Elektro Rüegg AG
Voa Principala 28, 7078 Lenzerheide, +41 81 385 17 17
La Fola 7, 7083 Lantsch/Lenz, +41 81 385 17 17
www.ruegg-elektro.ch, info@ruegg-elektro.ch

AUFTRAGSBEARBEITUNGSVERTRAG (ADV)
(Vereinbarung)

zwischen

Kunde der " Einverständniserklärung in den Auftragsbearbeitungsvertrag"

Verantwortlicher (Auftraggeber)

und

Elektro Rüegg AG
Voa Principala 28, 7078 Lenzerheide als

Auftragsbearbeiter (Auftragnehmer)

Verantwortlicher und Datenauftragsbearbeiter einzeln **Partei** und zusammen **Parteien**

betreffend

Auftragsbearbeitung nach dem Recht der Schweiz

1 Gegenstand

(a) Zwischen den Parteien besteht ein Rechtsverhältnis, für dessen Durchführung Personendaten vom Verantwortlichen an den Auftragsbearbeiter übertragen werden. Diese Vereinbarung wird zwischen den Parteien geschlossen, um bei der Übertragung von Personendaten einen angemessenen Schutz zu gewährleisten. Bei Widersprüchen zwischen dieser Vereinbarung und anderen Verträgen geht diese Vereinbarung vor, sofern und soweit sie mit der Verarbeitung von Personendaten durch den Auftragnehmer unter dem existierenden Vertrag in Zusammenhang steht.

1.1 Definitionen

(a) Solange in dieser Vereinbarung nicht abweichend bestimmt, sollen alle Begrifflichkeiten dieselbe Bedeutung haben, wie im Schweizer Bundesdatenschutzgesetz ("**DSG**") vom 19. Juni 1992 bzw. vom 20. September 2020, sobald letzteres in Kraft ist. Jede Bezugnahme auf das DSG soll stets einen Bezug auf die aktuelle Verordnung zum DSG ("**VDSG**") beinhalten und auch zu jeder anderen Rechtsvorschrift des zugrunde liegenden Schweizer Datenschutzrechts.

(b) Ferner unterstützt diese Vereinbarung die Parteien bei der Einhaltung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 ("EU-DSGVO"). Verweise auf die EU-DSGVO sind nur für diejenigen Datenbearbeitungen relevant, auf welche die EU-DSGVO anwendbar ist. Führen Verweise auf die EU-DSGVO zu einem Widerspruch zum Schweizer Datenschutzrecht, geht letzteres vor.

1.2 Beschreibung der Datenbearbeitung

(a) Die von dieser Auftragsbearbeitung umfassten Personendaten und Zwecke der Bearbeitung sind im Anhang 1 zu dieser Vereinbarung beschrieben. Anhang 1 ist integraler Bestandteil dieser Vereinbarung und kann von Zeit zu Zeit durch den Verantwortlichen einseitig geändert werden.

2 Pflichten des Verantwortlichen

(a) Der Verantwortliche gewährleistet,

(1) dass die Übertragung von Personendaten und die Bearbeitung solcher Daten durch den Auftragsbearbeiter wie in dieser Vereinbarung niedergelegt, nach dem anwendbaren Recht zulässig sind und der Verantwortliche bewirkt, dass die Übertragung an den Auftragnehmer im Einklang mit dem anwendbaren Recht erfolgt und

(2) dass keine andere gesetzliche Bestimmung die Übertragung der Datenbearbeitung verbietet.

(b) Der Verantwortliche hat sich davon überzeugt, dass die durch den Auftragsbearbeiter eingesetzten, in Anhang 2 beschriebenen, technischen und organisatorischen Massnahmen ausreichend sind, um für die übertragenen Personendaten einen angemessenen Datenschutz sicher zu stellen.

3 Pflichten des Auftragsbearbeiters

3.1 Allgemein

(a) Der Auftragsbearbeiter sichert in Bezug auf die Bearbeitung der Personendaten gemäss Anhang 1 zu, dass er

(1) diese Personendaten in Einklang mit dieser Vereinbarung und ausschliesslich für die Zwecke, die der Verantwortliche verfolgt, bearbeiten wird,

(2) die Zwecke, die der Verantwortliche verfolgt, sich aus Anhang 1 oder aus den ausdrücklichen Weisungen des Verantwortlichen ergeben oder durch eine andere Vereinbarung mit dem Verantwortlichen festgelegt werden,

(3) dem Verantwortlichen diejenigen Informationen zur Verfügung stellen wird, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind,

(4) bei seinen Arbeitsmitteln, Produkten, Anwendungen oder Dienstleistungen die Grundsätze des Data Privacy by Design und by Default berücksichtigen,

(5) den Verantwortlichen informieren wird, wenn er diese Vereinbarung nicht mehr einhalten kann oder voraussichtlich nicht mehr einhalten können wird,

(6) dem Verantwortlichen die Kontaktadresse für Datenschutzanfragen mitteilen und diesbezügliche Änderungen von sich aus kommunizieren wird,

(7) den Verantwortlichen bei Datenschutz-Folgenabschätzungen (insb. gem. Art. 35 EU-DSGVO) oder Vorabkonsultationen (insb. gem. Art. 36 EU-DSGVO) angemessen unterstützt und

(8) mit den zuständigen Aufsichtsbehörden im gesetzlich zulässigen Rahmen kooperieren wird.

(b) Weisungsberechtigte Personen des Verantwortlichen werden dem Auftragsbearbeiter zu Beginn der Auftragsbearbeitung in Textform mitgeteilt. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Auftragnehmer unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Mündliche Weisungen sind nur bei unmittelbarer schriftlicher Bestätigung des Verantwortlichen verbindlich. E-Mail ist für die Wahrung der Schriftform ausreichend.

(c) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstosse gegen Gesetzesvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis ihre Gesetzmässigkeit durch den Verantwortlichen bestätigt oder die Weisung geändert wird.

3.2 Datensicherheit

(a) Der Auftragsbearbeiter setzt während der Dauer dieser Vereinbarung angemessene technische und organisatorische Massnahmen ein, wie sie durch das DSG und Art. 32 EU-DSGVO gefordert werden. Der Auftragsbearbeiter hat dabei den Stand der Technik, die Implementierungskosten und die Art, den Umfang und die Zwecke der Bearbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Grund- und Persönlichkeitsrechte betroffener Personen berücksichtigt. Die Massnahmen sind in Anhang 2 beschrieben und werden periodisch überprüft. Änderungen der Massnahmen sind zulässig, sofern das bisherige Sicherheitsniveau nicht unterschritten wird.

(b) Der Auftragsbearbeiter wird

(1) bei der Durchführung der Arbeiten nur Beschäftigte einsetzen, die vertraglich oder durch gesetzliche Bestimmungen zur Vertraulichkeit verpflichtet sind und die zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden,

(2) den Verantwortlichen unverzüglich informieren und mit ihm kooperieren, wenn er der Ansicht ist, dass er nicht länger in der Lage sein könnte oder nicht länger in der Lage ist, diese Vereinbarung und insbesondere die Pflichten zur Datensicherheit einzuhalten,

(3) den Verantwortlichen mit angemessenen Massnahmen bei der Sicherstellung eines dem Risiko angemessenen Datenschutzniveaus unterstützen,

(4) dem Verantwortlichen eine Verletzung der Datensicherheit (inkl. des unbefugten Zugangs zu Personendaten gemäss Anhang 1) unverzüglich melden und dokumentieren, damit dieser die Verletzung innert 72 Stunden einer Aufsichtsbehörde (insb. gem. Art. 33 EU-DSGVO) oder den betroffenen Personen (insb. gem. Art. 34 EU-DSGVO) melden kann. Die Meldung beinhaltet mindestens i) Art der Verletzung der Datensicherheit, ii) Folgen der Verletzung (insb. für Daten gem. Anhang 1), iii) ergriffene Massnahmen und iv) geplante Massnahmen.

(c) Der Auftragnehmer wird Berichte zur Datensicherheit auf rechtmässiges Verlangen dem Verantwortlichen zugänglich machen. Der Verantwortliche hat zudem das Recht, die Einhaltung der vereinbarten Datensicherheit auf eigene Kosten zu prüfen oder durch einen zur Verschwiegenheit verpflichteten Dritten prüfen zu lassen. Kontrollen sind rechtzeitig anzumelden und mit dem Auftragnehmer abzustimmen..

3.3 Subunternehmer

(a) Der Auftragsbearbeiter wird ohne vorherige Zustimmung des Verantwortlichen keine Datenbearbeitung an Subunternehmer übertragen. Die Zustimmung darf der Verantwortliche nicht unvernünftiger Weise verweigern. Stimmt der Verantwortliche einem Subunternehmer zu, entbindet dies den Auftragnehmer in keiner Weise von seiner Verantwortung für die ausgelagerte Datenbearbeitung.

(b) Der Auftragsbearbeiter ist verpflichtet, mit den Subunternehmern Verträge zu schliessen, die mindestens für ein dieser Vereinbarung entsprechendes Datenschutzniveau sorgen.

(c) In der Regel nicht als Unterauftragsbearbeitung gelten Nebenleistungen für den Auftragnehmer ohne Bezug zu den Daten des Verantwortlichen gemäss Anhang 1 (z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservices oder die Entsorgung von Datenträgern sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software). Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei Nebenleistungen angemessene Kontrollmassnahmen zu ergreifen.

3.4 Bekanntgabe ins Ausland

(a) Die Bearbeitung der Daten gemäss Anhang 1 findet grundsätzlich in der Schweiz oder einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über

den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein anderweitiges Drittland darf nur erfolgen, wenn die entsprechenden gesetzlichen Voraussetzungen (Art. 6 DSG bzw. Art. 16 f. DSG vom 20. September 2020; Art. 44 ff. EU-DSGVO) erfüllt sind.

(b) Setzt der Auftragsbearbeiter Subunternehmer in Staaten ein, die gemäss Eidgenössischem Datenschutz- und Öffentlichkeitsbeauftragten, Anhang zur VDSG oder EU-Kommission kein angemessenes Datenschutzniveau besitzen, stellt der Auftragsbearbeiter die datenschutzrechtliche Zulässigkeit der Bekanntgabe durch entsprechende, dem jeweiligen Datentransfer angemessene Massnahmen sicher. Dies erfolgt in der Regel dadurch, dass der Auftragsbearbeiter hierfür mit diesen Subunternehmern die Standardvertragsklauseln gemäss Durchführungsbeschluss (EU) 2021/914 der EU-Kommission ("modernisierte Standardvertragsklauseln") vereinbart. Der Auftragnehmer wird hierbei das richtige Modul (in der Regel Modul 3) der modernisierten Standardvertragsklauseln vereinbaren und insbesondere folgende Anpassungen für die Bearbeitung von Daten vornehmen, die dem Schweizer Datenschutzrecht unterstehen:

(1) Referenzen auf die EU-DSGVO sind als Referenzen auf das schweizerische DSG zu verstehen,

(2) der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte wird als Aufsichtsbehörde bezeichnet,

(3) der Wohnsitz-Gerichtstand von betroffenen Personen mit Wohnsitz in der Schweiz soll nicht ausgeschlossen werden und

(4) bis Inkrafttreten des DSG vom 20. September 2020 umfasst der Begriff "Personendaten" ebenfalls die Daten, die sich auf juristische Personen beziehen.

(c) Für die bestehende Zusammenarbeit mit Subunternehmern in Staaten ohne angemessenes Datenschutzniveau, die sich noch auf die unter der RL 95/46/EG erlassenen Standardvertragsklauseln stützt, werden bis zum 27. Dezember 2022 die modernisierten Standardvertragsklauseln oder eine andere angemessene Garantie vereinbart werden.

4 Rechte der betroffenen Personen

(a) Der Verantwortliche ist dafür verantwortlich, dass die Betroffenen die Informationen erhalten, die ihnen hinsichtlich ihrer Rechte auf Information (Auskunftsrecht), Datenherausgabe- und Übertragung, Berichtigung, Sperrung, Unterdrückung oder Löschung nach dem DSG bzw. Kapitel III EU-DSGVO zustehen. Der Auftragsbearbeiter wird:

(1) dem Verantwortlichen unverzüglich jegliche Anfragen weiterleiten, die Daten gemäss Anhang 1 betreffen, ohne diese selbst zu beantworten,

(2) mit dem Verantwortlichen zusammenarbeiten sowie die erforderlichen Unterstützungsleistungen erbringen, damit der Verantwortliche die Rechte der Betroffenen gemäss DSG oder Kapitel III EU-DSGVO erfüllen kann und

(3) Anfragen des Verantwortlichen bezgl. der Betroffenenrechte innert 15 Arbeitstagen vollständig und wahrheitsgemäss beantworten oder innert dieser Frist erklären, weshalb die Beantwortung länger dauert. In keinem Fall darf die Verzögerung aber dazu führen, dass der Verantwortliche seinen Pflichten nicht nachkommen kann.

5 Dauer und Beendigung

(a) Sofern nicht anders schriftlich vereinbart, endet diese Vereinbarung automatisch mit Beendigung des Hauptvertrags oder Kündigung der "Einverständniserklärung in den Auftragsbearbeitungsvertrag". Die Bestimmungen dieser Vereinbarung überdauern die Beendigung des Hauptvertrages jedoch und bestehen solange fort, wie der Auftragnehmer die Personendaten in seinem Besitz hat.

(b) Der Verantwortliche ist jederzeit zu einer ausserordentlichen Kündigung dieser Vereinbarung aus

wichtigem Grund berechtigt, sofern der Auftragsbearbeiter den wichtigen Grund trotz Mahnung nicht innert angemessener Frist beseitigt. Ein wichtiger Grund liegt vor, wenn der Auftragnehmer

(1) seine Pflichten aus dieser Vereinbarung schwerwiegend verletzt,

(2) Bestimmungen des schweizerischen Datenschutzgesetzes oder der EU-DSGVO vorsätzlich oder grob fahrlässig verletzt, oder

(3) Weisungen des Verantwortlichen nicht ausführt.

(c) Bei Beendigung dieser Vereinbarung, gleich weshalb, hat der Auftragsbearbeiter:

(1) jegliche unter dieser Vereinbarung übertragenen Personendaten und Kopien hiervon zu zerstören oder unwiederbringlich zu löschen, Subunternehmer zu einer Zerstörung oder Löschung zu veranlassen und dem Verantwortlichen zu bestätigen, dass dies durchgeführt wurde.

(2) oder, nach Wahl des Verantwortlichen, sofort jegliche unter dieser Vereinbarung übertragenen Personendaten zurückzugeben und Subunternehmer zu einer Rückgabe zu veranlassen,

(d) Sofern die Gesetzgebung, der der Auftragsbearbeiter unterliegt, es ihm verbietet, die Personendaten oder Teile davon zurückzugeben oder zu zerstören, setzt der Auftragsbearbeiter den Verantwortlichen hiervon in Kenntnis, behandelt solche Personendaten vertraulich und bearbeitet sie nicht aktiv.

6 Verschiedenes

6.1 Ergänzungen

(a) Änderungen, Ergänzungen oder Aufhebungen von Bestimmungen dieser Vereinbarung bedürfen zu ihrer Gültigkeit der Schriftform. Eine Änderung dieser Verpflichtung bedarf ihrerseits zu ihrer Gültigkeit einer schriftlichen Vereinbarung. Adressänderungen sind der anderen Partei unverzüglich in der oben vereinbarten Weise mitzuteilen.

6.2 Bearbeitungsverzeichnis

(a) Jede Partei trägt die Verantwortung dafür, ein Verzeichnis über die Datenbearbeitungen zu führen, sofern keine gesetzliche Ausnahme greift.

6.3 Kosten

(a) Die Kosten im Zusammenhang mit der Durchführung dieser Vereinbarung und der Erfüllung der darin festgelegten Verpflichtungen sind in der Vergütung enthalten, die im Hauptvertrag zwischen den Parteien vereinbart wurde.

6.4 Haftung

(a) Führt die grobfahrlässige oder vorsätzliche Nichteinhaltung dieser Vereinbarung durch den Auftragnehmer zu Schäden beim Verantwortlichen oder Ansprüchen Dritter gegen den Verantwortlichen, wird der Auftragnehmer den Verantwortlichen hiervon schadlos halten.

6.5 Salvatorische Klausel

(a) Sollte eine Bestimmung dieser Vereinbarung nicht vollstreckbar oder ungültig sein, so fällt sie nur im Umfang ihrer Unvollstreckbarkeit oder Ungültigkeit dahin und ist im Übrigen durch eine gültige und vollstreckbare Bestimmung zu ersetzen, die der rechtlichen und wirtschaftlichen Bedeutung der unwirksamen Bestimmung möglichst entspricht. Die übrigen Bestimmungen dieses Vertrags bleiben bindend und in Kraft.

6.6 Abtretungsverbot

(a) Die Zulässigkeit der Abtretung von Rechten und Pflichten aus dieser Vereinbarung ist nach den Regeln des Hauptvertrags zu beurteilen. Fehlt es an einer Regelung im Hauptvertrag, ist es den Parteien ohne vorgängige schriftliche Zustimmung der anderen Partei untersagt, diesen Vertrag oder Rechte und Pflichten aus diesem Vertrag ganz oder teilweise an Dritte abzutreten oder zu übertragen und eine Abtretung oder Übertragung, die ohne vorgängiges schriftliches Einverständnis erfolgt, ist nichtig.

6.7 Anwendbares Recht

(a) Diese Vereinbarung untersteht materiellem schweizerischem Recht, unter Ausschluss der Bestimmungen des Kollisionsrechts und des Wiener Kaufrechts.

6.8 Gerichtsstand

(a) Ausschliesslich zuständig für alle sich aus oder in Zusammenhang mit dieser Vereinbarung ergebenden Streitigkeiten sind die ordentlichen Gerichte am Sitz des Verantwortlichen

Anhang 1

Zweck der Bearbeitung	Gegenstand der Bearbeitung von Personendaten durch den Auftragsbearbeiter ist die Erbringung der im Hauptvertrag beschriebenen Wartungs- und Supportdienstleistungen für den Verantwortlichen.
Dauer der Bearbeitung	Personendaten werden nur für die Dauer des Hauptvertrags oder der Dauer der "Einverständniserklärung in den Auftragsbearbeitungsvertrag" verarbeitet.
Kategorien von betroffenen Personen	Mitarbeiter, Kunden, Partner.
Kategorien von Personendaten	Name, E-Mail, Telefonnummer, Anschrift, Geburtsdatum, Beruf oder weitere Informationen, Aussagen, die sich auf eine bestimmte oder mittels der Information bestimmbare Person beziehen.
Ort der Lagerung und Bearbeitung	An die Geschäftsadresse des Verantwortlichen und seiner zugelassenen Unterauftragsbearbeiter.
Vor-Ort-Prüfungen	Nein
Unterdatenauftragsbearbeiter	Zugelassene Unterdatenauftragsbearbeiter für die Erbringung der im Hauptvertrag beschriebenen Wartungs- und Supportdienstleistungen für den Verantwortlichen.
Überweisung ausserhalb der EU/EWR Schweiz	Nicht erlaubt.
Spezifische Anweisungen oder andere Sonderbestimmungen	Keine weiteren.

Anhang 2: Technische- und organisatorische Massnahmen

Beschreibung der technischen und organisatorischen Sicherheitsmassnahmen, die von dem/den Auftragsbearbeiter(n) durchgeführt werden:

1 Organisatorische Sicherheitsmassnahmen

1.1 Sicherheitsmanagement

(a) Sicherheitskonzept und -verfahren: Der Auftragsbearbeiter verfügt über ein dokumentiertes Sicherheitskonzept für die Bearbeitung von Personendaten.

(b) Rollen und Verantwortlichkeiten:

(1) Die Rollen und Verantwortlichkeiten im Zusammenhang mit der Bearbeitung von Personendaten sind klar definiert und im Einklang mit dem Sicherheitskonzept zugewiesen.

(2) Bei internen Umstrukturierungen oder Kündigungen und beim Wechsel des Arbeitsplatzes ist der Widerruf von Rechten und Zuständigkeiten mit entsprechenden Übergabeverfahren klar definiert.

(c) Politik der Zugangskontrolle: Jeder Rolle, die an der Bearbeitung von Personendaten beteiligt ist, werden nach dem Need-to-know-Prinzip spezifische Zugriffskontrollrechte zugewiesen.

(d) Verwaltung der Ressourcen/Vermögenswerte: Der Auftragsbearbeiter verfügt über ein Register der für die Bearbeitung von Personendaten verwendeten IT-Ressourcen (Hardware, Software und Netzwerk). Eine bestimmte Person ist mit der Pflege und Aktualisierung des Registers betraut.

(e) Änderungsmanagement: Der Auftragsbearbeiter stellt sicher, dass alle Änderungen am IT-System von einer bestimmten Person (z.B. dem IT- oder Sicherheitsbeauftragten) registriert und überwacht werden. Dieser Prozess wird regelmässig überwacht**.**

1.2 Reaktion auf Zwischenfälle und Geschäftskontinuität

(a) Umgang mit Zwischenfällen / Verletzungen des Schutzes von Personendaten:

(1) Es wird ein Plan für die Reaktion auf Zwischenfälle mit detaillierten Verfahren festgelegt, um eine wirksame und ordnungsgemässe Reaktion auf Zwischenfälle im Zusammenhang mit personenbezogenen Daten zu gewährleisten.

(2) Der Auftragsbearbeiter meldet dem Verantwortlichen unverzüglich jeden Sicherheitsvorfall, der zu einem Verlust, einem Missbrauch oder einer unbefugten Kenntnisnahme von Personendaten des Verantwortlichen geführt hat.

(b) Geschäftskontinuität: Der Auftragsbearbeiter hat die wichtigsten Verfahren und Kontrollen festgelegt, die zu befolgen sind, um das erforderliche Mass an Kontinuität und Verfügbarkeit des IT-Systems zur Bearbeitung von Personendaten (im Falle eines Zwischenfalls/einer Verletzung des Schutzes von Personendaten) zu gewährleisten.

1.3 Humanressourcen

(a) Vertraulichkeit des Personals: Der Auftragsbearbeiter stellt sicher, dass alle Mitarbeiter ihre Verantwortlichkeiten und Pflichten im Zusammenhang mit der Bearbeitung von Personendaten kennen. Die Rollen und Zuständigkeiten werden während des Verfahrens vor der Einstellung und/oder bei der Einarbeitung klar kommuniziert.

(b) Schulung: Der Auftragsbearbeiter stellt sicher, dass alle Mitarbeiter angemessen über die Sicherheitskontrollen des IT-Systems informiert sind, die sich auf ihre tägliche Arbeit beziehen. Die mit der Bearbeitung von Personendaten befassten Mitarbeiter werden ausserdem durch regelmässige Sensibilisierungskampagnen angemessen über die einschlägigen Datenschutzanforderungen und rechtlichen Verpflichtungen informiert.

2 Technische Sicherheitsmassnahmen

2.1 Zugangskontrolle und Authentifizierung

(a) Ein Zugangskontrollsystem, das für alle Benutzer, die auf das IT-System zugreifen, gilt, wurde eingeführt. Das System ermöglicht das Anlegen, Genehmigen, Überprüfen und Löschen von Benutzerkonten.

(b) Die Verwendung von gemeinsamen Benutzerkonten wird vermieden. In Fällen, in denen dies notwendig ist, wird sichergestellt, dass alle Benutzer des gemeinsamen Kontos die gleichen Rollen und Verantwortlichkeiten haben.

(c) Bei der Gewährung des Zugangs oder der Zuweisung von Nutzerrollen ist der Grundsatz "Kenntnis nur, wenn nötig" zu beachten, um die Zahl der Nutzer, die Zugang zu Personendaten haben, auf diejenigen zu beschränken, die diesen Zugang für die Erfüllung der Bearbeitungszwecke des Auftragsbearbeiters benötigen.

(d) Wenn die Authentifizierungsmechanismen auf Passwörtern beruhen, verlangt der Auftragsbearbeiter, dass das Passwort mindestens acht Zeichen lang ist und sehr strengen Passwortkontrollparametern entspricht, einschliesslich Länge, Zeichenkomplexität und Nichtwiederholbarkeit.

(e) Die Authentifizierungsdaten (z. B. Benutzer-ID und Passwort) dürfen niemals ungeschützt über das Netz übertragen werden.

(f) Die Authentifizierungsdaten und die Zugangskontrollen auf die Systeme des Verantwortlichen liegen ausserhalb der Kontrolle des Auftragsbearbeiters.

2.2 Protokollierung und Überwachung:

(a) Für jedes System/jede Anwendung, das/die für die Bearbeitung von Personendaten verwendet wird, werden Protokolldateien aktiviert. Sie umfassen alle Arten des Zugriffs auf Daten (Ansicht, Änderung, Löschung).

(b) Eine Protokollierung der Authentifizierung/Zugriffe wird durch den Verantwortlichen durchgeführt.

2.3 Sicherheit von Daten im Ruhezustand

(a) Server-/Datenbank-Sicherheit

(1) Datenbank- und Anwendungsserver sind so konfiguriert, dass sie unter einem separaten Konto mit minimalen Betriebssystemprivilegien laufen, um korrekt zu funktionieren.

(2) Datenbank- und Anwendungsserver bearbeiten nur die Personendaten, deren Bearbeitung zur Erreichung des Bearbeitungszwecks tatsächlich erforderlich ist.

(3) Die Sicherheit der produktiven Server und Datenbanken wird durch den Verantwortlichen gewährleistet und liegt ausserhalb der Kontrolle des Auftragsbearbeiters.

(b) Sicherheit am Arbeitsplatz:

(1) Die Benutzer können die Sicherheitseinstellungen nicht deaktivieren oder umgehen.

(2) Die Antiviren-Anwendungen und Erkennungssignaturen werden regelmässig konfiguriert.

(3) Benutzer haben keine Berechtigung, nicht autorisierte Softwareanwendungen zu installieren oder zu deaktivieren.

(4) Das System verfügt über Sitzungszeitüberschreitungen, wenn der Benutzer eine bestimmte Zeit lang nicht aktiv war.

(5) Kritische Sicherheitsupdates, die vom Entwickler des Betriebssystems veröffentlicht werden, werden regelmässig installiert.

2.4 Netz-/Kommunikationssicherheit:

(a) Bei jedem Zugriff über das Internet wird die Kommunikation durch kryptographische Protokolle verschlüsselt.

(b) Der Verkehr zum und vom IT-System wird durch Firewalls und Intrusion Detection Systeme überwacht und kontrolliert.

2.5 Backups:

(a) Sicherungs- und Datenwiederherstellungsverfahren sind definiert, dokumentiert und klar mit Rollen und Verantwortlichkeiten verknüpft.

(b) Backups werden in angemessenem Umfang physisch und ökologisch geschützt, entsprechend den Standards, die für die ursprünglichen Daten gelten.

(c) Die Ausführung der Backups wird auf Vollständigkeit überwacht.

(d) Die Backup-Strategie der Systeme wird durch den Verantwortlichen bestimmt und liegt ausserhalb der Kontrolle des Auftragsbearbeiters.

2.6 Mobile/tragbare Geräte:

(a) Es werden Verfahren für die Verwaltung mobiler und tragbarer Geräte festgelegt und dokumentiert, die klare Regeln für deren ordnungsgemässe Verwendung enthalten.

(b) Mobile Geräte, die auf das Informationssystem zugreifen dürfen, werden vorab registriert und autorisiert.

(c) Die Verwaltung und Authentifizierung/Zugriffe über mobile Geräte werden durch den Verantwortlichen sicher gestellt.

2.7 Sicherheit im Lebenszyklus von Anwendungen

(a) Während des Entwicklungszyklus werden bewährte Praktiken, der Stand der Technik und anerkannte sichere Entwicklungsverfahren oder -standards befolgt.

2.8 Löschung/Entsorgung von Daten:

(a) Die Datenträger werden vor ihrer Entsorgung mit Software überschrieben. In Fällen, in denen dies nicht möglich ist (CDs, DVDs usw.), werden sie physisch vernichtet.

(b) Papier und tragbare Datenträger, auf denen Personendaten gespeichert sind, werden vernichtet.

2.9 Physische Sicherheit:

(a) Die physische Umgebung der IT-Systeminfrastruktur ist für nicht autorisiertes Personal nicht zugänglich. Durch geeignete technische Massnahmen (z.B. Einbruchmeldeanlage, chipkartengesteuertes Drehkreuz, Ein-Personen-Sicherheitszugangssystem, Schliessanlage) oder organisatorische Massnahmen (z.B. Wachdienst) sind die Sicherheitsbereiche und deren Zugänge gegen das Betreten durch Unbefugte zu schützen.

(b) Die physische Sicherheit der IT-Systeminfrastruktur wird durch den Verantwortlichen gewährleistet und liegt ausserhalb der Kontrolle des Auftragsbearbeiters.