UNTERNEHMENSRICHTLINIE ZUR DATENSCHUTZ-ORGANISATION.

der **ADMEDES GmbH** I Rastatter Str. 15 I 75179 Pforzheim, Germany

INHALTSVERZEICHNIS

VORWORT

Sehr geehrte Damen und Herren,

im digitalen Zeitalter werden ständig Daten erfasst und verarbeitet. Hierbei gilt für uns der Grundsatz:
Wo Daten gespeichert und gesendet werden, muss ein hohes Maß an Datenschutz und Datensicherheit gewährleistet sein. Dies gilt für Daten von Kunden, Interessenten und Geschäftspartnern genauso wie für Mitarbeiterdaten. Denn Datenschutz ist Schutz der Person.

Unser Anspruch ist es, dass die ADMEDES GmbH nicht nur für Ideen, Expertise und Passion steht, sondern auch Standards beim Datenschutz setzt. Denn die Persönlichkeitsrechte und die Privatsphäre eines jeden Einzelnen zu wahren, ist für uns die Basis für vertrauensvolle Geschäftsbeziehungen.

In unserer Unternehmensrichtlinie zum Datenschutz haben wir strenge Voraussetzungen für die Verarbeitung personenbezogener Daten von Kunden, Interessenten, Geschäftspartnern und Mitarbeitern geregelt.
Diese entspricht den Anforderungen der Europäischen Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG). Dadurch setzen wir einen Datenschutz und Datensicherheitsstandard in unserem Unternehmen.

Alle Beschäftigten der ADMEDES GmbH sind verpflichtet, diese Unternehmensrichtlinie zum Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze zu wahren.

1. GELTUNGSBEREICH UND ÄNDERUNG DER DATENSCHUTZRICHTLINIE

Diese Datenschutzrichtlinie gilt für die ADMEDES GmbH, sowie für alle Tochtergesellschaften. Der Anwendungsbereich der Datenschutzlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten.
Daten, die anonymisiert wurden, z. B. für statistische Auswertungen, unterliegen nicht dieser Datenschutzrichtlinie. Eine Änderung dieser Datenschutzrichtlinie erfolgt ausschließlich in Abstimmung mit dem Datenschutzbeauftragten (DSB). Die aktuellste Version der Datenschutzrichtlinie kann auf der Internetseite der ADMEDES GmbH, www.admedes.com , abgerufen werden.

2. GRUNDSÄTZE

Der Schutz personenbezogener Daten ist ein wichtiges Anliegen der ADMEDES GmbH. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden sowie Geschäftspartner im Rahmen der gesetzlichen Vorschriften zur Datenverarbeitung und Datensicherheit.
In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Des Weiteren beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn sie Fragen zu unserem Vorgehen im Datenschutz haben.
Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei der ADMEDES GmbH bestehenden Verantwortlichkeiten. Alle Mitarbeiter sind zur Einhaltung der Richtlinie verpflichtet.
Dabei gelten folgende Grundsätze:
Hard- und Software, die personenbezogene Daten verarbeitet, ist nur für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern.
Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter (Benutzer) über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.
Der DSB berät bei der Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem DSB auskunftspflichtig.

3. DER BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE/DATENSCHUTZKOORDINATOR

3.1. Die ADMEDES GmbH hat nach Maßgabe des Artikels 37 DSGVO einen betrieblichen Datenschutzbeauftragten (DSB) bestellt. Der DSB nimmt die ihm durch das Gesetz und aus dieser Richtlinie übertragenen Aufgaben eigenhändig unter Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr.

3.2. Aufgaben des DSB:

- Unterrichtung und Beratung der Unternehmensleitung und Beschäftigten hinsichtlich ihrer Datenschutzpflichten
- Überwachung der Einhaltung der Datenschutzvorschriften
- Ausarbeitung von Strategien für den Schutz personenbezogener Daten mit den Verantwortlichen
- Zuweisung von Zuständigkeiten
- Sensibilisierung und Schulung der Mitarbeiter

3.3. Im Falle risikoreicher Datenverarbeitungen steht der DSB dem Verantwortlichen beratend bei der Risikoabwägung zur Seite.

3.4. Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Unternehmensleitung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

3.5. Soweit es sich organisatorisch als notwendig erweist, ernennt die Geschäftsleitung einen Datenschutzkoordinator.

3.6. Der Koordinator sorgt mit dem DSB für die Einhaltung der für das Unternehmen geltenden Datenschutzvorschriften. Er informiert den DSB über vor Ort aufgetretene Datenschutzfragen.

3.7. Das Unternehmen hat ein Verzeichnis über alle Verarbeitungstätigkeiten (VVT) zu führen. In jeder Fachabteilung wird mindestens einer Person die Verantwortung übertragen, die dafür notwendigen Informationen zu den Verfahren der jeweiligen Abteilung zusammenzutragen und diese entsprechend den Anforderungen des Art. 30 DSGVO zu dokumentieren. Bei Unklarheiten hinsichtlich der gesetzlich geforderten Informationen kann der DSB beratend hinzugezogen werden. Dem DSB ist eine Kopie des VVTs zu übergeben. Das VVT ist durch Unterstützung des DSB immer auf dem aktuellen Stand zu halten. Auf Anfrage stellt das Unternehmen der Aufsichtsbehörde das VVT zur Verfügung. Im Einvernehmen mit der Unternehmensleitung ist hierfür der DSB zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

3.8. Jeder Mitarbeiter kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den DSB wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

3.9. Der DSB berichtet jährlich in einem Tätigkeitsbericht der Geschäftsführung und dem Datenschutzkoordinator über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel. Soweit der Bericht die Verarbeitung von Personaldaten oder Fragen der betrieblichen Organisation betrifft, wird er auch dem Betriebsrat zugänglich gemacht.

4. BESCHAFFUNG VON HARD- UND SOFTWARE

4.1. Die Beschaffung von Hard- und Software erfolgt grundsätzlich durch die IT Abteilung. Bereits bei der Auswahl von Hard- und Software wird der Datenschutz durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

4.2. Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden.

4.3. Die IT-Abteilung führt ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme. Der DSB erhält eine Kopie.

4.4. Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind die IT Abteilung und der DSB unverzüglich zu informieren.

5. VERPFLICHTUNG/SCHULUNG DER MITARBEITER

5.1. Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Merkblatts „Mitarbeiterinformation Datenschutz" und in deren in „Anlage 1" angehängten Formulars, welches die Verpflichtung auf das Datengeheimnis nach § 53 BDSG beinhaltet.

5.2. Mitarbeiter, die besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis nach § 88 TKG) unterliegen, werden von den Vorgesetzten ergänzend schriftlich verpflichtet. Die jeweilige Verpflichtungserklärung ist den Personalakten beizulegen.

5.3. Der DSB ist für die Verpflichtung von Mitarbeitern und deren Arbeitsplatz zwecks von ihm vorzunehmender weiterer Schulungen und die Feststellung evtl. Kontrollbedarfs verantwortlich. Er ist über neu zu schulende Mitarbeiter zu informieren.

5.4. Für in Abstimmung mit den jeweiligen Abteilungsleitungen angesetzte Schulungstermine sind die betroffenen Mitarbeiter freizustellen.

6. PRINZIPIEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

6.1. Fairness und Rechtmäßigkeit
Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden.

6.2. Zweckbindung
Die Verarbeitung personenbezogener Daten darf lediglich die zuvor festgelegten Zwecke verfolgen. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

6.3. Transparenz
Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- Die für die Verarbeitung verantwortliche Stelle
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an welche die Daten gegebenenfalls übermittelt werden

6.4. Datenvermeidung und Datensparsamkeit
Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches
Recht vorgeschrieben oder erlaubt.

6.5. Löschung
Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben. Dies ist der Fall bis die schutzwürdigen Interessen rechtlich geklärt wurden oder die Archive des Unternehmens den Datenbestand auf seinen historischen Zweck und damit über die Archivaufnahme untersuchen konnten.

6.6. Sachliche Richtigkeit und Datenaktualität
Personenbezogene Daten sind richtig, vollständig und soweit erforderlich auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nichtzutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

6.7. Vertraulichkeit und Datensicherheit
Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene technische und organisatorische Maßnahmen (TOM) gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

7. ZULÄSSIGKEIT DER DATENVERARBEITUNG

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Berechtigungen vorliegt. Eine solche Erlaubnis ist auch dann erforderlich, wenn es um eine bloße Zweckänderung der Erhebung, Verarbeitung und Nutzung geht.

7.1. KUNDEN- UND PARTNERDATEN

7.1.1. Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung den von ihnen angegebenen Daten kontaktiert werden. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten. Für darüberhinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter 7.1.2 beachtet werden. Kundennamen werden bei der ADMEDES GmbH pseudonymisiert, was bedeutet, dass der Kundenname durch ein Pseudonym ersetzt wird.

7.1.2. Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an die ADMEDES GmbH (z.B. Wunsch nach Zusendung von Informationsmaterial), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig. Darüber hinausgehende Maßnahmen bedürfen weiterer rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt-und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene soll über die Freiwilligkeit der Datenangabe für diese Zwecke informiert werden. Im Rahmen der Kommunikation mit dem Betroffenen soll eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden.

7.1.3. Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß 6.3. dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Die Erteilung einer mündlichen Einwilligung muss dokumentiert werden.

7.1.4. Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

7.1.5. Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der ADMEDES GmbH erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

7.1.6. Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der DSB oder Datenschutzkoordinator im Vorfeld zu informieren.

7.1.7. Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, finden bei der ADMEDES GmbH keinerlei Anwendung.

7.1.8. Nutzerdaten und Internet

Die Information, welche personenbezogenen Daten beim Besuch der Website der ADMEDES GmbH erhoben, verarbeitet und genutzt werden, können aus den Datenschutz- und Cookie-Hinweisen auf der Website entnommen werden. Die Datenschutz- und Cookie-Hinweise sind so integriert, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind. Es gibt keine registrierungspflichtigen Bereiche. Die über das Kontaktformular oder über was Bewerberportal eingegebenen Daten werden nur zu den Zwecken gespeichert und verarbeitet, zu denen sie erhoben wurden. Diese Daten werden ohne eine Einwilligung nicht an Dritte weitergegeben und werden nach den Regelfristen für die Löschung der Daten gelöscht.

7.2. MITARBEITERDATEN

7.2.1. Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Für Bewerberdaten gilt die „DATENSCHUTZERKLÄRUNG der ADMEDES GmbH zu Bewerbungen".
Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Berechtigungen für die Datenverarbeitung eingreift. Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen. Für Verarbeitungen von personenbezogenen Daten, die mit dem Arbeitsverhältnis zusammenhängen, jedoch nicht der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

7.2.2. Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Voraussetzung für die Verarbeitung personenbezogener Mitarbeiterdaten ist des Weiteren im Gesetz verankert. Art und Umfang des Datenverarbeitungsvorgangs müssen sich nach den staatlichen Rechtsvorschriften richten und somit die Anforderungen an die gesetzlich zulässige Datenverarbeitung erfüllen. Besteht bei der Auslegung der gesetzlichen Bestimmungen Handlungsspielraum, so sind die schutzwürdigen Interessen des Mitarbeiters zu berücksichtigen.

7.2.3. Kollektivregelungen für Datenverarbeitungen

Geht eine Verarbeitung über den Vertragszweck hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts zu gestalten.

7.2.4. Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß 6.3. dieser Datenschutzrichtlinie informiert werden.

7.2.5. Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der ADMEDES GmbH erforderlich ist.
Begründungen eines berechtigten Interesses sind in der Regel:

- rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche)
- wirtschaftlich (z.B. Bewertung von Unternehmen)

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen. Kontrollmaßnahmen, die Mitarbeiterdaten verarbeiten, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei begründetem Anlass muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters abgewogen werden und dürfen nur bei Angemessenheit durchgeführt werden. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

7.2.6. Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft werden. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, staatlichen Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der DSB für den Datenschutz im Vorfeld zu informieren.

7.2.7. Automatisierte Entscheidungen

Im Beschäftigungsverhältnis finden bei der ADMEDES GmbH keinerlei automatisierte Verarbeitungen personenbezogener Daten statt.

7.2.8. Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet werden in erster Linie im Rahmen der Erfüllung betrieblichen Aufgaben durch das Unternehmen zur Verfügung gestellt. Eine private Nutzung ist nicht erlaubt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der im Mitarbeiterhandbuch festgehaltenen „Verbindliche Hinweise für den Gebrauch und die Nutzung von Geräten" genutzt werden. Vertrauliche Texte mittels Übersetzungsplattformen (wie z.B. „Google Übersetzter") übersetzen zu lassen ist untersagt, da solche Übersetzungsplattformen die gesamten Texte verarbeiten und somit personenbezogene und vertrauliche Daten preisgegeben werden könnten. Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer werden regelmäßige, mehrstufige Auswertungen von Protokollen, Virenschutz, Firewall und Email-Filtersystem durchgeführt und das redundante Backup-Systemen auf seine ordnungsgemäße Funktion überprüft. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der ADMEDES GmbH erfolgen. Diese Kontrollen müssen verhältnismäßig sein und dürfen nur durch ermittelnde Bereiche erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Unternehmensregelungen.

8. ÜBERMITTLUNG PERSONENBEZOGENER DATEN

Eine Übermittlung von personenbezogenen Daten an Empfänger innerhalb sowie außerhalb der ADMEDES GmbH unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt 7. Im Falle einer Datenübermittlung innerhalb der ADMEDES GmbH sowie an Tochter- oder Muttergesellschaften, dürfen diese ohne Einwilligung des Betroffenen nur weitergegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der DSB zu kontaktieren.
Im Falle einer Datenübermittlung an einen Empfänger außerhalb der ADMEDES GmbH muss der Empfänger der Daten darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.
Im Falle einer Datenübermittlung an einen Empfänger außerhalb der ADMEDES GmbH in einem Drittstaat muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Eine solche gesetzliche Verpflichtung kann sich aus dem Recht des Standortes der ADMEDES GmbH oder aus dem Recht des Standortes des Datenempfängers ergeben. Der Empfänger der Daten ist verpflichtet mit der Aufsichtsbehörde zu kooperieren und die Feststellungen der Aufsichtsbehörde im Hinblick auf die übermittelnden Daten zu beachten.

Im Fall eines von einem Betroffenen behaupteten Verstoßes gegen diese Datenschutzrichtlinie durch den Empfänger der Daten mit Sitz in einem Drittstaat verpflichtet sich die ADMEDES GmbH den Betroffenen, dessen Daten bei der ADMEDES GmbH erhoben worden sind sowohl bei der Sachverhaltsaufklärung zu unterstützen als auch die Durchsetzung seiner Rechte gemäß dieser Datenschutzrichtlinie gegenüber dem Empfänger der Daten sicherzustellen. Darüber hinaus ist der Betroffene berechtigt, seine Rechte auch gegenüber der ADMEDES GmbH geltend zu machen. Bei einem behaupteten Verstoß muss die ADMEDES GmbH gegenüber dem Betroffenen den Nachweis erbringen, dass der Empfänger der Daten in einem Drittland bei einer Weiterverarbeitung der erhaltenen Daten ein Verstoß gegen diese Datenschutzrichtlinie nicht zuzurechnen ist.
Im Falle einer Datenübermittlung von Dritten an die ADMEDES GmbH muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.
Im Fall einer Übermittlung personenbezogener Daten von der ADMEDES GmbH an eine Tochter- oder Muttergesellschaft mit Sitz in einem Drittstaat hat die ADMEDES GmbH den Betroffenen, dessen personenbezogene Daten im Europäischen Wirtschaftsraum erhoben worden sind, bei zurechenbaren Verstößen der Tochter- oder Muttergesellschaft mit Sitz in einem Drittstaat gegen diese Datenschutzrichtlinie haftungsrechtlich so zu stellen als hätte die ADMEDES GmbH den Verstoß begangen. Gerichtsstand ist das zuständige Gericht am Sitz der ADMEDES GmbH.

9. EXTERNE DIENSTLEISTER/AUFTRAGSVERARBEITUNG/WARTUNG

9.1. Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung,Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist ein Vertrag zur Auftragsdatenverarbeitung abzuschließen.

9.2. Entsprechendes gilt, falls die ADMEDES GmbH entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

10. RECHENSCHAFTS- UND DOKUMENTATIONSPFLICHT

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein („Accountability“). Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

Pforzheim, den 12.07.2019

ADMEDES GmbH

Dr. Axel Pfrommer
Geschäftsführer