Anlage 11

zur Vereinbarung zwischen dem Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland und der Kassenärztlichen Vereinigung gemäß § 80 SGB X

Sicherheitsziele der Vertrauensstelle DSSGmbH

Übergreifende Sicherheitsziele der DSSG-Vertrauensstelle
Die DSSG mbH-Vertrauensstelle übernimmt als IT-Dienstleister im Auftrag seiner Kunden die Pseudonymisierung von personenbezogenen Daten und die Bereitstellung der erzeugten Pseudonyme. Zur Sicherstellung der übertragenen Verantwortung sind gesamtübergreifende Ziele festgelegt:

1. Die Geschäftsdaten bestehen hauptsächlich aus Daten, die den Datenschutzgesetzen unterliegen und daher einen hohen Schutzbedarf haben, was sich auf alle Bereiche der Vertrauensstelle auswirkt. Die Daten sind Eigentum des Auftraggebers und haben bzgl. der Anforderungen ein über die bestehenden Gesetze orientiertes Niveau. Die vertrauliche Behandlung dieser Daten hat äußerste Priorität und es gelten grundsätzlich, bis auf explizit genannte Ausnahmen, maximalen Anforderungen an Vertraulichkeit und Integrität.

2. Die verwendeten IT-Systeme und Anwendungen sind in ihrer korrekten Funktion zu überwachen und stellen die Basis für die Integrität der Systeme und Produktionsdaten (Pseudonyme) dar, insbesondere erfahren die Schlüssel und Geheimnisse zur Nutzung der Systeme und Anwendungen höchsten Schutzbedarf.

3. Die möglichen Ausfallzeiten und Lieferverzögerungen sind gering zu halten. Während der Lieferung und Produktion ist insgesamt eine sehr gute Verfügbarkeit anzustreben.

4. Die eingesetzten IT-Sicherheitsmaßnahmen werden nach den Anforderungen an die Systeme festgelegt. Weiterhin müssen die eingesetzten IT-Sicherheitsmaßnahmen in einem wirtschaftlich vertretbaren Ausmaß liegen und sich in die gesamte Sicherheitsarchitektur der Vertrauensstelle einbetten. Schadensfälle mit Verlust von Informationen oder der Initiierung von Folgeprozessen zur Korrektur müssen verhindert werden.

5. Alle Mitarbeiter halten sich an die gesetzlichen und vertraglichen Regelungen (z.B. Bundesdatenschutzgesetz, Berliner Datenschutzgesetz, Strafgesetzbuch, Geheimhaltungsvereinbarungen, etc.). Schädigungen durch Gesetzesverstöße oder sonstige Umstände mit negativen, insbesondere finanziellen oder rufschädigen Folgen für die Kunden, das Unternehmen bzw. die Mitarbeiter, sind zu vermeiden.

6. Alle Mitarbeiter und die Unternehmensführung sind sich ihrer Verantwortung beim Umgang mit Informationen und Informationstechnik bewusst und unterstützen die IT-Sicherheitsstrategie nach besten Kräften, Wissen und Gewissen.

Die der DSSG mbH-Vertrauensstelle anvertrauten Informationen (Daten) unterliegen technischen und organisatorischen Sicherungen und Maßnahmen (Detailkonzepte), welche den Erhalt der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit sicherstellen. Die kontinuierliche Weiterentwicklung von Sicherheitskonzepten und ordnungsgemäße Umsetzung soll an dieser Stelle ergänzend zu den oben genannten übergreifenden Zielen genannt werden.

Detaillierte Sicherheitsziele der DSSG-Vertrauensstelle
Die in der Vertrauensstelle zu verarbeitenden Daten unterliegen auf Grund ihrer Beschaffenheit den höchsten Vertraulichkeitsanforderungen. Der gute Ruf in Bereitstellung und Umgang von Daten ist mit allen Mitteln zu bewahren, daher kommen diesen Bereichen erhöhte Anforderungen bzgl. Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu. Durch den Verlust oder Diebstahl können erhöhte Arbeitsaufwendungen und evtl. auch ein Vertrauensverlust entstehen; ein wesentlich größeres Risiko stellt jedoch die Verletzung der Integrität und Vertraulichkeit dar, insbesondere wenn fehlerhafte Daten an Auftraggeber weitergegeben werden. Insbesondere müssen folgende Punkte berücksichtigt werden:

1. Ein Missbrauch oder sonstiger Vertrauensverlust der Daten kann schwerwiegende rechtliche Konsequenzen nach sich ziehen und ist unbedingt durch geeignete Maßnahmen zu vermeiden. Durch technische Maßnahmen und die hohe Aufmerksamkeit der Mitarbeiter wird die Vertraulichkeit geschützt und Manipulationen vorgebeugt.

2. Ein Integritätsverlust der Daten kann schwerwiegende terminliche und damit auch finanzielle Folgen haben und muss durch geeignete Maßnahmen evtl. unter Einbeziehung des Auftraggebers streng kontrolliert werden.

3. Der Verlust der Produktionsdaten zur Rekonstruktion und Repseudonymisierung (Mapping-Tabellen) würde nicht kompensierbare, finanzielle und organisatorische Auswirkungen auf den Betrieb und evtl. auch auf den Fortbestand der Vertrauensstelle implizieren. Einem Datenverlust durch Ausfall von Technik oder unsachgemäße Wahl oder Lagerung der Sicherungsmedien ist unbedingt entgegen zu wirken.

4. Die in der Vertrauensstelle verarbeiteten Daten und die fristgerechte Bereitstellung dieser sind essentiell für die Erfüllung der vertraglichen Aufgaben; eine Nichteinhaltung kann finanzielle und rufschädigende Folgen haben. Aus diesem Grund ist eine gleichbleibende Qualität, Kontinuität und Routinefestigkeit für die Abläufe, die Software und die Hardware sicherzustellen. Während der Produktionszeiträume müssen die Verfügbarkeit und die Fehlerfreiheit der Produktionssysteme sichergestellt werden. Stillstandzeiten des Produktionsbetriebs sind nur in einem sehr geringen Maße akzeptabel, da sie die Gesamtlaufzeit der nachfolgenden Prozesse beeinflussen. Bei einem Systemausfall während der Produktion können zentrale Geschäftsprozesse nur schwer aufrecht erhalten werden, Ziel ist es daher die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

5. Die Vertrauensstelle der DSSG mbH soll auch im Umgang mit ihren Auftraggebern jederzeit Vertrauen ausstrahlen, daher sind Kommunikationen jeder Art bzgl. der Aufgaben und Auftragsarbeiten der Vertrauensstelle höchst vertraulich, äußerst sensibel und besonders freundlich zu handhaben. Durch die Verletzung dieses Ziels können Wettbewerbsnachteile entstehen und eine Rufschädigung nicht ausgeschlossen werden.

Die Geschäftsführung muss jederzeit über den Betrieb und Zustand der Vertrauensstelle informiert sein und trägt die Hauptverantwortung für den ordnungsgemäßen Betrieb. Sie muss sich jeden Arbeitstag den korrekten Betrieb bestätigen lassen und in Abwesenheit diese Aufgabe an einen verantwortlichen Mitarbeiter der Vertrauensstelle delegieren.

Über die Datenschutzgesetze hinaus, welche die Sicherstellung der Vertraulichkeit der Mitarbeiter- und Auftraggeberdaten verlangen, ist zusätzlich die Sicherstellung bzw. Geheimhaltung der Arbeitsumgebung und Geschäftsprozesse einzuhalten.