

Allgemeine Nutzungsbedingungen myDMScloud

§ 1 Allgemeine Regelungen

(1) Die nachstehenden Bedingungen gelten für alle Leistungen im Rahmen des Konzeptes myDMScloud (einheitlich „Leistungsgegenstand“ oder „Leistung“), die comTeam Business Solutions GmbH (nachfolgend „comTeam BS“) gegenüber dem Vertragspartner erbringt. Dies gilt auch, wenn comTeam BS in Kenntnis entgegenstehender Bedingungen des Vertragspartners Leistungen vorbehaltlos erbringt. Die Wirkung etwaiger Allgemeiner Geschäftsbedingungen des Vertragspartners wird ausgeschlossen.

(2) comTeam BS behält sich das Recht vor, diese Nutzungsbedingungen, damit verbundene Leistungsbeschreibungen und Leistungsinhalte jederzeit und ohne Angabe von Gründen zu ändern. Das gilt auch für die Änderung von Vergütungen. Die Änderungen werden rechtzeitig, jedoch mindestens einen Monat vor dem Zeitpunkt, zu dem sie in Kraft treten sollen bekanntgegeben. Änderungen gelten als genehmigt, wenn der Vertragspartner nicht binnen einer Frist von zwei Wochen nach Bekanntgabe der Änderung widerspricht. comTeam BS wird der Vertragspartner in der Mitteilung auf die Bedeutung seines Schweigens und den Zeitpunkt des beabsichtigten Wirksamwerdens der Änderung hinweisen. Widerspricht der Vertragspartner, so steht ihm ein Kündigungsrecht mit Wirkung zum Zeitpunkt des beabsichtigten Wirksamwerdens der Änderung zu. Ein Anspruch auf Leistungserfüllung nach Maßgabe der vor der Änderung geltenden Nutzungsbedingungen besteht nicht.

(3) Die vorliegende Nutzungsvereinbarung gilt für das Hauptgeschäft (Anschrift gemäß Vertragsrumpf) und alle in der Anlage 2 aufgelisteten zugehörigen Filialen.

§ 2 Leistungen

(1) comTeam BS räumt dem Vertragspartner zur eigenen Nutzung die Teilnahme an den Leistungen myDMScloud ein. Bei den Leistungen myDMScloud handelt es sich um eine virtuelle Archivierungs- und DMS-Lösung, die es dem Vertragspartner ermöglicht Eingangsrechnungen von Lieferanten elektronisch zu empfangen zu speichern (Archivierung Basic). Die jeweils teilnehmenden Lieferanten sind im Infontet zu finden. Ändern sich zwingende rechtliche Vorschriften, die für die Leistungserbringung von Bedeutung sind, so wird comTeam BS binnen angemessener Frist die Leistungen anpassen. Bei der Bestimmung dieser Frist ist zugunsten von comTeam BS zu berücksichtigen, das comTeam BS nicht Herstellerin der Software ist und auf Anpassungen des Herstellers angewiesen ist. Die Verpflichtung zur Anpassung entfällt, wenn die Anpassung für comTeam BS mit unzumutbaren Kosten und/oder Aufwand verbunden ist. In einem derartigen Fall wird die Anpassung nur gegen eine zusätzliche Vergütung vorgenommen.

(2) comTeam BS bietet dem Vertragspartner über die Servicekategorie Archivierung Basic hinausgehend weitere Servicekategorien, etc. an.

Der Leistungsumfang und der Funktionsumfang der jeweils gewählten Servicekategorie, etc., ergibt sich aus der Preisliste und Leistungsübersicht, Anlage 1.

(3) comTeam BS ist nicht verantwortlich für die Rechtmäßigkeit, inhaltliche Richtigkeit, etc. von Inhalten, die gespeichert werden.

(4) Die Leistungen von comTeam BS beschränken sich auf die Bereitstellung des Leistungsgegenstandes, so dass comTeam BS eine Einflussnahme außerhalb ihrer Systeme nicht zur Verfügung steht. Von comTeam BS nicht geschuldet ist die Herstellung und Aufrechterhaltung der Datenverbindung zwischen dem IT-System des Vertragspartners und dem von comTeam BS betriebenen Server. Ein Anspruch des Vertragspartners auf den Einsatz einer neueren Version des Leistungsgegenstandes als in der Übersicht der Anlage 1 besteht nicht.

(5) Das Vertragspartner übernimmt es, eine Datenverbindung zwischen den von ihm zur Nutzung vorgesehenen Arbeitsplätzen und dem von comTeam BS definierten Datenübergabepunkt herzustellen. comTeam BS ist berechtigt, den Datenübergabepunkt jederzeit neu zu definieren. Der Vertragspartner wird in diesem Fall eine Verbindung zu dem neu definierten Übergabepunkt herstellen.

(6) Die vertragsgemäße Inanspruchnahme der Leistungen von comTeam BS ist davon abhängig, dass die vom Vertragspartner eingesetzte Hard- und Software, einschließlich Arbeitsplatzrechnern, Routern, Datenkommunikationsmitteln etc., den technischen Mindestanforderungen an die Nutzung der vertragsgegenständlichen Leistung entsprechen und die vom Vertragspartner zur Nutzung der Leistung berechtigten Nutzer mit der Bedienung der Leistung vertraut sind. Die Konfiguration seines IT-Systems ist Aufgabe des Vertragspartners. Die Mindestanforderungen im vorge-nannten Sinne ergeben sich aus der jeweils aktuellen Leistungsübersicht myDMScloud, auch zu finden unter: <https://mydmscloud.de/About>.

(7) comTeam BS räumt dem Vertragspartner das nicht ausschließliche und nicht übertragbare Recht ein, den in dieser Nutzungsbedingung bezeichneten Leistungsgegenstand nach Maßgabe der gewählten Servicekategorie bezogen auf das lizenzierte Hauptgeschäft und die ggf. vertraglich vereinbarten Filialen während der Dauer der Nutzungsvereinbarung bestimmungsgemäß zu nutzen. Der Vertragspartner darf die Leistung nur durch die im Vertrag angegebene Anzahl von Nutzern gleichzeitig nutzen. Erfolgt eine Nutzung durch mehr als die dort angegebene Anzahl von Nutzern gleichzeitig, zahlt das Vertragspartner die in der Preisübersicht genannte Vergütung je Person und Zugriff gemäß der Servicekategorie „Archivierung Vollnutzer – Preisklasse 1-3; sonstige Ansprüche von comTeam BS bleiben unberührt.

(8) comTeam BS darf sich zur Vertragserfüllung Dritter bedienen.

(9) comTeam BS wird den Vertragspartner über die teilnehmenden Lieferanten und deren Zugang und Abgang regelmäßig informieren. Ein Anspruch auf die Teilnahme von bestimmten Lieferanten und/ oder eine bestimmte Teilnehmendenzahl von Lieferanten besteht nicht.

(10) comTeam BS wird eine arbeitstäglige Sicherung der Daten des Vertragspartners auf dem Datenserver durchführen.

(11) Für die Beachtung der handels- und steuerrechtlichen Aufbewahrungspflichten ist der Vertragspartner verantwortlich.

§ 3 Zulassung und Zugang

(1) Die technischen Voraussetzungen unterliegen der Fortentwicklung des Leistungsgegenstandes und können sich daher ändern. Der Vertragspartner wird seine technische Infrastruktur anpassen.

(2) Der Zugriffe auf den Leistungsgegenstand erfolgt webformularbasiert. Applikationen verbleiben auf den Systemen von comTeam BS.

(3) comTeam BS ist berechtigt, einem Vertragspartner den Zugang zum Leistungsgegenstand zu sperren, falls ein hinreichender Verdacht besteht, dass es gegen diese Nutzungsbedingungen verstößt.

(4) Alle Logins sind individualisiert und dürfen nur vom Vertragspartner und seinen Nutzern verwendet werden. Der Vertragspartner ist verpflichtet, Login und Passwort geheim zu halten und vor dem unberechtigten Zugriff Dritter zu schützen. Der Vertragspartner wird die Nutzer auf die Geheimhaltung verpflichten und entsprechend anweisen. Bei Verdacht des Missbrauchs durch einen Dritten wird der Vertragspartner comTeam BS hierüber unverzüglich informieren. Sobald comTeam BS von der unberechtigten Nutzung Kenntnis erlangt, wird comTeam BS den Zugang sperren. comTeam BS behält sich das Recht vor, Login und Passwort eines Vertragspartners zu ändern; in einem solchen Fall wird comTeam BS den Vertragspartner hierüber unverzüglich informieren.

§ 4 Verfügbarkeit und Datensicherung

comTeam BS bemüht sich den Betrieb des Leistungsgegenstandes bezogen auf eine monatliche Basis abzüglich der Wartungszeiten mit einer Verfügbarkeit von 98,0 % zur Verfügung zu stellen. comTeam BS wird sich bemühen, Routinewartungsarbeiten vorher mit einer angemessenen Frist anzukündigen. Während der Wartungsarbeiten steht der Leistungsgegenstand nicht oder nur eingeschränkt zur Verfügung. Eine Haftung für eine bestimmte oder Verfügbarkeit übernimmt comTeam BS nicht. Im Übrigen gelten die Haftungsvorschriften des § 12 dieser Nutzungsbedingungen.

§ 5 Inhalte

Der Vertragspartner wird keine Inhalte einstellen, die nach der jeweils für den intendierten Vertrag maßgeblichen Rechtsordnung gegen gesetzliche Vorschriften, behördliche Anordnungen oder gegen die guten Sitten verstoßen würde. Der Vertragspartner haftet dafür, dass die vertragsgegenständlichen Leistungen nicht zu rassistischen, diskriminierenden, pornographischen, den Jugendschutz gefährdenden, politisch extremen oder sonst gesetzeswidrigen Zwecken verwendet wird oder entsprechende Daten erstellt und/oder auf dem Server gespeichert werden. comTeam BS ist berechtigt, solche Inhalte unverzüglich, auch ohne vorherige Abmahnung, zu entfernen und den Vertrag außerordentlich fristlos zu kündigen.

§ 6 Rechte

Der Vertragspartner räumt comTeam BS das Recht ein, die von comTeam BS für den Vertragspartner zu speichernden Daten vervielfältigen zu dürfen, soweit dies zur Erbringung der vertragsgegenständlichen Leistungen erforderlich ist. comTeam BS ist auch berechtigt, die Daten in einem Ausfallrechenzentrum vorzuhalten. Zur Beseitigung von Störungen ist comTeam BS berechtigt, Änderungen an der Struktur der Daten oder dem Datenformat vorzunehmen. Der Vertragspartner ist nicht berechtigt, Dritten die Inanspruchnahme der vertragsgegenständlichen Leistungen zu gestatten.

§ 7 Sonstige Pflichten des Vertragspartners

- (1) Der Vertragspartner ist verpflichtet,
 - (a) die erforderlichen Datensicherungsvorkehrungen im Übrigen während der gesamten Vertragslaufzeit einzurichten und aufrechtzuerhalten;
 - (b) in seinem Bereich eintretende technische Änderungen comTeam BS umgehend mitzuteilen, wenn sie geeignet sind, die Leistungserbringung oder die Sicherheit des Leistungsgegenstandes zu beeinträchtigen;
 - (c) bei der Aufklärung von Angriffen Dritter auf den Leistungsgegenstand mitzuwirken, soweit diese Mitwirkung durch das Vertragspartner erforderlich ist;
- (2) Der Vertragspartner verpflichtet sich, alle Maßnahmen zu unterlassen, welche die Funktionsweise des Leistungsgegenstandes gefährden oder stören, sowie nicht auf Daten zuzugreifen, zu deren Zugang er nicht berechtigt ist. Weiterhin hat er dafür Sorge zu tragen, dass seine eingestellten und übertragenden Inhalte und Daten nicht mit Viren, Würmern oder Trojanischen Pferden behaftet sind. Der Vertragspartner verpflichtet sich comTeam BS alle Schäden zu ersetzen, die aus der Nichtbeachtung dieser Pflichten entstehen und comTeam BS von allen Ansprüchen Dritter freizustellen, die aufgrund der Nichtbeachtung dieser Pflichten gegen comTeam BS Ansprüche geltend machen.

§ 8 Vergütung

- (1) Der Vertragspartner hat für die von ihm gewählte Servicekategorie, etc., gemäß den Vereinbarungen in der Anlage 1 und die sich daraus ergebenden Entgelte an comTeam BS zu zahlen.
- (2) Die Vergütungsrechnungen werden dem Vertragspartner monatlich übermittelt.
- (3) Vergütungen werden innerhalb von 10 Tagen nach Rechnungsstellung durch SEPA-Firmenlastschrift abgebucht.
- (4) Vergütungen werden zuzüglich MwSt. in der jeweils anfallenden gesetzlichen Höhe geschuldet.

§ 9 Schulung, Supporthotline

- (1) comTeam BS stellt dem Vertragspartner zur Unterstützung von Fragen im Rahmen der Nutzung des Leistungsgegenstandes eine Supporthotline zu Verfügung, die über Email und Telefon erreichbar ist. Vertragspartner-Anfragen werden in der Reihenfolge ihres Eingangs bearbeitet. Störungen sind ausschließlich gegenüber der Störungsstelle zu melden.
- (2) comTeam BS bietet den Vertragspartnern gegen ein gesondertes Entgelt die Schulung des Vertragspartners und seiner Mitarbeiter an. Dazu bedarf es des Abschlusses einer gesonderten Vereinbarung.

§ 10 Datenherausgabe

Der Vertragspartner kann jederzeit die Herausgabe der gespeicherten Daten auf einem üblichen Datenträger oder nach Wahl von comTeam BS im Wege der Datenfernübertragung verlangen. Der Vertragspartner ist verpflichtet die dafür gemäß der Preisliste von comTeam BS geforderten Entgelte zu zahlen. Soweit dafür keine Preisliste existiert, so wird der Vertragspartner nach Aufwand und ortsüblichen Entgelten die Leistungen von comTeam BS vergüten.

§ 11 Gewährleistungsansprüche

Sollten auf Leistungen von comTeam BS im Einzelfall Gewährleistungsrecht anwendbar sein und die erbrachten Leistungen mangelhaft sein, so verjähren Mängelansprüche in einem Jahr. Ansprüche nach § 12 bleiben unberührt. Der Vertragspartner hat comTeam BS Mängel unverzüglich schriftlich anzuzeigen. Die verschuldensunabhängige Haftung für Mängel, die bereits bei Vertragsschluss vorhanden waren, wird ausgeschlossen.

§ 12 Haftung

- (1) Eine Haftung von comTeam BS, gleich aus welchem Rechtsgrund, tritt nur ein, wenn der Schaden
 - a) durch schuldhaftes Verletzung einer der Kardinalpflichten oder wesentlichen Nebenpflichten in einer das Erreichen des Vertragszwecks gefährdenden Weise verursacht worden ist oder
 - b) auf grobe Fahrlässigkeit oder Vorsatz von comTeam BS zurückzuführen ist.
- (2) Haftet comTeam BS gemäß § 12 (1) a) für die Verletzung einer wesentlichen Vertragspflicht, ohne dass grobe Fahrlässigkeit oder Vorsatz vorliegen, so ist die Haftung auf denjenigen Schadensumfang begrenzt, mit dessen Entstehen comTeam BS bei Vertragsschluss aufgrund der ihr zu diesem Zeitpunkt bekannten Umstände typischerweise rechnen musste. Die Haftung für Folgeschäden, insbesondere auf entgangenen Gewinn oder auf Ersatz von Schäden Dritter, wird ausgeschlossen, es sei denn, es fallen comTeam BS Vorsatz oder grobe Fahrlässigkeit zur Last.
- (3) Schadenersatzansprüche nach dem Produkthaftungsgesetz und für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit bleiben durch die vorstehenden Haftungsbeschränkungen unberührt.
- (4) Die vorstehenden Haftungsbeschränkungen gelten auch zugunsten von eventuell eingebundenen gesetzlichen Vertretern und Erfüllungsgehilfen von comTeam BS.
- (5) Die Haftung erstreckt sich nicht auf Beeinträchtigungen des vertragsgemäßen Gebrauchs der von comTeam BS erbrachten Leistungen, die durch eine unsachgemäße oder fehlerhafte Inanspruchnahme durch den Vertragspartner verursacht worden sind.
- (6) Soweit über die Leistungsgegenstände eine Möglichkeit der Weiterleitung auf Datenbanken, Websites, Dienste, etc. Dritter, z.B. durch die Einstellung von Links oder Hyperlinks gegeben ist, haftet comTeam BS weder für Zugänglichkeit, Bestand oder Sicherheit dieser Datenbanken oder Dienste, noch für den Inhalt derselben. Insbesondere haftet comTeam BS nicht für deren Rechtmäßigkeit, inhaltliche Richtigkeit, Vollständigkeit, Aktualität, etc.

§ 13 Datenschutz und Datenweitergabe

- (1) Verarbeitet der Vertragspartner im Rahmen dieses Vertragsverhältnisses personenbezogene Daten, so ist er für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. comTeam BS wird die vom Vertragspartner übermittelten Daten nur im Rahmen der Weisungen des Vertragspartners verarbeiten. Die Allgemeinen Bedingungen zur Auftragsdatenverarbeitung in der myDMScloud sind Vertragsbestandteil.
- (2) comTeam BS ist berechtigt Lieferantenrechnungen an die Zentralregulierung der angebundenen Kooperationen zu übermitteln.

§ 14 Abtretung und Aufrechnung

- (1) Eine teilweise oder vollständige Übertragung der Rechte des Vertragspartners aus dem Vertrag mit comTeam BS auf Dritte ist ausgeschlossen. comTeam BS ist berechtigt, die sich aus dem Nutzungsvertrag ergebenden Rechte und Pflichten auf einen Dritten zu übertragen.
- (2) Zur Aufrechnung gegenüber comTeam BS ist der Vertragspartner nur mit unbestrittenen oder rechtskräftigen Gegenforderungen berechtigt. comTeam BS ist berechtigt, gegen die Forderungen des Vertragspartners oder eines Konzernunternehmens des Vertragspartners mit sämtlichen Forderungen, die comTeam BS oder ElectronicPartner Handel SE (ElectronicPartner) oder einer in deren Konzernabschluss einbezogenen Gesellschaft gegen den Vertragspartner oder ein Konzernunternehmen des Vertragspartners zustehen, aufzurechnen. Auf Wunsch wird comTeam BS die in den Konzernabschluss von ElectronicPartner einbezogenen Gesellschaften bekanntgeben.

§ 15 Geheimhaltung

Der Vertragspartner verpflichtet sich zum Stillschweigen über sämtliche geschäftliche Angelegenheiten, die ihm im Rahmen des Nutzungsvertrages und der Durchführung der Nutzung zur Kenntnis gelangen. Das gilt insbesondere für sämtliche erhobenen Daten und Konditionen.

§ 16 Vertragsdauer

(1) Der Vertrag läuft zunächst fest für einen Zeitraum von 24 Monaten ab Vertragsunterzeichnung. Nach Ablauf dieser Frist läuft der Vertrag auf unbestimmte Zeit, wenn er nicht mit einer Frist von drei Monaten zum Ablauf des fest vereinbarten Zeitraumes oder danach jeweils mit einer Frist von drei Monaten gekündigt wird.

(2) Jede Partei hat das Recht, den Vertrag aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist zu kündigen. Zusätzlich ist es für comTeam BS neben den in dieser Nutzungsbedingung geregelten Gründen ein wichtiger Grund, der zur außerordentlich fristlosen Kündigung führt, wenn

- a) über das Vermögen des Vertragspartners das Liquidationsverfahren oder das Insolvenzverfahren beantragt oder eröffnet wird oder ein Antrag auf Eröffnung des Ausgleichs-/ Insolvenzverfahren mangels hinreichenden Vermögens abgewiesen wird;
- b) der Vertragspartner eine deliktische Handlung oder der Versuch einer solchen, z.B. Betrug, begeht;
- c) Verzug des Vertragspartners mit der Zahlungspflicht um mehr als 14 Tage trotz Setzung einer Nachfrist besteht;

- d) eine andauernde Betriebsstörungen infolge von höherer Gewalt besteht, die außerhalb der Kontrolle von comTeam BS liegen, wie z. B. Naturkatastrophen, Brand, unverschuldeter Zusammenbruch von Leitungsnetzen;
 - e) der Vertragspartner seinen Geschäftsbetrieb aufgibt, auf einen Dritten überträgt oder einen Dritten mehrheitlich beteiligt.
- (3) Jede Kündigung muss schriftlich erfolgen.
- (4) Endet die Mitgliedschaft des Mitglieds in der Kooperation, so endet auch der Nutzungsvertrag auf den die Nutzungsbedingungen Bezug nehmen, ohne das es einer weiteren Erklärung von comTeam BS bedarf.

§ 17 Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gerichtsstand für alle Rechtsstreitigkeiten ist Düsseldorf. comTeam BS ist daneben berechtigt, auch am allgemeinen Gerichtsstand des Vertragspartners zu klagen.

(2) Sollten einzelne Bestimmungen dieser Nutzungsbedingungen unwirksam sein oder werden und/oder den gesetzlichen Regelungen widersprechen, so wird hierdurch die Wirksamkeit der Nutzungsbedingungen im Übrigen nicht berührt. Die unwirksame Bestimmung wird von den Vertragsparteien einvernehmlich durch eine solche Bestimmung ersetzt, welche dem wirtschaftlichen Zweck der unwirksamen Bestimmung in rechtswirksamer Weise am nächsten kommt. Die vorstehende Regelung gilt entsprechend bei Regelungslücken.

Anlage 2

Filialen des Hauptgeschäfts

Bitte hier die Mitgliedsnummern der Filialen angeben:

[illegible]

Nutzungsvereinbarung – myDMScloud

Anlage 4: Allgemeinen Bedingungen zur Auftragsdatenverarbeitung in der „myDMScloud“

1. Allgemeines

Gegenstand der Vereinbarung ist die Vereinbarung der Rechte und Pflichten des Vertragspartners (nachfolgend auch „Auftraggeber“) und der comTeam Business Solutions GmbH (nachfolgend auch „Auftragnehmer“ oder „comTeam BS“ genannt) sofern im Rahmen der Leistungserbringung des Service myDMScloud durch comTeam BS eine Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten für den Vertragspartner im Sinne von § 11 Bundesdatenschutzgesetz (BDSG) durch comTeam BS erfolgt.

2. Gegenstand und Dauer des Auftrages

comTeam BS verarbeitet im Rahmen des Service myDMScloud personenbezogene Daten im Auftrag des Auftraggebers. Der Umfang der Tätigkeit ergibt sich aus dem Hauptvertrag myDMScloud sowie aus etwaigen Einzelweisungen. Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags myDMScloud.

3. Konkretisierung des Auftragsinhalts

3.1. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

comTeam BS erhebt, verarbeitet und nutzt personenbezogene Daten, welche der Auftraggeber selbst oder Lieferanten, die am Service myDMScloud teilnehmen, in die jeweils genutzte(n) Datenbank(en) einpflegen. Der Auftraggeber bzw. der Lieferant kann auf den Service entweder direkt über einen von comTeamBS bereitgestellten (z.B. browserbasierten) Zugang oder über eine Schnittstelle (API) zugreifen. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 §§ 4b, 4c BDSG (Artikel 44 – 50 EU-DSGVO) erfüllt sind.

3.2 Art der Daten/Kreis der Betroffenen

Die Art und Menge der vom Service genutzten personenbezogenen Daten und betroffenen Personengruppen hängt vom Einsatz/ Nutzung des Service myDMScloud ab. Bei dem Service myDMScloud handelt es sich um eine Archivierungslösung zum Zwecke des Empfangs und der Archivierung von elektronischen Rechnungen des Lieferanten an den Auftraggeber. In diesen Rechnungen können insbesondere E-Mail-Adresse, Anrede, Titel, Vorname, Nachname von Mitarbeitern beinhaltet sein.

4. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots, sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung etc., die im **Anhang 1** „Datenschutzkonzept der comTeam BS“ gesondert beschrieben werden. Diese technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG (Artikel 30 Abs. 2 EU-DSGVO) dem Auftraggeber zur Verfügung zu stellen.

5. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG (bzw. Artikel 28 EU-DSGVO) folgende Pflichten:

- Schriftliche Bestellung, soweit gesetzlich vorgeschrieben, eines Datenschutzbeauftragten, der seine Tätigkeit gemäß §§ 4f, 4g BDSG (bzw. Abschnitt 4 EU-DSGVO) ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG (bzw. Artikel 28 Abs. 3 b EU-DSGVO). Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage (bzw. Artikel 32 EU-DSGVO).
- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG (bzw. Artikel 57 und 58 EU-DSGVO). Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG (bzw. Artikel 57 und 58 EU-DSGVO) beim Auftragnehmer ermittelt.
- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

7. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Ziffer 6 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.

Die in **Anhang 2** genannten Subunternehmer sind für den Auftragnehmer mit dem dort genannten Auftragsinhalt in dem dort genannten Umfang tätig. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. der Anlage zu § 9 BDSG (bzw. Artikel 28 Abs. 3 d i.V.m. Artikel 28 Abs. 2 und 4 EU-DSGVO) beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der

datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Tele-kommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Ebenso sind Hersteller von Softwaremodulen (z. B. Plug-ins oder Add-ons) bzw. Integrationen, die lediglich eine von comTeam BS zur Verfügung gestellte Schnittstelle in myDMScloud nutzen, keine Subunternehmer im Sinne dieser Vereinbarung.

8. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die der Anlage zu § 9 BDSG (bzw. Artikel 32 EU-DSGVO) vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Der Auftraggeber lässt die Kontrolle nur durch eine Person durchführen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragnehmers, dessen Ausstattung, Geschäftsgeheimnisse und Sicherheitsmaßnahmen verpflichtet ist. Wird die Kontrolle nicht durch eine der in **Anhang 3** genannten Person durchgeführt, muss der Auftraggeber oder die kontrollierende Person deren/ihre Legitimation mindestens 5 (fünf) Werktage vor der Kontrolle schriftlich oder per Fax nachweisen. Der Auftragnehmer behält sich vor, etwaig entstehende interne oder externe Kosten für diese Kontrollen in den Geschäftsräumen des Auftragnehmers dem Auftraggeber in Rechnung zu stellen. Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG (bzw. Artikel 28 Abs. 3 h) EU-DSGVO) vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage (bzw. Artikel 32 EU-DSGVO) nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditor, Qualitätsauditor) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

9. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Es ist bekannt, dass nach § 42a BDSG (bzw. Artikel 33 und 34 EU-DSGVO) Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG (bzw. Artikel 33 und 34 EU-DSGVO) treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

10. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl.

§ 11 Abs. 3 Satz 1 BDSG bzw. Art. 28 Abs. 3 a) EU-DSGVO). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich, per E-Mail (in Textform) oder per Fax bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG bzw. Art. 28 Abs. 3, letzter Absatz zu informieren, wenn er der Meinung ist, eine Weisung verstöße gegen datenschutzrechtliche Vorschriften. Diese Hinweispflicht beinhaltet keine umfassende rechtliche Prüfung. Der Auftragnehmer ist berechtigt (aber nicht verpflichtet), die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber schriftlich oder per Telefax bestätigt oder geändert wird.

11. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Wahrung von Geschäftsgeheimnissen

Die Parteien verpflichten sich zu strikter Vertraulichkeit Dritten gegenüber. Die Parteien sind insbesondere verpflichtet, alle ihnen anlässlich der Durchführung des Auftrags bekannt werdenden 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. Die Weitergabe solcher Informationen ist nur mit vorheriger schriftlicher Zustimmung der anderen Partei zulässig. Die vorgenannte Verpflichtung findet insoweit keine Anwendung, als die Partei darlegen kann, dass Informationen öffentlich zugänglich und zum Zeitpunkt der Offenlegung verfügbar oder danach der Öffentlichkeit zugänglich geworden sind, und zwar ohne Verletzungshandlung oder -unterlassung durch diese Partei oder eines ihrer Vertreter oder Angestellten, oder vor dem Erhalt von der anderen Partei im Besitz der Partei oder ihr bekannt waren, oder der Partei durch eine andere Person ohne Einschränkung rechtmäßig offen gelegt wurden, oder von der Partei ohne Zugang zur Information der anderen Partei unabhängig entwickelt wurden, oder nach gesetzlichen oder verwaltungsrechtlichen Vorschriften offen gelegt werden müssen, wenn der anderen Partei dieses Erfordernis unverzüglich bekannt gegeben wird und der Umfang solcher Offenlegung soweit wie möglich eingeschränkt wird, oder aufgrund einer gerichtlichen Entscheidung offen gelegt werden müssen, wenn der anderen Partei von dieser Entscheidung unverzüglich Nachricht gegeben wurde und wenn nicht die Möglichkeit besteht, diese Entscheidung anzufechten.

13. Kontaktpersonen

Soweit Weisungen oder Hinweise nach dieser Vereinbarung gegenüber der jeweils anderen Partei gegeben werden, sind sie an einen der in **Anhang 3** genannten Weisungsberechtigten oder -empfänger zu richten. Jede Partei kann einseitig ihre Kontaktpersonen durch schriftliche Erklärung gegenüber der anderen Partei ändern.

Nutzungsvereinbarung – myDMSCloud

Anhang 1 zu den Allgemeinen Bedingungen zur Auftragsdatenverarbeitung in der „myDMSCloud“

Datenschutzkonzept:

Technische und organisatorische Maßnahmen i. S. d. § 9 BDSG

der comTeam Business Solutions GmbH, Mündelheimer Weg 40, 40472 Düsseldorf

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

x Alarmanlage

- ☐ Automatisches Zugangskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren

x Lichtschranken / Bewegungsmelder

x Schlüsselregelung (Schlüsselausgabe etc.)

- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal

- ☐ Absicherung von Gebäudeschächten

x Chipkarten-/Transponder-Schließsystem

- ☐ Manuelles Schließsystem

x Videoüberwachung der Zugänge

x Sicherheitsschlösser

x Personenkontrolle beim Pfortner / Empfang

x Sorgfältige Auswahl von Reinigungspersonal

- ☐ Tragepflicht von Berechtigungsausweisen

Anmerkungen

- Begleitung des Besuchers/Wartungsarbeiters durch Mitarbeiter
- Protokollierung der Zutritte (Serverraum)
- Trennung von Bearbeitungs- und Publikumszonen
- Türsicherung

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

x Zuordnung von Benutzerrechten

x Passwortvergabe

x Authentifikation mit Benutzername / Passwort

- ☐ Gehäuseverriegelungen
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Einsatz von Intrusion-Detection-Systemen

x Verschlüsselung von Smartphone-Inhalten

x Einsatz von Anti-Viren-Software

x Einsatz einer Hardware-Firewall

x Erstellen von Benutzerprofilen

- ☐ Authentifikation mit biometrischen Verfahren
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen

x Einsatz von VPN-Technologie

- ☐ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pfortner / Empfang
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen
- ☐ Verschlüsselung von mobilen Datenträgern

x Einsatz von zentraler Smartphone-Administrations Software (z. B. zum externen Löschen von Daten)

x Verschlüsselung von Datenträgern in Laptops / Notebooks

x Einsatz einer Software-Firewall

Anmerkungen

- 2-Faktor-Authentifizierung: Citrix Receiver + TAN per SMS / E-Mail
- Active Directory –Benutzerverwaltung
- Zentrales anlegen des Benutzers
- Passwortvergabe durch den Benutzer
- Schulung zu Passwortanwendung
- Sperre ausgeschiedener Beschäftigter
- Automat. Bildschirmschoner
- Viren-Scanner für Server
- Viren-Scanner für Clients
- Verschlüsselung von W-LAN

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

x Erstellen eines Berechtigungskonzepts

x Verwaltung der Rechte durch Systemadministrator

x Anzahl der Administratoren auf das „Notwendigste“ reduziert

x Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

x Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten IP-Adresse wird geloggt

x Sichere Aufbewahrung von Datenträgern

x physische Löschung von Datenträgern vor Wiederverwendung

x ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

x Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

x Protokollierung der Vernichtung

Anmerkungen

- Rechtevergabe benutzerspezifisch nach Aufgabe
- Regelmäßige Überprüfung des Berechtigungssystems
- Verschlüsselung von Datenträgern

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

x Einrichtungen von Standleitungen bzw. VPN- Tunneln

☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

x E-Mail-Verschlüsselung

☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen

☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

**x Beim Physischen Transport:
Auswahl von Transportpersonal und –Fahrzeugen**

Nutzungsvereinbarung – myDMScLOUD

Anmerkungen

- Mitgliederdaten (Firmenname + Adresse) werden per SFTP (verschlüsselt) von der ElectronicPartner Infrastruktur in die dbc Cloud übertragen und dort in einer per Zugriffskontrolle geschützten Datenbank persistiert.
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
- Transportsicherung
- Datenschutzgerechte Entsorgung Papierdokumente mit Papiertonne/Schredder mit der Sicherheitsstufe 3
- Protokollierung

5. Eingabe Kontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

x Protokollierung der Eingabe, Änderung und Löschung von Daten

x Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

x Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
= kein Einsatz

x Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Anmerkungen

- Protokollierung der Eingabe; Änderung und Löschung von Daten auf Feldebene in Anwendungsprogrammen

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

x Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

x vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

x Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG

x Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)

x Auftragnehmer hat Datenschutzbeauftragten bestellt Beendigung

x Sicherstellung der Vernichtung von Daten nach des Auftrages

x Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

x laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Anmerkungen

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- | | |
|---|---|
| x Unterbrechungsfreie Stromversorgung (USV) | x Klimaanlage in Serverräumen |
| x Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | x Schutzsteckdosenleisten in Serverräumen |
| x Feuer- und Rauchmeldeanlagen | x Feuerlöschgeräte in/vor Serverräumen |
| ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen = Schlüsselkonzept | x Erstellen eines Backup- & Recoverykonzepts |
| x Testen von Datenwiederherstellung | x Erstellen eines Notfallplans |
| x Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort | x Serverräume nicht unter sanitären Anlagen |
| ☐ In Hochwassergebieten: Serverräume über der Wassergrenze | |

Anmerkungen

- Einsatz von Virtualisierungstechnologie
- Virenschutz / Firewall
- Spiegeln von Festplatten, z.B. RAID-Verfahren

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- | | |
|--|---|
| ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | ☐ Logische Mandantentrennung (softwareseitig) |
| x Erstellung eines Berechtigungskonzeptes | ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
| x Versehen der Datensätze mit Zweckattributen/Datenfeldern | ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
| x Festlegung von Datenbankrechten | x Trennung von Produktiv- und Testsystem |

Anmerkungen

- Trennung durch Berechtigungssystem
- Eigenständige Datenbank
- Mandantenfähigkeit

Aufnahme am Datum: 02.02.2018

Beteiligte Personen der Aufnahme: Felix Bruske, Alexandra Storms, Ralf Heitmann

Anhang 2 zu den Allgemeinen Bedingungen zur Auftragsdatenverarbeitung in der „myDMScLOUD“

Genehmigte Subunternehmer:

C&P Capeletti & Perl Gesellschaft für Datentechnik mbH

DATEV

QSA GmbH

comTeam Systemhaus GmbH

Aufgaben des Subunternehmers:

C&P: Hardware Infrastruktur

DATEV: Hardware Infrastruktur

QSA: Betrieb der Software Komponenten und Weiterentwicklung

comTeam Systemhaus: Datenerfassung und First Level Support

Anhang 3 zu den Allgemeinen Bedingungen zur Auftragsdatenverarbeitung in der „myDMScLOUD“

Kontaktpersonen beim Auftraggeber

Name: Vertretungsberechtigtes Organ des Vertragspartners gemäß Stammdaten

E-Mail: gemäß Stammdaten

Telefon: gemäß Stammdaten

Kontaktpersonen des Auftragnehmers

Name: Alexandra Storms , Neele Bölling

E-Mail: mydmscloud@comteam.de