18. Informationssicherheit

18.1 Vorab-Risikobewertung

Soweit sich aus der vor Vertragsabschluss von Seiten der SKH durchgeführten Vorab-Risikobewertung relevante Aspekte zur Einhaltung der Informationssicherheitsvorgaben ergeben, werden diese gegenüber dem Auftragnehmer mitgeteilt. Der Auftragnehmer ist in diesem Zusammenhang dazu verpflichtet, entsprechende risikomindernde Informationssicherheitsmaßnahmen zu treffen.

18.2 IT-Berechtigungsvergabe

18.2.1 Die SKH vergibt die Berechtigungen zu ihren IT-Systemen, das heißt den Zugang zu den IT-Systemen und den Zugriff auf die Daten, sowie die Zutrittsrechte zu Räumen an den Auftragnehmer beziehungsweise dessen Mitarbeiter nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip). Jeder Mitarbeiter erhält dabei nur die Rechte, die er für seine Tätigkeit benötigt. Der Auftragnehmer muss dabei die Funktionstrennung wahren und Interessenkonflikte vermeiden, wobei die Zugriffe und Zugänge jederzeit zweifelsfrei einer handelnden beziehungsweise verantwortlichen Person zuzuordnen sein müssen.

18.2.2 Die Mitarbeiter des Auftragnehmers, die mit den Daten der SKH in Kontakt kommen, müssen über die hierfür notwendigen Fachkenntnisse auf Basis einer geeigneten Ausbildung, Schulung oder Erfahrung verfügen.

18.2.3 Die vergebenen IT-Berechtigungen dürfen von der SKH anlassbezogen geprüft werden.

18.2.4 Die erteilten Berechtigungen werden unverzüglich deaktiviert beziehungsweise gelöscht, wenn die Gefahr einer missbräuchlichen Verwendung droht, zum Beispiel bei einer fristlosen Kündigung eines Mitarbeiters. Die Einrichtung, Änderung, Deaktivierung sowie Löschung von Berechtigungen und die Überprüfung der eingeräumten Berechtigungen sind vom Auftragnehmer nachvollziehbar und auswertbar zu dokumentieren.

18.2.5 Von Seiten der SKH werden gegebenenfalls technisch-organisatorische Maßnahmen getroffen, die eine Umgehung der Vorgaben der Berechtigungskonzepte vorbeugen, insbesondere die Auswahl angemessener Authentifizierungsverfahren, unter anderem starke Authentifizierung im Falle von Fernzugriffen, die Implementierung einer Richtlinie zur Wahl sicherer Passwörter, die automatische passwortgesicherte Bildschirmsperre, die Verschlüsselung von Daten sowie die manipulationssichere Implementierung der Protokollierung. Diese Maßnahmen müssen vom Auftragnehmer entsprechend umgesetzt werden.

18.3 IT-Risiken

18.3.1 Der Auftragnehmer ist verpflichtet ein Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen einzurichten. Dies umfasst insbesondere die Segmentierung und Kontrolle des Netzwerks, einschließlich der Endgeräte, die sichere Konfigurationen von IT-Systemen, die Verschlüsselung von Daten bei Speicherung und Übertragung, den mehrstufigen Schutz der IT-Systeme, zum Beispiel vor Datenverlust, Manipulation oder Verfügbarkeitsangriffen oder vor

nicht autorisiertem Zugriff sowie den Perimeterschutz von zum Beispiel Liegenschaften, Rechenzentren und anderen sensiblen Bereichen.

18.3.2 Der SKH ist das Vorhandensein eines solchen Schwachstellenmanagements unter Vorlage eines Risikoberichtes unter Nennung der Veränderungen an der Risikosituation ohne zusätzliche Aufforderung der SKH zu Beginn eines jeden Kalenderjahres nachzuweisen. Die SKH kann die Vorlage eines solchen Risikoberichtes vierteljährlich verlangen. Weiterhin hat der Auftragnehmer bei der Überprüfung der Maßnahmen zum Schutz der Informationssicherheit durch die SKH deren Anweisungen Folge zu leisten.

18.3.3 Sollte es Indizien für Bedrohungen oder Schwachstellen geben, wird der Auftragnehmer geeignete technische und organisatorische Maßnahmen zur Behebung ergreifen. Maßnahmen können zum Beispiel die direkte Warnung von Mitarbeitern, das Sperren von betroffenen Schnittstellen und den Austausch von betroffenen IT-Systemen umfassen.

18.3.4 Der Auftragnehmer hat potentiell sicherheitsrelevante Informationen, insbesondere Protokolldaten, Meldungen und Störungen, die Hinweise auf eine Verletzung der Informationssicherheit geben können, angemessen zeitnah, regelbasiert und zentral auszuwerten. Sollten sich in diesem Zusammenhang Hinweise auf eine Verletzung der Informationssicherheit ergeben, die den Datenaustausch zwischen den Parteien betreffen, und insbesondere nicht autorisierte Zugriffsversuche stattgefunden haben, erwartete Protokolldaten nicht mehr angeliefert werden oder die Uhrzeiten der anliefernden IT-Systeme voneinander abweichen, so wird der Auftragnehmer die SKH umgehend informieren und im Anschluss allen Aufforderungen zur Beseitigung oder Reduzierung des Informationssicherheitsrisikos Folge leisten.

18.4 Informationssicherheitsbeauftragter und Ansprechpartner

18.4.1 Der von der SKH gegenüber dem Auftragnehmer zu benennende Informationssicherheitsbeauftragte ist Ansprechpartner für alle Fragen der Informationssicherheit, die den Datenaustausch zwischen den Parteien betreffen.

18.4.2 Der Auftragnehmer ist verpflichtet, den Informationssicherheitsbeauftragten über alle bekannt gewordenen informationssicherheitsrelevanten Sachverhalte, die den Datenaustausch zwischen den Parteien betreffen, sofort und umfassend zu unterrichten. Der Auftragnehmer hat den Anweisungen des Informationssicherheitsbeauftragten hinsichtlich möglicher Nachsorgemaßnahmen wegen eines etwaigen Informationssicherheitsvorfalls des Auftragnehmers Folge zu leisten.

18.4.3 Der Auftragnehmer hat ebenfalls einen Ansprechpartner für alle Fragen der Informationssicherheit, die den Datenaustausch zwischen den Parteien betreffen, zu benennen.

18.5 IT-Betrieb und Kommunikation

18.5.1 Der Auftragnehmer ist verpflichtet, die IT-Systeme regelmäßig zu aktualisieren. Nicht mehr vom Hersteller unterstützte IT-Systeme dürfen vom Auftragnehmer für den Datenaustausch zwischen den Parteien nicht genutzt werden.

18.5.2 Sollte der Auftragnehmer Änderungen an seinen IT-Systemen vornehmen, sind diese sicher umzusetzen. Die sichere Umsetzung umfasst dabei insbesondere

- die Vornahme einer Risikoanalyse in Bezug auf die bestehenden IT-Systeme (insbesondere auch das Netzwerk und die vor- und nachgelagerten IT-Systeme), auch im Hinblick auf mögliche Sicherheits- oder Kompatibilitätsprobleme, als Bestandteil der Änderungsanforderung;

- Tests von Änderungen vor Produktivsetzung auf mögliche Inkompatibilitäten der Änderungen sowie mögliche sicherheitskritische Aspekte bei bestehenden IT-Systemen;
- Tests von Patches vor Produktsetzung unter Berücksichtigung ihrer Kritikalität;
- die Datensicherung der betroffenen IT-Systeme;
- Rückabwicklungspläne, um eine frühere Version des IT-Systems wiederherstellen zu können, wenn während oder nach der Produktivsetzung ein Problem auftritt sowie
- alternative Wiederherstellungsoptionen, um dem Fehlschlagen primärer Rückabwicklungspläne begegnen zu können.

18.5.3 Die SKH wird dem Auftragnehmer mitteilen, auf welchem Weg die Kommunikation mit diesem stattzufinden hat, insbesondere unter Verwendung eines Ticketsystems oder unverschlüsselt/verschlüsselt per E-Mail.

18.6 IT-Notfallmanagement

18.6.1 Der Auftragnehmer hat einen IT-Notfallplan festzulegen, der insbesondere einen Wiederanlauf-, einen Notbetriebs- und einen Wiederherstellungsplan inkl. der Wiederanlaufzeit des maximal tolerierbaren Zeitraums, in dem Datenverlust hingenommen werden kann und die Konfiguration für den Notbetrieb umfasst.

18.6.2 Der Auftragnehmer hat den IT-Notfallplan durch mindestens einen jährlichen IT-Notfalltest zu überprüfen.

18.6.3 Auf Verlangen der SKH hat der Auftragnehmer das Vorliegen eines solchen IT-Notfallplans nachzuweisen.

18.7 Subdienstleister

18.7.1 Sollte der Auftragnehmer gemäß den weiteren Regelungen dieser AZB Subdienstleister einsetzen, so hat dieser die SKH unverzüglich hierüber zu informieren und diese bekannt zu geben.

18.7.2 Der Auftragnehmer hat sicherzustellen, dass die in dieser Ziff. 18 vereinbarten Regelungen an die Informationssicherheit von den eingesetzten Subdienstleistern ebenfalls eingehalten werden.

18.8. Vertragsende

Sollte sich aus diesen AZB bzw. aus den einzelvertraglichen Regelungen zwischen SKH und dem Auftragnehmer nichts anderes ergeben, so hat der Auftragnehmer sämtliche von der SKH erhaltenen Daten und sonstigen Informationen nach Beendigung des Vertragsverhältnisses unverzüglich an die SKH zurückzugeben bzw. auf deren Anforderung zu vernichten und der SKH die Vernichtung nachzuweisen. Die Vernichtung hat gegebenenfalls auf die nach dem Stand der Technik sichersten Weise zu erfolgen, soweit dies möglich und zumutbar ist.

18.9 Vertragsstrafe

18.9.1 Verstößt der Auftragnehmer gegen eine der in Ziff. 18 genannten Verpflichtungen zur Einhaltung der IT-Sicherheit, insbesondere gegen seine Unterrichtungs- oder Handlungspflicht bezüglich der vom Informationssicherheitsbeauftragten der SKH ihm gegenüber erteilten Anweisungen gemäß Ziff. 18.3.2 , so hat er für jede schuldhafte Zuwiderhandlung eine 25.000,00 Euro betragende Vertragsstrafe an die SKH zu leisten.

Handelt es sich dabei um einen andauernden Verstoß, so ist der Auftragnehmer für jeden Monat, den dieser Verstoß andauert, zu einer weiteren Zahlung an die SKH in Höhe von 10.000,00 Euro verpflichtet.

18.9.2 Die Geltendmachung eines darüber hinausgehenden Schadensersatzes bleibt unberührt. Die Vertragsstrafe wird auf einen darüberhinausgehenden Schadensersatz angerechnet.