumentieren und dem Auftraggeber auf Anforderung zur Prüfung vorzulegen. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

4. Auskunft, Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Dasselbe gilt für Auskünfte an Dritte oder den Betroffenen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden.

(4) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO angemessen zu unterstützen.

(5) Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn ihm Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers bekannt werden.

(6) Der Auftragnehmer wird ohne die vorherige schriftliche Zustimmung des Auftraggebers keine Einreichungen, Mitteilungen, Meldungen, Pressemitteilungen oder Berichte zu irgendeinem Datenschutzvorfall freigeben oder veröffentlichen, sofern der Auftragnehmer hierzu nach geltendem Recht nicht verpflichtet ist. Im letztgenannten Fall wird der Auftragnehmer den Verantwortlichen innerhalb einer angemessenen Frist schriftlich hierüber in Kenntnis setzen.

(7) Der Auftragnehmer hat einen Datenschutzbeauftragten schriftlich bestellt, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(8) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

(2) Werden Unterauftragnehmer durch den Auftragnehmer eingeschaltet, sind die vertraglichen Vereinbarungen so zu gestalten, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen dem Auftraggeber und dem Auftragnehmer entsprechen.

(3) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.

a) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Hetzner Online GmbH	Industriestr.25, 91710 Gunzenhausen	Speicherung von Zeiterfassungsdaten , Aktivierungsdaten, sowie optional GPS-Daten

b) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
   - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
   - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
   - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform) sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber und weitere Unterstützungsleistungen kann der Auftragnehmer einen Vergütungsanspruch geltend machen. Der tatsächlich anfallende Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

8. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzes, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ i.S.d. Art. 4 Nr. 7 DS-GVO). Hinsichtlich der dieser Vereinbarung zugrundeliegenden Auftragsdatenverarbeitung ist der Auftraggeber dem Auftragnehmer gegenüber weisungsbefugt.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Hauptvertrag/in der Leistungsvereinbarung bereits vereinbart.

(3) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

10. Haftung

Eine zwischen den Parteien im Hauptvertrag/in der Leistungsvereinbarung vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart ist.

11. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Goch, den 16. Mai 2018

_____

- Auftragnehmer –

Anlage – Technisch-organisatorische Maßnahmen

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

Zutrittskontrolle

Die Zutrittskontrolle verhindert den unbefugten Zutritt zu den Firmenbereichen und den Außenanlagen des Unternehmens und regelt innerhalb des Unternehmens den Schutz besonders sensibler Bereiche.

Zutrittskontrollsystem

Der Zutritt zu den einzelnen Bereichen des Firmengebäudes wird durch ein elektronisches Zutrittskontrollsystem gesichert und kontrolliert. Alle Zugangstüren zum Gebäude sind grundsätzlich verschlossen. Besucher nutzen die Klingel am Haupteingang. Die Türöffnung erfolgt manuell durch einen Mitarbeiter. Ein unbefugter oder unbemerkter Zugang zum Geschäftsbereich ist damit ausgeschlossen. Der Zugang für Mitarbeiter wird über Fingerprints geregelt. Jeder Funktionsbereich ist ebenfalls durch Fingerprints gesichert. Es befinden sich keine Schlüssel bei betriebsfremden Personen. Alle berechtigten Schlüsselinhaber werden in einer Schlüsselliste geführt. Alle Schlüsselinhaber haben eine Belehrung zur Aufbewahrung erhalten. Die Reinigung der Büroräume erfolgt während der Geschäftszeiten durch eine fest angestellte Mitarbeiterin. Der Innenbereich ist in Sicherheitszonen gegliedert, für die zeitlich begrenzt unterschiedliche Berechtigungen eingerichtet sind. Derartige Sicherheitszonen sind insbesondere Archive und der IT-Bereich und innerhalb des IT-Bereichs mit zusätzlichen Einschränkungen das Rechenzentrum. Jeder Mitarbeiter erhält einen Zugangscode, der einer Gruppe zugeordnet ist, die den Bereich und die Zugangszeiten genau regelt. Das Zutrittskontrollsystem zeichnet auf, wann eine bestimmte Person eine Sicherheitszone betritt, nicht aber, wenn die Sicherheitszone wieder verlassen wird. Wird außerhalb der zugelassenen Zeitzonen ein Zutritt zu den gesicherten Bereichen erforderlich, wird auf Antrag gegen Nachweis eine entsprechende Zutrittsberechtigung vergeben.

Es ist ein zentraler Empfang eingerichtet, der den Zutritt von betriebsfremden Personen kontrolliert. Innerhalb des Firmenbereichs werden Besucher geführt. Jeder Mitarbeiter ist für seine Besucher verantwortlich.

Nebenausgänge, Fluchttüren und sonstige Notausgänge können von außen nicht geöffnet werden und werden gesondert überwacht.

Sicherheitsmaßnahmen:

Die Außentüren sind einbruchsicher und mit doppelten Schließzylindern ausgestattet, die Schließzylinder sind aufbohr- und ausziehsicher. Schlüsselkopien können nur unter Vorlage des Sicherheitszertifikates beim Hersteller erzeugt werden. Das Zertifikat befindet sich bei der Geschäftsleitung. Das eingezäunte Grundstück wird 24 Stunden videoüberwacht. Im Gebäude sind verknüpfte Rauchmelder installiert, die einen Innenalarm auslösen. Die Server befinden sich in einem unterirdischen sowie gesicherten und videoüberwachten Raum mit abgeschlossenen Serverschränken und sind nur einem autorisierten Personenkreis zugänglich.

Videoüberwachung

Zusätzlich zum Zutrittskontrollsystem besteht eine Videoüberwachungsanlage. Mit der Videoüberwachungsanlage werden folgende Bereiche überwacht:

- Haupteingang
- Ausgänge
- Lieferbereiche
- Innenbereiche (Lager, Notausgänge, Treppenhaus)

Die Kameras sind in den Ausgangsbereichen so montiert und ausgerichtet, dass sie nur Firmenbereiche überwachen. Öffentliche Bereiche im Vorfeld werden nicht überwacht. Die Kameras sind nicht schwenkbar. Die Aufnahmen werden aufgezeichnet und manuell nach Auffälligkeiten, die z.B. auf einen Diebstahl hinweisen könnten, ausgewertet. Zweifelhafte Vorgänge werden mit den betroffenen Personen besprochen und aufgeklärt.

Die Aufnahmen werden in einem sich selbst überschreibenden Speicher nach dem Prinzip „First in – First out“ gespeichert. Die Speicherdauer beträgt 10 Tage.

Standorte, Art der Kameras und Kameraaufstellung, Aufnahmebereiche sowie Einzelheiten des Betriebs sind im Installationsplan, und Fragen der Speicherung von Aufzeichnungen sowie deren Nutzungen, Speicherdauer, die Beteiligung der Mitarbeitervertretung und die Information der Betroffenen über eventuelle Auswertungen zu ihrer Person sind in den IT-Sicherheitsrichtlinien geregelt.

Zugangskontrolle

Die Zugangskontrolle verhindert, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können. Der Zugang zu den Datenverarbeitungssystemen ist mit Benutzerkennung und einem sicheren Passwort geschützt.

Es sind Passwortregeln zur Bildung eines sicheren Passworts festgelegt. Die Einhaltung der Passwörter wird automatisiert kontrolliert. Die Regelungen hierzu befinden sich in den IT-Sicherheitsrichtlinien.

Die Systemnutzung ist hierarchisch aufgebaut. Jede Anmeldung erfolgt über eine individuelle und geheime Anmeldung mit Name und verschiedenen Passwörtern. Die Passwörter sind geheim und werden an keiner Stelle im Klartext gespeichert. Jeder Nutzer hat die Möglichkeit sein Passwort in einzelnen Systembereichen und Anwendungsprogrammen selbst zu ändern. Die Mitarbeiter werden regelmäßig im Rahmen einer Unterweisung über die Notwendigkeit der Passwortkonventionen unterrichtet und sich gezwungen, diese auch anzuwenden. Alle Passwörter bestehen aus Großbuchstaben, Kleinbuchstaben, Zahlen und/oder einem Sonderzeichen.

Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Auf allen Servern, Workstations und Notebooks wird zum Schutz gegen Schadsoftware eine professionelle Antivirensoftware eingesetzt. Die Signaturdateien werden automatisch aktualisiert. Veraltete Signaturen werden mit einem Warnhinweis angezeigt. Erkannte Malware wird gelöscht oder in Quarantäne gesetzt. Zudem wird der Vorfall per E-Mail und auf der Admin-Konsole gemeldet. Eingehende E-Mails werden vorher auf Schadsoftware überprüft. Die EDV wird durch eigene Techniker regelmäßig gewartet und Updates eingespielt. Arbeiten an den Servern werden protokolliert.

In den Datenverarbeitungssystemen sind rollenbasierte Berechtigungsprofile hinterlegt, in denen die zugriffsberechtigten Personen festgelegt und ihre Rechte hinterlegt sind. Die Rechte werden in einem geregelten Verfahren vergeben, und die Notwendigkeit der bestehenden Rechte wird regelmäßig kontrolliert.

Trennungsgebot

Das Trennungsgebot gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die Trennung der Datenverarbeitung erfolgt je nach Verfahren auf Betriebssystem- oder Anwendungsebene. Test- und Produktionsdaten sind ebenfalls voneinander getrennt. Nähere Informationen enthalten die Erhebung zu den technischen und organisatorischen Maßnahmen für das Verfahrensverzeichnis und die Rechenzentrumsrichtlinien.

Die Netzwerke der Sander + Partner GmbH sind in Funktionsbereiche unterteilt und getrennt. Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert. Datensicherungen erfolgen ebenfalls auf logisch und/oder physikalisch getrennten Systemen. Die zweckgebundenen Benutzerrechte werden zentralisiert durch die Gruppe der Administratoren vergeben und protokolliert. Zudem werden die Zugriffsmöglichkeiten in der betriebseigenen WinWorker Software durch eine Rechteverwaltung vergeben.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Soweit technisch möglich, wird bei der Auftragsdurchführung eine Pseudonymisierung durchgeführt.

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

Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Die personenbezogenen und sonstigen vertraulichen Daten sind auf unterschiedliche Weise gegen unbefugten Zugriff und gegen unbefugtes Kopieren geschützt. Für die Speicherung auf mobilen Datenträgern dürfen nur zugelassene und kontrollierte Datenträger verwendet werden. Personenbezogene und vertrauliche Daten müssen auf mobilen Datenträgern verschlüsselt werden. Eine elektronische Übertragung geschieht nur verschlüsselt und über sichere Leitungen mit einer zuverlässigen Identifizierung und Authentifizierung der Empfänger.

Personenbezogene Daten verbleiben ausschließlich auf den internen Servern der Sander + Partner GmbH. Es findet kein physischer Transport dieser Daten statt. Alle System- und Funktionsbereiche sind in separate Netzwerke untergliedert. Externe Zugriffe sind nur über VPN möglich und werden protokolliert.

Schutz vertraulicher Informationen

Der Schutz der vertraulichen Informationen ist in einer Vertraulichkeitsrichtlinie geregelt. Vertrauliche Informationen sind insbesondere:

- Geschäftsplanung
- Personal- und Mitarbeiterdaten sowie alle sonstigen personenbezogenen Daten über Kunden, Lieferanten, Geschäftspartner etc.
- Preise und Angebote
- Rechtsangelegenheiten und Rechtsdaten
- Budget- und Finanzdaten
- Lizenzierte und „copyright“-geschützte Informationen
- Sicherheitsbezogene Informationen
- Alle Informationen mit Vertraulichkeitsvermerken

Am Arbeitsplatz gilt das Prinzip des aufgeräumten Schreibtischs (Clean-Desk-Prinzip), d.h. jeder ist verpflichtet und dafür verantwortlich, personenbezogene Daten und vertrauliche Informationen und Datenträger mit entsprechenden Daten in seinem Bereich insbesondere bei Abwesenheit und nach Geschäftsschluss sicher und ordnungsgemäß aufzubewahren (in verschlossenen Schränken und Schreibtischen, passwortgesichertem PC etc.).

Bei einer Vernichtung vertraulicher Unterlagen ist wie folgt zu verfahren:

Vertrauliche Unterlagen werden in Aktenvernichtern vernichtet.

Vertrauliche Unterlagen sind nur nach dem in den IT-Sicherheitsrichtlinien beschriebenen Verfahren zu vernichten und dürfen nicht in die Papierkörbe an den Arbeitsplätzen gegeben werden. Sowohl bei der externen Entsorgung als auch bei der internen Vernichtung ist die Sicherheitsstufe 3 nach DIN 32757-1 einzuhalten.

An den Arbeitsplätzen zu entsorgende oder nicht mehr lesbare Magnetdatenträger, z.B. Disketten, CDs, DVDs, USB-Sticks u.a. werden unverzüglich von jedem Mitarbeiter selbst sicher vernichtet. Das Verfahren ist in den IT-Sicherheitsrichtlinien geregelt.

Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabe oder Veränderung von personenbezogenen Daten werden nach den sich aus der Schutzstufe und den Schutzzielen ergebenden Anforderungen protokolliert. Veränderungen an personenbezogenen Daten können nur über die betriebsinterne WinWorker Software oder der Administrationskonsole des zentralen Microsoft SQL Server vorgenommen werden. Darüber hinaus gibt es keine weitere händische Möglichkeit, die Daten zu verändern oder zu löschen. Veränderungen an Kundendatensätzen in der WinWorker Software werden geloggt. Dieser Zugriff ist nur einer bestimmten Anwendergruppe möglich und wird durch die Rechteverwaltung eingeschränkt. Der Zugriff auf die passwortgeschützte Konsole des Microsoft SQL Servers ist nur einer bestimmten Personengruppe möglich. Jede händische Aktion an der Microsoft SQL Datenbank wird im Transaktionslog festgehalten.

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

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, dazu gehören Maßnahmen zur Sicherung der Anlagen ebenso wie zur Sicherung der Daten. Die Anforderungen an die Verfügbarkeit der einzelnen Datenverarbeitungsverfahren und der Daten ist von den verantwortlichen Fachbereichen festzulegen und in den Schutzeinstufungen zu dokumentieren. Zur Gewährleistung einer zeitgerechten Wiederherstellung der Verfügbarkeit sind dem Stand der Technik entsprechende Sicherungstechnologien eingerichtet. Für die Datenverarbeitungsverfahren mit einem erhöhten Verfügbarkeitsanspruch besteht ein Notfallhandbuch. Einzelheiten sind im Notfallhandbuch beschrieben.

Aufbewahrungsfristen

Aufbewahrungspflichtige Unterlagen werden nach Ablauf der Aufbewahrungsfrist datenschutzgerecht vernichtet und entsorgt. Soweit für relevante Unterlagen eine Aufbewahrungsfrist gesetzlich nicht festgelegt wurde, ist diese im Verfahrensverzeichnis bzw. in den Aufbewahrungsrichtlinien gesondert geregelt. Ansonsten gilt die Aufbewahrungsfrist für Geschäfts- bzw. Handelsunterlagen von sechs Jahren.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

Bei den getroffenen Maßnahmen zur Datenwiederherstellung in Form eines Backup- & Recoverykonzepts wird eine rasche Wiederherstellbarkeit in der Folge eines physischen oder technischen Zwischenfalls berücksichtigt und angemessen sichergestellt.

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

Datenschutz-Management

Der Auftragnehmer hat umfangreiche Maßnahmen zum Schutz von personenbezogenen Daten getroffen. Insgesamt handelt es sich bei den getroffenen Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit wird der Auftragnehmer über einen längeren Zeitraum diese Maßnahmen regelmäßig prüfen und nach Bedarf adäquate Maßnahmen umsetzen. Dabei wird das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Der Auftragnehmer trifft im Rahmen der Entwicklung seines Produkts angemessene Maßnahmen zur Einhaltung des Grundsatzes Privacy by Default. Soweit gesetzlich erforderlich, erfolgt eine Verarbeitung personenbezogener Daten nur nach vorheriger Zustimmung des Betroffenen.

Auftragskontrolle

Die Auftragskontrolle gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden dürfen.

Soweit eine Datenverarbeitung im Auftrag durchgeführt wird, wird der Auftraggeber vor Aufnahme der Datenverarbeitung nach den Vorschriften der Art. 28 f. EU-DSGVO auf die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen überprüft. Das Ergebnis der Überprüfung wird dokumentiert. Über jeden Auftrag wird ein Vertrag nach den Vorschriften der EU-DSGVO abgeschlossen. Dies gilt auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und über Softwarepflege und sonstige IT-Unterstützungsverträge, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Soweit Wartungsarbeiten im Rahmen der Fernwartung durchgeführt werden, werden besondere Maßnahmen zur Überwachung der Wartungstätigkeit ergriffen.

Bei der Überprüfung der Auftragnehmer und der Vergabe von Aufträgen im Rahmen einer Datenverarbeitung im Auftrag ist der Datenschutzbeauftragte einzuschalten.

Der Nachweis über die bestehenden Verträge über eine Datenverarbeitung im Auftrag einschließlich der Unterlagen über die Prüfung der technischen und organisatorischen Maßnahmen beim Auftraggeber und über die Prüfung durch den Datenschutzbeauftragten befindet sich im in der Vertragsübersicht. Soweit die Datenverarbeitung im Auftrag Verfahren betrifft, die im Verfahrensverzeichnis erfasst sind, ist die datenschutzrechtliche Prüfung der Verträge auch im Verfahrensverzeichnis bescheinigt.