Anhang 3: Technisch-organisatorische Sicherheitsmaßnahmen

In diesem Anhang werden die technisch-organisatorischen Maßnahmen dokumentiert, die durch den Auftragnehmer zur ordnungsgemäßen Erfüllung der erbrachten Dienstleistung umgesetzt werden.

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle);

Vor-Ort-Tätigkeiten beim Auftraggeber:

Alle Mitarbeiter, die in den Räumlichkeiten des Auftraggebers Wartungstätigkeiten erbringen, können sich gegenüber dem Auftraggeber als Mitarbeiter des Auftragnehmers ausweisen (kenntlich durch Besucher- bzw. BUSOL-Namensschild) bzw. wurden vorher namentlich benannt. Die Zutrittskontrolle wird durch den Auftraggeber sichergestellt.

Fernwartung:

Die Arbeitsplatzrechner, die der Auftragnehmer nutzt, um sich ggf. mit dem Netzwerk des Auftraggebers zu verbinden befinden sich in zutrittsgeschützten Räumen, die durch eine Einbruchmeldeanlage gesichert sind.

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle);

Vor-Ort-Tätigkeiten beim Auftraggeber:

Der Auftragnehmer stellt sicher, dass etwaige Zugangsdaten zu den Systemen des Auftraggebers, die der Auftraggeber dem Auftragnehmer mitgeteilt hat, nur befugten Mitarbeitern zugänglich sind und informiert den Auftraggeber über etwaig erforderlich werdende Passwortwechsel (z.B. Ausscheiden von Mitarbeitern des Auftragnehmers mit Kenntnis des Passwortes).

Fernwartung:

Jeder Mitarbeiter des Auftragnehmers verfügt über einen eigenen Nutzer-Account und ein eigenes Passwort, mit welchem er sich an seinem Arbeitsplatzrechner anmelden muss. Die Vorgaben bzgl. Passwortkomplexität lauten wie folgt: Mindestens 8 Zeichen, darunter mindestens einen Buchstaben, eine Zahl und ein Sonderzeichen. Ein regelmäßiger Wechsel der Passwörter wird empfohlen und von den Mitarbeitern des Auftragnehmers erwartet.

Die Verbindung mit dem Netzwerk des Auftraggebers erfolgt über eine verschlüsselte Verbindung. Das im Rahmen der Verbindung erforderliche Passwort wird dem Auftragnehmer vom Auftraggeber zur Verfügung gestellt und kann vom Auftraggeber jederzeit geändert werden. Das Passwort erfüllt ebenfalls die o.g. Passwortkomplexität und wird dem Auftragnehmer sicher übermittelt (es wird dem Auftraggeber empfohlen, pro Mitarbeiter des Auftragnehmers ein separater Nutzername/Passwort zu verwenden).

Der Auftragnehmer stellt sicher, dass das Passwort nur befugten Mitarbeitern zugänglich ist und informiert den Auftraggeber über etwaig erforderlich werdende Passwortwechsel (z.B. Ausscheiden von Mitarbeitern des Auftragnehmers mit Kenntnis des Passwortes).

Alternativ: Neben dem Passwort ist zur Anmeldung zudem der Besitz eines zweiten Faktors zur Authentifizierung auf Seiten des Aufragnehmers erforderlich.

Alternativ: Der Auftraggeber hat eine IP-Adresskreisbeschränkung eingerichtet, die gewährleistet, dass sich der Auftragnehmer nur aus bekannten, statischen IP-Adresskreisen mit dem Netzwerk des Auftraggebers verbinden kann.

Im Rahmen der Fernwartung wird vom Auftragnehmer protokolliert, wann Zugriffe durch wen erfolgten. Der Auftragnehmer dokumentiert die Zwecke der Zugriffe. Weitere Protokollierungsmaßnahmen erfolgen bei Bedarf durch den Aufraggeber.

Der Auftraggeber sollte zudem jeden Zugangs-/ Zugriffsversuch von außerhalb des Netzwerks des Auftraggebers protokollieren und insbesondere Fehlversuche unter der festgelegten Wartungskennung protokollieren, auswerten und entsprechend reagieren.

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle);

Vor-Ort-Tätigkeiten beim Auftraggeber und Fernwartung:

Der Auftraggeber beschränkt den Zugriff des Auftragnehmers. Alle Mitarbeiter des Auftragnehmers wurden darüber informiert, dass ein Zugriff auf Daten des Auftraggebers nur erfolgen darf, soweit dieser zur Aufgabenerfüllung zwingend erforderlich ist.

4. zu 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 (Weitergabekontrolle);

Vor-Ort-Tätigkeiten beim Auftraggeber und Fernwartung:

Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet. Es erfolgen zudem regelmäßige Datenschutzschulungen, die insbesondere auch auf die Besonderheiten und Pflichten der Auftragsdatenverarbeitung eingehen (u.a. Weisungsgebundenheit, Hinweispflicht, Datengeheimnis).

Fernwartung:

Die Verbindung erfolgt mittels einer verschlüsselten Verbindung, welche nach BSI - IT-Sicherheitskriterien als sicher eingestuft wird.

Die Verbindung kann jederzeit durch den Auftraggeber abgebrochen werden.

Nach zeitlich begrenzter „Nicht-Aktivität“ des Auftragnehmers erfolgt zwangsweise ein „Log-out“.

Nach Beendigung der Fernwartungsmaßnahme wird die Verbindung geschlossen, um nicht autorisierte Anmeldeversuche zu verhindern.

Hinweis zum Umgang mit defekten Datenträgern:

Für Inhalte auf defekten Datenträgern, die nach Absprache mit dem Auftraggeber zur Reparatur bzw. zum Garantieaustausch eingesendet werden sollen, trägt der Auftragnehmer keine Verantwortung. Der Auftraggeber trägt Sorge dafür, dass Inhalte auf defekten Datenträgern entweder verschlüsselt sind oder vor dem Einsenden angemessen gelöscht wurden. Alternativ

erwirbt der Auftraggeber bei Kauf der Datenträger eine „Non Returnable Disk Option“ oder vernichtet defekte Datenträger und ersetzt diese auf eigene Kosten durch neue.

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle);

Wartung beim Auftraggeber und Fernwartung:

Die Eingabe, Veränderung oder Löschung personenbezogener Daten ist nicht Gegenstand des Auftrags.

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle);

Vor-Ort-Tätigkeiten beim Auftraggeber und Fernwartung:

Der Umfang der Tätigkeiten ist durch den Leistungsvertrag der Parteien sowie dem Vertrag zur Auftragsdatenverarbeitung geregelt.

Die Tätigkeit des Auftragnehmers stellt eine Auftragsdatenverarbeitung dar, da ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Ein entsprechender Vertrag zur Auftragsdatenverarbeitung wurde geschlossen.

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle);

Vor-Ort-Tätigkeiten beim Auftraggeber und Fernwartung:

Der Auftrag umfasst nicht die Speicherung von Daten auf Systemen oder Datenträgern des Auftragnehmers. Vertraglich definierte Managed Service Dienstleistungen können von dieser Regelung ausgeschlossen sein und werden bei Bedarf in einem separaten Vertrag geregelt.

Der Auftragnehmer informiert den Auftraggeber rechtzeitig über Änderungen am System, welche die Verfügbarkeit gefährden könnten.

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Vor-Ort-Tätigkeiten beim Auftraggeber und Fernwartung:

Da eine Speicherung der Daten beim Auftragnehmer nicht erfolgt und die Verarbeitung von personenbezogenen Daten nicht Gegenstand des Auftrags ist, wird das Trennungsgebot erfüllt.

Vertraglich definierte Managed Service Dienstleistungen mit Speicherung der Daten auf Systemen des Auftragnehmers können von dieser Regelung ausgeschlossen sein und werden bei Bedarf in einem separaten Vertrag geregelt.