Auftrag gemäß Art. 28 DSGVO
für Fernwartung

zwischen

_____

_____

_____

- nachstehend „Auftraggeber“ genannt -

und

awinta GmbH
Robert-Bosch-Str. 7-9
74321 Bietigheim-Bissingen

- nachstehend „Auftragnehmer“ genannt -

1. Gegenstand und Dauer des Auftrags

Diese Vereinbarung ist Bestandteil des bereits mit dem Auftraggeber bestehenden Software-Service-Vertrages (Hauptvertrag) und konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus der im Hauptvertrag vereinbarten Fernwartung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Fernwartung in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen (können). Die Dauer dieser Vereinbarung richtet sich nach der Dauer des Hauptvertrages.

2. Anlagen

Verbindlicher Bestandteil dieser Vereinbarung sind folgende, fortlaufend durchpaginierte (Seite 2 - 7) Anlagen:

- ANLAGE 1 - Konkretisierung des Auftragsinhalts und Rechte und Pflichten der Parteien
- ANLAGE 2 - Allgemeine technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Bietigheim-Bissingen, den _____ _____
(Ort, Datum)

_____ _____
awinta GmbH (Inhaber der Apotheke)

ANLAGE 1 ***zum Auftrag gemäß Art. 28 DSGVO für Fernwartung***

Konkretisierung des Auftragsinhalts und Rechte und Pflichten der Parteien

1. Konkretisierung des Auftragsinhalts

Gegenstand, Art und Zweck der Verarbeitung und Art der Daten:

Der Auftragnehmer führt Fernwartungsarbeiten an den Systemen des Auftraggebers durch. Der Umfang der im Rahmen der Fernwartung zu erbringenden Tätigkeiten ergibt sich aus dem Hauptvertrag.

Es kann nicht ausgeschlossen werden, dass der Auftragnehmer im Rahmen der Fernwartungsarbeiten Zugriff auf personenbezogene Daten erlangt, die in den zu wartenden Systemen gespeichert sind und dort verarbeitet werden. Dies betrifft folgende Daten:

Datenkategorie	Art der Daten
Kundendaten	Name, Firmenname, Adresse, Geburtsjahr, Geschlecht, Kommunikationsdaten, Zahlungsdaten
Mitarbeiterdaten	Name, Benutzerkürzel
Lieferantendaten	Name, Firmenname, Adresse, Kommunikationsdaten, Umsatzdaten
Arztdaten	Fachnummer, Name des Arztes, Adresse, Fachgebiet
Krankenkassendaten	Nummer, Name
Einkaufsdaten	Preise, Artikelinformationen, Lagerortdaten
Verkaufsdaten	Preise, Artikelinformationen, Rezeptinformationen
Lagerdaten	Enthalten keine personenbezogene Daten

Kategorien betroffener Personen

Der Kreis, der durch den möglichen Zugriff auf ihre personenbezogenen Daten im Rahmen der Fernwartung potentiell betroffenen Personen umfasst:

- Auftraggeber
- Kunden des Auftraggebers
- Verschreibende Ärzte
- Beschäftigte i. S. d. § 26 Abs. 8 BDSG in der Fassung ab dem 25.05.2018 des Auftraggebers
- Lieferanten des Auftraggebers

Zweckbestimmung

Personenbezogene Daten, die dem Auftragnehmer im Rahmen der Durchführung der Fernwartungsarbeiten bekannt werden, darf der Auftragnehmer nur für Zwecke der Fernwartung verwenden. Eine Weitergabe dieser Daten an Dritte ist dem Auftragnehmer untersagt. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

2. Verantwortlichkeit, Ort der Fernwartung

2.1. Der Auftragnehmer darf die Fernwartungsarbeiten, ausschließlich im Rahmen der dokumentierten Weisungen des Auftraggebers durchführen (vgl. Art. 28 Abs. 3 S. 2 lit. a) DSGVO). Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können von dem Auftraggeber danach in Schriftform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden, soweit dies für die Einhaltung der datenschutzrechtlichen Verpflichtungen des Auftraggebers gegenüber den betroffenen Personen erforderlich ist. In dringenden Fällen kann der Auftraggeber Weisungen unter Verzicht auf das Schriftformerfordernis erteilen. Der Auftraggeber bestätigt mündliche Weisungen unverzüglich schriftlich, d.h. per Brief oder Fax.

2.2. Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO).

2.3. Die Durchführung der Fernwartungsarbeiten erfolgt ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.

3. Pflichten des Auftragnehmers

3.1. Der Auftragnehmer trifft technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust, die den gesetzlichen Anforderungen an Datenschutz und Datensicherheit gemäß Art. 28 Abs. 3 S. 2 lit. c) DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO entsprechen und stellt durch ein effektives Kontrollsystem im erforderlichen Umfang sicher, dass diese Maßnahmen sowie die zulässigen Weisungen des Auftraggebers eingehalten werden. Insbesondere gestaltet der Auftragnehmer seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er gewährleistet in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen, technischen und organisatorischen Maßnahmen.

3.2. Der Auftragnehmer, wird soweit erforderlich insbesondere

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen sicherstellen, sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Die Vertragsparteien vereinbaren die in der Anlage 2 niedergelegten konkreten Datensicherheitsmaßnahmen. Diese Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer darf alternative Maßnahmen einsetzen, wenn diese mindestens das Sicherheitsniveau der gemäß Anlage 2 vereinbarten Maßnahmen erreichen.

3.3. Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

3.4. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b) DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3.5. Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten in der gesetzlich vorgeschriebenen Weise und mit den gesetzlich vorgeschriebenen Aufgaben bestellt. Der Auftragnehmer teilt dem Auftraggeber auf Anfrage die Kontaktdaten seines betrieblichen Datenschutzbeauftragten sowie diesbezügliche Änderungen mit.

3.6. Der Auftragnehmer unterrichtet den Auftraggeber unabhängig von der Frage des Verschuldens bei schwerwiegenden Störungen des Betriebsablaufes, die Einfluss auf die Sicherheit der Fernwartungsarbeiten haben können, bei Verdacht eines Verstoßes gegen Vorschriften zum Schutz personenbezogener Daten oder die im Hauptvertrag oder dieser Vereinbarung getroffenen Festlegungen oder andere Unregelmäßigkeiten bei einem möglichen Zugriff auf personenbezogene Daten des Auftraggebers. Der Auftragnehmer hat in diesen Fällen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen mit dem Auftraggeber abzustimmen und umzusetzen.

3.7. Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

3.8. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

3.9. Im Verantwortungsbereich des Auftragnehmers sind bei der Sicherung von Daten des Auftraggebers, wenn und soweit eine solche Sicherung geschuldet ist, Schutz- und Sicherungsmaßnahmen nach dem jeweils geltenden Stand der Technik zu beachten, um jederzeit Datenbestände verlust- und archivieren und wiederherstellen zu können.

3.10. Sämtliche personenbezogenen Daten und ihre Trägermedien, gleich welcher Form, sind vom Auftragnehmer spätestens nach Auftragsdurchführung oder auf Weisung des Auftraggebers an diesen zurück zu geben. Angefertigte Kopien hiervon sowie Test- und Ausschussmaterial sind vom Auftragnehmer datenschutzkonform zu löschen oder zu vernichten; dies ist dem Auftraggeber vom Auftragnehmer auf Verlangen unter Vorlage des Löschprotokolls schriftlich zu bestätigen. Ein Zurückbehaltungsrecht des Auftragnehmers an personenbezogenen Daten und ihren Trägermedien ist ausgeschlossen. Der Auftragnehmer ist jedoch berechtigt, Vervielfältigungen der personenbezogenen Daten anzufertigen und entsprechend gesichert für sich datenschutzkonform zu behalten, soweit und solange diese für eine ordnungsgemäße Abrechnung der Vergütung nach dem Hauptvertrag benötigt werden und die Daten für andere Zwecke gesperrt werden. Der Auftraggeber kann auch nach der Laufzeit des Hauptvertrages und nach Beendigung dieser Vereinbarung hinsichtlich der Daten, die Gegenstand dieses Auftrags sind, die Herausgabe sämtlicher Datenträger und die datenschutzkonforme Löschung der beim Auftragnehmer gespeicherten Daten verlangen. Über die Herausgabe oder Löschung der Daten nach Vertragsende muss der Auftraggeber innerhalb einer vom Auftragnehmer gesetzten angemessenen Frist entscheiden.

4. Pflichten des Auftraggebers

4.1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Zusammenhang mit der Fernwartung Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2. Vom Auftraggeber zu erteilende Weisungen haben grundsätzlich schriftlich zu erfolgen. Ausnahmsweise mündlich erteilte Weisungen hat der Auftraggeber auf Wunsch des Auftragnehmers unverzüglich schriftlich zu bestätigen.

4.3. Wenn der Auftragnehmer wegen der Ausführung einer vom Auftraggeber erteilten Weisung von einem Dritten, der nicht Partei dieses Auftrags ist, insbesondere von einer betroffenen Person in Anspruch genommen wird, ist der Auftraggeber verpflichtet, dem Auftragnehmer die diesem in diesem Zusammenhang entstehenden Schäden zu ersetzen.

5. Rechte betroffener Personen auf Auskunft, Berichtigung, Löschung und Sperrung

5.1. Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche betroffener Personen auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

5.2. Der Auftragnehmer darf personenbezogene Daten des Auftraggebers, auf die er im Rahmen der Fernwartung Zugriff erhält, nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g) DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

5.3. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6. Kontrollrechte des Auftraggebers und Vertraulichkeit

6.1. Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen gemäß der Anlage 2 sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren. Dazu kann der Auftraggeber oder ein beauftragter Prüfer die Datenverarbeitungsanlagen und die Datenverarbeitungsprogramme des Auftragnehmers inspizieren.

6.2. Der Auftragnehmer ist verpflichtet, dem Auftraggeber zu den üblichen Geschäftszeiten Zutritt zu den Räumlichkeiten zu gewähren, in denen die Daten des Auftraggebers physisch oder elektronisch verarbeitet werden. Der Auftraggeber stimmt die Durchführung der Inspektionen mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird.

6.3. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der technischen und organisatorischen Maßnahmen sowie der Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zur Verfügung. Zu diesen Informationen gehören insbesondere aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, externe Sachverständige, IT-Sicherheits- oder Datenschutzauditoren) und geeignete Zertifizierung (z.B. nach BSI-Grundschutz). Der Auftragnehmer erteilt dem Auftraggeber unverzüglich konkrete Auskunft im Einzelfall.

6.4. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses, insbesondere im Zusammenhang mit durchgeführten Kontrollen erlangte Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers streng vertraulich zu behandeln.

7. Unterauftragsverhältnisse

7.1. Aufträge, die die Datenverarbeitung nach dieser Vereinbarung betreffen, dürfen durch den Auftragnehmer an Subunternehmer vergeben werden, wenn sichergestellt ist, dass durch den Einsatz des jeweiligen Subunternehmers die Einhaltung der datenschutzrechtlichen Verpflichtungen des Auftragnehmers aus dieser Vereinbarung nicht gefährdet ist.

7.2. Zurzeit werden folgende Subunternehmer eingesetzt:

- NOVENTI Health SE, Tomannweg 6, 81673 München (nur Bereitstellung von IT-Leistungen /-Infrastruktur)
- Kronsoft Development SRL, Str. Canalului Nr. 44, 505600 Săcele, Braşov, Rumänien (NOVENTI Group)

7.3. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

7.4. Wenn Subunternehmer durch den Auftragnehmer eingeschaltet werden, so werden die vertraglichen Vereinbarungen mit diesen so gestaltet, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Parteien dieses Vertrages entsprechen. Der Auftragnehmer ist auf schriftliche Anforderung des Auftraggebers verpflichtet, Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erteilen, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

7.5. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Leistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich (Art. 28 Abs. 3 S. 2 lit. f, Art. 33 Abs. 2 DSGVO). Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen. Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

8.2. Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen gemäß Art. 34 DSGVO.

ANLAGE 2 *zur Vereinbarung nach Art. 28 DSGVO*

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Der Auftragnehmer verpflichtet sich insbesondere zur Umsetzung der nachfolgend einzeln aufgeführten technischen und organisatorischen Maßnahmen, die er regelmäßig einer Überprüfung unterzieht.

Technische und organisatorische Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 DSGVO)

1. Zutrittskontrolle

Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:

- **<u>Zutrittskontrollen Rechenzentrum:</u>**

  Die Zutrittskontrolle im Rechenzentrum erfolgt über das Sicherheitspersonal des RZ Betreibers, das 24/7 den Zutritt kontrolliert. Der Zutritt ist unbefugten Dritten nicht möglich. Der Zugang zum Rechenzentrum muss beim Sicherheitsleitstand zuvor schriftlich avisiert werden. Eine Avisierung kann nur durch zuvor definierte Key-User vorgenommen werden. Der Leitstand ist 24/7 besetzt.

- Das Rechenzentrumsgelände ist 2stufig durch eine detektierte Zaunanlage gesichert.
- Protokollierung, Überwachung und Verfolgung sämtlicher Zugänge zu dem Rechenzentrum, in dem die personenbezogenen Daten gehostet werden, durch Sicherheitspersonal des RZ Betreibers. Videoüberwachung der Außenbereiche mit einer Aufzeichnungszeit von 3 Monaten, zusätzliche Videoüberwachung der Flure und Serverräume.
- Avisierte Mitarbeiter ohne eigene Sicherheitsausweise des RZ Betreibers werden vom Sicherheitspersonal in die Serverräume geführt.
- Sicherung des Zutritts zu Serverräumen im Rechenzentrum durch kontaktloses Ausweissystem. Nur autorisiertes Personal der Awinta IT verfügt über einen Ausweis. Zutritte sind nur in freigeschaltete Bereiche möglich.
- Sicherung der einzelnen Server-Racks im Rechenzentrum zusätzlich durch PIN-Code oder Schlüssel.

- **<u>Zutrittskontrollen Niederlassungen:</u>**

- Sicherung des Zutritts durch Schlüsselkarten, Ausweise
- Festlegung von Vorschriften über die Verwendung von Ausweisen, Schlüsselkarten
- Vergabe von Ausweisen, Schlüsselkarten nur an autorisiertes Personal
- Standort-Serverräume sind durch kontaktlose Ausweise oder Schlüssel gesichert. Zutritt nur durch autorisiertes Personal der IT.

2. **Zugangskontrolle:**

Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen und –verfahren gehindert werden:

- Der Aufbau der Fernwartungsverbindung erfolgt nur unter Mitwirkung des Auftraggebers. Eine Fernwartung ohne aktive Zustimmung des Auftraggebers ist dadurch ausgeschlossen.
- Fernwartungsarbeiten dürfen nur begonnen werden, wenn sich das Fernwartungspersonal mit Benutzerkennung und Passwort angemeldet hat.
- Konsolenzugänge zu Server-/Netzwerkgeräten sind passwortgeschützt, nach Nutzungsunterbrechung erfolgt eine automatische Abmeldung oder erneute Passwort-Abfrage.
- Identifizierung des Datenterminal-Nutzers beim Zugriff auf das Datenverarbeitungssystem (Passwortschutz); die Passwörter werden regelmäßig alle 6 Monate geändert.
- Automatisches Logout des Datenterminals bei längerer Nutzungsunterbrechung (10 Minuten), Wiederaufnahme nur nach Identifizierung und Passworteingabe

Die Passwortvergabe, -wahl und -verwaltung erfolgt nachfolgenden Kriterien:

Passwortaufbau

Ein Passwort muss:

- mindestens acht Zeichen lang sein
- nicht nur Buchstaben beinhalten, sondern aus Groß- und Kleinbuchstaben, Sonderzeichen (Satzzeichen u. ä.) und Zahlen bestehen
- möglichst kein Wort sein, das im Duden oder in einem anderen Wörterbuch aufgeführt ist
- nicht aus einem Trivialpasswort bestehen (z. B. Namen von Prominenten, Passwort)
- nicht aus Zeichen aufgebaut sein, die auf der Tastatur nebeneinander liegen (z. B. 123456)

- nicht das gleiche Zeichen mehrfach hintereinander enthalten (z. B. AAAA)
- keinen Bezug zum Benutzer erkennen lassen (z. B. nicht Benutzerkennung, Name, Geburtsdatum, Kraftfahrzeugkennzeichen, usw.)

- ***Passwortvergabe und -verwendung***

- Zu jeder Benutzerkennung gehört ein eigenes Passwort.
- Die Passwortvergabe erfolgt durch den Benutzer selbst.
- Das Passwort darf nur dem Benutzer bekannt sein.
- Die Passworteingabe muss verdeckt erfolgen.
- Voreingestellte Passworte (z. B. im System- und Anwendungsbereich) sind sofort zu ändern.

- ***Passwortverwaltung***

- Das neue Passwort wird zur Sicherheit ein zweites Mal eingegeben.
- Das Passwort kann durch Benutzer jederzeit selbst geändert werden.
- Besteht der Verdacht, dass das Passwort einer anderen Person bekannt wurde, ist es unverzüglich zu ändern.
- Passworte dürfen nicht auf Funktionstasten gelegt bzw. in einem Makro gespeichert werden.
- Passworte dürfen nicht auf Zetteln notiert und keiner anderen Person (auch nicht dem Vorgesetzten oder dem Systemverwalter) mitgeteilt werden.
- Gewährung von Zugang zu den Systemen und Ausgabe von Identifizierungscodes (Benutzername und Passwort) nur an autorisiertes Personal; es findet alle sechs Monate eine Prüfung des Rollen- und Berechtigungskonzepts der Personen statt, die Zugang zu den Systemen haben, ob das „need to know" der jeweiligen Personen noch gegeben ist und – sofern dies entfallen ist – eine Sperrung des betroffenen Zugangs. Eine Zugangssperrung erfolgt auch bei Ausscheiden betroffener Mitarbeiter oder einem internen Zuständigkeitswechsel.
- Zuteilung einzelner Datenterminal-Nutzer und Identifizierungsmerkmale ausschließlich durch bestimmte Personen; Dies erfolgt durch einen System-Administrator, der direkt der Geschäftsführung berichtet.
- Schutz vor externen Zugriffen durch den jeweiligen Stand der Technik entsprechende Firewalls. Verschlüsselungsverfahren entsprechend dem jeweiligen Stand der Technik (SSL und HTTPS Verschlüsselung bei der Übertragung personenbezogener Daten), die Daten selbst werden nicht verschlüsselt gespeichert.

3. Zugriffskontrolle:

Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass bei der Fernwartung solche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Der Auftragnehmer darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Fernwartungsarbeiten unerlässlich notwendigen Umfang Gebrauch machen.

- Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen. Soweit der Auftragnehmer daran mitwirken muss, gewährleistet er, dass dies möglich ist.

4. Weitergabekontrolle:

Maßnahmen, die sicherstellen, 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:

- Ausschließlich verschlüsselte Datenübertragung auf Basis eines RSA Public-/Private Key Exchange und AES (256 Bit) Session Encoding.

- Schutz der Datenleitungen, die bei der Übertragung genutzt werden, durch Verwendung entsprechender Firewalls, nach dem jeweiligen Stand der Technik und dem Einsatz von sicheren Verschlüsselungsmethoden wie IPSec oder SSL-Verschlüsselung bei Übertragung von personenbezogenen Daten.

5. Auftragskontrolle

Maßnahmen, die gewährleisten, dass die Fernwartung nur entsprechend den Weisungen des Auftraggebers durchgeführt wird:

- Prozess zur Entgegennahme und Umsetzung von Weisungen des Auftraggebers auch im Hinblick auf eventuell eingesetzte Unterauftragnehmer

Die vorstehenden Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Der Auftragnehmer darf alternative Maßnahmen einsetzen, wenn diese mindestens das Sicherheitsniveau der vereinbarten Maßnahmen erreichen.

Weitere nach Art. 32 DSGVO zu treffende technische und organisatorische Maßnahmen sind für die Fernwartung nicht einschlägig oder liegen im Verantwortungsbereich des Auftraggebers. Insoweit sind durch den Auftragnehmer keine Maßnahmen zu veranlassen.