Technische und organisatorische Maßnahmen

- i.S.d. Art 32 I DSGVO der Apotheken-Dienstleistungsgesellschaft mbH -

Präambel

Übersicht und Definition technischer und organisatorischer Maßnahmen (im Folgenden „TOM“) zur Sicherstellung von Anforderungen hinsichtlich des Datenschutzes und der Informationssicherheit innerhalb der Apotheken-Dienstleistungsgesellschaft mbH.

Kontakt

Sollten Ihrerseits (als Lieferant, Kunde oder sonstiger Kooperationspartner der ADG) Fragen oder Anmerkungen zu diesen technischen und organisatorischen Maßnahmen bestehen, stehen Ihnen die Folgenden Kontaktmöglichkeiten zur Verfügung. Bitte nennen Sie dabei möglichst konkret den Grund Ihrer Kontaktaufnahme.

- datenschutz@adg.de
- informationssicherheit@adg.de

Inhaltsübersicht

Historie

Version	Status	Datum	Autor(en)	Erläuterung
0.6	In Arbeit	20.07.2022	M. Rosignol	Erste inhaltliche Erarbeitung.
0.7	In Arbeit	18.08.2022	M. Rosignol, S. Langner	Vervollständigung von Inhalten, Überarbeitung und Kommentierung.
0.9	In Arbeit	15.02.2023	M. Rosignol	Ergänzung und Anpassung an Kommentierung.
1.0	Final	21.02.2023	J. von Morstein	Freigabe der Version.
Juli 2024	Final	18.07.2024	M. Rosignol	Neues Layout und kleine inhaltlicher Ergänzungen.

Vorbemerkungen

In dem vorliegenden Dokument werden technische und organisatorische Maßnahmen i.S.d. Art 32 I DSGVO und BDSG n.F. gültig für die nachfolgend benannte verantwortliche Stelle beschrieben. Berücksichtigt werden in diesem Dokument sämtliche Standorte der ADG inkl. Hauptverwaltung, Geschäftsstellen und Rechenzentrum.

Nicht Bestandteil dieses Dokuments und daher nicht berücksichtigt, werden technische und organisatorische Maßnahmen von Erfüllungsgehilfen, Kooperationspartnern, Kunden und sonstigen Geschäftspartnern der ADG. Diese sind selbst für die Einhaltung Ihrer technischen und organisatorischen Maßnahmen verantwortlich.

Zweck dieser Maßnahmen ist den Schutz von Informationen und personenbezogener Daten zu gewährleisten. Die verantwortliche Stelle ist dabei berechtigt, die Maßnahmen an sich ändernde Rahmenbedingungen anzupassen, sofern das bisher erreichte Sicherheitsniveau unterschritten wird oder nicht mehr dem Stand der Technik entspricht.

Verantwortliche Stelle

ADG Apotheken-Dienstleistungsgesellschaft mbH
Salzachstraße 15
68199 Mannheim
im Folgenden „ADG“ oder „verantwortliche Stelle“ genannt

Kontaktdaten		Vertreten durch Geschäftsführungsmitglieder
Tel.:	+49 621 8505 520	Joachim von Morstein (Vorsitzender)
Fax:	+49 621 8505 501	Mihai Diga
E-Mail:	adg-hv@adg.de	Tobias Osterloher

Standorte

ADG Hauptverwaltung Salzachstraße 15 68199 Mannheim	ADG Hauptverwaltung Breslauer Straße 10 90766 Fürth	ADG Rechenzentrum (Noris Rechenzentrum Nürnberg) Thomas-Mann-Straße 16 – 20 90471 Nürnberg

Geschäftsstellen

Bad Kreuznach Uhlandstraße 1 55543 Bad Kreuznach	Berlin Lengeder Straße 42 13407 Berlin	Fürth Breslauer Straße 10 90766 Fürth
Gotha Am Kindleber Feld 3 99867 Gotha	Hamburg Rahlau 88-90 22045 Hamburg	Hanau Donaustraße 11 63452 Hanau
Herne Friedrich der Große 24 44628 Herne	Köln Kirschbaumweg 23 50996 Köln	Mannheim Salzachstraße 15 68199 Mannheim
München Riesstraße 19 80992 München	Stuttgart Riedstrasse 25 73760 Ostfildern-Ruit	

1. Geltungsbereich

Die technischen und organisatorischen Maßnahmen gelten für die verantwortliche Stelle und die in der Stelle erfolgenden Verarbeitungsprozesse von Informationen, personenbezogener Daten sowie einschließlich besonderer Kategorien personenbezogener Daten - „sensible Daten“. Unter personenbezogene Daten sind sämtliche Informationen zu verstehen, die Rückschlüsse auf natürliche Personen direkt oder indirekt zulassen. Diese technischen und organisatorischen Maßnahmen gelten für die verantwortliche Stelle selbst sowie für

a. Mitarbeiter der verantwortlichen Stelle;
b. Unternehmen und deren Mitarbeiter die direkt auf die Informationsbestände der verantwortlichen Stelle zugreifen, die in deren Eigentum oder Besitz stehen. Hierunter sind insbesondere Erfüllungsgehilfen (bspw. Zulieferer) zu subsumieren.

2. Ziel und Zweck

ADG verarbeitet personenbezogene Daten von Kunden, Auftraggebern und Dienstleistern sowie eigenen Mitarbeitern ausschließlich im Rahmen einer rechtmäßigen Verarbeitung i.S.d. Art. 6 DSGVO. Dies vorausgeschickt, darf eine Verarbeitung personenbezogener Daten ausschließlich

a. für festgelegte, eindeutige und legitime Zwecke und in einer für die betreffende Person nachvollziehbaren Weise erfolgen;
b. nicht in einer mit dem jeweiligen Zweck der Verarbeitung nicht zu vereinbarenden Art und Weise durchgeführt werden.

Eine Übermittlung personenbezogener Daten ist nur dann zulässig, wenn dem Empfänger aufgrund einer Rechtsvorschrift, interner Richtlinien oder sonstiger Vereinbarungen ein Recht auf Verarbeitung jener Daten eingeräumt wurde und dieser zu einem vertraulichen Umgang mit den Informationen verpflichtet wurde. Die Herleitung dieser Rechtmäßigkeit ist nachweislich zu dokumentieren.

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen der verantwortlichen Stelle um Informationen (siehe Begriffsbestimmung) rechtskonform und sicher verarbeiten zu können. Dabei werden Maßnahmen definiert, um einen dem Stand der Technik entsprechenden angemessenen Schutz für die erfolgende Informationsverarbeitung zu gewährleisten.
Die verantwortliche Stelle hat folgende Maßnahmen zur Sensibilisierung der Mitarbeiter in Bezug auf Informationssicherheit und Datenschutz ergriffen.

a. Benennung jeweils eines Datenschutz- und Informationssicherheitsbeauftragten;
b. Sensibilisierung der Mitarbeiter (Online-Schulungen, Bereitstellung von Flyern, Standards oder Arbeitshilfen);
c. Selbstverpflichtung der Mitarbeiter auf Wahrung des Datengeheimnisses;
d. Benennung von Datenschutzkoordinatoren in den jeweiligen Bereichen / Abteilungen des Unternehmens wo personenbezogene Daten verarbeitet werden.

3. Überblick über die Technischen und organisatorischen Maßnahmen

Zur Gewährleistung der klassischen Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit) definiert die verantwortliche Stelle die nachfolgenden in diesem Dokument festgehaltenen Kontrollmaßnahmen technischer und organisatorischer Natur. Sie dienen der Gewährleistung der in Art. 32 und 25 DSGVO festgehaltenen Eigenschaften zur Sicherheit der Verarbeitung personenbezogener Daten als auch von Informationen der verantwortlichen Stelle im Allgemeinen.

Vertraulichkeit - Zugangs und Zutrittskontrolle - Zugriffs- und Benutzerkontrolle - Weitergabe- und Übertragungskontrolle - Trennungskontrolle	**Integrität** - Eingabekontrolle - Datenträgerkontrolle
Verfügbarkeit und Belastbarkeit - Verfügbarkeitskontrolle - Wiederherstellbarkeit	**Überprüfung, Bewertung und Evaluierung** „kontinuierlicher Verbesserungsprozess“ - Auftragskontrolle - Incident-Response-Management

4. Technische und organisatorische Maßnahmen zur Vertraulichkeit

4.1. Zugangs- und Zutrittskontrolle

Unbefugten soll der Zutritt bzw. Zugang zu Systemen der Datenverarbeitung verwehrt bleiben, dies ist Ziel der Zugangskontrolle. Hierfür wird in der verantwortlichen Stelle die folgende Umsetzung vorgenommen als auch die nachfolgend definierten Maßnahmen umgesetzt.

4.1.1. Umsetzung

In der ADG wurden personenbezogen Zutrittsberechtigungen erteilt, die Zutrittsberechtigung kann durch manuelle Schlüsselverwaltung und -vergabe oder durch Berechtigungen auf dem Zugangschip erfolgen. Ein Zugang zu Büros, örtlichen Bereichen ist nur mit der passenden Berechtigung möglich. Schränke, Sideboards und Rollcontainer sind alle abschließbar und stets bestimmten Personen oder Personengruppen zugeordnet. Bezgl. der Herausgabe von Zutrittsmöglichkeiten „Zugangsberechtigungen“ an Mitarbeiter generell wird von der Konzern Personalabteilung dokumentiert,

- Name des Mitarbeiters,
- Datum der Schlüsselherausgabe
- Datum der Schlüsselzurückgabe
- Unterschrift des Mitarbeiters

Erfüllungsgehilfen und sonstige Nichtunternehmenszugehörige wird der Zugang in Technikräume der ADG nur in Begleitung eines zugangsberechtigten Mitarbeiters gewährt. Außerhalb der Geschäftszeiten werden die Betriebsstätten durch einen Sicherheitsdienst (Unternehmen Securitas) überwacht.

4.1.2. Technische Maßnahmen

Unbefugten soll der Zutritt zu den Räumlichkeiten, Datenverarbeitungsanlagen der verantwortlichen Stelle erschwert werden. Hierdurch soll eine Nachvollziehbarkeit geschaffen werden, welche Person sich wann in dem Gebäude / Räumlichkeit aufgehalten hat. Hierfür sind die folgenden Maßnahmen umgesetzt worden.

- Alarmanlage
- Datenschutzkonforme Videoüberwachung
- Verschlossene Bereiche
- Sicherheitsschlösser
- Sicherung von Gebäude, Fenster und Türen
- Bewegungsmelder
- Zäune, Pforten und andere Begrenzungen und Zugangsbeschränkungen

Darüber hinaus soll unbefugten die Nutzung von Systemen und sonstigen Datenverarbeitungsanlagen nicht ermöglicht werden. Die verantwortliche Stelle hat hierfür folgende Maßnahmen etabliert.

- Authentifikation mittels Passworteingabe
- Anti-Viren-Software
- Sichere VPN-Verbindungen mittels 2-Faktor-Authentifizierung
- Benutzerprofile
- Firewall
- E-Mail-Anhang Scanner
- Schlüsselregelungen
- Administratorregelungen

4.1.3. Organisatorische Maßnahmen

Unabhängig zu den bereits in Ziffer 4.1.2 genannten Maßnahmen, werden folgende organisatorische Maßnahmen in der verantwortlichen Stelle umgesetzt.

- Besucheranmeldung
- Vertrauenswürdiges Personal für die Reinigung der Räumlichkeiten
- Passwortregeln inkl. Vorgabe zur Komplexität des Passworts
- Schlüsselregelungen

4.2. Zugriffs- und Benutzerkontrolle

Es soll verhindert werden, dass IT-Systeme der verantwortlichen Stelle von Unbefugten eingesetzt werden können. Für Unberechtigte soll die Nutzung automatisierter Verarbeitungsprozesse der verantwortlichen Stelle durch die Einrichtung und Etablierung sicherheitsförderlicher Datenübertragungsmechanismen verhindert werden.

4.2.1. Umsetzung

Benutzer werden administrativ verwaltet, gleichermaßen wie Administratoren selbst. Zugriffe erfolgen ausschließlich über das interne Konzernnetzwerk und sonst über definierte externe Ports (bspw. VPN-Konnektivität). Die Authentizität soll durch 2-Faktor Authentifizierung in den im Unternehmensnetzwerk betriebenen Systemen und Portalen sichergestellt werden. Die Nutzung von Endgeräten, Server oder sonstiger zentraler Hard- und Software-Systeme ist nur mit gültiger Benutzerkennung zusammen mit gültigem Passwort möglich. Anmeldeversuche und Systembenutzungen können untersucht werden. Allgemein wird die Zugriffskontrolle durch Benutzerkennung und anlegen individueller Passwörter durch die Administration bzw. anschließend durch den jeweiligen Benutzer sichergestellt.

4.2.2. Technische Maßnahmen

Um zu gewährleisten, dass Berechtigte ausschließlich auf Daten zugreifen können, für welche sie die Berechtigung haben „Need-To-Know-Prinzip“ und dass ausschließlich eine zweckgebundene Verarbeitung personenbezogener Daten erfolgt, werden folgende technische Maßnahmen in der verantwortlichen Stelle umgesetzt.

- Passwortregel (mit Mindestanforderungen)
- Protokollierung von Zugriffen bei Anwendungen und Serversystemen
- Administratoren-management (Anpassung der Anzahl und Berechtigung von Administratoren) bei Serversystemen
- Anti-Viren-Software
- Authentifikation durch Benutzername und Passwort oder Mehrfaktor-Authentifikation

4.2.3. Organisatorische Maßnahmen

Unbefugte Personen sollen keinen Zugang zu automatisierte Verarbeitungssysteme erhalten. Es ist in der verantwortlichen Stelle sicherzustellen, dass bei Authentifizierung überprüft wird, ob der Benutzer berechtigt ist Daten zu verarbeiten oder Systeme nutzen zu dürfen. Hierfür werden folgende organisatorische Maßnahmen neben den in Ziffer 4.2.2 definiert.

- Berechtigungskonzept
- Regelmäßige Kontrollen hinsichtlich der Berechtigungen
- Festlegung zugangsberechtigter Nutzer und passende Zuteilung von Benutzerprofilen

4.3. Weitergabe- und Übertragungskontrolle

Durch die Übertragungskontrolle soll geprüft und festgestellt werden, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

4.3.1. Umsetzung

Grundsätzlich ist das Personal der verantwortlichen Stelle nur berechtigt, eigens zugewiesenes technisches Equipment einzusetzen oder mitzunehmen. D.h. Endgeräte und Datenträger anderer Personen oder von Arbeitskollegen sind nicht von unberechtigten Personen mitzunehmen oder einzusetzen.

4.3.2. Technische Maßnahmen

Informationen der verantwortlichen Stelle als auch personenbezogene Daten, die bei der verantwortlichen Stelle verarbeitet werden, dürfen während des Transports-, der Weitergabe, Übertragung oder Übermittlung nicht von Unbefugten verarbeitet werden. Die Gewährleistung der Sicherheit jener Informationen ist Ziel der Weitergabe- und Übertragungskontrolle, hierfür wurden folgende technische Maßnahmen entsprechend dem Stand der Technik in der verantwortlichen Stelle eingeführt und umgesetzt.

- Authentifikationsmaßnahmen (bspw. OTP, Geräteauthentifizierung)
- VPN-Technologie

4.3.3. Organisatorische Maßnahmen

Darüber hinaus wurden zur Realisierung der Weitergabe- und Übertragungskontrolle die folgenden organisatorischen Maßnahmen in der verantwortlichen Stelle eingeführt und umgesetzt

- Sichere und zertifizierte Datenträgervernichtung, siehe Datenträgerkontrolle (Ziffer 5.2)
- Richtlinien oder Verfahrensanleitungen bspw. zur Datenklassifizierung, Passwörter oder Berechtigungen

4.4. Trennungskontrolle

Informationen als auch personenbezogene Daten sollen ausschließlich zweckgebunden verarbeitet werden dürfen, dies gilt unabhängig davon, ob die Leistung im Auftrag erfolgt oder nicht.

4.4.1. Umsetzung

Die Trennung der Daten je nach Zweck soll bei der verantwortlichen Stelle u.a. durch folgende Maßnahmen erreicht werden.

- Personenbezogene Zugriffsregelung,
- Trennung von Test- und Betriebsumgebungen,
- Mandantentrennung.

5. Technische und organisatorische Maßnahmen zur Integrität

5.1. Eingabekontrolle

Die Eingabekontrolle dient einer Überprüfbarkeit der erfolgenden Verarbeitung von Informationen. Hierdurch soll eine Kontrolle der Veränderung oder gar Löschung von Informationen ermöglicht werden.

5.1.1. Umsetzung

Mit Hilfe der Eingabekontrolle kann eine Nachvollziehbarkeit ermöglicht werden, welche Informationen zu welcher Zeit von welchem Datenverarbeitenden System eingebunden worden sind.

5.1.2. Technische Maßnahmen

Innerhalb der verantwortlichen Stelle wurden folgende Maßnahmen eingeführt, um eine Verarbeitung von Informationen nachvollziehen zu können.

- Vergabe von Zugriffsberechtigungen und Digitales Berechtigungskonzept (Active Directory)
- Einrichtung und Verwendung von individuellen personenbezogenen Benutzernamen

5.2. Datenträgerkontrolle

Unbefugtes Lesen, Kopieren, Verändern oder Löschen von Datenträgern soll mit Hilfe der Datenträgerkontrolle ausgeschlossen werden.

5.2.1. Umsetzung

Neben einer ausschließlich ordnungsgemäß industrienormenkonformen (DIN 66399) Vernichtung von Datenträgern wurden in der verantwortlichen Stelle technische und organisatorische Maßnahmen eingerichtet, um eine sichere und zweckkonforme Verarbeitung von Informationen und personenbezogenen Daten zu ermöglichen.

5.2.2. Technische und organisatorische Maßnahmen

In der Verantwortlichen Stelle wurden, um eine unbefugte Verarbeitung von Informationen zu verhindern die nachfolgend genannten technischen und organisatorischen Maßnahmen eingerichtet.

- Digitales Berechtigungskonzept,
- Sichere Aufbewahrung von Datenträgern, durch verschlossene Räumlichkeiten und Behälter,
- Richtlinien und Vorgaben zum Umgang mit Datenträgern

6. Technische und organisatorische Maßnahmen zur Verfügbarkeit und Belastbarkeit

Es gilt seitens der verantwortlichen Stelle sicherzustellen, dass personenbezogene Daten gegen zufällige oder sonstig unrechtmäßige Zerstörung oder Verlust geschützt werden „Kontrolle der Verfügbarkeit und Wiederherstellbarkeit“.

6.1.1. Umsetzung

Um die Wiederherstellbarkeit von Informationen sicherzustellen sind Systeme fehlertolerant auszugestalten, um Nichtverfügbarkeiten von Informationen zu reduzieren.

6.1.2. Technische und organisatorische Maßnahmen

Neben Maßnahmen zum Angriffs- und Virenschutz werden bei der verantwortlichen Stelle Informationen sowie personenbezogene Daten durch ein umfassendes Sicherungskonzept geschützt, dies beinhaltet die nachfolgend aufgelisteten Maßnahmen.

- Plattenspiegelung (RAID) zentraler Speichermedien (Server),
- Unterbrechungsfreie Stromversorgung bei Servern
- Überspannungsfilter,
- Bedarfsgerechte Backups von Serverdaten

7. Kontinuierlicher Verbesserungsprozess technischer und organisatorischer Maßnahmen

7.1. Auftragskontrolle

Informationen und insb. personenbezogene Daten, die im Auftrag verarbeitet werden, sind nur entsprechend konkreter zweckgebundener Erlaubnistatbestände zu verarbeiten.

7.1.1. Umsetzung

Die Datenverarbeitung erfolgt ausschließlich im Sinne rechtlich legitimer Vorgaben. Erfolgt eine Verarbeitung personenbezogener Daten im Auftrag, werden Einzelheiten zur Auftragsausführung und -kontrolle in einem Vertrag über die im Auftrag erfolgende Verarbeitung durch die Vertragsparteien festgelegt.

7.1.2. Technische und organisatorische Maßnahmen

Seitens der verantwortlichen Stelle ist zu gewährleisten, dass eine Verarbeitung von Daten und Informationen ausschließlich nach Weisungen des Auftraggebers erfolgen. Hierfür wurden seitens der verantwortlichen Stelle insbesondere die folgenden Maßnahmen eingeführt und umgesetzt.

- Sorgfältige Auswahl von Auftragnehmer,
- Überprüfung der Datenvernichtung nach Auftragsende, sofern nicht steuerrechtliche oder sonstige gesetzliche Aufbewahrungspflichten einer Löschung entgegenstehen. Sollte keine Vernichtung rechtlich möglich sein, werden die Daten gesperrt,
- Überprüfung von Lieferanten, Zulieferer oder sonstiger externer Vertragspartner vor Beginn des Rechtsgeschäfts.

7.2. Incident-Response und Compliance Management

Im Rahmen des Incident-Response-Managements wurden Maßnahmen in der verantwortlichen Stelle eingerichtet, um mit Datenschutz- oder Informationssicherheitsvorfällen umzugehen, diese sind nachfolgend dargestellt.

- Ticketsystem; dient dem Umgang von Datenschutz- und Compliance-Vorfällen. In dem System können Compliance oder Datenschutzvorfälle gemeldet, verwaltet und bearbeitet werden.
- Durchführung von Notfallübungen,

- Brandschutz- und Ersthelfer im Falle von Notfällen
- Definitionen von Richtlinien und Standards
- Überprüfung von Lieferanten und sonstigen Vertragspartnern

8. Schlussbestimmungen

Die technischen und organisatorischen Maßnahmen gelten für die verantwortliche Stelle in Deutschland, deren Mitarbeiter, als auch jene die zur Berufsausübung schweigepflichtiger Personen. Sie beschreiben Maßnahmen, um die Sicherheit der Verarbeitung von Informationen und personenbezogener Daten zu gewährleisten.

Im Falle neuer gesetzlicher, behördlicher Anforderungen oder Anforderungen resultierend aus Industrienormen, behält sich die verantwortliche Stelle vor, diese Maßnahmen bedarfsgerecht anzupassen. Diese technischen und organisatorischen Maßnahmen sind von der Unternehmensleitung genehmigt und herausgegeben worden. Technische und organisatorische Maßnahmen werden in aktueller genehmigter Fassung von dem Auftraggeber unter folgender URL (https://www.adg.de/rechtliches/download) bereitgestellt.

In der Zukunft werden innerhalb der verantwortlichen Stelle Schulungen, Informationsflyer oder Checklisten angeboten, um das Verständnis für Datenschutz und dessen Anforderungen im Unternehmen für alle Mitarbeiter und Erfüllungsgehilfen zu erhöhen und transparent zu gestalten. Die in diesem Dokument definierten Maßnahmen sind einzuhalten.

Begriffsbestimmungen

Für die vorliegenden technischen und organisatorischen Maßnahmen i.S.d. Art 32 I DSGVO werden die folgenden Begriffsbestimmungen definiert.

Begriff	Erläuterung
Klassische Schutzziele der Informationssicherheit	Technische und organisatorische Maßnahmen sind bei der Verarbeitung personenbezogener Daten so einzusetzen, dass eine Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Daten sichergestellt ist. - Vertraulichkeit: Personenbezogene Daten sind vor unbefugter oder unbeabsichtigter Preisgabe zu schützen. - Integrität: Personenbezogene Daten sind vollständig und korrekt bereitzustellen - Verfügbarkeit: Personenbezogene Daten müssen dann zur Verfügung stehen, wenn sie benötigt werden. Dies setzt die Möglichkeit zur Widerherstellung voraus. - Belastbarkeit: Fehlertoleranz des Systems auf welches personenbezogene Daten verwahrt werden. Inbegriffen sind Schutzmaßnahmen wie Backupkonzept, Angriffs- und Virenschutz.
Dritte	Sind außenstehende natürliche oder juristische Personen, die nicht Mitarbeiter des Unternehmens oder eines verbundenen Unternehmens sind. Exklusive Erfüllungsgehilfen.
DSGVO	Datenschutzgrundverordnung VO (EU) 2016/679 – Verordnung des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
Erfüllungsgehilfe	Freie Mitarbeiter, beauftragte Freiberufler, kooperierende oder verbundene Unternehmen, Auftragsverarbeiter des Unternehmens sowie Personen, die unter der unmittelbaren Verantwortung des Unternehmens oder des Auftragsverarbeiters befugt sind Informationen zu verarbeiten.
Freiberufler	Ein freier Beruf oder Freiberuf ist ein selbständig ausgeübter wissenschaftlich, künstlicher, schriftstellerischer, unterrichtender oder erzieherischer Beruf. Beispielsweise Rechtsanwälte, Wirtschaftsprüfer oder Steuerberater.
Geschäftsleitung	Personen, die mit der Leitung und Verantwortung der Geschäfte eines Unternehmens betraut sind und die Gesellschaft als Organ gerichtlich und außergerichtlich organschaftlich vertreten können. Geschäftsführung einer GmbH / UG (haftungsbeschränkt), Inhaber einer Einzelunternehmung oder Vorstand einer Aktiengesellschaft.

Information	Sämtliche Daten, Datenbestände und sonstige Informationen, irrelevant ihres Mediums oder Übertragungsform, die sich auf eine Person (personenbezogene Daten) oder auf das Unternehmen des Arbeitgebers eines Mitarbeiters oder auf verbundene Unternehmen beziehen.
Informations- und Kommunikationstechnik	Sämtliche technischen Geräte des Unternehmens, welche dieses infrastrukturell oder seinen Mitarbeitern zur dienstlichen und oder zugleich zur persönlichen Nutzung zur Verfügung stellt. Hierzu zählen u.a. Laptops, Server, Tablet-Computer, oder Smartphones.
ISO / ISB	„Information Security Officer“ (ISO) oder „Informationssicherheitsbeauftragter“ (ISB). Die Begriffe sind synonyme füreinander.
Übermittlung	Jede durchgeführte Offenlegung oder sonstige Bekanntgabe von Informationen durch das Unternehmen, dessen Mitarbeiter, Organe oder Erfüllungsgehilfen an Dritte.
Mitarbeiter	Hierzu zählen sämtliche Arbeitnehmer (Vollzeit-, Teilzeitangestellte und Auszubildende), Mitarbeiter mit disziplinarischer Funktion (Führungskraft) sowie Praktikanten als auch sonstige Erfüllungsgehilfen unseres Unternehmens oder mit diesem verbundenen Unternehmen.
Personenbezogene Daten (pbD)	Sind sämtliche Informationen, die sich auf identifizierbare oder identifizierte natürliche Personen beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann; vgl. Art. 4 lit. 1 DSGVO. Irrelevant des Dateiformats und der Übermittlungsform.
Sensible Daten / Besondere Kategorien pbD	Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt, vgl. besondere Kategorien personenbezogener Daten, Art. 9 Abs 1 DSGVO. Ausnahmen hierzu siehe Art. 9 Abs 2f DSGVO
Sichere Passwörter	Ein Einsatz trivialer Begrifflichkeiten (Begriffe, Namen) oder Zahlenfolgen als Passwörter ist grundsätzlich untersagt. Ein Passwort hat mindestens verschiedene Buchstaben in Groß- und Kleinschreibung, Zahlen als auch Sonderzeichen zu beinhalten damit es als sicher zu erachten ist. Es sind die für Passworte gültigen Regelungen (Policies) der ADG oder beim Fehlen solcher die der Phoenix Gruppe einzuhalten.
URL	Uniform Resource Locator „URL“ identifiziert und lokalisiert Webseiten oder sonstige Ressourcen, welche über das Internet zugänglich sind.
Verarbeiten	Jeder Vorgang im Zusammenhang mit Informationen (insb. personenbezogenen Daten), welcher mit oder ohne Hilfe automatisierter Verfahren erfolgt. Bspw. das Erheben, Organisieren, Speichern, Anpassen,

	Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung oder die Vernichtung von Informationen, vgl. Art. 4 lit. 2 DSGVO.
Verbundene Unternehmen	Hierunter sind sämtliche verbundene, im Mehrheitsbesitz stehende, abhängige oder herrschende Unternehmen i.S.d. §§ 15 ff. AktG zu verstehen – Synonym: „Konzernunternehmen“. Dies gilt, solange die Anteile bzw. Stimmrechte gehalten werden.