Technisch-organisatorische Maßnahmen

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

- **Zutrittskontrolle**
  Die Büroräume der PrimaNeo GmbH befinden sich in einem Bürohaus in Hamburg. Die Zugänge zu den Büroräumen der PrimaNeo GmbH sind Tag und Nacht verschlossen. Zugang zu den Büroräumen haben nur die Angestellten der Bürogemeinschaft PrimaNeo GmbH und stella distribution GmbH. Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt. Zutrittsberechtigungen und die Schlüsselvergabe werden direkt durch die Geschäftsführung durchgeführt. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen. Besucher erhalten erst nach elektronischer Türöffnung durch den Empfang Zutritt zu den Büroräumen. Der Empfang kann die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet. Jeder Besucher wird von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet.

- **Zugangskontrolle**
  Innerhalb der Bürogemeinschaft sind Zugänge zu den Arbeitsplätzen strikt voneinander getrennt. Für die Zugangskontrolle sind nachfolgende Maßnahmen von PrimaNeo GmbH getroffen worden: Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Der Antrag wird direkt durch die Geschäftsführung erteilt. Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts. Remote-Zugriffe auf IT-Systeme der PrimaNeo GmbH erfolgen stets über verschlüsselte Verbindungen. Im Netzwerk der PrimaNeo GmbH Intrusion-Prevention- System im Einsatz. Alle Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist. Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden. Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt. Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Passwörter werden grundsätzlich verschlüsselt gespeichert.

- **Zugriffskontrolle**
  Berechtigungssystem- Zugriff nur auf freigegebene Verzeichnisse. Protokollierung der Systemanmeldungen, Kontrolle stichprobenartig Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.

- **Trennungskontrolle**
  Die Daten werden zweckgebunden und mandantenbezogen in unterschiedlichen Datenbanken, getrennte Ordnerstrukturen gespeichert. Daraus ergibt sich, dass die zu unterschiedlichen Zwecken erhobenen Daten getrennt verarbeitet werden können.

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

- **Weitergabekontrolle**
  Eine Weitergabe von Daten erfolgt nur an den Dienstleister für Druckaufträge, Versanddurchführung sowie auf Weisung des Verantwortlichen an weitere Dienstleister. Der Datentransfer erfolgt über gesicherte IPSEC-Verbindungen (z.B. VPN, WebDav, SFTP oder Telebox) oder durch Verschlüsselung.

- **Eingabekontrolle**
  In der Shop- oder Aboverwaltungssoftware werden Neuanlagen und Änderungen userbasierend protokolliert

- **Auftragskontrolle**
  Sofern Unterauftragsverarbeiter eingesetzt werden, die personenbezogenen Daten im Rahmen dieser Auftragsverarbeitung verarbeiten, werden diese sorgfältig ausgewählt und geprüft. In Abhängigkeit von der Tätigkeit wurde entweder eine AV-Vereinbarung nach Art. 28 DS-GVO oder eine geeignete Vertraulichkeitsvereinbarung abgeschlossen.
  Bei Einsatz externer IT-Dienstleister werden Vereinbarungen über den Informationsaustausch abgeschlossen, die die Sicherheit der Daten berücksichtigen. Vor Aufnahme einer Auftragsverarbeitung wird mit jedem Dienstleister festgelegt, wie Informationen/Daten zu handhaben sind.

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

- Für die Verfügbarkeit der Zugriffe auf die Kundensysteme sind folgende Maßnahmen etabliert
  - Redundante Arbeitsplätze und Infrastruktur (Router / Firewall / Leitungen)
  - Das Risiko von Datenschutzverletzungen wird sofern möglich durch Trennung von Verantwortlichkeiten (z. B. Trennung Fachbereich und Systemadministration) reduziert.

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

- Zentrale Dokumentation im internen Wikipedia Verzeichnis der Verarbeitungstätigkeiten und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki)
- Bestellter Datenschutzbeauftragter mit Nachweis der Fachkunde
- Interne und externe Beschäftigte, die personenbezogene Daten im Verantwortungsbereich der PrimaNeo GmbH verarbeiten, werden in den Datenschutz eingewiesen, auf diesen verpflichtet, für ihre Verarbeitungstätigkeiten/Anwendungen geschult und u.s. auf die Folgen von Verletzungen des Datenschutzes hingewiesen.
- Datenschutzkonzept
  - Regelmäßige Überprüfung der etablierten technischen und organisatorischen Maßnahmen
  - Prozess für die Geltendmachung der Betroffenenrechte einschl. Vorlagen und regelmäßigen Überprüfungen
  - Prozess für die Handhabung von Datenschutzverletzungen und IT-Sicherheitsvorfälle
  - Verzeichnis der Verarbeitungstätigkeiten für Auftragsverarbeiter einschl. regelmäßiger Aktualisierung
  - Prozess zur Durchführung von Prüfungen inkl. Prüfplan für das laufende Jahr einschl. regelmäßiger Überprüfung
  - Prozess zur Risikobewertung / Feststellung der Notwendigkeit einer Datenschutz-Folgenabschätzung einschl. regelmäßiger Überprüfung der etablierten Auftragsverarbeiter