



**Vereinbarung zum Datenschutz und zur Datensicherheit  
in Auftragsverhältnissen gem. Art. 28 DSGVO  
(Auftragsdatenverarbeitung)**

zwischen dem Auftraggeber:

┌

┐

└

┘

(nachstehend „AG“ genannt)

und

**@I-DATA**  
**anja lange-huber datenkommunikation e.K.**  
**Bakumer Str. 53**  
**49324 Melle**

(nachstehend @I-DATA genannt)

Sparkasse Melle  
IBAN: DE 79 265 522 86 0000 777 219  
BIC: NOLA DE21 MEL

Ust-IdNr.: DE240776439  
Steuernummer: 65 1261 3191

Geschäftsführerin: Anja Lange-Huber  
Hauptbetriebsstätte / BSNR  
Bakumer Straße 53, 49324 Melle

Nebenbetriebsstätte / NBSNR  
Westerhausener Straße 78, 49324 Melle

Telefon: +49 (0) 5422-930 744  
Telefax: +49 (0) 5422-930 745  
Mobil: +49 (0) 171-746 87 81  
Spanien: +34 636 34 12 49  
email: info@al-data.net  
web: www.al-data.net

**medatixx**  
Premiumpartner

## **Präambel**

AG hat @I-DATA vertraglich zur Erbringung definierter Leistungen beauftragt. Darüber liegen gesonderte Leistungsverträge vor. Bei diesen Leistungen kann @I-DATA auch Zugriff auf von AG gespeicherte oder von AG sonstwie @I-DATA zur Verfügung gestellte personenbezogene Daten haben, so dass es sich bei der Leistung von @I-DATA um Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO handeln kann. Zum Schutz der personenbezogenen Daten treffen die Vertragspartner die nachfolgenden Vereinbarungen zum Datenschutz.

### **§ 1 Datenschutz, Auftragsdatenverarbeitung**

- 1.1 @I-DATA beachtet das jeweils geltende Datenschutzrecht und trifft alle notwendigen organisatorischen Maßnahmen, um die Einhaltung des Datenschutzrechts zu gewährleisten.
- 1.2 @I-DATA wird nur solche Mitarbeiter einsetzen, die @I-DATA vorab auf das Datengeheimnis sowie, falls einschlägig, auf das Fernmeldegeheimnis gem. § 88 TKG und/oder das Sozialgeheimnis gem. § 35 SGB I verpflichtet hat. @I-DATA hat die Mitarbeiter über einschlägige Strafbestimmungen, insbesondere § 203 StGB, belehrt.

### **§ 2 Definitionen und Festlegungen**

- 2.1 Gegenstand und Dauer des Auftrags ergeben sich aus dem in der Präambel genannten Vertrag. Für den Fall, dass der Auftraggeber zur Betreuung seiner Praxissoftware regionale Servicepartner von @I-DATA oder andere Fremdunternehmen mit der Arbeit an seinen Daten beauftragt, schließt der Auftraggeber einen eigenen Vertrag mit diesen Unternehmen ab. Die vorliegende Vereinbarung bezieht sich ausschließlich auf Leistungen von @I-DATA.
- 2.2 Soweit @I-DATA Zugriff auf personenbezogene Daten hat, die AG speichert oder AG sonstwie @I-DATA zur Verfügung stellt und die @I-DATA zur Erbringung der von @I-DATA geschuldeten Leistungen verarbeitet oder nutzt (diese Daten werden im Folgenden die „Nutzerdaten“ genannt), erfolgt dies im Auftrag und auf Weisung von AG gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO).
- 2.3 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu 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 (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- 2.4 Die Nutzerdaten sind in Anlage 1 genannt.

### **§ 3 Weisungsgebundenheit; Erhebung, Nutzung und Verarbeitung der Daten durch @I-DATA**

- 3.1 **@I-DATA** wird die Nutzerdaten nur im Rahmen der dokumentierten Weisungen von AG erheben, verarbeiten oder nutzen. AG wird mündliche Weisungen unverzüglich schriftlich bestätigen, E-Mail genügt. **@I-DATA** wird die Nutzerdaten nur in dem Maße nutzen und verarbeiten, wie es für die Erfüllung der von **@I-DATA** nach dem in der Präambel genannten Vertrag geschuldeten Leistungen erforderlich ist. **@I-DATA** darf die Verarbeitung im Auftrag auch im Wege von Home-Office und mobiler Telearbeit durch **@I-DATA** unterstellte Personen erbringen.
- 3.2 **@I-DATA** wird alle technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die für **@I-DATA** anwendbaren Vorschriften der DSGVO zu erfüllen, insb. die in Art. 32 DSGVO genannten Anforderungen.

Die konkreten Maßnahmen ergeben sich aus dem Dokument „Technische und Organisatorische Maßnahmen“, das dieser Vereinbarung als Anlage 2 beigelegt ist.

### **§ 4 Pflichten von @I-DATA, Rechte von AG**

- 4.1 **@I-DATA** wird AG auf schriftliches Verlangen von AG bei der Wahrung der Rechte der Betroffenen, insb. im Hinblick auf die Benachrichtigung, Auskunftserteilung sowie die Berichtigung, Sperrung oder Löschung der Nutzerdaten im Rahmen der Möglichkeiten von **@I-DATA** unterstützen, insbesondere wird **@I-DATA**
- angesichts der Art der Verarbeitung AG nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Pflicht von AG zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen, wenn AG **@I-DATA** diese Anträge übermittelt und unter Zitat des entsprechenden Gesetzestexts nachweist, dass diese Anträge berechtigt sind;
  - AG unter Berücksichtigung der Art der Verarbeitung und von **@I-DATA** zur Verfügung stehenden Informationen unterstützen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten von AG (Sicherheit der Verarbeitung; ggf. Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde; ggf. Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; bei voraussichtlich hohem Risiko für die Rechte und Freiheiten natürlicher Personen Datenschutz-Folgenabschätzung mit ggf. vorheriger Konsultation der Datenschutzbehörde), soweit AG gegenüber **@I-DATA** nachweist, dass AG im konkreten Einzelfall, für den AG Unterstützung verlangt, derartige Pflichten hat.
- 4.2 **@I-DATA** wird alle Nutzerdaten vertraulich behandeln und sicher verwahren. **@I-DATA** darf die Nutzerdaten nicht an Dritte weitergeben, außer AG hat zuvor ausdrücklich zugestimmt. **@I-DATA** gewährleistet, dass **@I-DATA** die Pflichten aus Art. 28 DSGVO erfüllt. Insbesondere gewährleistet **@I-DATA**, dass der Datenschutzbeauftragte von **@I-DATA**, und die für **@I-DATA** im Bereich Datenschutzrecht zuständigen Aufsichtsbehörden ihre gesetzlichen Aufsichts- und Kontrollrechte wahrnehmen können.
- 4.3 **@I-DATA** ist berechtigt, für die Datenverarbeitung gemäß dieser Zusatzvereinbarung Unterauftragnehmer einzusetzen. **@I-DATA** wird AG immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informieren, wodurch AG die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (siehe Anlage 3).

Soweit @I-DATA von diesem Recht Gebrauch macht, hat @I-DATA sicherzustellen, dass alle in dieser Vereinbarung und in Art. 28 DSGVO genannten Pflichten von @I-DATA auch von den betreffenden Unterauftragnehmern eingehalten werden, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

- 4.4 AG hat das Recht, im Benehmen mit @I-DATA Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig, jedoch mindestens drei (3) Wochen vorher anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Für die Ermöglichung von Kontrollen durch AG kann @I-DATA einen - dem tatsächlichen Aufwand entsprechenden - Vergütungsanspruch geltend machen.
- 4.5 @I-DATA teilt AG auf Wunsch die Kontaktdaten des Datenschutzbeauftragten von @I-DATA mit.
- 4.6 @I-DATA wird AG auf Anforderung von AG alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO beschriebenen Pflichten von @I-DATA zur Verfügung stellen, wenn AG konkret unter Zitat der entsprechenden gesetzlichen Formulierung benennt, für welche Pflicht von @I-DATA gem. Art 28 DSGVO AG Informationen benötigt.
- 4.7 Wenn @I-DATA erfährt, dass im Verantwortungsbereich von @I-DATA gegen geltendes Datenschutzrecht oder gegen Regelungen aus dieser Zusatzvereinbarung verstoßen worden ist, wird @I-DATA AG unverzüglich darauf hinweisen.
- 4.8 AG darf @I-DATA Weisungen nur im Rahmen der vertraglichen Pflichten von @I-DATA erteilen.

## **§ 5 Hinweispflicht, Pflichten bei Vertragsbeendigung**

- 5.1 @I-DATA wird AG unverzüglich darauf hinweisen, wenn @I-DATA der Ansicht ist, dass eine Weisung von AG gegen geltendes Datenschutzrecht verstößt.
- 5.2 Spätestens einen (1) Monat nach Beendigung des Vertrags wird @I-DATA von AG übergebene Datenträger, die Nutzerdaten enthalten, an AG zurückgeben und die bei @I-DATA gespeicherten Nutzerdaten nach Wahl von AG entweder löschen oder zurückgeben. Dies gilt nicht, soweit @I-DATA aufgrund Unionsrecht oder dem Recht der Mitgliedstaaten der EU zur Speicherung der personenbezogenen Daten verpflichtet ist. Im Falle einer solchen längeren gesetzlichen Aufbewahrungs- bzw. Speicherungspflicht wird @I-DATA die betreffenden Datenträger zurückgeben und die Nutzerdaten löschen, sobald das Gesetz dies zulässt.
- 5.3 @I-DATA behält sich vor, bei Änderungen der Rechtslage oder der Arbeitsweisen, diese Vereinbarung anzupassen. Die jeweils aktuelle Version dieser Vereinbarung kann jederzeit schriftlich bei @I-DATA angefordert werden.

**§ 6 Schlussbestimmungen**

- 6.1 Diese Zusatzvereinbarung bedarf der Schriftform, die elektronische Form ist ausgeschlossen. Änderungen bedürfen der Schriftform, die elektronische Form wahrt die Schriftform.
- 6.2 Sollten Bestimmungen dieser Zusatzvereinbarung rechtsunwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die rechtsunwirksamen Bestimmungen sind von den Vertragspartnern unverzüglich durch solche Bestimmungen zu ersetzen, die dem wirtschaftlich gewollten Zweck der Vertragspartner entsprechen. Das gilt entsprechend für Lücken im jeweiligen Vertrag.
- 6.3 Es gilt deutsches Recht. Gerichtsstand ist Melle.

---

Ort, Datum

Unterschrift Auftraggeber

Stempel Auftraggeber

---

---

Vor- und Nachname in Druckbuchstaben

---

---

Ort, Datum

Unterschrift Auftragnehmer  
Geschäftsführung @I-DATA

---

## **Anlage 1 Nutzerdaten**

**@I-DATA erhält Zugriff auf die nachfolgend genannten Nutzerdaten:**

- Kategorie betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
  - Auftraggeber
  - Patienten des Auftraggebers
  - Mitarbeiter des Auftraggebers
  - Dienstleister des Auftraggebers
  
- Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 3, 4, 13, 14 und 15 DSGVO) :
  - allgemeine Personendaten (Name, Geburtsdaten, Anschrift, Telefonnummer, Familienstand, Staatsangehörigkeit, E-Mail-Adresse, Krankenkassen; Beruf, Arbeitgeberdaten)
  - Kennnummern (Kundennummer, Nummer bei den Krankenkassen, sonst. Versicherungsnr., Arztnummer)
  - Bankdaten
  - Administrative Daten (betriebsstättenbezogene Daten)
  - physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur)
  - Medizinische Dokumentationsdaten
  - Onlinedaten (IP-Adresse, Webbrowserversion, Teamviewer-Daten)
  - Software Lizenzdaten, Versionsdaten
  - Hard- und Softwareinformationen
  - Arbeitszeiten der Mitarbeiter vom AG
  - Personaldaten des AG im Rahmen der elektronischen Zeiterfassung

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

### **Generelle Beschreibung**

- Aufgrund der Lage der Geschäftsräume sind Einwirkversuche von außen über die Fenster ausreichend durch elektrische Jalousien verhindert. Die Geschäftsräume sind nur durch Personal mit entsprechenden Transpondern oder Schlüsseln zu betreten.
- Zusätzlich wird das Gebäude außerhalb der Bürozeiten verschlossen.
- Ausgabe und Rückgabe von Transpondern und Schlüsseln ist geregelt, mit Schlüsselbuch bzw. durch Systemdokumentation.
- Betriebsfremde Besucher werden am Empfang begrüßt, stets von Mitarbeitern von @l-DATA im Büro begleitet und können sich nicht unkontrolliert im Bürobereich aufhalten.

In den folgenden Abschnitten sind einige technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO konkret beschrieben:

#### **1. Zugangskontrolle**

Die Zugangskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt (physikalische Sicherheit) zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

#### **Maßnahmen von @l-DATA im Einzelnen:**

- @l-DATA verpflichtet auch Auftragnehmer, die keinen Kontakt zur Datenverarbeitung haben (beispielsweise den Gebäudereiniger), die eigenen Mitarbeiter über den Datenschutz aufzuklären und diese aufzufordern, sich vorsichtig zu verhalten, insbesondere Schlüssel sorgfältig zu verwahren.
- Der Zutritt zu den Serverräumen ist durch eine separate digitale Schließanlage abgesichert. Die Zutrittserlaubnis ist auf das unbedingt notwendige Personal (Systemadministratoren) beschränkt. Personen, die nicht für die Wartung und den Betrieb der Server zuständig sind, erhalten keinen Zutritt zu den Serverräumen.

#### **2. Datenträgerkontrolle**

Die Datenträgerkontrolle umfasst Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen (logische Sicherheit) durch Unbefugte verhindert wird.

#### **Maßnahmen von @l-DATA im Einzelnen:**

- Externer Zugriff von @l-DATA-Mitarbeitern auf @l-DATA-Server ist nur via VPN und Authentifizierung am @l-DATA-LAN möglich.
- Trennung Gast-WLAN vom Firmennetzwerk.
- @l-DATA-WLAN wird mit WPA2 betrieben.
- Anti-Viren-Software auf allen eingesetzten IT/DV-Anlagen.
- Akten unter Verschluss. Zugang nur für berechtigte Personen.
- Der Zugang zu den IT-Systemen ist durch Zugangsberechtigungen geregelt. Eine Firewall verhindert ungewollte Zugriffe von außen.

- Werden Passwörter mehrfach fehlerhaft eingegeben, erfolgt eine Sperrung. Diese kann nur durch einen Administrator rückgängig gemacht werden.
- Die Mitarbeiter sind gehalten, Notebooks vor unberechtigtem Zugriff zu schützen und so wenig Daten wie möglich aus dem Bereich des Auftraggebers auf dem Notebook zu speichern (sondern möglichst nur innerhalb der zentralen Server von @l-DATA).
- Wenn ein Mitarbeiter ausscheidet, gibt er die ihm zur Verfügung gestellten Geräte an @l-DATA zurück. Alle Online-Zugänge ausscheidender Mitarbeiter werden durch @l-DATA gesperrt

### **3. Speicherkontrolle**

Die Speicherkontrolle umfasst Maßnahmen, mit denen die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert wird.

#### **Maßnahmen von @l-DATA im Einzelnen:**

- Zugriffe auf die Server von @l-DATA erfolgen durch Authentifizierung (Benutzername/Passwort) mit entsprechenden Zugriffsberechtigungen. Bei Daten von Auftraggebern wird die Zugriffsberechtigung in der Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gem. Art: 28 DSGVO (Auftragsdatenverarbeitung) geregelt.
- Über Zugriffsberechtigungen wird außerdem sichergestellt, dass die Mitarbeiter nur auf die Datenbanken, Anwendungen und Daten zugreifen können, die sie für ihre Aufgabenerfüllung benötigen.
- Bei Zugriff auf Daten beim Auftraggeber ist durch die von @l-DATA eingesetzten Fernwartungssoftware sichergestellt, dass berechtigte Mitarbeiter von @l-DATA ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass alle Zugriffe in der Kundendokumentation protokolliert werden.
- Wenn ein Mitarbeiter ausscheidet, werden ihm die Zugriffsrechte entzogen.
- Die Datenfernübertragungssysteme von @l-DATA sind mit Datenverschlüsselung versehen und werden auf dem jeweils aktuellen technischen Stand gehalten.
- Aufgrund der aufgeführten Maßnahmen ist es Unbefugten nicht möglich, Daten aus dem Auftraggeberbereich zu lesen, zu kopieren, zu ändern oder zu entfernen.
- Wenn @l-DATA die Daten aus dem Auftraggeberbereich nicht mehr benötigt, werden die Datenträger nach DIN 32757-1 und gemäß den Bestimmungen des Datenschutzes vernichtet. Eventuell angefertigte Kopien der Daten, die zum Zweck der Aufgabenerfüllung erstellt wurden, werden gelöscht.
- s. im Übrigen Datenträgerkontrolle und Zugriffskontrolle.

### **4. Benutzerkontrolle**

Die Benutzerkontrolle umfasst Maßnahmen, mit denen die Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte verhindert wird.

#### **Maßnahmen von @l-DATA im Einzelnen:**

- s. Datenträgerkontrolle und Zugriffskontrolle.



## 5. Zugriffskontrolle

Die Zugriffskontrolle umfasst Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

### Maßnahmen von @l-DATA im Einzelnen:

- Vorhandensein eines Berechtigungskonzepts.
- Datenträgerverwaltung, Datensicherung, Aufbewahrung außerhalb des Gebäudes, Verschlüsselung.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.
- Verbot der Nutzung privater Datenträger.
- Zugriff auf Notebooks, PC und Server von @l-DATA nur mit Username und Passwort möglich.
- Passwörter unterliegen definierten Passwortrichtlinien (hohen Anforderungen).
- Administratoren sind für Vergabe und regelmäßige Änderung von Passwörtern verantwortlich.
- Betrieb von Arbeitsplatz-PC und Servern nur nach Anmeldung mit Benutzername und Passwort.
- Automatische Bildschirmsperre mit Passwort-Aktivierung.
- Zugangsprotokollierung.
- Sperrung nach mehrmaligen fehlerhaften Anmeldeversuchen.
- Löschung und Zwischenlagerung defekter Datenträger bis zur datenschutzkonformen Vernichtung.
- Vernichtung ausgedruckter Daten im Aktenvernichter bzw. durch zugelassene Fachunternehmen.
- Umgang mit Datenträgern sowie Verwendung von USB-Sticks, PDAs, externen Festplatten, Tablets und Smartphones und anderer externer Geräte durch Arbeitsanweisung schriftlich geregelt.

## 6. Übertragungskontrolle

Die Übertragungskontrolle umfasst Maßnahmen, die gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

### Maßnahmen von @l-DATA im Einzelnen:

- Regelungen zur Datenübertragung sind vorhanden.
- Übermittlung und Zur-Verfügung-Stellen von Daten wird protokolliert.
- Die @l-DATA bearbeitet die Daten nur im Rahmen der Weisungen des Auftraggebers.
- Die Speicherung von Daten aus dem Auftraggeberbereich erfolgt nur während der Arbeiten zur Mängelbeseitigung oder zur Unterstützung des Einsatzes der von @l-DATA gelieferten Systeme bzw. von Systemen, für die @l-DATA Serviceleistungen erbringt. Daten aus dem Bereich des Auftraggebers werden an einen Dritten nur weitergegeben, sofern der Auftraggeber das im Einzelfall schriftlich wünscht.
- Der Auftraggeber kann @l-DATA die Daten entweder verschlüsselt über eine gesicherte Fernwartungsverbindung auf einen Server von @l-DATA übertragen oder als Datenbank auf einem Datenträger zur Verfügung stellen.

## **7. Eingabekontrolle**

Die Eingabekontrolle umfasst Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt worden sind.

### **Maßnahmen von @I-DATA im Einzelnen:**

- Regelungen zur Dateneingabe sind vorhanden.
- Erstellung und Änderung von Daten wird protokolliert.
- Es ist nicht vorgesehen, dass @I-DATA personenbezogene Daten aus dem Bereich des Auftraggebers in die Software eingibt.
- Werden personenbezogene Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche an @I-DATA übertragen, werden diese Daten nach Beendigung der Fehlersuche gelöscht. Eine Veränderung oder Entfernung im Sinne des Datenschutzrechts findet nicht statt, es sei denn, dass der Auftraggeber dies vorher ausdrücklich schriftlich beauftragt hat.
- Keine Möglichkeit für Mitarbeiter von @I-DATA, Daten in den operativen Systemen vom Auftraggeber einzugeben, zu ändern oder zu entfernen.

## **8. Transportkontrolle**

Die Transportkontrolle umfasst Maßnahmen, die gewährleisten, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

### **Maßnahmen von @I-DATA im Einzelnen:**

- Firewall.
- Versendung personenbezogener Daten mit verschlüsselter elektronischer Verbindung.
- Datenträger mit personenbezogenen Daten werden nur auf dem Postweg versandt, wenn diese Daten durch sichere Verschlüsselungsverfahren (AES-256) auf dem Datenträger gesichert wurden.
- Abholung der Daten durch einen @I-DATA Mitarbeiter

## **9. Wiederherstellbarkeit**

Die Wiederherstellbarkeit umfasst Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

### **Maßnahmen von @I-DATA im Einzelnen:**

- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Datenträgerverwaltung, Datensicherung, Aufbewahrung außerhalb des Gebäudes.
- Zugriff zu den Festplatten mit Datensicherung nur für bestimmte Personen.
- Dokumentation von Datenträgerwechseln und Aufbewahrungsorten.

## **10. Zuverlässigkeit**

Die Zuverlässigkeit umfasst Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

### **Maßnahmen von @l-DATA im Einzelnen:**

- Monitoring.  
Weiteres siehe Verfügbarkeitskontrolle.

## **11. Datenintegrität**

Die Datenintegrität umfasst Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

### **Maßnahmen von @l-DATA im Einzelnen:**

- s. Verfügbarkeitskontrolle.

## **12. Auftragskontrolle**

Die Auftragskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen verarbeitet werden können.

### **Maßnahmen von @l-DATA im Einzelnen:**

- Alle @l-DATA-Mitarbeiter sind angewiesen, nur nach den vereinbarten Vertragsinhalten zu arbeiten.
- Alle vom Auftraggeber bereit gestellten Daten verbleiben ausschließlich in der Verfügungsmacht von @l-DATA.
- Weitergabe personenbezogener Daten erfolgt nur nach schriftlicher Einwilligung vom Auftraggeber.
- @l-DATA führt Arbeiten, bei denen sie Kontakt zu personenbezogenen Daten aus dem Bereich des Auftraggebers bekommen kann oder bekommen soll, nur durch, wenn dieser diese im Einzelfall anfordert. Dies ist beispielsweise dann der Fall, wenn der Auftraggeber an die @l-DATA einen Fehler oder ein Problem meldet. Die Mitarbeiter von @l-DATA sind angewiesen, solche Maßnahmen vorsorglich mit dem Auftraggeber abzustimmen.
- Alle Mitarbeiter von @l-DATA, die mit personenbezogenen Daten aus dem Bereich des Auftraggebers in Kontakt kommen können, sind schriftlich auf die Einhaltung des Datenschutzes verpflichtet. Sie sind entsprechend belehrt und angewiesen, dass sie Arbeiten gemäß dem vorstehenden Absatz nur auf Anforderung des Auftraggebers durchführen dürfen.

## **13. Verfügbarkeitskontrolle**

Die Verfügbarkeitskontrolle umfasst Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

#### **Maßnahmen von @l-DATA im Einzelnen:**

- Tägliche Datensicherung.
- Feuerlöscher in ausreichender Anzahl im Gebäude.
- Rauchverbot im gesamten Gebäude
- Serverraum mit unterbrechungsfreier Stromversorgung, Überspannungsschutz.
- Back-Up-Verfahren für Server und Arbeitsplatz-PCs.
- Alle betroffenen Server verfügen über RAID-Systeme, welche das Verlustrisiko minimieren.
- Von einem Auftraggeber übergebene Datenträger werden unter Verschluss verwahrt.
- Sicherungskopien außerhalb des Gebäudes.
- Gespiegelte Server-Festplatten.
- Virenschutzprogramme auf allen Computersystemen.
- @l-DATA setzt eine Firewall und aktuelle Virens Scanner zur Absicherung sowohl des zentralen Datenbankservers als auch des E-Mail-Servers ein. Die Virensignaturen des verwendeten Virens Scanners werden täglich mehrmals aktualisiert.
- Arbeitsplatzrechner werden laufend durch aktuelle Scannerprogramme auf schadhafte Software überprüft. E-Mail-Anhänge werden auf Infizierung überwacht.
- Die Mitarbeiter sind angehalten, personenbezogene Daten, die sie auf ihren Notebooks gespeichert haben, möglichst bald auf ein zentrales System von @l-DATA zu überspielen.

#### **14. Trennbarkeit**

Das Trennungsgebot umfasst Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

#### **Maßnahmen von @l-DATA im Einzelnen:**

- Es ist nicht vorgesehen, dass @l-DATA personenbezogene Daten aus dem Bereich des Auftraggebers verarbeitet.
- Wenn Daten aus dem Bereich des Auftraggebers zum Zwecke der Fehlersuche oder deren Wiederherstellung übertragen werden, werden diese gesondert von Daten anderer Auftraggeber gespeichert.

### Anlage 3 Unterauftragnehmer

Andreas Baumann  
IMU Hard- und Softwareservice  
Saalmanstr. 7-9, Gebäude 2 TH3  
D-13403 Berlin

mediDOK® Software  
Entwicklungsgesellschaft mbH  
Handschuhsheimer Landstraße 11  
D-69221 Dossenheim

NovaStor AG  
Poststrasse 18  
CH-6301 Zug, Schweiz

AMEDTEC  
Medizintechnik Aue GmbH  
Schneeberger Str. 5  
08280 Aue, Germany

Geratherm Respiratory GmbH  
Sparkassenpassage 1  
97688 Bad Kissingen

WORTMANN AG  
Bredenhop 20  
32609 Hüllhorst

Brother International GmbH  
Im Rosengarten 11  
61118 Bad Vilbel

TAROX AG  
Stellenbachstr. 49-51  
44536 Lünen

Microsoft Deutschland GmbH  
Walter-Gropius-Straße 5  
80807 München

medatixx GmbH & Co. KG  
Im Kappelhof 1  
65343 Eltville/Rhein

Securepoint GmbH  
Bleckeder Landstraße 28  
21337 Lüneburg

G DATA Software AG  
Königsallee 178  
D-44799 Bochum

Ulrich & Martin Meyer GmbH & Co. KG  
Hindenburgring 11  
32339 Espelkamp

EWE TEL GmbH  
Cloppenburg Straße 310  
26133 Oldenburg

Telekom Deutschland GmbH  
Landgrabenweg 151  
53227 Bonn

IMEDAC GmbH  
Institut für Medizinisches Datenmanagement und Consulting  
Siemensstraße 40  
32105 Bad Salzuflen

I-Motion GmbH  
Gesellschaft für Kommunikation und Service  
Nordring 23  
90765 Fürth

Krämer IT Solutions GmbH  
Alte Koßmannschule  
Koßmannstr. 7  
66571 Eppelborn

TeamViewer GmbH  
Jahnstr. 30  
73037 Göppingen

Plustek Technology GmbH  
Ewige Weide 13  
22926 Ahrensburg

ComService GmbH - Honorar Plus  
Im Technologiepark 1  
15236 Frankfurt (Oder)

egs Computer Vertrieb GmbH  
Steinhof 5 A  
40699 Erkrath

Nuance Communications GmbH  
Sonnenweg 11b  
52070 Aachen, Germany

Entersoftware - Enter Srl  
Via C.A. Dalla Chiesa, 18  
Grottammare (AP) 63066

Mittwald CM Service GmbH & Co. KG  
Königsberger Straße 4-6  
32339 Espelkamp