Anhang 1 zur Vereinbarung gemäß Art. 28 DS-GVO bzw. § 80 SGB X

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DS-GVO

1 Vertraulichkeit gem. Art. 32 Abs. 1 lit. DS-GVO

1.1 Zutrittskontrolle

Maßnahmen zur Verhinderung, dass unbefugte Personen einen Zutritt zu Datenverarbeitungsanlagen erhalten werden durch den Auftraggeber erbracht.

1.2 Zugangskontrolle

Maßnahmen zur Verhinderung einer unbefugten Systembenutzung beim Auftragnehmer.

Maßnahme
Zugang auf Systeme mittels personalisierter Logins
Richtlinie „Sicheres Passwort“
Einsatz Anti-Viren-Software auf Clients
Regelmäßiges installieren von Sicherheitsupdates
Firewall
Einsatz von VPN für Remote-Zugriffe
Vergabe von bedarfsgerechten Berechtigungen
Richtlinie „Clean Desk“

1.3 Zugriffskontrolle

Maßnahmen zur Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernen von Informationen innerhalb des Systems des Auftragnehmers.

Maßnahme
Richtlinie „Löschen / Vernichten“
Ordnungsgemäße Vernichtung von Datenträgern und Akten (DIN 32757)
Protokollierung von Zugriffen auf Anwendungen, bei der Eingabe, Änderung und Löschung von Daten
Anzahl der Administratoren auf das „Notwendigste“ reduziert

Deutsche Apotheker- und Ärztebank eG Dresden
IBAN DE37 3006 0601 0003 1272 57
BIC DAAEDEDDXXX
IK 207904758
Vorstandsvorsitzender:
Dr. med. Klaus Heckemann

1.4 Trennungskontrolle

Maßnahmen für die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden und beim Auftragnehmer gespeichert sind.

Maßnahme
Datentrennung verschiedener Auftraggeber

2 Integrität

2.1 Weitergabekontrolle

Maßnahmen zur Verhinderung eines unbefugten Lesens, Kopierens, Veränderns oder Entfernen von Informationen bei elektronischer Übertragung oder Transport.

Maßnahme
Datenübertragung über sichere Verbindungen (bspw. SFTP, HTTPS)
Einsatz von Standleitungen bzw. VPN-Tunnel

2.2 Eingabekontrolle

Maßnahmen zur Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen des Auftraggebers eingegeben, verändert oder entfernt worden sind, werden durch den Auftraggeber erbracht

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

Maßnahmen zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust werden durch den Auftraggeber erbracht

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

4.1 Management

Maßnahme
Betrieb eines Informationssicherheitsmanagementsystems (ISMS)
Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen
Mitarbeiter auf Vertraulichkeit/ Datengeheimnis verpflichtet
Jährliche Sensibilisierung der Mitarbeiter zum Datenschutz und Informationssicherheit
Allgemeine Richtlinie zum Datenschutz
Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/Datenpannen