alphaflow Eingangsrechnungen (alphaflow-incominginvoice)
Auftragsverarbeitungsvertrag

Zwischen
Ihnen / Kunde
- nachfolgend „Auftraggeber“ -

und
der alphaflow GmbH
- nachfolgend „alphaflow“ -

- gemeinsam nachfolgend „Vertragspartner“ genannt -

Die Parteien schließen diesen Vertrag zur Auftragsverarbeitung (AVV) zu den AGB über die Inanspruchnahme der Leistungen der **alphaflow Eingangsrechnungen App** (technisch: ***alphaflow-incominginvoice***):

1. Vertragsgegenstand

1.1. Im Rahmen der Leistungserbringung nach dem Vertrag über die Bereitstellung der App alphaflow Eingangsrechnungen (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „Daten“ genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragspartner im Zusammenhang mit dem Umgang des Auftragnehmers mit den Daten zur Durchführung des Hauptvertrags.

1.2. Konkret umfasst die Auftragsverarbeitung folgende Gegenstände:

Die alphaflow Eingangsrechnungen App (technisch: alphaflow-incominginvoice) bietet die Möglichkeit eingehende Rechnungen und Gutschriften zu verwalten und über einen Workflow durch einen individuellen Freigabeprozess zu leiten. Die einzelnen Workflow-Schritte werden hierbei protokolliert.

2. Art, Dauer und Zwecke der Verarbeitung, Art der Daten sowie Kategorien betroffener Personen

2.1. Die Verarbeitung betrifft folgende Daten:
- Stammdaten (Adressen)
- Personal- und Identifikationsnummern
- Kundenverhaltensdaten
- Vertragsdaten
- Nutzerkennungen
- E-Mails
- Passwörter
- Zugangsdaten

2.2. Die von der Verarbeitung betroffenen Personen sind abhängig vom jeweiligen Einsatz der App. Die Verarbeitung kann sich regelmäßig auf Daten auf folgende Kategorien betroffener Personen beziehen:

- Beschäftigte
- Auszubildende und Praktikanten
- freie Mitarbeiter
- Gesellschafter, Organe der Gesellschaft
- Kunden
- Interessenten
- Lieferanten und Dienstleister
- Mieter
- Geschäftspartner
- externe Berater

2.3. Die Datenverarbeitung durch den Auftragnehmer umfasst unter anderem die Erfassung, Speicherung, Übermittlung, Organisation, Verknüpfung, Pseudonymisierung, Anonymisierung und Löschung der Daten.

2.4. Die Datenverarbeitung durch den Auftragnehmer kann je nach Einsatz der App durch den Auftraggeber zu den folgenden Zwecken erfolgen:

- Unterstützung bei der Durchführung von Verträgen oder Aufträgen
- Vertrieb oder Versand von Waren oder Erbringung von Leistungen
- Betreuung von Kunden und Geschäftspartnern
- Gewährleistung der ordentlichen und gesetzeskonformen Buchhaltung
- Rechnungsstellung für Waren oder Leistungen
- Pflege und Verwaltung von Beschäftigtendaten
- Dokumentation von Arbeitszeiten
- Zahlung von Gehältern und Lönen
- Planung und Verwaltung von Fortbildungs- und Trainingsmaßnahmen
- Dokumentation und Festlegung von Compensations und Benefits für Beschäftigte
- Überwachung betrieblicher Einrichtungen
- Gewährleistung des Zutrittsschutzes
- Gewährleistung der ordnungsgemäßen Akten- und Datenträgervernichtung
- Kommunikation mittels elektronischer Medien
- Ermöglichung der Kontaktierung von Beschäftigten
- Dokumentation von Terminen von Beschäftigten
- Zugangsverwaltung hinsichtlich Technik (einschließlich Telekommunikation, Netzwerk)
- Verwaltung von Berechtigungen
- Verwaltung von Lizenzen / Software Asset Management
- Telekommunikationskostenabrechnung
- Pflege und Verbesserung von Kommunikationsprozessen
- Qualitätssicherung

2.5. Die Datenverarbeitung durch den Auftragnehmer endet mit der Beendigung dieses Vertrags nach Ziffer 13.

3. Verantwortlichkeit des Auftraggebers

3.1. Der Auftragnehmer verarbeitet die Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Vertragspartner zueinander gem. Art. 4 Nr. 7 DSGVO verantwortlich.

3.2. Dem Auftraggeber obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag in vertragsgemäßer Qualität zur Verfügung zu stellen. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seiner Weisungen feststellt.

3.3. Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Datenverarbeitung gemäß diesem Vertrag zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so hat der Auftraggeber den Auftragnehmer auf erstes Anfordern bei der ordnungsgemäßen Erfüllung dieser Verpflichtung zu unterstützen.

3.4. Sofern durch den Auftrag Sozialdaten oder Daten verarbeitet werden, die dem Bankkundengeheimnis, dem Post- oder Fernmeldegeheimnis oder einem Berufsgeheimnis unterliegen, wird der Auftraggeber den Auftragnehmer vor Auftragsbeginn darüber in Kenntnis setzten und den Auftragnehmer über von den Regelungen der DSGVO und des BDSG abweichende gesetzliche Vorgaben informieren.

4. Weisungsbefugnisse des Auftraggebers

4.1. Der Auftragnehmer verarbeitet die Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

4.2. Die Weisungen des Auftraggebers sind grundsätzlich in den Bestimmungen dieses Vertrags festgelegt und dokumentiert. Weitere Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen der Textform. Mündliche Weisungen sind unverzüglich durch den Auftraggeber in Textform zu bestätigen. Durch Einzelweisungen bedingte Mehrkosten und Aufwände des Auftragnehmers sind vom Auftraggeber zu übernehmen.

4.3. Der Auftragnehmer gewährleistet, dass er die Daten wie in Ziffer 4.1. beschrieben im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen.

4.4 Beim Verdacht von Unregelmäßigkeiten der Datenverarbeitung wird der Auftraggeber den Auftragnehmer unverzüglich darüber informieren.

5. Nachweise und Überprüfungen

5.1. Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

5.2. Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen.

5.3. Zur Durchführung von Inspektionen ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten nach rechtzeitiger Vorankündigung (in der Regel mindestens zwei Wochen zuvor) ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen die Datenverarbeitung stattfindet. Die Geheimhaltungsverpflichtung besteht auch nach Beendigung dieses Vertrages fort.

5.4. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen zuvor) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen.

5.5. Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund dieser Ziffer gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, der Dritte unterliegt einer beruflichen Verschwiegenheitsverpflichtung. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten vor Beginn der Überprüfung vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

5.6. Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt durch eine Inspektion auch durch die Vorlage einer geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung, z.B. nach BSI-Grundschutz, erbracht werden, wenn diese es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

5.7. Gemäß den anwendbaren Datenschutzvorschriften unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Verlangen der Vertragspartner werde diese sich im Rahmen von behördlichen Aufsichtsverfahren gegenseitig unterstützen, soweit die vertragsgegenständliche Datenverarbeitung Gegenstand des Aufsichtsverfahrens ist.

5.8. Die durch die Nachweise und Überprüfungen nach dieser Ziffer veranlassten Kosten und Aufwendungen trägt der Auftraggeber. Das gilt nicht für die jährliche Überprüfung.

6. Rechte der betroffenen Personen

6.1. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen nach Kapitel III DSGVO (Betroffenenrechte) nachzukommen.

6.2. Sofern eine betroffene Person die ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6.3. Der Auftragnehmer wird auf Weisung des Auftraggeber die Daten berichtigen, löschen oder die weitere Verarbeitung einzuschränken.

7. Anforderungen an Personal

Der Auftragnehmer hat alle mit der vertragsgegenständlichen Datenverarbeitung befassten Personen, die keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, zur Vertraulichkeit zu verpflichten.

8. Mitteilungs- und Unterstützungspflichten bei Datenschutzvorfällen

Im Fall einer Datenschutzverletzung i.S.d. Art. 4 Nr. 12 DSGVO, die eine gesetzliche Melde- oder Benachrichtigungspflicht des Auftraggebers nach Art. 33, 34 DSGVO auslösen kann, wird der Auftragnehmer den Auftraggeber über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich unverzüglich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung dieser Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Erforderlichen unterstützen.

9. Sonstige Unterstützungspflichten

9.1. Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Kosten und Aufwendungen bei gegebenenfalls vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

9.2. Der Auftragnehmer wird den Auftraggeber unverzüglich benachrichtigen, sofern dessen Daten aufgrund einer drohenden Insolvenz, Pfändung, Beschlagnahme oder durch sonstige Ereignisse in Gefahr sind. Der Auftragnehmer wird Dritten, die dadurch in Besitz der Daten gelangen, unverzüglich über die Verantwortlichkeit des Auftraggebers informieren.

10. Verarbeitung im Ausland

Die Verarbeitung der Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, die Daten unter Einhaltung der Bestimmungen dieses Vertrags auch

außerhalb des EWR zu verarbeiten oder Daten an eine internationale Organisation zu übermitteln, wenn die Voraussetzungen der Art. 44 - 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

11. Inanspruchnahme weiterer Auftragsverarbeiter

11.1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Zustimmung, weitere Auftragsverarbeiter (im Folgenden: „Subauftragnehmer“) hinzuzuziehen. Generell nicht zustimmungsbedürftig sind Vertragsverhältnisse, die reine Nebenleistungen wie Prüfungs-, Wartungs-, Reinigungs- oder sonstige Dienste zum Gegenstand haben, sofern ein angemessenes Schutzniveau gewährleistet wird.

11.2. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Subauftragnehmern informieren. Dies umfasst zunächst die Mitteilung des Namens, der Anschrift und der vorgesehenen Tätigkeit des Subauftragnehmers. Der Auftraggeber ist berechtigt, gegen jede beabsichtigte Änderung aus wichtigem Grund innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch zu erheben. Danach gilt die Zustimmung als erteilt. Erhebt der Auftraggeber Einspruch, ist dem Auftragnehmer die beabsichtigte Änderung untersagt; der Auftragnehmer ist berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen. Als bereits vom Auftraggeber genehmigte Subauftragnehmer gelten:

d.velop AG
Schildarpstraße 6-8
48712 Gescher

zur Bereitstellung von Software für die Vorschau von PDF-Dokumenten und die Verwaltung von Aufgaben sowie das Speichern von Dokumenten;

sowie

DEXPRO Solutions GmbH
Gotenstraße 6
20097 Hamburg

für die Beleglesung von Dokumenten.

11.3. Der Auftragnehmer hat die vereinbarten Pflichten im Verhältnis zwischen dem Auftraggeber und dem Auftragnehmer auch im Verhältnis zwischen dem Auftragnehmer und dem Subauftragnehmer auf diesen umzulegen. Die Vertragspartner stimmen überein, dass diese Anforderung erfüllt ist, wenn die Vereinbarung mit dem Subauftragnehmer ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem Subauftragnehmer die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind. Soweit der Auftraggeber dem Auftragnehmer die Verletzung datenschutzrechtlicher Vorgaben durch den Subauftragnehmer nachweist, gelten für die Haftung die gesetzlichen Regelungen.

12. Sicherheit der Verarbeitung

12.1. Gemäß Art. 32 DSGVO werden geeignete technische und organisatorische Maßnahmen ergriffen, die unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Daten zu gewährleisten. Die zum Zeitpunkt des Vertragsschlusses bestehenden technischen und organisatorischen Maßnahmen sind dem Datenschutz- und Sicherheitskonzept (Anlage 1) zu entnehmen.

12.2. Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, sofern sie weiterhin den gesetzlichen Anforderungen genügen und das vereinbarte Schutzniveau nicht unterschritten wird.

13. Vertragsdauer und Kündigung

13.1. Dieser Vertrag endet spätestens mit der Beendigung des Hauptvertrags. Die Regelungen zur ordentlichen Kündigung des Hauptvertrags gelten entsprechend.

13.2. Der Auftraggeber ist zu einer jederzeitigen außerordentlichen Kündigung dieses Vertrags sowie des Hauptvertrags aus wichtigem Grund ohne Einhaltung einer Frist berechtigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer gegen eine Pflicht aus diesem Vertrag oder gesetzliche Vorgaben zum Datenschutz verstößt, es sei denn, dieser Verstoß ist im Einzelfall nicht schwerwiegend.

13.3. Der Hauptvertrag darf im Falle einer Beendigung dieses Vertrags nur fortgeführt werden, wenn ausgeschlossen ist, dass der Auftragnehmer Daten des Auftraggebers verarbeitet. Der Hauptvertrag und dieser Vertrag sind derart miteinander verbunden, dass die Kündigung eines der beiden Verträge zugleich als Kündigung des jeweils anderen Vertrages gilt.

14. Löschung und Rückgabe der Daten

14.1. Mit Beendigung dieses Vertrages wird der Auftragnehmer auf Weisung des Auftraggebers die Daten entweder löschen oder an den Auftraggeber zurückgeben. Dies gilt nicht, sofern eine weitere Speicherung beim Auftragnehmer zur Erfüllung gesetzlicher Pflichten oder zur Geltendmachung von Rechtsansprüchen erforderlich ist. Sofern der Auftraggeber nicht mindestens zwei Wochen vor Beendigung dieses Vertrages dem Auftragnehmer durch Weisung mitteilt, ob die Daten mit Vertragsbeendigung gelöscht oder zurückgegeben werden sollen, wird der Auftragnehmer die Daten bei Vertragsbeendigung zurückgeben.

14.2. Die Regelungen in Absatz 1 gelten nicht für Dokumentationen, die dem Nachweis der vertrags- und ordnungsgemäßen Datenverarbeitung dienen.

15. Aufwandserstattung und Haftung

15.1. Sofern der Auftraggeber bei der Ausführung dieses Vertrags einen Aufwand veranlasst, zu dem der Auftragnehmer gesetzlich nicht verpflichtet ist, hat der Auftragnehmer dem Auftraggeber diesen Aufwand zu erstatten. Für Personalkosten gelten die aktuellen Stundensätze des Auftraggebers.

15.2. Die Vertragspartner haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Im Falle einer Inanspruchnahme werden sich die Vertragspartner gegenseitig bei der Abwehr dieser Ansprüche im Rahmen des Zumutbaren unterstützen.

16. Schlussbestimmungen

16.1. Die Vertragspartner sind sich darüber einig, dass vertragliche Nebenabreden hinsichtlich des Datenschutzes nicht bestehen. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Vertragspartnern, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

16.2. Sofern in dieser Vereinbarung nicht abweichend geregelt, bedürfen Änderungen und Ergänzungen dieses Vertrages der Textform. Dies gilt auch für eine Änderung dieses Formerfordernisses.

16.3. Sollte sich herausstellen, dass einzelne Bestimmungen dieses Vertrags unwirksam sind oder der Vertrag eine Lücke aufweist, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Vertragspartner verpflichten sich, zur Ausfüllung der Lücke oder anstelle der unwirksamen Regelung eine gesetzlich zulässige zu vereinbaren, die dem Zweck der Vereinbarung am nächsten kommt und den Anforderungen des Art. 28 DSGVO gerecht wird.

16.4. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts. Art. 3 Abs. 3, Abs. 4 Rom-I-VO bleiben unberührt. Sofern gesetzlich kein anderer Gerichtsstand vorgeschrieben ist, ist der Gerichtsstand Dortmund.

_____, den _____ _____

<… (Name)>
<… (Position)>
<… (Auftraggeber)>

_____, den _____ _____

<… (Name)>
Geschäftsführung
alphaflow GmbH

Anlage 1

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Die Parteien treffen zum Auftragsverarbeitungsvertrag ergänzend folgende Festlegungen über die alphaflow umzusetzenden technischen und organisatorischen Maßnahmen:

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

Zutrittskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

- Alarmanlage
- Kameraüberwachung und Aufzeichnung mit Infrarotsystem
- Automatisches Zugangskontrollsystem mit biometrischen Zugangsdaten über Fingerabdruckleser
- Protokollierung sämtlicher Zu- und Ausgänge
- Unterteilung der Flächen in 3 zutrittsgeschützte Räume
- Zugang erfolgt ausschließlich durch Schleusen
- es ist 24x7 Personal vor Ort anwesend
- abgetrennte und gesicherte Räume für Batterien, USV und Stromversorgung
- Automatisches Zugangskontrollsystem mit Chipkarten

Zugangskontrolle

Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben:

- Zuordnung von Benutzerrechten und Einrichtung eines Benutzerstammsatzes pro Nutzer
- Erstellung von Benutzerprofilen
- differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Passwort vergaben
- Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
- automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
- Authentifikation mit Benutzernamen und Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie bei Übertragung von Daten
- Sperren externer Schnittstellen (USB etc.)
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Protokollierung der Besucher
- Sorgfältige Auswahl von Reinigungspersonal
- Sorgfältige Auswahl von Wachpersonal
- Tragepflicht von Berechtigungsausweisen
- Einsatz von Intrusion-Detektion-Systemen
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall

Zugriffskontrolle

Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
- Anzahl der Administratoren ist das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- physische Löschung von Datenträgern vor Wiederverwendung ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

Trennungskontrolle

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

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische softwareseitige Mandantentrennung
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern und Signaturen
- pseudonymisierte Daten: Trennung der Zuordnungsdatei und der Aufbewahrung in einem getrennten und abgesicherten IT-System
- Interne Mandantenfähigkeit des Systems
- Funktionstrennung von Produktiv- und Testsystem]

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

Die Verarbeitung von Daten erfolgt so, 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. Es erfolgt eine Pseudonymisierung in folgender Art und Weise: personenbezogene Daten werden von Kundenstammdaten, Umsatzdaten strikt getrennt gehalten. Sofern möglich, werden beim elektronischen Transport die personenbezogenen Daten verschlüsselt.

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

Weitergabekontrolle

Es ist sichergestellt, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert, entfernt oder sonst verarbeitet werden können und überprüft werden kann, welche Personen oder Stellen Zugriff auf Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Einsatz von VPN-Tunneln
- Protokollierungssystem
- Schnittstellenanalyse
- Verschlüsselung der Kommunikationswege
- Verschlüsselung physischer Datenträger bei Transport
- Übertragung mit elektronischer Signatur
- Transportsicherung

Eingabekontrolle

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

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

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

- redundante unterbrechungsfreie Stromversorgung (USV) mit bis zu 2.1000kVA Leistung, GreenPower USV Systeme von Socomec
- zwei getrennte Stromfeeds durch 2 Unterverteilungen in jedem Rack
- 10kw Stromaufnahme je Rack und mehr möglich
- Notstromversorgung durch 1000kVA Dieselaggregate
- direkter Nachbar des Umspannwerkes
- 3-Stufiger Überspannungsschutz – Grobschutz in Hauptverteilung, Mittel- / Feinschutz in Unterverteilungen, optionaler weiterer Schutz durch kundeneingene Stromanschlußleisten
- VESDA System zur Früherkennung von Rauchentwicklung
- CO2-Feuerlöscher in allen Bereichen sofort griffbereit
- VDS-Alarmanlagen
- direkte Alarmierung des technischen Personals vor Ort sowie externer Mitarbeiter
- Klimatisierung der Serverräume mit einer Mischung aus direkter und indirekter Freikühlung
- Kaltwasserversorgung durch energiesparende Aggregate von Emerson Networks
- Luftaustausch durch Geräte jüngster Generation von Weiss Klimatechnik
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts

- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- belastbares Datensicherungs- und Widerherstellungskonzept vorhanden
- Maßnahmen zur Datensicherung (physikalisch / logisch)
- Backup-Verfahren
- Spiegelung von Festplatten mittels Raid-Verfahren
- Einsatz eines Monitoring-Programms
- permanente Überwachung der ordnungsgemäßen Funktionalität
- Einsatz von CWDM Technik für hohe Skalierung der Bandbreiten
- Routing durch moderne Juniper Router
- Coreswitching durch moderne Cisco Switches
- Uplinks wahlweise in 100Mbit, 1GBit oder 10Gbit
- Redundante Netzversorgung durch zahlreiche Carrier wie Tiscali International oder die deutsche Telekom
- Peeringverbindungen an diversen Exchangepunkten wie DECiX, AMSiX, KleyReX, ViX und NIX

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

Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Datenschutzleitbild von alphaflow
- Datenschutz-Richtlinie von alphaflow
- Verpflichtung der Mitarbeiter auf die Vertraulichkeit

Management bei Datenschutzverletzungen

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

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber betroffenen Personen (Art. 34 DSGVO)

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

Datenschutzfreundliche Voreinstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Verarbeitungen zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben oder Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden) oder die Verfügbarkeit bestimmter Verarbeitungen, Funktionen oder Protokollierungen.

Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass Daten nur nach Weisungen des Kunden verarbeitet werden:

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten der Parteien
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Verpflichtung der Beschäftigten auf die Vertraulichkeit
- standardisiertes Vertragsmanagement zur Kontrolle von Unterauftragnehmern