Vereinbarung zur Auftragsverarbeitung – Datenschutz und Informationssicherheit

Zwischen der

media**DIALOG** Gesellschaft für Softwareentwicklung mbH

und

media**DIALOG** Service & Support GmbH

vertreten durch ihre jeweils einzelvertretungsberechtigten Geschäftsführer

Andreas Varnholt, Jan-Philip Sasse und Christopher Bock,

inländische Geschäftsanschrift: Bismarckstraße 38, D-57076 Siegen

- im Folgenden „Auftragnehmer“ genannt -

und der

KUNDE / AUFTRAGGEBER

- im Folgenden „Auftraggeber“ genannt -

wird die nachfolgende

Vereinbarung zur Auftragsverarbeitung – Datenschutz und Informationssicherheit

geschlossen:

Inhalt

§ 1 Beschreibung

Zwischen Auftraggeber und Auftragnehmer werden als Ergänzung zu allen zwischen den Parteien bestehenden Vereinbarungen, anlässlich derer der Auftragnehmer oder durch ihn beauftragte Personen und Unterauftragnehmer in Kontakt mit personenbezogenen Daten im Sinne der deutschen und europäischen Datenschutzgesetze kommen, die Allgemeinen Vorschriften Datenschutz und Informationssicherheit (nachfolgend „AVDI") einbezogen, die als Anlage 1 Bestandteil dieser Vereinbarung sind. Von den Regelungen sind u.a. folgende Verträge betroffen (nicht abschließend): Supportverträge, Remoteverträge, Hosting-Verträge, Nutzungsverträge, etc.

§ 2 Gegenstand der Verträge

Gegenstand der Verträge ist es, die Verfügbarkeit der beim oder für den Auftraggeber im Einsatz befindlichen Anwendungen des Auftraggebers zu gewährleisten, zu optimieren, Störungen und Ausfälle möglichst zu vermeiden sowie die rasche Beseitigung von auftauchenden Problemen und Fehlern sicherzustellen.

§ 3 Dauer

Die Dauer der einzelnen Verträge ergibt sich aus den jeweiligen Verträgen im Sinne Ziffer 1 dieser Vereinbarung. Der Auftraggeber kann diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen der EU-Datenschutzgrundverordnung (EU-DSGVO) oder des neuen Bundesdatenschutzgesetzes (BDSG-neu) oder gegen diese Vereinbarung vorliegt, der Auftragnehmer einer Weisung des Auftraggebers nicht nachkommt oder sich einer angemessenen Datenschutzkontrolle entzieht. Eine Kündigung kann nur schriftlich erfolgen.

Mitgeltende Anlagen:

Anlage 1: Allgemeine Vorschriften Datenschutz und Informationssicherheit (AVDI)
Anlage 2: Selbstauskunft: Technische und organisatorische Maßnahmen
Anlage 3: Ergänzende Regelungen zur Fernwartung
Anlage 4: Liste der Ansprechpartner
Anlage 5: Liste der Subunternehmer/Unterauftragnehmer
Anlage 6: Meldeformular für Datenschutzverstöße

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Name, Funktion	Geschäftsführung media**DIALOG**
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer (media**DIALOG**)

Anlage 1: Allgemeine Vorschriften Datenschutz und Informationssicherheit (AVDI)

(Stand August 2022)

§ 1 Präambel

(1) Diese AVDI basieren auf der EU-DSGVO (EU-Datenschutz-Grundverordnung) und insbesondere Festlegungen nach Art. 28 EU-DSGVO zur Auftragsverarbeitung, sowie den Erweiterungen und Konkretisierungen der EU-DSGVO im BDSG-neu (Bundesdatenschutzgesetz). Diese Festlegungen stellen an den Auftraggeber wie den Auftragnehmer zusätzliche Anforderungen. Beide Parteien haben bei Missachtung mit empfindlichen Bußgeldern bis hin zum Verbot der Datenverarbeitung zu rechnen.

(2) Obwohl Wartung, Pflege und Service prinzipiell vom Aufraggeber so gestaltet werden können, dass auf IT-Ebene ein Zugriff auf personenbezogene Daten durch den Auftragnehmer ausgeschlossen werden könnte, ist dieser Ausschluss praktisch oft nicht umsetzbar. Entsprechend unterwirft sich der Auftragsnehmer den strengen Regeln der Auftragsverarbeitung und unterstützt den Auftraggeber bei der Einhaltung und Umsetzung dieser gesetzlichen Anforderungen nach Art. 28 EU-DSGVO.

§ 2 Vertrauliche Beziehungen

Zwischen Auftraggeber und Auftragnehmer werden als Ergänzung zu allen zwischen den Parteien bestehenden Vereinbarungen, anlässlich derer der Auftragnehmer oder durch ihn beauftragte Dritte in Kontakt mit personenbezogenen Daten im Sinne der EU-DSGVO kommen, die nachfolgenden Regelungen getroffen.

Die Datenverarbeitung erfolgt durch den Auftragnehmer als weisungsgebundene Tätigkeit nach Maßgabe der nachstehenden Vereinbarungen im Auftrag des Auftraggebers im Sinne von Art. 28 Abs. 3a) EU-DSGVO. Gegenüber den betroffenen Personen und Dritten trägt allein der Auftraggeber die Verantwortung für die Zulässigkeit der in seinem Auftrag durchgeführten Verarbeitungen personenbezogener Daten, soweit dies nicht anderes spezifiziert wurde oder gesetzlich vorgesehen ist. Die Datenverarbeitung im Auftrag als gemeinsame, gleichberechtigte Verantwortungsaufgabe von Auftraggeber und Auftragnehmer nach Artikel 26 EU-DSGVO findet nicht statt. Betroffene Verträge sind insbesondere Fernwartungsvereinbarungen.

§ 3 Definitionen

Der Auftraggeber ist Verantwortlicher gemäß Art. 4 Nr. 7 EU-DSGVO. Der Auftragnehmer ist Auftragsverarbeiter gemäß Art. 4 Nr. 8 EU-DSGVO. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Datenverarbeitung im Auftrag ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers. Verarbeitung meint die Verwendung personenbezogener Daten. Diese umfasst insbesondere die Erhebung, Speicherung, Übermittlung, Sperrung / Einschränkung, Löschung sowie das Anonymisieren, Pseudonymisieren, Verschlüsseln oder die sonstige Nutzung von Daten.

§ 4 Umfang, Art und Zweck

§ 4.1 Umfang, Art und Zweck der Erhebung

Anlässlich der Durchführung der betroffenen Verträge ist es nicht ausgeschlossen, dass der Auftragnehmer zufällig Kenntnis von personenbezogenen Daten erhält. Im Übrigen verarbeitet der Auftragnehmer keine personenbezogenen Daten des Auftraggebers im ursprünglichen Sinne. Auf Wunsch stellt der Auftragnehmer die Anwendung als SaaS zur Verfügung und sorgt für einen ordnungsgemäßen Betrieb. Es ist nicht intendiert, dass der Auftragnehmer Daten des Auftraggebers in diese Anwendung eingibt, verändert oder löscht. Dies obliegt dem Auftraggeber. Siehe auch § 4.3.

§ 4.2 Arten der Daten und Kreis der Betroffenen

Die durch den Auftraggeber erzeugten Daten können sowohl „einfache" personenbezogene Daten darstellen als auch besondere personenbezogene Daten (sensible Daten) im Sinne von Art. 9 Abs. 1 EU-DSGVO sein. Der Kreis der Betroffenen kann insbesondere Beschäftigte, Kunden und Interessenten des Auftraggebers umfassen. Der Auftraggeber sichert dem Auftragnehmer zu, dass die personenbezogenen Daten rechtmäßig erhoben wurden. Kommt es zu einer Schädigung beim Auftragnehmer aufgrund einer nicht rechtskonformen Erhebung, dann übernimmt der Auftraggeber die durch die Schädigung entstandenen die Kosten.

§ 4.3 Berechtigung, Sperrung und Löschung von Daten, Betroffenenrechte

(1) Der Auftragnehmer wird ohne Weisung des Auftraggebers keine Berichtigung, Sperrung oder Löschung von Daten vornehmen. Die Parteien stellen klar, dass eine solche Nutzung nicht Gegenstand der Verträge i. S. v Ziffer 2 ist.

(2) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anfragen von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

§ 5 Weisungen des Auftraggebers

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Der Auftraggeber ist berechtigt, vollumfänglich Weisungen zu erteilen. Mündliche Weisungen hat der Auftraggeber schriftlich zu bestätigen.

§ 6 Erforderliche Verpflichtungen

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers den Datenschutz gemäß EU-DSGVO / BDSG-neu sowie gem. § 3 TTDSG sowie ggf. Sondergesetzen wie z.B. SGB V zu wahren. Er verpflichtet sich also, die gleichen Datenschutzschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Soweit der Auftraggeber Sondergesetzen des Datenschutzes unterliegt, die über EU-DSGVO, BDSG-neu, Telekommunikation-Telemedien-Datenschutzgesetz TTDSG hinausgehen, ist der Auftraggeber verpflichtet, den Auftragnehmer auf die Geltung dieser Gesetze ausdrücklich hinzuweisen. Der Auftragnehmer wird sodann unverzüglich seine daraus folgenden Verpflichtungen feststellen und einhalten. Er wird nur Mitarbeiter beschäftigen, deren Zuverlässigkeit und Vertrauenswürdigkeit er sich zuvor versichert hat. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die Einhaltung der datenschutzrechtlichen Vorschriften überwacht. Der Auftragnehmer sichert zu, dass seine mit der Verarbeitung

der Daten des Auftraggebers beschäftigten Mitarbeiter stets auf die Vertraulichkeit im Sinne der EU DSGVO sowie gem. §3 TTDSG schriftlich auf das Daten- und das Fernmeldegeheimnis verpflichtet sind.

(2) Die Verarbeitung der Daten findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind.

(3) Auskünfte über Daten und Gegebenheiten im Zusammenhang mit der Auftragsausführung des Auftragnehmers für den Auftraggeber darf der Auftragnehmer Dritten gegenüber nur nach vorheriger schriftlicher Zustimmung erteilen. In diesem Vertrag ausdrücklich geregelte oder gesetzlich vorgeschriebene Auskunftsrechte bzw. Auskunftspflichten bleiben hiervon unberührt. Auskünfte nach Datenschutzrecht erteilt allein der Auftraggeber als verantwortliche Stelle. An der Erstellung notwendiger Verarbeitungsbeschreibungen hat der Auftragnehmer auf Anforderung des Auftraggebers mitzuwirken. Er hat dem Auftraggeber insoweit die erforderlichen Angaben zuzuleiten.
Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der in diesem Vertrag vereinbarten sowie der allgemeinen technischen und organisatorischen Maßnahmen (TOMs) gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 EU-DSGVO zu. Er wird also seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird TOMs zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen. Der Auftragnehmer dokumentiert von Ihm ergriffene Maßnahmen zur Einhaltung seiner Verpflichtungen aus den vorstehenden Ziffern schriftlich und nachvollziehbar.

§ 7 Geschäftsgeheimnis

(1) Der Auftragnehmer verpflichtet sich, über nicht allgemein bekannte, geschäftlich relevante und bedeutsame Angelegenheiten des Auftraggebers (Geschäftsgeheimnisse) Verschwiegenheit zu wahren. Er wird auch seine Mitarbeiter zur Verschwiegenheit verpflichten, vgl. dazu auch 6(1). Dem Auftraggeber bleibt es unabhängig davon unbenommen, entsprechende Verschwiegenheitsverpflichtungen direkt mit den Mitarbeitern des Auftragnehmers zu vereinbaren.

(2) Soweit nicht näher im Hauptvertag beschrieben, gilt, dass sich die Parteien zu strikter Vertraulichkeit Dritten gegenüber verpflichten. Die Parteien sind insbesondere verpflichtet, alle ihnen anlässlich der Durchführung des Auftrags bekanntwerdenden Geschäfts- und Betriebsgeheimnisse, Herstellungsverfahren, Arbeitsmethoden und sonstigen geschäftlichen bzw. betrieblichen Tatsachen, Unterlagen und Informationen der anderen Partei sowie

ihrer Kunden und Geschäftspartner streng vertraulich zu behandeln, in keiner Weise Dritten zugänglich zu machen oder sonst zu verwenden, vorbehaltlich anderer vertraglicher Absprachen. Die Weitergabe solcher Informationen ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig.

§ 8 Technische und Organisatorische Maßnahme (TOM) und Nutzung von Zertifikaten (z.B. ISO 27001), Testaten und Selbstauskünften

(1) Der Auftragnehmer gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft TOMs zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust, die den Forderungen des Art. 32 DSGVO entsprechen und in § 64 BDSG-neu konkretisiert werden: Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übertragungs-, Eingabe-, Transport-, Wiederherstellbarkeit, Auftrags- und Verfügbarkeitskontrolle, sowie Zuverlässigkeit, Datenintegrität und Trennbarkeit. Bei Maßnahmen hinsichtlich der Zugangs-, Transport-, Übertragungs-, Datenträger- und Benutzerkontrolle ist insbesondere auf die Verwendung von auf dem Stand der Technik entsprechenden Verschlüsselungsverfahren zu achten.

(2) Insbesondere sichert der Auftragnehmer die Einhaltung der TOMs zu, die er in der Anlage 2 Selbstauskunft TOMs aufgeführt hat. Die TOMs unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insbesondere ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Verfügt der Auftragnehmer über ein datenschutzrelevantes Zertifikat, kann dieses unter folgenden Voraussetzungen zur Unterstützung der Vorabkontrollen und Überwachungen durch den Auftraggeber genutzt werden:

1. Das Zertifikat muss gültig sein.
2. Die Auftragsverarbeitung des Auftragsnehmers muss im Scope der Zertifizierung liegen.
3. Das Statement of Applicability (SoA) darf keine Ausschlüsse aufweisen hinsichtlich der in Art. 32 EU-DSGVO genannten TOMs.
4. Es werden lückenlos interne und externe Audits durchgeführt.
5. Der Auftraggeber bekommt auf Anforderung Einsicht in den letzten Audit Report.

Ebenso können Datenschutz-Testate von sachverständigen Dritten sowie Selbstauskünfte des Auftragnehmers Verwendung finden. Bitte beachten Sie, dass Zertifikate, Testate und Selbstauskünfte die Vorabkontrolle und Überwachung durch den Auftraggeber erheblich erleichtern, jedoch nicht ersetzen.

§ 9 Ansprechpartner

Die Parteien sind sich darüber einig, dass es notwendig ist, Regelungen zur Kommunikation zu treffen, um eine sichere, störungsfreie und datenschutzgerechte Auftragsausführung zu gewährleisten. Der Auftragnehmer hat den Auftraggeber vor wichtigen Eingriffen in das EDV-System über beabsichtigte Änderungen und Eingriffe unverzüglich zu informieren und diese nur nach entsprechender Freigabe durch den Auftraggeber zu veranlassen bzw. durchzuführen. Die Parteien benennen wechselseitig Ansprechpartner und werden diesbezügliche Änderungen dem jeweils anderen Vertragspartner unverzüglich schriftlich mitteilen. Der Auftragnehmer darf Auskünfte ausschließlich gegenüber den vom Auftraggeber autorisierten Personen erteilen. Der Auftragnehmer verpflichtet sich durch TOMs sicherzustellen, dass nur die für die Auftragsbearbeitung erforderlichen Mitarbeiter Zugang zu den zu betreuenden EDV-Systemen und Zugriff auf die zu verarbeitenden Daten des Auftraggebers erlangen können (need-to-know-Prinzip). Die Parteien benennen ihre jeweiligen Ansprechpartner in Anlage 5: Liste der Subunternehmer / Unterauftragnehmer.

§ 10 Pflichten, Kontrolle- und Betretungsrechte, Meldepflichten

(1) Der Auftragnehmer arbeitet datenschutzrechtlich ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt. Er verwendet etwaige zur Verarbeitung überlassene Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien und sonstige Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder zur Durchführung des Auftrages erforderlich sind, sowie Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(2) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Meldung zum Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO notwendigen Angaben zur Verfügung. Ebenso unterstützen

sich Auftragnehmer und Auftraggeber soweit vertretbar und geboten bei etwaigen Datenschutzfolgeabschätzungen, die im Bereich dieser AVDI oder dem Hauptvertag liegen.

(3) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen (insbesondere bei Verdacht auf meldepflichtige Verletzungen des Schutzes personenbezogener Daten nach Art. 33 EU-DSGVO) oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 und Art. 34 EU-DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen.

(4) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften, Testaten eines Sachverständigen, Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie Betreten und Besichtigung der Räumlichkeiten des Auftragnehmers, welche die Leistungserbringung für den Auftraggeber betreffen. Der Auftragnehmer verpflichtet sich insoweit dem Auftraggeber oder von diesem beauftragten Dritten (Auditoren) zu diesem Zwecke Zugang zu den Firmenräumen zu gewähren. Wenn diese Prüfungen erhebliche Mehrkosten beim Auftragnehmer verursachen, dann trägt diese Kosten der Auftraggeber.

(5) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten datenschutzrechtlich relevante Unterlagen und erstellten datenschutzrechtlich relevante Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Vertragsverhältnis im Sinne von Ziffer 2 stehen, dem Auftraggeber auszuhändigen. Die verwendeten Datenträger des Auftragnehmers sind danach, soweit technisch möglich, physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich zu bestätigen. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung beziehungsweise Übergabe. Überlassene Datenträger sowie sämtliche hiervon gefertigte Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe, Löschung oder Aufbewahrung der Daten, so trägt diese der Auftraggeber.

(6) Der Auftragnehmer informiert unverzüglich den Auftraggeber darüber, wenn eine zuständige Behörde nach Art. 57 und 58 EU-DSGVO gegen den Auftragnehmer ermittelt.

§ 11 Subunternehmer / Unterauftragnehmer

(1) Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer ist zulässig. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der Anlage 5 zu diesem Vertrag angeben.

(2) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag an diese zu übertragen und zu prüfen, insbesondere dahingehend, dass TOMs nach Art. 32 EU-DSGVO umgesetzt sind. Erst danach ist eine Weiterleitung von Daten zulässig. Der Auftragnehmer informiert den Auftraggeber vor der Auftragserteilung über eine beabsichtige Beauftragung von Unterauftragnehmern. Der Auftraggeber kann der Beauftragung eines genannten Subunternehmers und der Weiterleitung von Daten an diesen widersprechen.

(3) Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Dem Auftraggeber werden Kontroll- und Überprüfungsrechte entsprechend Ziffer 10 eingeräumt. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(4) Nicht als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer von Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen u.a. Lohnbuchhaltungs- und Telekommunikationsdienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene schriftliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 12 Informationspflichten, Rechtswahl

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als verantwortlicher Stelle im Sinne der EU-DSGVO liegen. Es gilt deutsches Recht.

Anlage 2: Selbstauskunft TOMs

Folgende technische und organisatorische Maßnahmen werden vom Auftragnehmer umgesetzt. Auf Grundlage von Art. 25 und insbesondere Art. 32 EU-DSGVO gibt der Auftragnehmer hier an, welche technischen und organisatorischen Maßnahmen er zur Gewährleistung des Datenschutzes und der Datensicherheit getroffen hat. Wenn anwendbar und vertretbar wird eine Maßnahme nach dem Stand der Technik durchgeführt, dies gilt insbesondere für Verschlüsselungsverfahren.

Die folgende Auflistung gibt eine Übersicht der TOMs nach Maßnahmenbereichen an.

In allen folgenden Maßnahmenbereichen wurden TOMs – soweit anwendbar - zur Gewährung eines angemessen Datenschutz- und Informationssicherheitsniveaus eingeführt.

Zutrittskontrolle (Nr. 1):

Bauliche Maßnahmen:

- Einbruchmeldeanlage
- Bewegungsmelder
- Schließkontaktmelder
- Einschränkung des ungehinderten Zutritts für nicht Zutrittsberechtigte durch Türen mit Blindknauf, Zusatzschlösser und Riegel, Klingel für Besucher, Vergitterung der Fenster
- Gegensprechanlage
- Türsicherung (elektronische Türöffner, etc.)
- Zutritt zu den Sicherheitsbereichen (Serverräume) mit nochmals erhöhter Sicherheit nur mit RFID-Token
- Schaffung eines Sichtkontakts durch Fenster innerhalb von Türen einbruchhemmende Fenster und Türen
- vergitterte Fenster

Erläuterung:

Im Unternehmen ist eine Einbruchmeldeanlage installiert, die über Bewegungsmelder die Bewegungsräume im Unternehmen überwacht. Schließkontaktmelder an den Außentüren überwachen den physikalischen Abschluss der Türen. Generell sind alle Außentüren mit RFID-Schlössern ausgestattet. Fluchttüren lassen sich von der Außenseite her nicht bedienen, von der Innenseite her sind sie mit einem mechanischen Knauf ausgestattet. An der rückseitigen Türe sind zusätzlich engsitzende Riegel angebracht. Die Außentüren sind mit einem vergitterten Glaseinsatz versehen, so dass Besucher optisch erkannt werden können. Im Keller sind alle Fenster mit Eisengittern gesichert. Eine Türgegensprechanlage ist Bestandteil der Telefonanlage. Die Türe kann nach Kommunikation per Telefonanlage per elektronischem Türöffner geöffnet werden.

Der Serverraum ist mit einem separaten RFID-Schloss gesichert. Im Serverraum ist neben einem Bewegungsmelder ein Brandmelder und ein Melder angebracht, der auf akustische Signale (laute Geräusche) reagiert.

Die Fenster im Erdgeschoss sind mit verstärktem, bruchsicherem Glas ausgerüstet.

Die Einbruchmeldeanlage wird von einer Meldezentrale 24/7 überwacht. Bei Einbruchmeldung wird die naheliegende Polizeizentrale (Entfernung ca. 300 m), bei Feueralarm die Feuerwehrzentrale (Entfernung ca. 500 m) benachrichtigt.

Technische Maßnahmen:

- Einsatz von personalisiertem Zutrittskontrollsystem RFID-Token mit Zutrittsberechtigung nur für autorisierte Mitarbeiter
- mit RFID-Token gesicherte Serverräume
- Sicherheitsbereiche, Server- und Backupräume sind generell verschlossen
- Schaffung von alarmüberwachten Sicherheitszonen - Serverraum
- Auswahl von Identifikationsmedien zur Zutrittskontrolle (RFID-Token)
- Sperrmöglichkeiten bei Verlust des Zutrittskontrollmediums (RFID-Token)

Erläuterung:

Die Zutrittsberechtigungen werden mit Hilfe der programmierbaren RFID-Token vergeben. Zutritt zum Serverraum haben nur die Administratoren sowie die Geschäftsführung. Die Zutrittsberechtigungen können für jedes Schloss und jeden RFID-Token individuell vergeben werden.

Organisatorische Maßnahmen:

- Bestimmung eines Verantwortlichen für die Gebäudesicherheit
- Arbeitsanweisung zur Handhabung von Zutrittskontrollen
- Arbeitsanweisung zur Ausgabe von Schlüsseln und RFIDs
- Festlegung der berechtigten Personen, die Zutritt zu Datenverarbeitungsanlagen haben
- Zutrittsregelung für betriebsfremde Personen
- Abholung und Begleitung von Besuchern/betriebsfremden Personen
- Abschließen des Gebäudes nach Arbeitsende
- Sensibilisierung und Verpflichtung der Berechtigten bezüglich der Einhaltung der vorgegebenen Regelungen
- geregelte Verfahrensweise beim Ausscheiden von Berechtigten (z.B. Entzug der Berechtigungen)
- Reinigung der Serverräume nur unter Aufsicht der berechtigten Mitarbeiter
- Richtlinien zur Begleitung von Gästen im Gebäude
- Vergaberichtlinien für Zutrittsberechtigungen zu den Serverräumen
- Organisationsanweisung zur Ausgabe von Schlüsseln und anderen Zutrittsmitteln
- Aufbewahrung von Sicherungsbändern in zugriffsgeschütztem Safe

Erläuterung:

Der Datenschutzkoordinator überwacht die Gebäudesicherheit. Im unternehmenseigenen Wiki ist eine Anweisung zur Bedienung der Alarmanlage hinterlegt. Hier ist ebenfalls hinterlegt, welche Maßnahmen nach Arbeitsende und Verlassen des Gebäudes zu erfolgen haben. Zutrittszeiten sind mit der Meldezentrale vereinbart. Dort kann eine Ausnahme nur mit Nennung eines geheimen Kennwortes erwirkt werden. Die Meldezentrale überwacht zudem die Scharfschaltung der Meldeanlage. Besucher dürfen sich nur in Begleitung eines Mitarbeiters im Unternehmen bewegen und haben im Normalfall nur Zutritt zum dafür vorgesehenen Besprechungsraum.

Die Berechtigungen auf den RFID-Token werden gemäß der Funktion des Mitarbeiters vergeben. Zutritt zu Sicherheitsbereichen haben lediglich Personen, die dort auch eine Funktion haben, d.h. Administratoren oder Geschäftsführung. Die Sicherheitsbereiche werden durch die Personen gereinigt, die dazu eine Zutrittsberechtigung haben (d.h. Administratoren). Die verschlüsselten Sicherungsbänder werden in einem Safe aufbewahrt.

Im unternehmenseigenen Wiki gibt es eine Auflistung der Funktionen und der dazu gehörenden Berechtigungen.

Zugangskontrolle (Nr. 2):

Technische Maßnahmen:

- Verschlüsselungsverfahren nach dem Stand der Technik (wie verschlüsselte Übertragung von Zugangsdaten, verschlüsselte Ablage von Benutzerlisten)
- Absicherung der Übertragungsleitungen und des Datenstroms
- Identifikation der Zugangsberechtigten durch geeignete Maßnahmen (User-ID, RFID-Token)
- einheitliches Verfahren zur Vergabe der Identifikationsmedien
- regelmäßige Kontrolle der Gültigkeit von Berechtigungen
- Sperrung verloren gegangener Identifikationsmedien
- Abschottung interner Netzwerke gegen ungewollte oder gezielte Zugänge von außen durch Firewall
- technische Prüfung der Passwortqualität
- sichere Übertragung (DFÜ, Datenfernübertragung) der Identifikationsmerkmale (wie Passwörter)

- Beschränkung von Remote-Zugängen über das Internet auf ein Mindestmaß
- Zwei-Faktor-Authentifizierung (wie Benutzername/Passwort zusammen mit Token) abhängig vom jeweiligen Schutzbedarf
- Nutzung der Schutzfunktionalitäten von Betriebssystemen wie Windows, Linux oder UNIX
- Nutzung der Schutzfunktionalitäten von PCs und Notebooks
- Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte, verschlüsselte Verbindung administrierbar
- Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar

Erläuterung:

Das Intranet ist durch aktuelle Firewalls von Watchguard abgesichert. Bei einer Einwahl der Mitarbeiter in das Intranet wird eine Zwei-Faktor-Authentifizierung durchgeführt. Hier wird die empfohlene Vorgehensweise von Microsoft / Apple, etc. angewandt. So kommt zum Beispiel eine Authentifizierungs-App zum Einsatz, die biometrische Parameter des Mitarbeiters abfragt. Die Zugangsberechtigungen werden gegen das AD geprüft. Die Gruppen innerhalb des ADs werden regelmäßig geprüft und aktualisiert, da viele Zuordnungen und Berechtigungen hierüber gesteuert werden und für die täglichen Arbeiten zuverlässig sein müssen. (z.B. VPN, Zugang zu Arbeitsplanung, Wiki, etc.)

Organisatorische Maßnahmen:

- Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passwörtern
- Benutzervorgaben über eine automatische, passwortgestützte Bildschirm- und Rechnersperre bei Abwesenheit
- Bildschirm für Fremde nicht einsehbar
- verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter

- verbindliches Verfahren zur Vergabe von Berechtigungen
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner)
- Erarbeitung und Durchsetzung einer Richtlinie zum sicheren und ordnungsgemäßen Umgang mit Passwörtern
- Zugang für Servicepartner nur unter Gewährleistung einer sicheren und zuverlässigen Authentifizierung

Erläuterung:

Die Rechner werden bei Inaktivität automatisch nach 5 Minuten gesperrt. Bildschirme sind von außerhalb des Gebäudes nicht einsehbar. Die Bildschirme der Arbeitsplätze stehen in der Regel so, dass auch Kollegen diese nicht einsehen können. Es gibt nur personenbezogene Konten im Unternehmen. Zur automatisierten Softwareverteilung wird Software von Baramundi eingesetzt. Zum automatisierten Backup wird VEEAM benutzt. Eine aktuelle Virensoftware ist ebenfalls flächendeckend im Einsatz. Servicepartner müssen sich via Zwei-Faktor-Authentifizierung anmelden.

Zugriffskontrolle (Nr. 3):

Technische Maßnahmen:

- Einsatz von Verschlüsselungsverfahren nach dem Stand der Technik
- Einsatz der Zugriffsschutzfunktionen von Betriebssystemen und Anwendungen
- Verschlüsselung (auch bei mobilen Datenträgern)
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken
- Beschränkung des Zugriffs auf die für den Benutzer notwendigen Ressourcen und Peripheriegeräte im Netzwerk
- Abweisung nicht autorisierter Computer und Endgeräte im Netzwerk
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(gruppen)

- Verwendung von Benutzerkennungen
- Identifikation und Authentifizierung der Benutzer
- Protokollierung des Zugriffs auf bestimmte Dateien
- Trennung von Test- und Produktionsbetrieb
- Abschottung interner Netze

Erläuterung:

Die von VEEAM erstellten Backups sind verschlüsselt. Ebenfalls verschlüsselt sind die Volumes der NAS-Speicher. Datenträger werden zum Datenaustausch nicht verwendet. Müssen Daten übertragen werden, geschieht dies über ein gesichertes Austauschverfahren via Internet. Der Zugriff auf Datenbanken erfolgt mittels technischer Benutzer. Die Benutzerdaten sind nur autorisierten Mitarbeitern zugänglich. Der Zugriff auf Geräte im Netzwerk sind rollenbasiert und werden über das AD gesteuert. Nicht registrierte Rechner / Endgeräte werden vom internen Netzwerk abgewiesen. Für Gäste gibt es ein separates WLAN, um für Gäste Internetzugang zu gewährleisten. Authentifizierung von Benutzern erfolgt via Zwei-Faktor-Authentifizierung. Die Protokollfunktionen von Servern, Betriebssystemen und Anwendungen werden dort, wo es sinnvoll ist, benutzt. Für Test- und Produktionsbetrieb werden grundsätzlich unterschiedliche Server / Implementationen eingesetzt. Das interne Netz ist über Firewalls abgeschottet.

Organisatorische Maßnahmen:

- Kontrolle der Fernwartung
- Verzicht auf mobile Datenträger
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger / Unterlagen auf Papier
- zeitliche Begrenzung der Zugriffsmöglichkeiten
- Kontrolle der Aktivitäten der Systemadministration

- verbindliches Berechtigungsvergabeverfahren
- verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung von Projektleitung / Abteilungsleitung / Geschäftsleitung / Geschäftsführung)
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT-Abteilung

Erläuterung:

Termine zur Fernwartung werden mit dem Kunden abgesprochen. Der Kunde hat grundsätzlich die Möglichkeit, die Fernwartung zu kontrollieren und ggfs. abzubrechen. Auf die Verwendung von mobilen Datenträgern wird verzichtet. Sollten physikalische Unterlagen existieren, so werden diese nach Ende der Aufbewahrungszeit durch einen zertifizierten Entsorger vernichtet. Die zeitlichen Zugriffsmöglichkeiten auf Systeme der Kunden werden durch das terminliche Zeitfenster begrenzt. Grundsätzlich werden alle Tätigkeiten über die Arbeitsplanung dokumentiert.

Weitergabekontrolle (Nr. 4):

Technische Maßnahmen:

- technische Sicherung des Übertragungs- und Transportwegs nach dem Stand der Technik durch Verschlüsselungsverfahren
- Verwendung der elektronischen Signatur sowie von sicheren Leitungswegen (z.B. VPN = Virtual Private Network)
- Einsatz von Systemen zur Data Leak Prevention (DLP)
- Einsatz von Webfiltern und Web-Application-Firewalls (WAF)
- Datenverschlüsselung für Übermittlung, Transport und Speicherung
- Versand personenbezogener Daten, z.B. per Austauschprogramm
- Protokollierung der Datenübermittlung und der Empfänger

- Überprüfung der Datenträger auf Malware-Befall
- Einsatz von Checksummen-Verfahren und der elektronischen / digitalen Signatur zur Erkennung von Datenmanipulationen

Erläuterung:

Der Datenaustausch von Dateien findet grundsätzlich nicht per E-Mail statt, sondern es wird ein gesichertes Verfahren (Austauschprogramm) benutzt. Die Daten werden dabei verschlüsselt übertragen und im System protokolliert. Die Einwahl in das interne Netz kann nur per VPN von angemeldeten Benutzern erfolgen. Bei Fernwartungsaufgaben bestimmt der Kunde den Kommunikationsweg. Sämtlicher Traffic geht über aktuelle Watchguard Firewalls. Ein aktuelles Virenschutzprogramm testet auf Malware. Updates (sämtlicher Code) des Raumverwaltungsprogramms wird mit Checksummen versehen und kann entsprechend geprüft werden.

Organisatorische Maßnahmen:

- Festlegung der Übermittlungswege und der Datenempfänger
- Prüfung der Zulässigkeit einer Übermittlung

Erläuterung:

Ohne schriftlichen Vertrag über die Rechtmäßigkeit der Übermittlung von Daten findet diese nicht statt.

Eingabekontrolle (Nr. 5):

Technische Maßnahmen:

- Zugriffsberechtigungen für Remotezugriffe

Erläuterung:

Ohne schriftliche Unterlage finden keine Remotezugriffe statt. Die Zugriffsberechtigungen werden im VPN hinterlegt.

Organisatorische Maßnahmen:

- Definition der zur Eingabe, Änderung und Löschung personenbezogener Daten Berechtigten
- Administration der entsprechend Berechtigten (Zugangs- und Zugriffskontrolle)
- Ermittlung der DV-Systeme, in denen Daten eingegeben, geändert und gelöscht werden
- vertragliche Beschränkung der Arbeit mit personenbezogenen Daten des Auftraggebers auf die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeiter des Dienstleisters

Erläuterung:

Die media**DIALOG** GmbH stellt ein Programm zur Raumverwaltung zur Verfügung und konfiguriert dieses auf Kundenanforderungen. Es findet in der Regel keine Eingabe von personenbezogenen Daten statt. Sollten dennoch personenbezogene Daten innerhalb der Anwendung eingegeben oder verändert werden, dann nur auf genau detaillierte schriftliche Anweisung des Kunden.

Auftragskontrolle (Nr. 6):

Organisatorische Maßnahmen:

- Prüfung, ob eine Auftragsdatenverarbeitung zulässig ist
- schriftliche Verträge und Vereinbarungen
- klare Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Festlegung von Sicherheitsmaßnahmen, die der Auftragnehmer umzusetzen hat
- schriftliche Fixierung der Weisungen und Berichtspflichten
- Kontrolle der ordnungsgemäßen Vertragsausführung
- Sanktionen bei Vertragsverletzung
- Festlegung der Modalitäten von Übergabe und Transport der Daten
- Definition der Sicherheitsklasse der im Auftrag zu verarbeitenden Daten
- Definition der Unterauftragsverhältnisse
- Verhaltenskalender bei Störungen
- Kenntnisnahme der Verpflichtungserklärung der Auftragnehmer-Mitarbeiter durch den Auftraggeber
- Regelungen zur Sicherstellung der Datenlöschung
- Vertrag enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers
- Vertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Dienstleister außerhalb des schriftlich formulierten Auftrags

- der Dienstleister hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse

- auf Kundenwunsch kann im Vertrag eine verantwortliche Person beim Auftraggeber benannt werden, die in Bezug auf die vereinbarte Auftragsdatenverarbeitung gegenüber dem Dienstleister weisungsbefugt ist.

Erläuterung:

Obige Punkte werden beim Abschluss des AV-Vertrages geprüft.

Verfügbarkeitskontrolle (Nr. 7):

Technische Maßnahmen:

- Durchführung regelmäßiger Risiko- und Schwachstellenanalysen für den gesamten DV-Bereich

- Notfallvorsorge, unabhängige Stromversorgung

- redundante IT-Infrastruktur (Netzwerke, Speicher, Server, Clients)

- Nutzung eines Systems zur elektronischen Archivierung von Dokumenten

- Nutzung einer abgesicherten Fernwartung (schnelle Verfügbarkeit)

- vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger

- sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes (Virenschutzkonzept usw.)

- Einsatz von Festplattenspiegelung, z.B. RAID-Verfahren

- Einsatz unterbrechungsfreier Stromversorgung (USV)

Erläuterung:

Die Aufbewahrung der Datenträger für das Backup erfolgt in dafür vorgesehenen und geprüften Safes. Es werden von ferner von unternehmensrelevanten Daten nächtliche verschlüsselte Sicherungen per gesicherter Leitung auf verschlüsselte NAS-Speicher ausgeführt. Soweit sinnvoll sind die internen Systeme redundant ausgeführt. Es sind insgesamt drei Notstromversorgungen vorhanden, die ein automatisches, geregeltes Herunterfahren der Systeme erlauben.

Organisatorische Maßnahmen:

- regelmäßige Datensicherung
- getrennte Aufbewahrung von Backups
- Brandschutzmaßnahmen
- schnelle und geregelte Erreichbarkeit der Administratoren
- Funktionstrennung zwischen Fachabteilung und DV-Abteilung
- zentrale und einheitliche Beschaffungsstrategie für Hard- und Software
- formalisierte Freigabeverfahren für neue DV-Verfahren sowie bei wesentlichen Änderungen von Altverfahren
- Einsatz ausschließlich geprüfter Fremdsoftware
- Vorgaben für die Verfahrens- und Programmdokumentation
- Erlass von Dienstanweisungen und Sicherheitsrichtlinien für die Datensicherung
- Erstellen eines schriftlichen Notfallhandbuchs / Notfallplans
- Vorhandensein ausreichender Personalressourcen in der DV
- gründliche Schulung aller Mitarbeiter
- Nachweis der sicheren und ordnungsgemäßen Archivierung in physisch geschütztem Archiv und verbindlicher Regelung der Zugriffsberechtigten

Erläuterung:

Zur Datensicherung wird die Software VEEAM benutzt. Dort sind die automatisierten Datensicherungsaktivitäten hinterlegt und werden dort auch protokolliert. Eine automatische Benachrichtigung über den Status der Sicherungen findet statt. Backups werden in geeigneten und gesicherten Safes hinterlegt. Die DV-Abteilung ist unabhängig von allen anderen Abteilungen.

Trennungsgebot (Nr. 8):

Technische Maßnahmen:

- restriktiver Einsatz von Datenbankabfragen (insbesondere SQL)
- Einrichtung logischer Datenbanken
- strikte Trennung von Entwicklungs- und Produktionsumgebungen
- logische Trennung des Netzwerks in Aufgabenbereiche
- Einsatz von Routern zur Bildung von Netzwerksegmenten
- Trennung der Zugriffe über Anwendungen durch Firewalls bis auf Applikationsebene
- „Interne Mandantenfähigkeit"

Erläuterung:

Die Implementationen für interne Verfahren und für Kundenprogramme sind streng getrennt. Jeder Kunde wird wie ein einzelner Mandant behandelt. Die Trennung der Systeme erfolgt nach der jeweiligen Funktion.

Organisatorische Maßnahmen:

- klare innerbetriebliche Vorgaben für die Datenerhebung, -speicherung und -verarbeitung
- ausführliche Dokumentation der verwendeten Datenbanken
- Einrichtung logischer Datenbanken
- klare Regelungen für die Archivierung
- die Daten des Auftraggebers und anderer Mandanten werden soweit möglich von unterschiedlichen Mitarbeitern des Dienstleisters verarbeitet
- es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Mandanten Rechnung trägt
- die in den verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzeptes

Erläuterung:

Jeder Mandant hat seine "eigene" Implementation mit klar getrennter Datenbank. In dem Verwaltungsprogramm "programMANAGER" ist die jeweilige Datenbank registriert. Nicht mehr benötigte Implementationen werden gelöscht. Die Archivierungsregeln sind in VEEAM hinterlegt und werden automatisiert verfolgt. Auf die Mandantensysteme haben nur die jeweils autorisierten Mitarbeiter Zugriff. Passwörter für die Zugriffe werden über einem am Berechtigungskonzept angeschlossenen Passwortmanager gespeichert. Die Gruppen für die Berechtigungen sind im AD hinterlegt.

Organisationskontrolle „Mensch“ (Nr. 9):

Organisatorische Maßnahmen:

- ein Datenschutzbeauftragter ist bestellt
- der Datenschutzbeauftragte unterzieht sich einer regelmäßigen Fortbildung

- Datenschutzkoordinatoren sind bestellt
- Verpflichtung aller internen und externen Mitarbeiter auf die Vertraulichkeit
- Verpflichtung aller Administratoren auf das Fernmeldegeheimnis nach § 88 TKG
- Verpflichtung der Mitarbeiter auf § 203 StGB (Privatgeheimnisse)
- die Verpflichtungen sind nachweisbar dokumentiert
- regelmäßige Durchführung und schriftliche Dokumentation von Mitarbeiterschulungen in den Bereichen Datenschutz und IT-Sicherheit
- Regelung der Privatnutzung von Internet und E-Mail im Unternehmen
- Datenschutz-Richtlinie ist vorhanden und wird gelebt
- IT-Sicherheits-Richtlinie ist vorhanden und wird gelebt

Erläuterung:

Alle Mitarbeiter sind entsprechend den Vorgaben des Datenschutzbeauftragten verpflichtet.

Anlage 3: Ergänzende Regelungen zur Fernwartung

Werden Auftragsleistungen im Wege der Fernwartung durchgeführt, gelten zusätzlich folgende Vereinbarungen:

(1) Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Die Fernwartung erfolgt, soweit möglich, ohne gleichzeitige Speicherung von Daten.

(2) Der Auftragnehmer muss personenbezogene Daten, die er bei der Fernwartung erhalten oder gewonnen hat, unverzüglich sicher löschen oder dem Auftraggeber zurückgeben, wenn sie für die Durchführung der Fernwartungsarbeiten nicht mehr erforderlich sind. Etwaige dem Auftragnehmer übergebene Papierausdrucke oder sonstige Datenträger mit personenbezogenen oder sonstigen vertraulichen Daten sind dem Auftragnehmer nach Abschluss der Fernwartungsarbeiten unverzüglich zurückgeben oder sicher zu vernichten.

(3) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen, Ausnahmen sind mit dem Auftraggeber abzustimmen.

(4) Der Beginn der Fernwartung ist vom Auftragnehmer anzukündigen, um dem Auftraggeber die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen. Ggf. entstehende Kosten übernimmt der Auftraggeber. Die Mitarbeiter des Auftragnehmers verwenden nach dem Stand der Technik hinreichend sichere Identifizierungs- und Einwahlverfahren. Die Fernwartung darf nur über nach dem Stand der Technik sichere Leitungen abgewickelt werden.

(5) Der Auftragnehmer verpflichtet sich, nur zur Vertragserfüllung, auf Grund von Störungsmeldungen oder auf Grund sonstiger ausdrücklicher Anforderungen des Auftraggebers mittels Fernwartung bzw. Remote-Zugriff auf Systeme, Software und Daten zuzugreifen und danach dem Auftraggeber Serviceberichte zu erstellen.

(6) Der Auftraggeber ist berechtigt, die Fernwartungsarbeiten von einem Kontrollbildschirm aus zu verfolgen (sofern technisch möglich). Beide Parteien sind berechtigt, die Fernwartungsaktivitäten zu protokollieren, die Protokolle zu überprüfen und eine angemessene Zeit aufzubewahren.

(7) Wird die Fernwartung von Privatwohnungen oder von einem dritten Ort aus durchgeführt, verpflichtet sich der Auftragnehmer, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Serviceleistung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung von der Wartungszentrale aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers.

(8) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, wenn der Auftragnehmer von den vereinbarten Sicherheitsmaßnahmen abweicht oder die Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten durchgeführt wird.

Anlage 4: Liste der Ansprechpartner

Gemäß Ziffer 9 der AVDI benennen die Parteien wechselseitig Ansprechpartner und werden diesbezügliche Änderungen dem jeweils anderen Vertragspartner unverzüglich schriftlich mitteilen.

Der Auftragnehmer meldet folgende Ansprechpartner:

1. Externer Datenschutzbeauftragter: Herr Thomas Ströbele
2. Interner Datenschutzkoordinator: Herr Volker Sasse

Die Ansprechpartner sind unter der Adresse des Auftraggebers bzw. der E-Mail-Adresse „Datenschutz@mediadialog.de“ erreichbar.

Der Auftraggeber meldet folgende Ansprechpartner:

Fachbereich	Name	Weisungsbefugnis

Erklärung: Die oben genannten Ansprechpartner sind die aktuell einzigen des Meldenden. Ältere Ansprechpartner-Listen verlieren hiermit ihre Gültigkeit.

_____	_____	_____
Ort, Datum	Name, Funktion	Unterschrift Meldender

Anlage 5: Liste der Subunternehmer / Unterauftragnehmer

Gemäß Ziffer 11 der AVDI meldet der Auftragnehmer hiermit folgende Subunternehmer, welche er zur Erfüllung seiner sich aus dieser Auftragsverarbeitung ergebenden vertraglich vereinbarten Leistung unterbeauftragt. Änderungen werden schriftlich mitgeteilt:

Subunternehmen	Anschrift	Leistungsteil
Dembach Goo Informatik GmbH & Co. KG	Hohenzollernring 72, 50672 Köln	Hosting, Betrieb des Rechenzentrums
OKTA	Neue Rothofstr. 13-19, 60313 Frankfurt	Authentifikation Provider
Chargebee	www.chargebee.com	Abonnementverwaltung
Stripe	Stripe.com	Zahlungsdienstleister
Sendinblue	Köpenicker Straße 126, 10179 Berlin	Mailversand

In Notfällen, die es dem Auftragnehmer unmöglich machen seine vertraglichen Leistungen zu erfüllen oder wenn Gefahr im Verzug ist, welche die Schutzziele des Datenschutzrechts wesentlich bedrohen und es im eigenen Interesse des Auftraggebers ist, kann der Auftragnehmer kurzfristig weitere Subunternehmer hinzuziehen, um den Notfall abzuwenden oder zu bewältigen. In diesem Fall wird die Zustimmung zur Zusammenarbeit mit diesen Subunternehmern umgehend beim Auftraggeber nachgeholt.

Erklärung: Die oben genannten Subunternehmer sind die aktuell einzigen betroffenen des Auftragnehmers. Ältere Subunternehmer-Listen verlieren hiermit ihre Gültigkeit.

Anlage 6: Meldeformular für Datenschutzverstöße

Dieses Formular ist im Falle von Datenschutzverletzungen auszufüllen.

1. Allgemeine Angaben zum Vorfall

1.1 Feststellung des Vorfalls

- Datum:
- Uhrzeit:

1.2 Zeitpunkt des Vorfalls, betroffener Zeitraum

- Datenverarbeitungsverfahren:
- Verantwortlicher Fachbereich:
- Verantwortlicher Bearbeiter für den Vorfall:

1.2 Beschreibung der Datenpanne

- Betroffene Systeme/Objekte:
- Wie hat sich der Vorfall ereignet?
- Welche Folgen wurden festgestellt?

1.3 Reaktionen und Zustand des Systems

-
- Reaktionen/Maßnahmen auf die Datenpanne:
- Aktueller Zustand des Systems:

2 Ergänzende Angaben zum Vorfall

2.1 Art des Vorfalls

- (Vorfälle sind z. B. Verlust der Vertraulichkeit, Datendiebstahl, Zerstörung oder Verfälschung der Daten, Übermittlung an unbefugte Stellen etc.)

2.2 Betroffene Personengruppen

2.3 Zahl der betroffenen Personen

2.4 Kategorien von personenbezogenen Daten

2.5 Wahrscheinliche Folgen/Risiken der Verletzung des Schutzes personenbezogener Daten:
(Hier sind die möglichen Risiken und Folgen für die Betroffenen anzugeben. Vgl. Checkliste zur Risiko- und Schutzbedarfsermittlung.)

3 Eingeleitete Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten

3.1 Eingerichtete Maßnahmen:
(Hier sind die Maßnahmen zu beschreiben, die zum Schutz der personenbezogenen Daten gegen Vorfälle dieser Art eingerichtet worden sind.)

3.2 Weitere beabsichtigte Maßnahmen:
(Hier sind die Maßnahmen zu beschreiben, deren Einrichtung aufgrund des Vorfalls zusätzlich noch geplant ist.)