Vertrag über Auftragsverarbeitung (AVV)

zwischen

– nachfolgend „Verantwortlicher“ genannt –

und

Univention GmbH

Mary-Somerville-Straße 1

28359 Bremen

– nachfolgend „Auftragsverarbeiter“ genannt

und gemeinsam als „Vertragsparteien“ bezeichnet – wird Folgendes vereinbart:

§ 1 Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen auf Grundlage des geschlossenen Dienstleistungsvertrags durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben.

§ 2 Weisungen der Verantwortlichen

1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in Anhang 1 aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

3 Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

§ 3 Technische und organisatorische Maßnahmen

1 Der Auftragsverarbeiter trifft mindestens die im Anhang 2 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

2 Die in Anhang 2 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

§ 4 Pflichten des Auftragsverarbeiters

1 Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

2 Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3 Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten im Anhang 1 mit. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

4 Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik

Deutschland, in einem Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

§ 5 Unterstützungspflichten des Auftragsverarbeiters

1 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

2 Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

3 Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

§ 6 Berechtigung zur Begründung von Unterauftragsverhältnissen

1 Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens drei Wochen im Voraus in Textform über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Einspruchsrechts zu entscheiden mit der Unterrichtung über die geplante Beauftragung zur Verfügung.

2 Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem

Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

3 Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Artikel 44 ff. DSGVO sicher, indem – sofern erforderlich - geeignete Garantien gemäß Artikel 46 DSGVO getroffen werden.

4 Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

5 Im Falle des § 6 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standardvertragsklauseln durch und stellt diese dem Verantwortlichen unaufgefordert zur Verfügung. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

6 Zum Zeitpunkt des Vertragsabschlusses werden seitens des Auftragsverarbeiters keine weiteren Unterauftragsverarbeiter im Rahmen der zugrunde liegenden Datenverarbeitung eingesetzt.

§ 7 Kontrollrechte des Verantwortlichen

1 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen.

1 Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten

oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

2 Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 8 Mitzuteilende Verstöße

1 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

2 Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 9 Beendigung des Auftrags

1 Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen. Mit der Beendigung des Hauptvertrags geht automatisch die Beendigung der Auftragsverarbeitung einher.

2 Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

3 Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

§ 10 Beitritt zum Vertrag

Diesem Vertrag können mit Zustimmung aller Parteien über eine Beitrittserklärung jederzeit weitere Parteien als Verantwortliche oder als Auftragsverarbeiter beitreten. Zusätzlich zur Beitrittserklärung sind – soweit erforderlich – die Anhänge 1 bis 3 auszufüllen. Ab dem Zeitpunkt des Beitritts gelten die beitretenden Parteien als Vertragsparteien dieses Vertrags mit den entsprechend ihrer Bezeichnung bestehenden Rechten und Pflichten.

§ 11 Schlussbestimmungen

1 Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

2 Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

3 Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

4 Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

5 Dieser Vertrag ist gültig ohne Unterzeichnung durch die Vertragsparteien.

Anhang 1

Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Support- und Fernwartungsdienstleistungen zur Erfüllung des geschlossenen Dienstleistungsvertrags.
Art und Zweck der Verarbeitung	Wartung und Support der durch den Auftragsverarbeiter bereitgestellten Softwarelösung. (Kooperationspartner).
Art der personenbezogenen Daten	Je nach Auftrag und geschlossenem Dienstleistungsvertrag können folgende personenbezogene Daten betroffen sein: Stammdaten, Kontaktdaten, Kommunikationsdaten, Funktionsdaten, Telemetriedaten, Diagnosedaten, Protokolldaten
Kategorien betroffener Personen	Je nach Support- bzw. Fernwartungsauftrag und geschlossenem Dienstleistungsvertrag können folgende Personen betroffen sein: Beschäftigte, Kunden, Nutzende
Dauer der Verarbeitung	Entspricht der Dauer des Subskriptions- und Dienstleistungsvertrags

Datenschutzbeauftragte/r des Verantwortlichen	
Datenschutzbeauftragte/r des Auftragsverarbeiters	Dr. Uwe Schläger datenschutz nord GmbH Konsul- Smidt-Straße 88 28217 Bremen

Anhang 2

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

UNTERAUFTRAGNEHMER	VERARBEITUNGSSTANDORT	BESCHREIBUNG DER VERARBEITUNG
IONOS SE Elgendorfer Str. 57 56410 Montabaur	Elgendorfer Str. 57 56410 Montabaur	Bereitstellung von Rechenleistung und Serverkapazitäten, Datenspeicherung
PlusServer GmbH Venloer Straße 47 50672 Köln	Venloer Straße 47 50672 Köln	Bereitstellung von Rechenleistung und Serverkapazitäten, Datenspeicherung

univention
be open.

Anhang 3

Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO

1 Überblick

Sowohl Auftraggeber als auch Auftragnehmer haben die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die getroffenen technischen und organisatorischen Maßnahmen müssen ein dem der Schwere des Risikos bzw. des drohenden Schadens für den Betroffenen angemessenes Schutzniveau gewährleisten. Die Maßnahmen müssen die Vertraulichkeit, Integrität, Verfügbarkeit der Daten und Belastbarkeit der Systeme sicherstellen. Der Erfüllung dieser Schutzziele stehen insbesondere die Gefährdungen Vernichtung, Verlust, Veränderung, unbefugte Offenlegung und unbefugter Zugang entgegen. Die nachfolgenden beschriebenen Maßnahmen umfassen die festgelegten technisch-organisatorischen Maßnahmen der Univention GmbH für die Erbringung des Produkt-Supports sowie der Unterstützung des Betriebs einer Identity-Managementplattform.

2 Standorte und physischer Zugang zu Standorten

2.1 Bürostandorte

Die Arbeitsplatzrechner, die der Auftragnehmer nutzt, um sich mit dem Netzwerk des Auftraggebers zu verbinden befinden sich in zutrittsgeschützten Räumen. Auf mobilen Endgeräten, wie z.B. Notebooks, werden sämtliche Daten auf vollverschlüsselten Datenträgern gespeichert. Die Univention GmbH unterhält Büroräume an den folgenden Standorten

- Mary-Somerville-Straße 1, 28359 Bremen
- Mariannenstr. 9-10, 10999 Berlin
- Egelstr. 4, 04103 Leipzig

An allen Standorten erfolgt der Zutritt zum Gebäude und den jeweiligen Räumlichkeiten über ein mechanisches Schließsystem. Die Schlüsselausgabe erfolgt protokolliert, der Verlust eines Schlüssels ist zu melden, ein definierter Prozess bei Ausscheiden eines Mitarbeiters stellt die Rückgabe ausgegebener Schlüssel sicher. Alle Türen und Fenster werden bei Geschäftsschluss auf ordnungsgemäßen Verschluss überprüft.

2.2 Rechenzentrum

Der Serverbetrieb für die Daten aus den oben genannten Verfahren erfolgt durch Univention in einem in Bremen ansässigem externen Rechenzentrum der Firma Briteline (Bremen Briteline GmbH Wiener Straße 5, 28359 Bremen), welches nach anerkannten Grundsätzen der IT-Sicherheit betrieben wird (TSI Level 2 zertifiziert) und gemäß dortigem IT-Sicherheitskonzept den Zutritt in eigener Zuständigkeit regelt. Der Zutritt zu unseren Serversystemen ist nur für berechtigte Mitarbeiter in Kombination mit einem RFID-Token und einer PIN möglich. Die Firma Briteline erbringt hier rein infrastrukturelle Dienstleistungen und hat keinen Zugang zum IT-Equipment von Univention. Der Betreiber überwacht die Räumlichkeiten durch eine Videoüberwachungsanlage. Das Rechenzentrum verfügt über eine redundante, unterbrechungsfreie Stromversorgung, eine redundante Klimaversorgung sowie diverse Sensoren zur Erkennung von Gefahrenquellen, wie z.B. Feuer, oder Rauchentwicklung.

Des Weiteren sind externe Rechenzentren im Einsatz, in der Teile der Infrastruktur und Anwendungen gehostet werden. Diese sind IONOS (IONOS SE, Elgendorfer Str. 57, 56410 Montabaur) und PlusServer (PlusServer GmbH, Venloer Straße 47, 50672 Köln). Die Firma IONOS ist ISO 27001 zertifiziert und hat keinen Zugriff auf die gehosteten Instanzen. Ausgewähltes Personal darf ausschließlich auf die Hardware zugreifen und tut dies alleinig zu Wartungszwecken. Die Firma PlusServer ist nach ISO 27001, BSI C5 Cloud Security, IDW PH 9.860.1 Datenschutz und ISAE 3402 zertifiziert.

3 Zugang zu IT Systemen

Der Zugang zu den IT-Systemen der Univention GmbH erfolgt auf Basis des internen Sicherheitskonzepts:

- Ein gültiges Benutzerkonto im internen Identity-Management-System ist notwendig.
- Das Benutzerkonto muss für das jeweilige System oder die jeweilige Anwendung berechtigt sein.
- Der Zugang erfolgt ausschließlich über das kabelgebundene Büronetzwerk oder über eine sichere VPN-Verbindung (das Mitarbeitern zur Verfügung gestellte WLAN ermöglicht Zugriffe auch nur über VPN).

- VPN-Verbindungen basieren auf den jeweils aktuellen technischen Standards und setzen den Besitz eines persönlichen SSL-Zertifikats und ein für den Aufbau von VPN-Verbindungen freigeschaltetes Benutzerkonto voraus.
- Mitarbeiter werden zur Benutzung von VPN-Verbindungen erst nach gesonderter Belehrung freigeschaltet.
- Benutzerkonten werden mittels eines Passworts geschützt, das im Hinblick auf Komplexität und Alter der Univention-Passwortrichtlinie entsprechen muss. Diese umfasst eine minimale Passwort-Länge und eine minimale Komplexität (bestehend aus verschiedenen Zeichentypen und dem Verbot von gängigen Wörterbucheinträgen). Die Passwortrichtlinie entspricht den gängigen Empfehlungen des BSI.
- Zur Sperrung von Konten und Widerruf erteilter Berechtigungen ausscheidender Mitarbeiter besteht ein definierter Prozess.
- In mobilen Geräten mit der Möglichkeit zum Zugang zu Univention-internen IT-Systemen werden ausschließlich verschlüsselte Datenträger verwendet.
- Alle Mitarbeiter sind angewiesen beim Verlassen des Arbeitsplatzes ihren Bildschirm zu sperren. Zusätzlich wird der Bildschirm bei Untätigkeit gesperrt.

Der Zugriff auf personenbezogene Daten im Rahmen der oben genannten Verfahren erfolgt nach dem Need-to-Know-Prinzip auf Basis des internen Rechte- und Rollenkonzeptes. Die dabei nötigen Verbindungen für Datenübertragungen werden nach Möglichkeit stets über etablierte, verschlüsselte Verfahren abgesichert und mit symmetrischen (AES-128, AES-256) und asymmetrischen (RSA, Elliptische Kurven) Verschlüsselungsverfahren gesichert. Die Sicherheit dieser Verfahren wird in regelmäßigen Abständen geprüft. Eine Fernverbindung bedarf der vorherigen technischen Freigabe des Auftraggebers. Die Verbindung kann jederzeit durch den Auftraggeber abgebrochen werden. Nach zeitlich begrenzter „Nicht-Aktivität" des Auftragnehmers erfolgt zwangsweise eine Trennung der Verbindung. Nach Beendigung der Fernwartungsmaßnahme wird die Verbindung geschlossen.

4 Umgang mit Personenbezogenen Daten

Grundsätzlich wird vermieden, personenbezogene Daten von Systemen des Auftraggebers in das Netz von Univention zu übertragen. Eine Übertragung findet nur statt, wenn sie für Analysezwecke z.B. im technischen Support notwendig ist.

Für die Übermittlung von personenbezogenen oder sensiblen Daten an uns bieten wir verschlüsselte Übertragungskanäle an, der Versand von personenbezogenen oder anderweitig sensiblen Daten an Kunden erfolgt ebenfalls verschlüsselt. Sollte im Einzelfall ein Kunde die Möglichkeiten der Verschlüsselung nicht nutzen oder nicht über entsprechende Infrastruktur verfügen, sind alle Mitarbeiter im Kundenkontakt angewiesen, den Kunden über die damit verbundenen Risiken aufzuklären und auf eine künftige verschlüsselte Übertragung hinzuwirken.

Der Auftraggeber protokolliert die Verbindungen bei Bedarf.

Die Art und der Umfang der Übermittlung dieser Daten erfolgt in enger Abstimmung mit dem Auftraggeber und sollte stets über sichere und verschlüsselte Kanäle erfolgen, die Auftraggeber und Auftragnehmer einigen sich gemeinsam auf die entsprechenden Verfahren. Diese sollten anerkannte Sicherheitsstandards, wie z.B. die Nutzung von symmetrischen und asymmetrischen Verschlüsselungsverfahren, erfüllen und regelmäßig überprüft werden.

Für die Kommunikation per E-Mail bietet Univention die Möglichkeit, Nachrichten über asymmetrische Verschlüsselungsmechanismen abzusichern. Hierbei bietet Univention die PGP- und S/MIME-Standards für das Senden und Empfangen von
E-Mails an.

Für den Transfer von größeren Dateien und Diagnose-Daten bietet Univention einen Upload-Dienst an, der die Übertragungswege über das HTTPS-Protokoll absichert.

Der Remote-Zugriff auf Systeme des Auftraggebers erfolgt standardmäßig über das verschlüsselte SSH-Protokoll und muss vom Auftraggeber initiiert werden. Der Auftraggeber kann die Verbindung jederzeit beenden.

Die Mitarbeiter von Univention sind gemäß Betriebsvereinbarung zur Verschwiegenheit verpflichtet. Es erfolgen regelmäßige Schulungen zu datenschutzrelevanten Themen, die insbesondere auf die Besonderheiten und Pflichten der Auftragsverarbeitung eingehen.

Zur Vernichtung papierener Unterlagen kommen Aktenvernichter sowie eine Datentonne zum Einsatz, zu entsorgende Datenträger werden vor der Entsorgung durch mehrfaches, zufälliges Überschreiben geleert und anschließend physisch zerstört.

Im Rahmen der oben genannten Verfahren erfolgt der Zugriff auf potentiell personenbezogene Daten von Kunden oder die Bereitstellung von potentiell personenbezogenen Daten durch Kunden ausschließlich anlassbezogen und nur bei Bedarf im Fall von Unterstützungs- oder Supportanfragen durch Kunden. Die Daten werden dabei nicht für den Kunden aufbereitet, verwaltet oder aufbewahrt, sondern dienen nur der Problemanalyse. Bei den Daten handelt es sich daher

grundsätzlich um Kopien oder Auszüge von Daten, die im Original unangetastet beim Kunden verbleiben. Die Daten werden darüber hinaus nur für einen sehr begrenzten Zeitraum während der Problemanalyse benötigt. Daher werden keine Maßnahmen durchgeführt, z.B. Backups, die zur langfristigen Speicherung dieser Daten auf unserer Seite beitragen. Etwaige durch den Auftraggeber bereitgestellte personenbezogene Daten auf Systemen des Auftragnehmers werden nach Abschluss der jeweiligen Supporttätigkeit unverzüglich gelöscht.

Zur Durchführung der oben genannten Verfahren werden keine Auftragsverarbeiter eingesetzt.

Der Auftragnehmer hat ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etabliert.