

# Vereinbarung zur Auftragsverarbeitung

Die Vertragsparteien

<b>Firma</b>	
<b>Straße, Hausnr.</b>	
<b>PLZ, Ort</b>	
<b>Land</b>	

– im Folgenden: Auftraggeber –

und

apomap UG (haftungsbeschränkt)  
Poststraße 12  
59955 Winterberg  
Deutschland

– im Folgenden: Auftragsverarbeiter –

schließen folgenden Vertrag:

## 1. Allgemeine Bestimmungen und Auftragsgegenstand

- 1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Vereinbarung sind Anlage 1 zu entnehmen.
- 1.2 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.
- 1.3 Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR- Abkommens statt. Die Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.
- 1.4 Die Vergütung wird außerhalb dieses Vertrags vereinbart.

## 2. Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

## 3. Weisungen des Auftraggebers

- 3.1 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung ggü. dem Auftragsverarbeiter zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen des Auftraggebers Folge leisten, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.
- 3.2 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragsverarbeiter substantiiert anzweifelt, ist

der Auftragsverarbeiter berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

- 3.3 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z.B. per E-Mail) zu erteilen. Mündliche Weisung sind auf Verlangen des Auftragsverarbeiters schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragsverarbeiter hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.
- 3.4 Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind dem Auftragsverarbeiter unverzüglich mitzuteilen.

#### **4. Kontrollbefugnisse des Auftraggebers**

- 4.1 Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Vertragslaufzeit regelmäßig im erforderlichen Umfang zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter wird diese Kontrollen dulden und sie im erforderlichen Maße unterstützen. Er wird dem Auftraggeber insbesondere die für die Kontrollen relevanten Auskünfte vollständig und wahrheitsgemäß erteilen, ihm die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme/ -systeme gewähren sowie Vorort-Kontrollen ermöglichen. Sofern der Auftraggeber der Verarbeitung der Daten außerhalb der Geschäftsräume (z.B. Privatwohnung) zugestimmt hat, hat der Auftragsverarbeiter dafür zu sorgen, dass der Auftraggeber auch diese Räume zu Kontrollzwecken begehen darf.
- 4.2 Der Auftraggeber hat dafür zu sorgen, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragsverarbeiters nicht mehr als erforderlich beeinträchtigen. Insbesondere sollen Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Vorlaufzeit erfolgen, sofern der Kontrollzweck einer vorherigen Ankündigung nicht widerspricht.
- 4.3 Die Ergebnisse der Kontrollen und Weisungen sind von beiden Vertragsparteien in geeigneter Weise zu protokollieren.

#### **5. Allgemeine Pflichten des Auftragsverarbeiters**

- 5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragsverarbeiter erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedstaatlicher Rechtsvorschriften zulässig (z.B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden). Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragsverarbeiter dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
- 5.2 Der Auftragsverarbeiter hat bei der Auftragsdurchführung sämtliche gesetzlichen Vorschriften einzuhalten. Er hat insbesondere die nach Art. 32 DSGVO notwendigen technischen und organisatorischen Maßnahmen implementieren und das nach Art. 30 Abs. 2 DSGVO erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit dies gesetzlich vorgeschrieben ist.
- 5.3 Sofern der Auftragsverarbeiter nach der DSGVO oder sonstigen gesetzlichen Vorschriften zur Benennung eines Datenschutzbeauftragten verpflichtet ist, bestätigt er, dass er einen solchen in Einklang mit den gesetzlichen Vorschriften ausgewählt hat und sichert dem Auftraggeber zu, diesen unter Angabe seiner Kontaktdaten zu benennen (z.B. per E-Mail). Änderungen über Person und / oder Kontaktdaten des Datenschutzbeauftragten sind dem Auftraggeber unverzüglich mitzuteilen.

- 5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragsverarbeiters oder der Subunternehmer und / oder in Privatwohnungen (z.B. Fernzugriff oder Homeoffice des Auftragsverarbeiters) ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.
- 5.5 Der Auftragsverarbeiter hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.
- 5.6 Der Auftragsverarbeiter wird die Erfüllung seiner Pflichten regelmäßig und selbstständig kontrollieren und in geeigneter Weise dokumentieren.

## **6. Technische und organisatorische Maßnahmen**

- 6.1 Der Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags festgehalten. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben nach Art. 32 DSGVO ausgewählt und mit dem Auftraggeber abgestimmt.
- 6.2 Der Auftragsverarbeiter wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen. Erforderliche Anpassungen werden vom Auftragsverarbeiter dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt. Wesentliche Änderungen, durch die das Schutzniveau verringert werden könnte, sind vorab mit dem Auftraggeber abzustimmen.

## **7. Unterstützungspflichten des Auftragsverarbeiters**

- 7.1 Der Auftragsverarbeiter wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Die Reichweite der Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung.
- 7.2 Der Auftragsverarbeiter wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflicht bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

## **8. Einsatz von Unterauftragsverarbeitern (Subunternehmer)**

- 8.1 Der Auftragsverarbeiter ist nur mit Zustimmung des Auftraggebers zum Einsatz von Unterauftragsverarbeitern (Subunternehmer) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden und durch den Auftraggeber ausdrücklich bestätigten Subunternehmerverhältnisse des Auftragsverarbeiters sind diesem Vertrag abschließend in Anlage 3 beigefügt. Für die in Anlage 3 aufgezählten Subunternehmer gilt die Zustimmung mit Unterzeichnung dieses Vertrags als erteilt. Beabsichtigt der Auftragsverarbeiter den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.
- 8.2 Subunternehmer werden vom Auftragsverarbeiter unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Nebenleistungen, die der Auftragsverarbeiter zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit Integrität der Hard- und Software sicherstellen sollen und keinen

konkreten Bezug zur Hauptleistung aufweisen. Der Auftragsverarbeiter wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards sicherstellen.

- 8.3 Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Die Subunternehmerverträge haben darüber hinaus sicherzustellen, dass die im vorliegenden Vertrag vereinbarten Kontroll- und Weisungsbefugnisse durch den Auftraggeber in gleicher Weise und in vollem Umfang auch gegenüber dem Unterauftragsverarbeiter ausgeübt werden können. Der Auftragsverarbeiter ist im Falle einer entsprechenden Aufforderung des Auftraggebers verpflichtet, Auskunft über die datenschutzrechtlich relevanten Verpflichtungen des Subunternehmers zu erteilen und erforderlichenfalls die entsprechenden Vertragsunterlagen oder Kontroll- und Aufsichtsergebnisse sowie entsprechende Dokumentationen, Protokolle und Verzeichnisse des Auftragsverarbeiters einzusehen oder die Übermittlung dieser Unterlagen in Kopie zu verlangen.
- 8.4 Im Vertrag mit dem Subunternehmer ist festzuschreiben, welche Verantwortlichkeiten der Subunternehmer hat, damit der Auftraggeber diese entsprechend überprüfen kann. Ferner muss der Vertrag mit dem Subunternehmer sicherstellen, dass der Auftraggeber ggü. dem Subunternehmer zur Ausübung der gleichen Kontrollrechte, wie ggü. dem Auftragsverarbeiter berechtigt ist. Der Auftragsverarbeiter hat sicherzustellen, dass die vom Auftraggeber erteilten Weisungen auch von den Subunternehmern befolgt und protokolliert werden. Die Einhaltung dieser Pflichten wird vom Auftragsverarbeiter vor Vertragsschluss mit dem Subunternehmer und sodann regelmäßig kontrolliert und dokumentiert.
- 8.5 Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Subunternehmer seine Pflichten nach Art. 32 Abs. 4 und 29 DSGVO ggü. den ihm unterstellten Personen erfüllt hat.
- 8.6 Der Auftragsverarbeiter ist für die Einhaltung der Datenschutzbestimmungen durch die von ihm eingesetzten Unterauftragsverarbeiter verantwortlich. Er haftet ggü. dem Auftraggeber für die Einhaltung der gesetzlichen und vertraglichen Datenschutzpflichten.
- 8.7 Der Auftragsverarbeiter hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.
- 8.8 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

## **9. Mitteilungspflichten des Auftragsverarbeiters**

- 9.1 Verstöße gegen diesen Vertrag, gegen die Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragsverarbeiter selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.
- 9.2 Der Auftragsverarbeiter ist verpflichtet, den Auftraggeber bei der Erfüllung seiner gesetzlichen Informationspflichten nach Art. 33 und 34 DSGVO zu unterstützen. Eigenständige Meldungen an Behörden oder Betroffene nach Art. 33 und 34 DSGVO darf der Auftragsverarbeiter erst nach vorheriger Weisung des Auftraggebers durchführen.
- 9.3 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragsverarbeiter um Auskunft, Berichtigung, Sperrung oder Löschung, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragsverarbeiter dem Ersuchen des Betroffenen ohne Zustimmung des Auftraggebers nachkommen.

9.4 Der Auftragsverarbeiter wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragsverarbeiter den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch die die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

## 10. Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine gesetzliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z.B. gesetzliche Aufbewahrungsfristen). Der Auftraggeber ist berechtigt, die Maßnahmen des Auftragsverarbeiters in geeigneter Weise zu überprüfen. Hierzu ist er insbesondere berechtigt, die einschlägigen Löschprotokolle und die betroffenen Datenverarbeitungsanlagen vor Ort in Augenschein zu nehmen.

## 11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragsverarbeiter ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln und einschlägige Geheimnisschutzregeln, denen der Auftraggeber unterliegt (z.B. § 203 StGB), zu beachten. Der Auftraggeber ist verpflichtet, den Auftragsverarbeiter bei Auftragserteilung auf ggf. bestehende besondere Geheimnisschutzregeln hinzuweisen.

11.2 Der Auftragsverarbeiter verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragsverarbeiter aufnehmen.

11.3 Der Auftragsverarbeiter wird die Einhaltung der in dieser Ziffer genannten Maßnahmen in geeigneter Weise dokumentieren. Die Dokumentation ist dem Auftraggeber auf Verlangen vorzulegen.

## 12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

\_\_\_\_\_, den \_\_\_\_\_  
Ort

Winterberg, den \_\_\_\_\_  
Datum

\_\_\_\_\_  
Unterschrift (Auftraggeber)

\_\_\_\_\_  
Unterschrift (Auftragnehmer)

## Anlage 1 – Auftragsdetails

Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

Bereitstellung eines Online-Portals zur automatischen Routenoptimierung und Verwaltung von Auslieferungsaufträgen von Apotheken oder ähnlichen Gewerben

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

Name, Vorname, Anschrift, Telefonnummer, private E-Mail-Adresse und Auftragsalden des Kunden;

Name, Vorname, Anschrift, Telefonnummer, dienstliche E-Mail-Adresse und Standort (bei Benutzung der App) des Fahrers

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

Kunden, Mitarbeiter

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

Manuelle Eintragung in eine Weboberfläche der apomap UG (haftungsbeschränkt), automatische Übertragung über die API-Schnittstelle (SSL-verschlüsselt) der apomap UG (haftungsbeschränkt)

Der Auftraggeber unterliegt folgenden besonderen Geheimnisschutzregeln, die auch vom Auftragsverarbeiter zu beachten sind:

Berufsgeheimnis nach § 203 Abs. 1 Nr. 1 StGB

## Anlage 2 - Technische und organisatorische Maßnahmen

### 1. Vertraulichkeit

#### 1.1 Zutrittskontrolle

Der Verantwortliche gewährleistet durch geeignete Maßnahmen, dass Unbefugten der Zutritt zu den Datenverarbeitungsanlagen, auf denen die personenbezogenen Daten verarbeitet werden, verwehrt wird. Dies geschieht durch:

- Alleinige Nutzung der Räumlichkeiten durch den Verantwortlichen
- Struktur und Aufteilung der Räumlichkeiten:
  - Abgrenzung von Arbeitsplätzen, an denen personenbezogene Daten verarbeitet werden
  - Abgrenzung von TK-Anlage, Netzwerkschichten, Routern und Servern
- Zutrittsabsicherung
  - Nutzung abschließbarer Türen mit Sicherheitsschloss
  - Alarmanlage
- Führen eines Schlüsselbuches
- Schließregelung zu Auf- und Abschließen von Räumen, insbesondere bei Arbeitsbeginn und Arbeitsende
- Trennung von Bearbeitungs- und Publikumszonen
- Begleitpflicht von Besuchern
- Zutrittsverbot für Unbefugte zu Zonen, in denen personenbezogene Daten verarbeitet werden

#### 1.2 Zugangskontrolle

Der Verantwortliche gewährleistet durch geeignete Maßnahmen, dass Unbefugten der Zugang zu den Datenverarbeitungsanlagen, auf denen die personenbezogenen Daten verarbeitet werden, verwehrt wird. Dies geschieht durch:

- Definierte Zugangsberechtigungen
- Passwortrichtlinien:
  - Passwort enthält Groß- und Kleinbuchstaben und Ziffern
  - Passwort ist mindestens 8 Zeichen lang
  - Bildschirmsperre nach 15 Minuten Inaktivität
  - Verwendung personalisierter Zugänge bei Zugang zu personenbezogenen Daten
- Verschlüsselung von externen Datenträgern
- Einsatz einer Hard- und Softwarefirewall
- Verschlüsselung des WLAN mit WPA2
- Regelmäßige Aktualisierung von Betriebssystem und Anwendungen, vor allem Anwendungen mit Internetzugriff (Browser, E-Mail-Clients)
- Separates Administrationskonto mit separatem Passwort

#### 1.3 Zugriffskontrolle

Der Verantwortliche gewährleistet, dass die zur Benutzung seines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Dies geschieht durch:

- Definierte und differenzierte Zugriffsrechte innerhalb eines Berechtigungskonzepts
- Verbot der Nutzung mobiler Datenträger ohne ausdrückliche Genehmigung des Verantwortlichen
- Richtlinie für das Löschen, Vernichten und Kopieren von Datenträgern und Dokumenten
- Sicheres Löschen von Datenträgern vor neuer Verwendung oder Weitergabe
- Automatische Sperre von Arbeitsstationen mittels eines Bildschirmschoners mit Passwortabfrage nach mindestens 15 Minuten Inaktivität
- Mitarbeiterschulung und -sensibilisierung
- Verbot der Privatnutzung von informationstechnischen Systemen

## 1.4 Trennungskontrolle

Der Verantwortliche gewährleistet durch geeignete Maßnahmen sicherzustellen, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben werden, getrennt gespeichert und verarbeitet werden. Dies geschieht durch:

- Trennung von Arbeitsplätzen (Clients) und Servern durch physische Trennung in verschiedenen Räumen/Zonen und unterschiedliche Nutzerkonten
- Trennung von Daten unterschiedlicher Kunden durch eindeutige Zuordnung in Datenbanken und softwareseitige Trennung
- Verwendung unterschiedlicher (Sub-)Systeme bei unterschiedlichen Verarbeitungszwecken

## 2. Integrität

### 2.1 Weitergabekontrolle

Der Verantwortliche gewährleistet, dass überprüft und festgestellt werden kann, an welche Stellen die personenbezogenen Daten durch seine Einrichtungen zur Datenübertragung übermittelt werden. Dies geschieht durch:

- Transport von Datenträgern nur, wenn anderweitig keine sichere Übertragung möglich ist
- Arten des Versands:
  - E-Mail (mit verschlüsselten Anhängen)
  - Post
  - Kurier
  - verschlüsselte elektronische Datenübertragung
- Dokumentation von Datenübertragungen

### 2.2 Eingabekontrolle

Der Verantwortliche gewährleistet, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von welchem Eingabepunkt in seine Datenverarbeitungssysteme eingegeben worden sind. Dies geschieht durch:

- Protokollierung von Änderungen und ändernden Nutzern und Änderungszeitpunkten
- Zugriffsbeschränkung auf Protokolle
- Aufbewahrung der Protokolle für ein Jahr
- Festlegung der Personen, die Datenträger bearbeiten und erstellen dürfen

## 3. Verfügbarkeitskontrolle

Der Verantwortliche gewährleistet, durch geeignete Maßnahmen die personenbezogenen Daten vor zufälligem Verlust, Löschung oder Änderung zu schützen. Dies geschieht durch:

- Brandmeldeeinrichtungen
- Generelles Rauchverbot in allen Räumlichkeiten
- Datensicherungskonzept
- Datenlöschkonzept und -vorschriften
- Trennung der Daten nach Verarbeitungszweck
- Zutritts-, Zugangs- und Zugriffsprotokolle
- Unterbrechungsfreie Stromversorgung
- Virenschutzsoftware
- Notfallplan

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Verantwortliche gewährleistet, dass die internen Vorkehrungen zum Datenschutz eingehalten und regelmäßig aktualisiert werden. Dies geschieht durch:

- Bestellung eines Datenschutzbeauftragten
- Mitarbeiterschulung und -sensibilisierung in regelmäßigen Abständen
- Bereithaltung eines Datenschutzkonzepts
- Datenschutz per Design



### Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

Unternehmensname und Anschrift	Leistungsbeschreibung	Ort der Leistungserbringung
Hochsauerland Informatiostechik GmbH Poststr. 12 59955 Winterberg Deutschland	Bereitstellung der Webserver-Infrastruktur, technische IT-Dienstleistungen	Winterberg, Nürnberg, Falkenstein, Frankfurt am Main
DIVE INN – Die Innovationsagentur GmbH Poststr. 12 59955 Winterberg Deutschland	Geschäftsführung, Controlling	Winterberg
Amazon Web Services EMEA SARL 38 avenue John F. Kennedy, L-1855 Luxembourg	Cloud-Dienstleistungen für Webserver-Hosting	Frankfurt am Main
Google Ireland Ltd Gordon House Barrow Street Dublin 4 Irland	Bereitstellung eines Frameworks (u.a. Android) auf Cloud-Basis für mobile App	Dublin, Republik Irland