herfurth.partner

Das Digitale Büro und Recht

Digitale Dokumentation, Informationen
und Aufbewahrungspflichten

Ein Leitfaden, 2. Aufl. | 2020

CASTON LAW & BUSINESS INFORMATION

Impressum

Redaktion

Dr. jur. Anne Knodel, Selina Diel, RAin Sabine Reimann
überarbeitete, 2. Auflage, Stand November 2019

Herausgeber

Herfurth & Partner
Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, 30159 Hannover
Fon 0511-307 656-0
Fax 0511-307 656-11
Mail info@herfurth.de
www.herfurth.de

Verlag

Caston GmbH
Law & Business Information
Luisenstr. 5, 30159 Hannover
Fon 0511-307 656-50
Fax 0511-307 656-60
Mail info@caston.de
www.caston.info

Disclaimer

Einführung

Inhalt

Einführung

Inhalt
Vorwort
Digital Business
Paper/Industrie 4.0

Das Digitale Büro und Recht

Digitale Dokumentation, Informationen und Aufbewahrungspflichten
Ein Leitfaden in Stichworten

Vorwort

Die Digitalisierung durchzieht inzwischen alle Bereiche in den Unternehmen und stellt oft eine Herausforderung dar. Einerseits sind es die großen Themen, die die Wirtschaft bewegen: Industrie 4.0, eCommerce, Plattformen und digitale Marktplätze, Big Data, Künstliche Intelligenz, Datenschutz, Datensicherheit und die Digitalisierung von Geschäftsstrukturen.

Andererseits stellen sich aber im täglichen Büroalltag viele Fragen zum Umgang mit digitalen Medien und Dokumenten: Aufbewahrung von Dokumenten, Löschung von Daten und Akten, Zustandekommen von Geschäften, Dateien als Beweismittel, aber auch Publikations- und Informationspflichten.

Diese Publikation will auf die wichtigsten Fragen Antworten und Hinweise geben – zumeist in einfachen Stichpunkten, kurzen Erläuterungen und nützlichen Hinweisen. Es ist eine Faktensammlung, die bewusst auf umfangreiche Darlegungen verzichtet.

Die Informationen wurden von Anne Knodel als wissenschaftlicher Mitarbeiterin im Sommer 2017 zusammengestellt und redaktionell bearbeitet. Ihr gebührt besonderer Dank für ihre Arbeit!

Für weitere Anregungen und Fragen unserer Leser sind wir dankbar.

Diese Publikation wurde mit der größtmöglichen Sorgfalt zusammengestellt, sie stellt jedoch keinen Anspruch an Vollständigkeit und es können daraus keine Haftungsansprüche gestellt werden. Eine weitere rechtliche, individuelle Beratung ist zwingend erforderlich.

Ulrich Herfurth, im November 2019

Herfurth & Partner

Herfurth & Partner ist als Rechtsanwaltsgesellschaft auf nationales und internationales Wirtschaftsrecht und Unternehmensrecht spezialisiert, sowohl für mittelständische Unternehmen im Familienbesitz als auch für nationale und internationale Industrieunternehmen und Konzerne. Die Kanzlei besteht aus 18 deutschen und internationalen Anwälten in Hannover und deckt alle Bereiche des allgemeinen Wirtschaftsrechts ab, einschließlich Unternehmensrecht, Finanzen, Handel und Vertrieb, Wettbewerb, Personal und Technologie.

Die Kanzlei ist Gründungsmitglied der internationalen Anwaltsgruppe Alliuris mit 32 Büros in Europa, USA, Brasilien, Russland, China und Indien.

Herfurth & Partner hat vor einigen Jahren die Expertengruppe Indy4 initiiert, die sich mit der Digitalisierung unter technischen, organisatorischen, wirtschaftlichen und rechtlichen Gesichtspunkten befasst.

Das *Digital Business* von Unternehmen deckt Herfurth & Partner mit Rechtsberatung ab:

Gesamtstruktur Digitaler Modelle

- Legal Scan zur Digitalisierung
- Legal design/strategische Rechtsberatung für digitale Geschäftsmodelle

Datenschutz und Persönlichkeitsrechte

- Legal Scan für Mitarbeiterdatenschutz
- Vorbereitung und Check zur Einhaltung EU-Datenschutzgrundverordnung
- Unternehmensrichtlinien zu Datenschutz und Privacy (intern und extern)
- Verfahren zu Datenschutzkonzepten (Privacy Management)
- Datenverarbeitungsverzeichnisse
- Mitarbeiterschulung zu Datenschutzanforderungen
- Auftragsdatenverarbeitungsverträge (DPA), national, EU, international
- Standardklauseln/Binding Corporate Rules (BCR) international
- Data Protection Impact Assessments (DPIA)
- Strategie zur Störfallvermeidung und zum Störfallmanagement
- Vertretung gegenüber nationalen und internationalen Datenschutzbehörden

Datensicherheit

- Definition von IT-Sicherheitspflichten des Managements
- Kontrolle von Provider-Verträge (IT System, Mail, Cloud, Web etc.)

- Kontrolle von Outsourcing-Verträgen
- Entwicklung von Unternehmensregeln zur Datensicherheit
- Check zu Cyberversicherung
- Check zu D&O Versicherungen
- Sicherheits- und Schutzkonzepte (z.B. BYOD), IT Compliance

Dateneigentum

- Analyse und Definition von Datenströmen (Kunden, Lieferanten, Parten)
- Analyse zu Schutzrechten für Geistiges Eigentum
- Schutzstrategie für überlassene Daten
- Datennutzungsvereinbarungen und Lizenzen mit Partnern
- IP Rechte Management und Schutz

Datencompliance

- Regulatorische Anforderungen/Telekommunikation, Medien, IT Sicherheit etc
- Kataloge zu Berichtspflichten
- Veröffentlichungspflichten
- Dokumentationspflichten
- Vertragsmanagement für Digitale Projekte

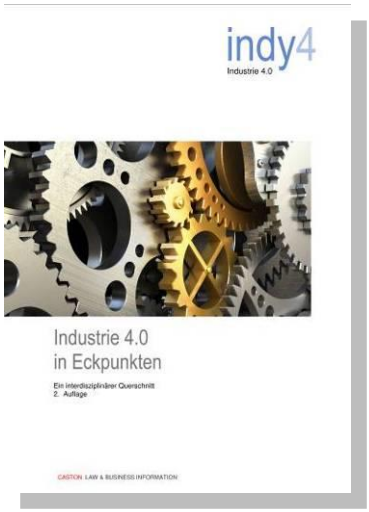
In unseren Konferenzen und Seminaren erhalten unsere Teilnehmer umfassende Einblicke in praktische Fragen der Rechtsanwendung für zukunftssichere Ausrichtung und Führung ihrer Unternehmen.

www.herfurth.de
www.indy4.de

ePaper

Industrie 4.0 in Eckpunkten

Ein interdisziplinärer Querschnitt



Die zweite Auflage des Reports und Eckpunktepapiers hat weiteren technischen Aspekten integriert – vornehmlich aus den Bereichen IT, Daten und Software und mit besonderem Augenmerk auf Sicherheit. Auch die rechtlichen Aspekte sind erweitert, insbesondere zu Datenschutz, Datensicherheit und geistigem und gewerblichem Eigentum an IT-Lösungen und Datenbeständen, sowie zu Netzen, Telekommunikation, Providern und Plattformen. Neu ist auch der Abschnitt zur internationalen Entwicklung in den Ländern USA, Brasilien, Russland, China und Indien.

Industrie 4.0 im Rechtsrahmen

Recht für die digitale Unternehmenspraxis

Der neue Report „Industrie 4.0 im Rechtsrahmen“ beschreibt in den verschiedenen Feldern, welche rechtlichen Rahmenbedingungen die Unternehmensprozesse steuern: Besondere Herausforderungen entstehen aus dem Umgang mit autonomen Prozessen in der Leistungskette, im Qualitätsmanagement, in unternehmens- und in länderübergreifenden Beziehungen und Abläufen. Generierung, Besitz, Verwendung und Verwertung der großen Datenmengen werfen neue Fragen zu Schutz und Zugriffsrechten auf – und verlangen eine privatrechtliche vertragliche Gestaltung. Industrie 4.0 berührt aber auch wichtige andere Bereiche wie Personal und Arbeitsgestaltung, Wettbewerbsrecht, Finanzierung und Rechnungswesen und Beziehungen zu Providern, Plattformen und Netzen. „Industrie 4.0 im Rechtsrahmen“ greift diese Fragen auf und gibt dazu aktuelle Lösungsansätze.

Sie erhalten die E-Paper kostenfrei unter
redaktion@herfurth.de

Das Digitale Büro

1 Digitaler Vertragsschluss

1.1 Formerfordernisse

Grundsätzlich besteht im deutschen Zivilrecht Formfreiheit:

- abgegebene Erklärungen sind in der Regel formlos gültig
- Wirksamkeit des Rechtsgeschäfts ist nicht von der gewählten Form abhängig (es sei denn, eine bestimmte Form ist gesetzlich vorgeschrieben)

Vertragsschluss ist möglich:

- mündlich, auch telefonisch
- per E-Mail
- durch konkludentes Handeln (z.B. Handschlag)

Anders ist es bei einem Schriftformerfordernis (§§ 126 ff. BGB) Zweck: Schutz der Vertragsparteien durch Warnfunktion, Beweisfunktion und, in den Fällen einer notariellen Belehrung, eine Beratungsfunktion.

Formmangel kann zur Nichtigkeit führen (§ 125 BGB), u. U. auch geheilt werden.

>> Die Vertragsparteien können die Form auch durch das Rechtsgeschäft bestimmen: Ein höheres (privates) Formerfordernis kann immer ein niedrigeres (auch gesetzliches) ersetzen, aber niemals umgekehrt.

1.2 Form der Erklärungen

1.2.1 Mündliche Erklärungen

- möglich, oftmals keine Beweismöglichkeit

1.2.2 Privatschriftlich

- jede schriftlich festgehaltene Erklärung, Aussteller der Urkunde muss erkennbar sein

1.2.3 Gesetzliche Schriftform

- vom Gesetzgeber vorgegebene Schriftform (vgl. § 126 BGB)
- Unterschrift durch Namensunterschrift oder ein notariell beglaubigtes Handzeichen (§ 40 BeurkG)
- Bei einem zweiseitigen Vertrag müssen beide Parteien auf derselben Urkunde unterschreiben oder jeweils auf einer von mehreren identischen Urkunden.

- Die Unterschrift muss den Text räumlich abschließen.

Beispiele für die gesetzliche Schriftform: Quittung (§ 368 BGB), Verbraucherdarlehensvertrag (§ 492 Abs. 1 BGB), Ratenlieferungsvertrag (§ 510 BGB), Kündigung von Mietverträgen (§ 568 Abs. 1 BGB), und weitere

1.2.4 Textform (gem. § 126b BGB)

Die Textform wurde in das Bürgerliche Gesetzbuch aufgenommen, um auch digitale Erklärungen zu erfassen:

- lesbare Erklärung, in der die Person des Erklärenden genannt ist
- in Form einer Urkunde oder auf andere dauerhafte, zur Wiedergabe geeignete Weise abgelegt z.B. eMails, Datenträger, Inhalt von Website nur nach Download
- handschriftliche Unterschrift ist keine Voraussetzung

Beispiele für zulässige Erklärungen in Textform: Garantieerklärung (§ 477 Abs. 2 BGB), Widerrufsbelehrung (Bundesgerichtshof (BGH), Urteil vom 15.05.2014 (Az.: III ZR 368/13)), Widerrufsrecht bei Verbraucherverträgen (§ 355 i.V.m. § 312c Abs. 1 BGB)

Für Anzeigen und Erklärungen darf vom Verbraucher keine strengere Form als die Textform verlangt werden (Ausnahme: notarielle Verträge) (neues AGB-Recht).

1.2.5 Elektronische Signatur (siehe unter Ziffer 3)

Die elektronische Form (vgl. §§ 126 III, 126a BGB) kann, soweit das Gesetz nichts anderes vorschreibt, die Schriftform ersetzen.

- Der Aussteller der Erklärung muss das Dokument mit seinem Namen und einer qualifizierten elektronischen Signatur (vgl. eIDAS-Verordnung) versehen.
- Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument elektronisch signieren.

1.2.6 Öffentliche Beglaubigung (vgl. § 129 BGB)

Die öffentliche Beglaubigung dient der Identifizierung des Ausstellers eine Urkunde:

- schriftlich abgefasste Erklärung
- Unterschrift des Erklärenden muss von einem Notar oder einer anderen öffentlichen Beglaubigungsstelle beglaubigt werden
- Bei einer mittels Handzeichen unterzeichneten Erklärung, muss dieses beglaubigt werden (vgl. § 126 Abs. 1 BGB).

Beispiele für die eine öffentliche Beglaubigung: Eintragung oder Änderung ins Vereinsregister (§ 77 BGB), Verwalterbestellung (§ 26 Abs. 3 WEG)

1.2.7 Notarielle Beurkundung (vgl. § 128 BGB)

Sofern gesetzlich vorgeschrieben, müssen Erklärungen in einer notariellen Verhandlung abgegeben werden. Die Beratung durch den Notar dient der Sicherheit der Beteiligten, zudem hat die notarielle Urkunde einen starken Beweischarakter:

- Die Identität der Parteien wird vom Notar festgestellt (Personalausweis).
- Der Notar überzeugt sich von der Geschäftsfähigkeit oder Testierfähigkeit der Person.
- Antrag und Annahme des Antrags müssen von einem Notar beurkundet werden.
- Das Original der Urkunde verbleibt beim Notar.

Beispiele für eine notarielle Beurkundung: Grundstückskaufvertrag (§ 311b Abs. 1 BGB), Schenkungsversprechen (§ 518 Abs. 1 BGB), Gründung einer GmbH (§ 2 Abs. 1 GmbHG), Feststellung der Satzung einer GmbH (§ 2 Abs. 1 GmbHG),
Abtretung von GmbH-Geschäftsanteilen (§ 15 Abs. 3 GmbHG), und weitere

1.3 Erklärung per Mausklick

Verträge im Bereich des eCommerce werden in der Regel per E-Mail oder per Mausklick auf der Website oder in der App des Anbieters abgeschlossen.
Grundsätzlich gelten für Verträge im Internet die gleichen Regelungen wie im übrigen Rechtsverkehr auch:

- Ein Vertrag kommt durch zwei übereinstimmende Willenserklärungen zustande: Antrag bzw. Angebot i.d.R. durch den Käufer/Annahme i.d.R. durch den Verkäufer
- Alle wesentlichen Vertragsbestandteile wie Preis, Kaufsache und Parteien (essentialia negotii) müssen feststehen.
- Das „Angebot“ auf einer Website ist i.d.R. eine unverbindliche Aufforderung, ein Angebot abzugeben (invitatio ad offerendum): das Vertragsangebot geht folglich nicht vom Websitebetreiber aus, sondern vom Nutzer.
- Voraussetzung für die Wirksamkeit einer empfangsbedürftigen Willenserklärung sind Abgabe und Zugang (§ 130 BGB).

Die Annahmeerklärung gilt als zugegangen, wenn sie in den Machtbereich des Empfängers gelangt ist, er diese zur Kenntnis nehmen kann und mit der Kenntnisnahme zu rechnen ist:

- Die elektronische Willenserklärung ist abgegeben, wenn der Käufer durch Mausklick den Vorgang im Internet beendet hat.
- Online abgegebenen Willenserklärungen gelten i.d.R. als Erklärungen unter Abwesenden.
- Eine wirksame Annahmeerklärung kann auch automatisch erzeugt werden (z.B. automatisierte Bestätigungsmail).

1.4 Erklärung per Chatbot

Chatbots simulieren entweder private oder öffentliche Unterhaltungen mit einem oder mehreren Menschen. Der Chatbot ist vergleichbar mit einem Warenautomaten: Beide arbeiten nach vorgegebenen Mustern, geschaffen durch den Hersteller bzw. Entwickler. Der Warenautomatenaufsteller füllt diese Muster mit Inhalt (z.B. dem gewünschten Preis pro Produkt). Sodann interagiert der Automat mit Menschen: Er prüft deren Eingaben (z.B. Produktwahl, Einwerfen von Geld etc.) und führt dementsprechend etwas aus. Ähnliches macht der Chatbot, wenn er für Vertragsabschlüsse eingesetzt wird. Sowohl beim Warenautomaten als auch beim Computerprogramm beruhen die Ergebnisse auf dem Willen des Verwenders. Damit ist auch die vom Chatbot angezeigte Willenserklärung eine Willenserklärung des Betreibers. Bislang finden Chatbots aufgrund hoher Fehlerquoten in der Kommunikation nur im Rahmen von Pilotprojekten Anwendung.

- Ein Chatbot ist weder Vertreter noch Bote.
- Rechtsgeschäftliches Handeln eines Chatbots wie die Abgabe einer Willenserklärung (auch „Computererklärung“) wird einer natürlichen oder juristischen Person zugerechnet („Agentenmodell“).

Bei Fehlfunktionen des Chatbots: Wenn es sich für den Nutzer aufdrängen muss, dass eine Fehlfunktion des Chatbots vorliegt und der Betreiber diese Erklärung gar nicht abgeben wollte, ist die automatisch generierte Erklärung entsprechend dem offensichtlichen Betreiberwillen gemäß §§ 133, 157 BGB auszulegen. Allerdings nur dann, wenn der Kunde weiß, dass es sich um einen Chatbot handelt und es deswegen zu technischen Fehlern kommen kann.

>> Es liegt im Interesse des Betreibers selbst, den Kunden so früh wie möglich darauf hinzuweisen, dass er mit einem Chatbot interagiert.

1.5 Smart Contracts

Smart Contracts sind Programmcodes, die Verträge abbilden und sich selbst ausführen.

- Bezeichnung als „Verträge“ durch Vergleichbarkeit mit dem Wirkungsfeld einer Transaktions- bzw. Vertragslogik und der Befolgung einer „Wenn-Dann-Konstellation“
- Transaktionskosten sollen verkleinert werden und die Vertragssicherheit soll erhöht werden.
- Smart Contracts würden das Risiko von Dateikopien und -weiterverbreitungen unbedenklich machen.

- Smart Contracts müssen nicht zwingend Bestandteile einer Blockchain sein.
- Blockchains schaffen Transparenz, Nachvollziehbarkeit und Verlässlichkeit in ihrer Ausführung.
- Ein Smart Contract kann aber auch Bestandteil einer Smartphone-App sein.
- Die App kann das Vertragsverhältnis abbilden und ausführen.
- z.B. bei „In-App-Käufen“ oder beim Kauf von Berechtigungen, die mit der App gespeichert und abgerufen werden

Risiken bei Geschäftsabwicklungen in der Blockchain:

- Programmierfehler können zu ungewollten Folgen führen (z.B. ungewollte Ausgabe von Geld).
- Virtueller Diebstahl stellt ein konkretes Risiko dar.

Datenschutzrechtliche Problematik bei Smart Contracts:

- Der Programmcode und die Nutzdaten sind in der Blockchain sichtbar und nachvollziehbar
- Personenbezogene Informationen können rekonstruiert und auch außerhalb der Blockchain identifiziert werden.

Ein Smart Contract wird unausführbar, wenn die Formvorschriften die Mitwirkung eines Dritten (z.B. Notar gem. § 311b BGB) für die Wirksamkeit des Vertrages vorschreiben.

>> Ein Smart Contract kann Aufklärungs-, Beratungs- und Warnfunktion nicht ersetzen.

1.6 Blockchain

Eine Blockchain ist eine erweiterbare Datenbankstruktur, die Transaktionen verzeichnet und sich auszeichnet durch Dezentralität, Unveränderlichkeit, Öffentlichkeit und Transparenz. Es existiert keine zentralisierte Version der Informationen. Die Blockchain gewährleistet die Sicherheit großer Datenmengen durch öffentliche und private Verschlüsselungstechnologien:

öffentlicher Schlüssel		privater Schlüssel
lange, zufällig generierte Zahlenfolge bzw. eine Benutzeradresse in der Blockchain	>>	Passwort, das Zugang zu digitalen Vermögenswerten gewährt

Die Blockchain bietet ausreichend sichere Infrastruktur, um beim Versenden von sensiblen Daten auf einen Mittelsmann verzichten zu können („Peer-to-Peer“ statt „Client/Server“).

Sie ist die Grundlage vieler digitaler Währungen (z.B. Bitcoin, Ethereum). Viele Börsen verwenden Muster-Blockchain-Anwendungen für ihre Dienstleistungen, z.B. Deutsche Börse (Frankfurter Börse), die ASX (Australian Securities Exchange), die JPX (Japan Exchange Group). Ansonsten wird Blockchain bislang nur im Rahmen von Pilotprojekten genutzt.

Vorteile:

- ermöglicht dezentrale Strukturen für Abwicklungen von Transaktionen ohne Intermediär
- ermöglicht automatisches Aufspüren von Schwachstellen in Geschäftsprozessen
- kaum Möglichkeiten für Fälschung, Manipulation, Betrug und Hacking

Nachteile:

- Umstieg ist teuer
- verrechnen von Transaktionen noch nicht möglich
- aufgetretene Fehler können im Nachhinein nicht korrigiert werden
- keine gesetzliche Regelung zur Eigentumsübertragung
- schwer verwaltbare Berechtigungen
- Einschränkungen beim Speicherplatz
- teilweise wird die Blockchain als „rechtsfreier Raum“ diskutiert
- juristischer Stellenwert einer Blockchain Transaktion ist nicht geklärt
- keine existente Rechtsbeziehung der Teilnehmer untereinander
- kein zur Vertretung berechtigtes Organ, welches die Verantwortung trägt
- „Kunde“ vertraut in eine sich selbst regulierende „Community“
- Schäden können i.d.R. nicht geltend gemacht werden

Im Datenschutz ist unklar, ob Registerdaten in der Blockchain für bestimmte Personen personenbezogene Daten i.S.d. Datenschutzrechts darstellen: Blockchain-„Community“ würde somit Daten erheben, verarbeiten und langfristig speichern ohne Einwilligung der Nutzer und ohne „Verantwortlicher“ i.S.d. Datenschutzrechts zu sein

1.7 Vertretung und Vollmacht

1.7.1 Stellvertretung

- Ein Vertrag kann i.d.R. durch eine Stellvertretung (i.S.d. §§ 164 ff. BGB) geschlossen werden.
- Ausnahmen sind höchstpersönliche Rechtsgeschäfte, wie z.B. die Ehe oder das Testament.

1.7.2 Generalvollmacht (gem. § 167 BGB)

- Bevollmächtigter kann Entscheidungen im Rahmen von einzelnen Handlungen treffen
- gilt als häufigste und umfangreichste Vollmacht

Verschiedene Arten von rechtsgeschäftlichen Vollmachten:

- Generalvollmacht ermächtigt für alle, für das Handelsgewerbe gewöhnlichen Geschäfte
- Artvollmacht (i.S.d. § 54 Abs. 1 HGB) ermächtigt für eine bestimmte Art von Geschäften
- Spezialvollmacht bzw. Sondervollmacht ermächtigt für ein konkret festgelegtes Geschäft
- Prokura (gem. § 49 HGB), geschäftliche Vollmacht, muss im Handelsregister eingetragen sein, zur Vertretung des Unternehmens, erteilt durch Geschäftsführer oder Vorstand
- Vorsorgevollmacht kombiniert Vollmacht für geschäftliche und persönliche Angelegenheiten (z.B. Klinikaufenthalt, medizinische Behandlung)

1.7.3 Handlungsvollmacht (gem. § 56 HGB)

- Die Handlungsvollmacht erstreckt sich automatisch auf alle Handlungen die in dem Geschäft üblich und zu erwarten sind.

Es gibt verschiedene Arten der Handlungsvollmacht:

- Die allgemeine Handlungsvollmacht erstreckt sich auf branchenübliche Geschäfte.

- Die Artenhandlungsvollmacht berechtigt zur wiederholten Tätigung einer bestimmten Art von Rechtsgeschäften. Die Artenvollmacht ist Spezialhandlungsvollmacht: Diese wird meist für ein ganz bestimmtes Rechtsgeschäft ausgestellt und erlischt im Anschluss daran. Sie ist sehr eng gefasst und erlaubt dem Inhaber nur sehr eingeschränkt tätig zu werden.

Eigenschaften der Handlungsvollmacht:

- Sie muss gegenüber dem Geschäftspartner offenlegelegt werden.
- Der Geschäftspartner ist gehalten zu erfragen, ob eine Handlungsvollmacht vorliegt. Bei Unterlassen muss er für mögliche Schäden selbst haften.
- Möglichkeit, eine zusätzliche Vollmacht zu einer bereits bestehenden Vollmacht zu erteilen.
- Der Bevollmächtigte kann nur dann eine Untervollmacht erteilen, wenn er dazu berechtigt ist.

- Sie kann jederzeit widerrufen werden-
- Sie erlischt außerdem bei Beendigung des Arbeitsvertrages, Insolvenz des Handelsgewerbes, Stilllegung des Betriebs u.a.

1.7.4 Notarielle Vollmacht

Für bestimmte Rechtsgeschäfte muss die Vollmacht in notarieller beglaubigter Form erteilt werden z.B. bei Verfügungen über Immobilien, nicht aber über GmbH-Geschäftsanteile. Eine nachträgliche Bevollmächtigung ist möglich.

1.7.5 Vertretung ohne Vertretungsmacht

Handelt der Vertreter ohne Vertretungsmacht bleibt das Rechtsgeschäft schwebend unwirksam (gem. § 177 Abs. 1 BGB). Der Vertretene kann es nachträglich genehmigen (gem. §§ 182, 184 BGB). Wird keine Genehmigung erteilt, haftet der Vertreter ohne Vertretungsmacht gegenüber dem Dritten, allerdings nicht, wenn der Dritte vom Fehlen der Vollmacht Kenntnis hatte bzw. haben müsste.

Duldungsvollmacht bzw. Rechtsscheinvollmacht

- entsteht durch Rechtsschein
- entsteht wenn der Vertretene die Handlung einer Person, die als Vertreter auftritt, bewusst duldet
- Vertreter darf nach Treu und Glauben (vgl. § 242 BGB) annehmen tatsächlich bevollmächtigt zu sein
- Bei formbedürftiger Erteilung einer Vollmacht kann es keine Duldungsvollmacht geben. Das Rechtsgeschäft ist schwebend unwirksam, bis der Vollmachtgeber das Rechtsgeschäft für wirksam erklärt.

Anscheinsvollmacht

- Der Handelnde hat keine Vertretungsmacht. Es liegt keine Vollmacht vor.
- Der Vertretene weiß nicht, dass in seinem Namen gehandelt wird.
- Hätte der Vertretene bei pflichtgemäßer Sorgfalt erkennen können, dass er vertreten wird, ist er so zu behandeln, als habe er den Vertreter bevollmächtigt.
- Leichte Fahrlässigkeit (i.S.v. § 276 Abs. 2 BGB) genügt.
- Der gutgläubige Dritte hat u.U. Erfüllungsanspruch gegenüber dem Vertretenen.

>> Bestimmen Sie bei der Erteilung von Vollmachten interne Schranken und das Erlöschen der Vollmacht. Prüfen Sie vorgelegte Vollmachten auf ihr Bestehen und ihre Wirksamkeit.

2 Digitale Unterschrift

2.1 Begriffsbestimmung

- Digitale Signatur: kryptographisches Verfahren, das Schlüsselpaar verwendet, das aus einem privaten (geheimen) und einem öffentlichen (nicht geheimen) Schlüssel besteht.
- Elektronische Signatur: rein rechtlicher Begriff. Ist weiter gefasst (umfasst digitale Signatur)

>> Werden oft synonym verwendet, sind aber nicht dasselbe!

2.2 Arten elektronischer Signatur

Es lassen sich drei Arten der elektronischen Signatur unterscheiden:

- einfache elektronische Signatur (z.B. Nennung des Namens unterhalb einer E-Mail, eingescannte Unterschrift)
- fortgeschrittene elektronische Signatur (z.B. PGP-Schlüssel, technisch gesehen = Software-Zertifikat)
- qualifizierte elektronische Signatur

2.2.1 Einfache elektronische Signatur (Art. 3 Nr.10 eIDAS-VO)

Eine einfache elektronische Signatur enthält Daten

- in elektronischer Form,
- die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und
- die der Unterzeichner zum Unterzeichnen verwendet.

Elektronische Signaturen haben per se also keinen Sicherheitswert, da auch eine ohne weiteres kopierbare oder entfernbare eingescannte Unterschrift diese Voraussetzungen erfüllt.

Im Rechtsstreit kann die einfache elektronische Signatur als Beweismittel des Augenscheins in Prozess eingeführt werden. Beweiswürdigung: Richter ist gem. § 286 Abs. 1 ZPO frei und kann grundsätzlich Integrität und Authentizität des elektronischen Dokuments in Zweifel ziehen und daher zu der Überzeugung gelangen, dass das Dokument nicht geeignet ist, den dokumentierten Sachverhalt zu beweisen. Darf aber nicht *per se* als Beweismittel abgelehnt werden.

Typischer Anwendungsbereich: formfreie Vereinbarungen (§ 127 BGB)

>> niedriges Sicherheitslevel (nicht verfälschungssicher)/geringe Beweiskraft vor Gericht

2.2.2 *Fortgeschrittene elektronische Signatur (Art. 26 eIDAS-VO)*

Die Fortgeschrittene elektronische Signatur:

- basiert auf dem asymmetrischen Verschlüsselungsverfahren (kryptografischen Verfahren)
- wirkt durch den Einsatz von zwei verschiedenen Schlüsseln (dem geheimen privaten und dem für jedermann zugänglichen öffentlichen Schlüssel), s.o.
- stellt noch keine bestimmten Sicherheitsanforderungen an die Schlüsselverwaltung und an die Software- und Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels (Signaturerstellungsdaten)
- muss mit einmaligem Signaturschlüssel erstellt worden sein; Signaturersteller muss bei Bedarf identifizierbar sein (entweder über ihm zugewiesenen Prüfschlüssel oder ggf. mittels erfasster biometrischer Unterschrift)

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

- Sie ist eindeutig dem Unterzeichner zugeordnet.
- Sie ermöglicht die Identifizierung des Unterzeichners.
- Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.
- Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Im Rechtsstreit wird die fortgeschrittene wie die einfache elektronische Signatur als Objekt des Augenscheins behandelt (s.o.).

Anwendungsbereich: formfreie Vereinbarungen (§ 127 BGB)

>> hohes Sicherheitsniveau/geringe Beweiskraft

2.2.3 *Qualifizierte elektronische Signatur (Art. 3 Nr. 12, 15, 23 eIDAS-VO)*

Die qualifizierte elektronische Signatur:

- setzt eine fortgeschrittene elektronische Signatur (Art. 26 eIDAS-VO) voraus

- beruht auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat
- wird mit einer qualifizierten Signaturerstellungseinheit erzeugt (Art. 3 Nr. 12, 15, 23 eIDAS-VO)

Im Rechtsstreit hat die qualifizierte elektronische Signatur Beweiskraft wie private Urkunde, vgl. § 371a Abs. 1 S. 1 ZPO.

Anwendungsbereich vor allem, wenn Gesetz Schriftform vorschreibt und gleichzeitig die elektronische Form zulässt.

>> sehr hohes Sicherheitsniveau/volle Beweiskraft

Die Einrichtung einer qualifizierten elektronischen Signatur erfordert:

- Signaturkarte (enthält privaten + öffentlichen Schlüssel)
- qualifiziertes Zertifikat (enthält Informationen zum Zertifikatsinhaber, zum Zertifikatsaussteller und dient der Zuordnung eines öffentlichen Schlüssels zu einer Person; wird von der Zertifizierungsstelle erstellt)
- Chipkartenleser
- Software

Die Einrichtung ist mit Kosten verbunden, sie variieren nach Anbieter. Akkreditierte Anbieter nennt die BNetzA.

Besondere Bedeutung hat die Gültigkeit:

- Die Elektronische Signatur ist immer gültig.
- Aber Verschlüsselungsalgorithmen sowie die verwendeten Zertifikate werden nach bestimmter Zeit ungültig. Verschlüsselungsalgorithmen sind längstens 5 Jahre gültig. Zertifikate sind 2-3 Jahre gültig, verfallen spätestens nach 5 Jahren (Zertifikat wird nicht ungültig, darf aber nicht mehr benutzt werden). Zertifikate müssen danach von akkreditierter Stelle 30 Jahre aufbewahrt werden.
- Auch wenn ein Zertifikat bereits lange ungültig ist bzw. der damit verknüpfte Signaturschlüssel nicht mehr verwendet werden darf, sind Dokumente, die innerhalb des Gültigkeitszeitraums signiert wurden, nach wie vor rechtsgültig.
- Für den Fall elektronischer Rechnungen und anderer Unternehmensdokumente gilt gemäß den Grundsätzen ordnungsgemäßer Buchführung (GoB) die Verpflichtung, Rechnungen für 10 Jahre revisionssicher zu archivieren. Wenn diese Bedingung durch ein entsprechendes elektronisches Archiv sichergestellt ist, ist eine erneute Signierung der einzelnen Dokumente nicht notwendig, da das revisionssichere Archiv die Unveränderbarkeit der im Archiv gehaltenen Dokumente garantiert.

>> Mit dem Ablauf des Zertifikats muss derjenige, der sich auf eine Signatur stützt, voll beweisen, dass die Signatur vor diesem Zeitpunkt gesetzt wurde. Dies kann durch eine Nachsignierung oder durch einen Zeitstempel geschehen.

Sicherheitsvorkehrungen:

- Signaturkarte inkl. PIN (falls vorhanden) muss vom Anwender vor fremdem Zugriff geschützt werden;
- Signier-PC muss vor unautorisiertem Zugriff geschützt werden;
- Bei Verwendung Signaturkarte: Nutzung eines Kartenlesers mit integriertem PinPad empfohlen
- Verwendung einer Server-Signatur: Authentifizierungsdaten für die Autorisierung der Erstellung der Signatur müssen hinreichend geschützt werden.

3 Dokumentenmanagementsystem (DMS)

Um die geordnete Ablage von Dokumenten, Einhaltung von gesetzlichen Aufbewahrungspflichten und ganz allgemein der Organisation von Information und Wissen in Unternehmen mit Hilfe von Strategien, Prozessen und technischen Lösungen sicherzustellen, werden IT-Systeme angeboten, die etwa unter folgenden Schlagwörtern bekannt sind:

- Content Management System (CMS)
- Dokumenten Management System (DMS)
- Document Related Technologies (DRT)
- Enterprise Content Management (ECM)
- Information Live Cycle Management (ILM)
- Records Management (RM)

Die Leistungen variieren nach Anbieter.

Folgende Punkte sollten nach Möglichkeit bei der Auswahl eines externen Dienstleisters berücksichtigt werden:

- Können Dokumentenklassen definiert werden, die vom DMS jeweils unterschiedlich behandelt werden können?
- Kann die DMS-Lösung die gesetzlichen Anforderungen (u.a. GoB, GoBD) erfüllen?
- Sind die Möglichkeiten der Rechnungserfassung gegeben?
- Was versteht der Anbieter konkret unter Revisionssicherheit?
- Wie ist die Möglichkeit zur Digitalisierung von Papierunterlagen realisiert?
- Sind die gesetzlichen Anforderungen an ein ersetzendes Scannen erfüllbar?
- Ist das E-Mailarchiv ins gesamte System integriert?

4 Ersetzendes Scannen

Beim Ersetzenden Scannen werden die Papierunterlagen gescannt und die Originale danach vernichtet.

- unproblematisch, soweit keine gesetzlichen Dokumentations-, Aktenführungs- oder Aufbewahrungspflichten bestehen
- In allen anderen Fällen gilt als Grundsatz, dass aus gesetzlichen Gründen aufbewahrungspflichtige Unterlagen im Original archiviert werden müssen (d.h. Papierrechnungen grundsätzlich in Papierform und elektronische Rechnungen/Auftragsbestätigungen etc. in elektronischer Form).
- Bei buchführungs- bzw. steuerrelevanten Papierunterlagen zulässig: GoBD schließen ein ersetzendes Scannen nicht *per se* aus, stellen aber hohe Anforderungen (s.o.).
- Ergebnisse einer 2013 durchgeführten Simulationsstudie zur gerichtlichen Beweisführung ersetzend gescannter Dokumente

Es gibt zwei Möglichkeiten, den tatsächlichen Scan-Zeitpunkt sicherzustellen:

- Dokumentation durch qualifizierten Zeitstempel (Art. 41 eIDAS-VO) als verlässlichste, aber kostenintensive Methode
- Dokumentation durch von Drittem betriebenes Dokumentenmanagementsystem (DMS)
- das DMS muss sicherstellen, dass Systemzeit nicht durch Nutzer veränderbar ist
- Scan-Produkt muss direkt (ohne Zwischenspeicherung) im DMS gespeichert werden, sodass zu keiner Zeit ungeschützter Zugriff auf das Dokument möglich ist
- das Entfernen des Scan-Produkts aus DMS muss protokolliert werden, da Nachweis des lückenlosen Schutzes sonst nicht mehr geführt werden kann

>> Der Nachweis des tatsächlichen Scan-Zeitpunkts ist von erheblicher Bedeutung. Je früher ein Dokument gescannt wurde, umso besser konnte dem Vorwurf der Fälschung begegnet werden.

Nachbearbeitung

- optische Nachbearbeitung kann u.U. geboten sein, um Lesbarkeit zu verbessern
- Bildbearbeitung ist transparent zu gestalten und in Verfahrensanweisung niederzulegen

- nachbearbeitete Dokumente sollten mit Transfervermerk versehen werden, der Form der Nachbearbeitung und ausführende Person dokumentiert

Farb-Scan

- ist Farbe in Originaldokument von Bedeutung (z.B. bei Haben- und Soll-Ausweisungen auf Kontoauszügen), muss Scan-Produkt ebenfalls farbig sein
- externe Dienstleister benötigen klare Anweisung, ob und unter welchen Bedingungen farbige Dokumente farbig zu scannen sind oder nicht

Standardisierter Scan-Prozess und Verfahrensdokumentation

- Nachweis der Standardisierung des Scan-Prozesses kommt überragende Bedeutung zu
- Leitlinien: TR-RESISCAN (Technische Richtlinie Rechtssicheres Scannen)

Qualitätssicherung

- plausible Stichprobenquote, die in Verfahrensdokumentation festgelegt ist
- Quote ist abhängig vom Schutzbedarf der Dokumente (besondere Dokumente – z.B. solche, an denen mehrere Personen Beweisinteresse haben – haben etwa erhöhten Schutzbedarf)
- Mangel am Scan-Produkt kann nicht mit Erklärung geheilt werden, es hätten Stichproben in ausreichendem Maß stattgefunden

Scannen durch Dritte

- vertrauenswürdiger als privates Scannen, insb. wenn Dritter zertifizierter Anbieter

Integritätsschutz

- zwei Möglichkeiten, Nachweis der Echtheit zu führen
- systembezogener Integritätsschutz
- Scan-Produkt muss unmittelbar nach Erzeugung ohne Eingriffsmöglichkeiten Dritter in DMS geladen werden
- Nachträgliche Veränderungen müssen ausgeschlossen sein.
- Jede Veränderung muss als neue Version gespeichert werden bzw. veränderter Zugriff ist zu protokollieren.

Dokumentenschutz

- mittels (fortgeschrittener/qualifizierter) elektronischer Signatur; Schlussfolgerungen zu Vorgängen am Dokument vor Anbringen der Signatur sind aber nicht möglich

>> Ersetzendes Scannen führt stets zu einem Verlust des Beweiswertes. Entscheidend sind das Scannen zum frühestmöglichen Zeitpunkt sowie detaillierte Scananweisungen und eine lückenlose Verfahrensdokumentation.

5 Beweiskraft elektronischer Dokumente

5.1 Begriff des elektronischen Dokuments

Ein elektronisches Dokument besteht aus elektronischen Daten, die dauerhaft auf einem Schriftkörper verkörpert sind, der ohne technische Hilfsmittel nicht gelesen werden kann.

- Ein einfaches elektronisches Dokument ist weder mit einer qualifizierten Signatur versehen noch mit De-Mail übermittelt worden.

- Begriffsverständnis ist in ZPO und materiellem Recht einheitlich

5.2 Beweiswert elektronischer Dokumente mit qualifizierter elektronischer Signatur

Privates elektronisches Dokument mit qualifizierter elektronischer Signatur:

- Beweiskraft wie private Urkunde (vgl. § 371a Abs. 1 S. 1 ZPO)
- entsprechend § 416 ZPO ist der volle Beweis erbracht, dass die im Dokument enthaltene Erklärung von dem Signierenden abgegeben ist (gilt auch für De-Mail übermittelte Dokumente)

Gesetzliche Beweisregel i.S.d. § 286 Abs. 2 ZPO für den Anschein der Echtheit einer elektronischen Erklärung (vgl. § 371a Abs. 1 S. 2 ZPO). Beachte: § 371a ZPO gilt nur für originär elektronische Dokumente (für gescannte Dokumente § 371b ZPO, s.u.).

5.3 Beweiswert gescannter Dokumente

Vgl. grundsätzlich die Ergebnisse der Simulationsstudie zur Beweisführung mit ersetzend gescannten Dokumenten.

Öffentliche Urkunde

- ist das Dokument durch Einscannen einer öffentlichen Urkunde entstanden: Beweiswert einer öffentlichen Urkunde (sofern der Scanvorgang durch Behörde/Notar erfolgt und eine Bestätigung über die bildliche und inhaltliche Übereinstimmung mit der Urschrift vorliegt), vgl. § 371b ZPO

- besitzt das Dokument eine qualifizierte elektronische Signatur: Echtheitsvermutung gem. § 437 ZPO, wenn der Scanvorgang dem Stand der Technik entspricht (Leitlinien bietet etwa die Technische Richtlinie Rechtssicheres Scannen „TR-RESISCAN“)

- besitzt das Dokument keine qualifizierte elektronische Signatur: § 437 ZPO (Echtheitsvermutung) greift nicht, Beweisführung schwierig

Private Dokumente

- § 371b ZPO findet keine Anwendung
- Objekt des Augenscheins (vgl. § 371 Abs. 1 S. 2 ZPO), das freier richterlicher Beweiswürdigung unterliegt (§ 286 Abs. 1 ZPO)
- Einhaltung bestimmter technischer Standards (z.B. „TR-RESISCAN“) nicht zwingend erforderlich
- Schutz gegen Einwand der nachträglichen Veränderung bieten elektronischer Zeitstempel und elektronische Signatur

6 Aufbewahrungspflichten

Aufbewahrungspflichten können sich etwa aus dem Handelsrecht (§ 257 HGB i.V.m. § 238 HGB) und dem Steuerrecht (§ 147 AO) ergeben. Die Grundsätze ordnungsgemäßer Buchführung (GoB) sowie die Grundsätze ordnungsmäßiger Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) präzisieren diese gesetzlichen Angaben als Gewohnheitsrecht.

6.1 Handelsrecht: § 257 HGB (i.V.m. § 238 HGB)

6.1.1 Persönlicher Anwendungsbereich

- Kaufmann i.S.d. §§ 1, 2 HGB
- inländische Zweigniederlassungen ausländischer Unternehmen

6.1.2 Aufzubewahrende Unterlagen

- Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen
- empfangene Handelsbriefe
- Wiedergaben der abgesandten Handelsbriefe
- Belege für Buchungen in den nach § 238 Abs. 1 HGB zu führenden Büchern (Buchungsbelege)

6.1.3 Aufbewahrungsform

- Dritten muss es gem. § 238 HGB möglich sein, die gesuchten Unterlagen innerhalb angemessener Zeit aufzufinden.
- Eröffnungsbilanzen (Jahres- und Konzernjahresabschlüsse sowie die Einzelabschlüsse) müssen im Original (d.h. mit Unterschrift und ggf. mit Testat) aufbewahrt werden.

>> Ersetzendes Scannen der Jahresabschlüsse ist nicht möglich!

- Übrige Unterlagen können auf Bild- oder anderen Datenträgern aufbewahrt werden, soweit dies den GoB entspricht und Übereinstimmung mit dem Original, jederzeitige Verfügbarkeit und prompte Lesbarkeit sichergestellt sind.

Bildträger:

- Solche Aufbewahrungsmittel, die geeignet sind, die ursprüngliche Vorlage in ihrer inhaltlichen und äußerlichen Aufmachung wiederzugeben (z.B. Fotos, Fotokopien, Microverfilmungen etc.).

Sonstige Datenträger:

- Jedes Medium, das es ermöglicht, die Aufzeichnungen unmittelbar und jederzeit reproduzierbar festzuhalten (z.B. Festplatten, USB-Träger, CD-ROM, DVD, Magnetbänder, Kassetten, Lochkarten etc.).

Empfangene Handelsbriefe/Buchungsbelege:

- bildliche Übereinstimmung erforderlich
- Unterlagen sind in der Form (ausgedruckt oder elektronisch) aufzubewahren, in der sie entstanden oder eingegangen sind.
- Ausnahme: Soweit Handels- und Geschäftsbriefe zwar elektronisch erstellt, sodann allerdings nur in ausgedruckter Form versendet wurden. Hier ist es ausreichend, wenn die Unterlagen nur in ausgedruckter Form aufbewahrt werden. Im Zweifel sollten immer beide Versionen (elektronisch und ausgedruckt) archiviert werden.
- ersetzendes Scannen: Bildliche (soweit notwendig auch farbliche) Übereinstimmung der Dokumente muss sichergestellt werden. Zur Dokumentation dessen empfiehlt sich die Erstellung einer Organisationsanweisung. Erst nach dem Scannen und der Dokumentation der Übereinstimmung darf ein Papierdokument vernichtet werden. (Achtung: betrifft nicht die Dokumente, die zwingend im Original aufzubewahren sind)

6.1.4 Aufbewahrungsfrist

- empfangene Handelsbriefe/Wiedergabe abgesandter Handelsbriefe: 6 Jahre
- übrige in § 257 HGB genannte Unterlagen: 10 Jahre
- Fristbeginn: Schluss des Kalenderjahres, in dem der Sachverhalt verwirklicht wird, der zur Aufbewahrungspflicht führt
- nach Fristablauf: Vernichtung möglich
- analoge Anwendung der Regelungen über die Aufbewahrungsfristen auf Unterlagen außerhalb des kaufmännischen Bereichs kommt mangels vergleichbarer Interessenlage i.d.R. nicht in Betracht

6.1.5 Aufbewahrungsort

- Aufbewahrung im Inland nicht vorgeschrieben
- Unterlagen müssen aber in angemessener Zeit vorgelegt werden können (§ 239 Abs. 4 S. 2 HGB).

6.2 Steuerrecht: § 147 AO

6.2.1 Persönlicher Anwendungsbereich

- Vollkaufleute
- alle, die nach Steuergesetzen oder anderen Gesetzen zur Führung von Büchern und Aufzeichnungen verpflichtet sind

6.2.2 Aufzubewahrende Unterlagen

- Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstige Organisationsunterlagen
- empfangene Handels- oder Geschäftsbriefe
- Wiedergaben der abgesandten Handels- oder Geschäftsbriefe
- Buchungsbelege
- Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union
- sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind

Die Pflicht zur Aufbewahrung von Unterlagen nach § 147 AO ist akzessorisch, d.h. sie setzt stets eine Aufzeichnungspflicht voraus und besteht grds. nur im Umfang der Aufzeichnungspflicht. Eine eigenständige Pflicht zur Aufbewahrung von Unterlagen, die nicht mit einer Pflicht zur Aufzeichnung in Zusammenhang stehen, ist § 147 nicht zu entnehmen.

6.2.3 Aufbewahrungsform, § 147 Abs. 2 AO

Aufbewahrung in Papierform

- Jahresabschlüsse, Eröffnungsbilanz und Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union müssen im Original aufbewahrt werden.

Aufbewahrung mittels Digitalisierung

- Alle übrigen Unterlagen können auch als Wiedergabe auf einem Bildträger oder auf einem Datenträger aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten (1) mit den empfangenen Handels- oder

Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden und (2) während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können.

- Datenspeicherung etwa möglich auf Computer-Festplatten, CD, Disketten, Blu-ray-Disk, Flash-Speicher, DVD (AEAO zu § 147 Nr. 3) oder auf externen Servern (Cloud Computing)

>> Es besteht keine Verpflichtung, Dokumente zu digitalisieren und digital aufzubewahren.

Originär digitale Unterlagen

- Dies sind Daten, die in das Datenverarbeitungssystem in elektronischer Form eingehen und die im Datenverarbeitungssystem erzeugt werden.
- Sie sind in dem elektronischen Format abzuspeichern, in dem sie empfangen bzw. erstellt worden sind (vgl. GoBD v. 14.11.2014, Abschn. 9.2, Tz 119, 131 und 133).
- Sie müssen zwingend auf einem maschinell lesbaren und auswertbaren Datenträger (§ 147 Abs. 2 Nr. 2 AO) archiviert werden. Aufbewahrungen in ausgedruckter Form/auf Mikrofilmen nicht ausreichend (vgl. dazu BMF v. 16.7.2001, BStBl. I 2001, 415).
- Die Pflicht zur Archivierung originär digitaler Unterlagen besteht nur dann nicht, wenn diese Unterlagen zwar DV-gestützt erstellt wurden, sie aber nicht zur Weiterverarbeitung in einem DV-gestützten Buchführungssystem geeignet sind, wie z.B. Textdateien oder E-Mails (BMF v. 16.7.2001, BStBl. I 2001, 415). E-Mails dürfen also zur weiteren Bearbeitung ausgedruckt und anschließend gelöscht werden.
- Alle E-Mails mit steuerlich relevantem Inhalt sind allerdings zu archivieren (vgl. BMF Fragen-und-Antwort-Katalog zum Datenzugriffsrecht der FVerw).
- Nicht aufbewahrt werden muss eine E-Mail, wenn sie nur als Transportmittel für eine im Anhang befindliche Rechnung oder einen Handelsbrief diente (aufbewahrungspflichtig ist dann nur der Anhang).
- originär in Papierform angefallene Unterlagen: Möglichkeit der Mikroverfilmung

Ersetzendes Scannen:

Zu den Voraussetzungen vgl. GoBD v. 14.11.2014 Abschn. 9.3, Tz 136 ff.

- ausführliche Organisationsanweisung, in der geregelt wird, wer, wie und wann scannen darf
- welches Schriftgut gescannt wird

- ob eine bildliche oder inhaltliche Übereinstimmung mit dem Original erforderlich ist
- wie die Qualitätskontrolle auf Lesbarkeit und Vollständigkeit zu erfolgen hat
- vollständige Farbwiedergabe erforderlich, wenn die Farbe Beweisfunktion hat
- nach dem Einscannen darf nur noch das elektronische Dokument bearbeitet werden, nicht aber das Papierdokument
- Nachvollziehbarkeit und Nachprüfbarkeit müssen gewährleistet sein

>> Wenn die Voraussetzungen für Ersetzendes Scannen erfüllt sind, darf das Papierdokument vernichtet werden.

6.2.4 Aufbewahrungsfrist

- Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, Buchungsbelege, Unterlagen nach Art. 15 Absatz 1 und Art. 163 des Zollkodex der Union: 10 Jahre (vgl. § 147 Abs. 3 AO)
- übrige in § 147 Abs. 1 AO genannte Unterlagen: 6 Jahre (vgl. § 147 Abs. 3 AO)
- Fristbeginn: Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Buch, das Inventar, die Eröffnungsbilanz, der Jahresabschluss oder der Lagebericht aufgestellt, der Handels- oder Geschäftsbrief empfangen oder abgesendet worden oder der Buchungsbeleg entstanden ist, ferner die Aufzeichnung vorgenommen worden ist oder die sonstigen Unterlagen entstanden sind

6.2.5 Lesbarmachung der Unterlagen

- vgl. § 147 Abs. 5 AO

6.2.6 Aufbewahrungsort

Der Aufbewahrungsort ist grundsätzlich in Deutschland, vgl. § 146 Abs. 2 AO. Die Zuständige Finanzbehörde kann auf schriftlichen Antrag des Steuerpflichtigen die Führung und Aufbewahrung elektronischer Bücher/sonstiger elektronischer Aufzeichnungen außerhalb Deutschlands bewilligen, wenn

- der Steuerpflichtige der zuständigen Finanzbehörde den Standort des Datenverarbeitungssystems mitteilt,
- der Steuerpflichtige seinen sich aus den §§ 90, 93, 97, 140 bis 147 und 200 Abs. 1 und 2 AO ergebenden Pflichten ordnungsgemäß nachgekommen ist,
- der Datenzugriff der Finanzverwaltung in vollem Umfang möglich ist und

- die Besteuerung hierdurch nicht beeinträchtigt wird.

Rechnungen:

- Aufbewahrung in Deutschland; bei elektronischer Aufbewahrung, die eine vollständige Fernabfrage der betreffenden Daten gewährleistet, darf der Unternehmer die Rechnungen auch im übrigen Gemeinschaftsgebiet aufbewahren
- Es ist jedoch dem Finanzamt mitzuteilen, wenn die Rechnungen nicht im Inland aufbewahrt werden (§§ 14, 14b UStG).

6.3 Grundsätze ordnungsgemäßer Buchführung (GoB)

6.3.1 Persönlicher Anwendungsbereich

- alle, die Pflicht zur Buchführung und Bilanzierung besitzen
- unbestimmter Rechtsbegriff der ordnungsgemäßen Buchführung wird bspw. in § 238 Abs. 1 S. 1 HGB genannt

6.3.2 Allgemeine Grundsätze

- Grundsatz der materiellen Richtigkeit und Willkürfreiheit:
  Die Geschäftsvorfälle müssen tatsächlich stattgefunden haben und objektiv aus den Büchern hergeleitet werden können.

- Grundsatz der Klarheit und Übersichtlichkeit
  Die Buchführung muss klar und übersichtlich durchgeführt werden, sodass auch sachverständige Dritte diese nachvollziehen können.

- Grundsatz der Einzelbewertung
  Alle Vermögensgegenstände müssen grds. einzeln bewertet werden.

- Grundsatz der Vollständigkeit
  Die Buchführung muss vollständig, d.h. lückenlos sein.

- Grundsatz der Ordnungsmäßigkeit:
  Alle Geschäftsvorfälle müssen zeitnah und chronologisch verbucht werden.

- Grundsatz der Sicherheit
  Alle Unterlagen müssen ordnungsgemäß archiviert werden.

- Grundsatz der Unveränderbarkeit
  Die Unterlagen dürfen nicht nachträglich veränderbar sein.

- Belegprinzip
  Keine Buchung ohne Beleg.

6.4 Grundsätze ordnungsmäßiger Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

>> Das BMF hat im Juli 2019 einen Entwurf zur Neufassung der GoBD herausgegeben, aber wieder zurückgezogen, da weiterer Abstimmungsbedarf bestehe. Die vorgenommenen Änderungen sind nur punktuell, noch nicht endgültig und in diesen Leitfaden noch nicht eingearbeitet.

6.4.1 Anwendungsbereich

- für Veranlagungszeiträume, die nach dem 31. Dezember 2014 beginnen
- betreffen grundsätzlich alle Steuerpflichtigen mit Gewinneinkünften i.S.d. § 5 EStG, § 4 Abs. 1 EStG sowie Einnahmen-Überschuss-Rechner, soweit diese ihre unternehmerischen Prozesse IT-gestützt abbilden und ihren Buchführungs- und Aufbewahrungspflichten in elektronischer Form nachkommen
- GoBD: Verwaltungsanweisung, die gegenüber den nachgeordneten Dienststellen Verbindlichkeitscharakter hat.

6.4.2 Aufzubewahrende Unterlagen

- Außersteuerliche und steuerliche Bücher, Aufzeichnungen und Unterlagen zu Geschäftsvorfällen
- Alle Unterlagen, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind.
- Neben Unterlagen in Papierform auch alle Unterlagen in Form von Daten, Datensätzen und elektronischen Dokumenten, die dokumentieren, dass die Ordnungsvorschriften umgesetzt und deren Einhaltung überwacht wurde.

6.4.3 Aufbewahrungsgrundsätze

(1) Anforderungen an Datensicherheit/<u>Unveränderbarkeit</u>

- Die steuerrelevanten DV-Systeme sind gegen Verlust zu sichern und gegen unberechtigte Eingaben und Veränderungen zu schützen.
- Werden Daten, Datensätze und elektronischen Dokumente nicht ausreichend geschützt und können daher nicht mehr vorgelegt werden, ist die Buchführung nicht mehr ordnungsgemäß.
- Buchungen oder Aufzeichnungen dürfen nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist.

- Die Unveränderbarkeit kann durch entsprechende Hardware, Software oder organisatorische Vorkehrungen gewährleistet werden.
- Spätere Änderungen sind so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, erkennbar bleiben.
- Bei der Änderung von Stammdaten (z. B. Abkürzungen oder Schlüssel) muss die eindeutige Bedeutung in den entsprechenden Bewegungsdaten erhalten bleiben.

(2) Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit

- Belegprinzip (jede Buchung muss durch Beleg nachgewiesen werden)
- Grundsatz der Wahrheit, Klarheit und fortlaufender Aufzeichnung

(3) Grundsatz der Vollständigkeit, Richtigkeit, Zeitgerechtheit, Ordnung und Unveränderbarkeit

- vollzählig und lückenlos
- Aufzeichnung jeden Geschäftsvorfalls (in Geld bestehende Gegenleistung, Inhalt des Geschäfts, Name des Vertragspartners)

(4) Anforderungen an die Aufbewahrung von Geschäftsvorfällen

- Alle Unterlagen, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind, sind aufzubewahren.
- Im DV-System erzeugte Dokumente sind im Ursprungsformat aufzubewahren.
- Eingehende elektronische Handels- oder Geschäftsbriefe und Buchungsbelege müssen in dem Format aufbewahrt werden, in dem sie empfangen wurden.
- Der Erhalt der Verknüpfung zwischen Geschäftsvorfall und Dokument muss während der gesamten Aufbewahrungsfrist gewährleistet sein.
- Ein elektronisches Dokument ist mit einem nachvollziehbaren und eindeutigen Index zu versehen.
- Unabhängig vom Ordnungssystem muss sichergestellt sein, dass ein sachverständiger Dritter innerhalb angemessener Zeit prüfen kann.
- Die Belege in Papierform oder in elektronischer Form sind zeitnah, d.h. möglichst unmittelbar nach Eingang oder Entstehung, gegen Verlust zu sichern.
- Besonderheiten sind bei der Konvertierung (in ein Inhouse-Format) sowie beim Einsatz von Kryptografietechniken zu beachten.

(5) Anforderungen an Systemwechsel, -änderung, Auslagerung

- Aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem müssen quantitativ und qualitativ gleichwertig in ein neues System überführt werden.
- Soweit Daten etwa in ein Archivsystem ausgelagert werden oder ein Systemwechsel (Migration) stattfindet, sind auch weiterhin quantitativ und qualitativ die gleichen Auswertungen in der Art zu ermöglichen, als wären die

aufzeichnungs- und aufbewahrungspflichtigen Daten noch im Produktivsystem enthalten.

(6) Anforderungen an die elektronische Erfassung von Papierdokumenten

- Das Scanergebnis ist so aufzubewahren, dass die Wiedergabe mit dem Original bildlich übereinstimmt, wenn es lesbar gemacht wird.
- Das Verfahren muss dokumentiert werden und der Steuerpflichtige sollte eine Organisationsanweisung erstellen.
- Im Anschluss an den Scanvorgang darf die weitere Bearbeitung nur mit dem elektronischen Dokument erfolgen bzw. muss nach Abschluss der Bearbeitung der bearbeitete Papierbeleg erneut eingescannt und ein Bezug zum ersten Scanobjekt hergestellt werden.
- Für Besteuerungszwecke ist eine elektronische Signatur oder ein Zeitstempel nicht erforderlich.
- Soweit Unterlagen mittels Scanprozess einer Digitalisierung zugeführt wurden, muss der Steuerpflichtige diese über sein DV-System lesbar machen
- Im Anschluss an den Scanvorgang dürfen Papierdokumente unter bestimmten Voraussetzungen vernichtet werden.

(7) Internes Kontrollsystem (IKS)

Für die Einhaltung der Ordnungsvorschriften des § 146 AO hat der Steuerpflichtige Kontrollen einzurichten, auszuüben und zu protokollieren. Hierzu gehören beispielsweise:

- Zugangs- und Zugriffsberechtigungskontrollen auf Basis entsprechender Zugangs- und Zugriffsberechtigungskonzepte
- Funktionstrennungen
- Erfassungskontrollen (Fehlerhinweise, Plausibilitätsprüfungen)
- Abstimmungskontrollen bei der Dateneingabe
- Verarbeitungskontrollen
- Schutzmaßnahmen gegen die beabsichtigte und unbeabsichtigte Verfälschung von Programmen, Daten und Dokumenten

>> Die konkrete Ausgestaltung des Kontrollsystems ist abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur sowie des eingesetzten DV-Systems.

6.5 Übersicht und Katalog (VOI)

6.5.1 Tabellarischer Überblick

Persönlicher Anwendungsbereich		
§ 257 HGB	§ 147 AO	GOB/GOBD
- Kaufmann i.S.d. §§ 1, 2 HGB - inländische Zweigniederlassungen ausländischer Unternehmen	- Vollkaufleute - alle, die nach Steuergesetzen oder anderen Gesetzen zur Führung von Büchern und Aufzeichnungen verpflichtet sind	- alle, die zur Buchführung und Bilanzierung verpflichtet sind

Aufzubewahrende Unterlagen		
§ 257 HGB	§ 147 AO	GOB/GOBD
- Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte [Auswahl] - empfangene Handelsbriefe - Wiedergaben der abgesandten Handelsbriefe - Belege für Buchungen in den nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege)	zusätzlich zu § 257 HGB: Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union - sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind → akzessorische Aufbewahrungspflicht	

Aufbewahrungsfrist		
§ 257 HGB	§ 147 AO	GOB/GOBD
- empfangene Handelsbriefe/Wiedergabe abgesandter Handelsbriefe: 6 Jahre - übrige in § 257 HGB genannte Unterlagen: 10 Jahre - Fristbeginn: Schluss des Kalenderjahres, in dem der Sachverhalt verwirklicht wird, der zur Aufbewahrungspflicht führt	- Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz, Buchungsbelege, Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union: 10 Jahre - übrige in § 147 Abs. 1 AO genannte Unterlagen: 6 Jahre - Fristbeginn: Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Buch, das Inventar, die Eröffnungsbilanz, der Jahresabschluss oder der Lagebericht aufgestellt, der Handels- oder Geschäftsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist	- ergeben sich aus übrigen gesetzlichen Pflichten

Aufbewahrungsort		
§ 257 HGB	§ 147 AO	GOB/GOBD
- Aufbewahrung im Inland nicht vorgeschrieben - Unterlagen müssen aber in angemessener Zeit vorgelegt und lesbar gemacht werden können (§ 239 Abs. 4 S. 2 HGB).	- grds. im Inland, vgl. § 146 Abs. 2 AO - außerhalb Deutschlands nach Bewilligung möglich - Rechnungen: grds. im Inland (bei elektronischer Aufbewahrung, die eine vollständige Fernabfrage der betreffenden Daten gewährleistet, auch im übrigen Gemeinschaftsgebiet möglich)	- keine Angaben

Aufbewahrungsform		
§ 257 HGB	§ 147 AO	GOB/GOBD
- Eröffnungsbilanzen (Jahres- und Konzernjahresabschlüsse sowie die Einzelabschlüsse): im Original - übrige Unterlagen: Aufbewahrung auf Bild- oder anderen Datenträgern möglich - Unterlagen sind in der Form (ausgedruckt oder elektronisch) aufzubewahren, in der sie entstanden oder eingegangen sind	- Jahresabschlüsse, Eröffnungsbilanz und Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union: im Original - übrige Unterlagen: Aufbewahrung auf Bildträger oder Datenträger möglich - originär digitale Unterlagen: Aufbewahrung in elektronischem Format, in dem sie empfangen/erstellt worden sind auf maschinell lesbaren und auswertbaren Datenträger - in Papierform angefallene Unterlagen: Möglichkeit der Mikroverfilmung	Grundsätze: - materielle Richtigkeit und Willkürfreiheit - Klarheit und Übersichtlichkeit - Einzelbewertung - Vollständigkeit - Ordnungsmäßigkeit - Sicherheit - Unveränderbarkeit - Belegprinzip

6.5.2 Grundsätze des Verbandes Organisations- und Informationssysteme (VOI)

(1) Jedes Dokument ist gemäß den rechtlichen Anforderungen aufzubewahren (s.o.!).

(2) Kein Dokument darf auf dem Weg ins Archiv oder im Archiv verloren gehen.

(3) Jedes Dokument ist zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren.

>> Organisatorische Vorkehrungen sind zu treffen; technische Maßnahmen müssen gewährleisten, dass die Archivdaten zeitnah auf das endgültige Archivierungsmedium übertragen werden.

(4) Jedes Dokument muss mit seinem Original übereinstimmen und unveränderbar archiviert werden. Hardware (z.B. durch unveränderbare und fälschungssichere Datenträger) und Software (z.B. durch Sicherungen, Sperren, Festschreibung, Löschmerker, automatische Protokollierung, Historisierungen) müssen durch Sicherheitsmaßnahmen geschützt sein.

>> Eine bloße Ablage im Dateisystem erfüllt die Anforderungen zur Unveränderbarkeit ohne zusätzliche Maßnahmen nicht.

(5) Jedes Dokument darf nur von entsprechend berechtigten Benutzern eingesehen werden.

(6) Jedes Dokument muss sich in angemessener Zeit finden und reproduzieren lassen.

(7) Jedes Dokument darf frühestens nach Ablauf seiner Aufbewahrungsfrist gelöscht werden (s.o.!).

(8) Jede Veränderung im elektronischen Archivsystem muss protokolliert werden.

(9) Sachverständige können das gesamte Verfahren der Archivierung jederzeit prüfen.

(10) Keine Migrationen und Änderungen am Archivsystem ohne die aufgeführten Grundsätze.

7 E-Mail-Management

7.1 Grundsätzliches und Problemlage

E-Mails besitzen nicht die Beweiskraft einer Urkunde (vgl. § 415 ZPO). Das Gericht kann aber den Ausdruck einer E-Mail im Rahmen der freien Beweiswürdigung in seine Entscheidung einfließen lassen!

Viele Mitarbeiter nutzen den Eingangs-Postkorb im Mailsystem als ihre Standardablage. Mitarbeiter entscheiden, wann was gelöscht wird. Eine zentrale Kontrolle der Aufbewahrungsfristen erfolgt auf diese Weise nicht. E-Mails befinden sich unternehmensweit zufällig verteilt in Mail-Servern, Backup-Tapes oder bei einem externen Dienstleister.

>> E-Mails müssen zentral und rechtsicher archiviert werden, um zur Dokumentation und als Nachweis geeignet zu sein. Das Speichern in Mitarbeiter Accounts reicht nicht.

7.2 Aufbau eines Archivierungskonzepts

Für den Aufbau eines Mail Archivs ist grundsätzlich zu klären:

- Was soll archiviert werden?
- Wo bzw. bei wem soll die Archivierung ansetzen?
- Was soll/muss wie lange gespeichert werden?
- Was muss und was darf wann gelöscht werden?
- Was soll/muss zentral archiviert werden? Alle eingehenden/ausgehenden E-Mails? Oder soll selektive Archivierung stattfinden? (empfehlenswert, soweit das Unternehmen z.B. private E-Mails erlaubt)

Das Konzept erfordert transparente, widerspruchsfreie Arbeitsanweisungen.

- Denkbar wäre beispielsweise, dass private E-Mails an den bzw. vom dienstlichen Account spätestens einen Tag nach Abruf/Versendung zu löschen sind.
- Innerhalb von drei Tagen nach Abruf/Versendung werden dann die sonstigen eingegangenen und gesendeten Mails aus dem dienstlichen Account automatisch ins zentrale Archiv „wegarchiviert“.

Eine solche Löschanweisung hinsichtlich privater E-Mails empfiehlt sich aus datenschutzrechtlichen Gründen und wegen der teilweise umstrittenen Reichweite des Fernmeldegeheimnisses bei E-Mails, die (noch) nicht an einem vom Betroffenen selbst gewählten Platz gespeichert sind, sondern etwa in einem zentralen Archiv.

>> Private E-Mails sind im Unternehmen tendenziell als „Gefahrgut“ zu werten und möglichst schnell aus den betrieblichen Systemen zu entfernen. Insbesondere bei Ausscheiden des betroffenen Mitarbeiters.

8 Organisations- und Dokumentationspflicht nach der DSGVO

Die datenverarbeitende Stelle muss jederzeit Nachweis der Einhaltung technisch-organisatorischer Anforderungen und der Datenschutzgrundsätze der DSGVO erbringen können, vgl. Art. 5 Abs. 2 i.V.m. Art. 24 Abs. 1 S. 1 DSGVO (Prinzip der „Accountability“).

Unternehmen treffen Dokumentationspflichten und Beweislastumkehr (datenverarbeitende Stelle muss zukünftig datenschutzkonformes Verhalten beweisen).

>> Die Verletzung der Pflichten zum Datenschutz ist mit Bußgeld belegt (Art. 83 Abs. 5 DSGVO).

Es ist eine sorgfältige Dokumentation für Nachweiserbringung und planmäßige Organisation erforderlich, deren Ziel muss sein:

- alle datenschutzrelevanten Vorgänge im Unternehmen und die daraus resultierenden Datenschutzrisiken zu minimieren
- risikoangemessene Sicherheitsmaßnahmen und Handlungsanleitungen zu implementieren
- Einhaltung und Umsetzung dieser Maßnahmen und Anleitungen effektiv zu kontrollieren
- Defizite in der Datenschutzorganisation frühzeitig zu erkennen und zu beseitigen

Der Verantwortliche muss zusätzlich alle Verarbeitungstätigkeiten, die in seiner Zuständigkeit liegen, dokumentieren, vgl. Art. 30 Abs. 1 S. 1 DSGVO (= Verzeichnis von Verarbeitungstätigkeiten).

Umfang, unter anderem:

- Personaldatenverwaltung (einschließlich z.B. Zeiterfassung, Lohnbuchhaltung, Personalinformations- und Entwicklungssysteme etc.)
- Kundendatenbank/Customer Relations-Systeme
- E-Mail- und Internetanschlüsse

Inhalt des Verzeichnisses:

- Name und Kontaktdaten des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- jeweiliger Zweck der Verarbeitung

- Kategorie von betroffenen Personen (z.B. Beschäftigte, Kunden und deren Mitarbeiter)
- Kategorie personenbezogener Daten (z.B. Name, Anschrift, E-Mail-Adresse, Personalstammdaten, Standortdaten, Gesundheitsdaten etc.)
- Kategorie von Empfängern, ggü. denen personenbezogene Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfängern in Drittländern
- Übermittlungen von personenbezogenen Daten in Drittländer und ggf. individuelle Garantien, auf die der Verantwortliche die Entscheidung zugunsten der Datenübermittlung stützt (vgl. Art. 49 Abs. 6 DSGVO)
- wenn möglich die Fristen für die Löschung personenbezogener Daten
- wenn möglich eine allgemeine Beschreibung der technisch-organisatorischen Maßnahmen, die der Verantwortliche in Erfüllung seiner Pflichten aus Art. 32 DSGVO implementiert

Eine Ausnahme von der Pflicht zur Führung des Verzeichnisses besteht für Verantwortliche mit weniger als 250 Beschäftigten (Art. 30 Abs. 5 DSGVO). Diese müssen dennoch ein Verzeichnis führen, wenn

- die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt,
- die Verarbeitung nicht nur gelegentlich erfolgt oder
- eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 erfolgt.

>> Im Ergebnis müssen auch KMU mit weniger als 250 Beschäftigten der Pflicht zur Verzeichnisführung für alle regelmäßig von ihnen vorgenommen Verarbeitungstätigkeiten nachkommen.

9 Online Bewerbungen

9.1 Erhebung von Bewerberdaten

Der Datenschutz für Mitarbeiter unterliegt besonderen Bestimmungen, die in Deutschland durch das Bundesdatenschutzgesetz in seiner neuen Fassung geregelt sind.

Das Erheben […] personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (§ 26 BDSG).

Das BDSG stellt Bewerber den Beschäftigten gleich (§ 26 Abs. 8 BDSG).

>> Stammdaten darf der Arbeitgeber stets erheben (Name, Anschrift, Telefonnummer, E-Mailadresse).

Welche Daten darüber hinaus erhoben werden dürfen, richtet sich nach den objektiven beruflichen Kriterien und dem vom Arbeitgeber festgelegten Anforderungsprofil

9.1.1 Elektronische Ablage/Vervielfältigungen

Werden Bewerbungen auf gemeinsamen Netzlaufwerk abgelegt (z.B. durch Einscannen oder Speichern von E-Mailanhängen) ist auf die Zugriffsberechtigung zu achten.

Ausgedruckte Unterlagen sollten nach Abschluss möglichst wieder an die organisatorisch verantwortliche Stelle zurückgegeben werden und dort datenschutzgerecht entsorgt werden (z.B. durch Schreddern).

Werden Unterlagen per E-Mail weitergeleitet, sollte der PC durch entsprechende Zugriffssperren vor Unbefugten geschützt sein.

>> Der Zugriff auf Mitarbeiterdaten sollte auf Personen beschränkt werden, die an der Auswahlentscheidung/den administrativen Tätigkeiten für das Verfahren beteiligt sind.

9.1.2 Aufbewahrungsdauer

Die Haltung von Mitarbeiterdaten ist zeitkritisch. Zulässig ist lediglich die Speicherung im Rahmen der Zweckbestimmung des Beschäftigungsverhältnisses (26 BDSG).

- bei Nichteinstellung: Daten sind zu löschen, auch im Back-up! (Art. 17 Abs. 1 lit. a DSGVO)
- Die Mindestaufbewahrungsfrist beträgt 2 Monate (wegen Möglichkeit einer AGG-Klage, vgl. § 15 Abs. 4 S. 1 AGG).
- Empfehlung des Landesdatenschutzbeauftragten Niedersachsen: Daten sind spätestens nach 6 Monaten zu löschen
- Ausnahme: Betroffener hat in die weitere Speicherung schriftlich eingewilligt

9.2 Auskunftsanspruch

Jeder Betroffene hat einen Auskunftsanspruch gegenüber dem Verarbeiter von Personendaten (Art. 15 DSGVO). Dieser muss folgende Informationen erteilen:

- Verarbeitungszwecke
- Kategorien personenbezogener Daten, die verarbeitet werden
- Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
- falls möglich die geplante Dauer der Speicherung
- verfügbare Informationen über die Herkunft der Daten
- Bestehen des Rechts auf Berichtigung/Löschung der sie betreffenden personenbezogenen Daten
- Bestehen eines Beschwerderechts bei der Aufsichtsbehörde

Sind über den Betroffenen keine Daten gespeichert, ist ihm auch dies mitzuteilen (sog. Negativauskunft). Stellt Person den Antrag elektronisch, ist Auskunft in gängigem elektronischem Format zu erteilen (Art. 15 Abs. 3 DSGVO). Kosten für erste Kopie dürfen nicht erhoben werden (Art. 15 Abs. 3 DSGVO).

10 Digitale Personalakte

10.1 Begriff der Personalakte/Gestaltungsfreiheit des Arbeitgebers

- gesetzlich nicht definiert
- = Sammlung aller Aufzeichnungen, Urkunden und Vorgängen, die sich auf die persönlichen und dienstlichen Verhältnisse des einzelnen Arbeitnehmers beziehen und in einem unmittelbaren, inneren Zusammenhang mit dem Arbeitsverhältnis stehen.
- Privatwirtschaft: keine gesetzliche/vertragliche Verpflichtung des Arbeitgebers, Personalakte zu führen
- bei Führung einer Personalakte: Organisationsermessen; betrifft u.a. die Frage, in welcher technischen (konventionell/digital) Form er die Akte führt
- Nach der DSGVO sind Dokumentationspflichten des Art. 30 Abs. 5 DSGVO zu beachten (s.u.).

10.2 Beteiligungsrechte der Arbeitnehmervertretung

- Grds.: Mitbestimmungsrecht des Betriebsrates gem. § 87 Abs. 1 Nr. 6 BetrVG bei Einführung/Anwendung technischer Einrichtungen (digitale Personalakte = technische Einrichtung in diesem Sinne)
- Mittel der Personalplanung: Beteiligungsrecht des Betriebsrats nach § 92 Abs. 1 BetrVG

10.3 Zulässige Inhalte der digitalen Personalakte

- Grds.: digitale Personalakte muss unmittelbar inneren Zusammenhang zum Arbeitsverhältnis aufweisen, allgemeines Persönlichkeitsrecht darf nicht verletzt werden, Bundesdatenschutzgesetz und DSGVO sind einzuhalten
- Einwilligung des Arbeitnehmers (AN)/Dienst-, Betriebsvereinbarung, ansonsten: § 26 BDSG

10.4 Grundsätze der Personalaktenführung

10.4.1 Richtigkeit

- Angaben der Personalakte müssen zutreffendes Bild über Beschäftigten geben
- Grundsatz der Richtigkeit bezieht sich auf Tatsachenbehauptungen, Werturteile, dienstliche Beurteilungen
- Berichtigungs-/Löschungs- und Sperrungsrecht des Arbeitnehmers: § 35 BDSG/Art. 16, 17 DSGVO (bei konventionell geführter Akte: §§ 242, 1004 BGB)
- Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der

Löschung als gering anzusehen, kann die Einschränkung der Verarbeitung verlangt werden (§ 35 Abs. 1 BDSG i.V.m. Art. 18 DSGVO).

10.4.2 Vollständigkeit

- AN hat keinen Anspruch, dass AG alle ihn und sein Arbeitsverhältnis betreffenden Unterlagen aufbewahrt (willkürliche Aufnahme/Entfernung einzelner relevanter Daten unzulässig)
- Gleichbehandlungsgrundsatz: Einige Beschäftigte dürfen nicht ohne Sachgrund im Vergleich zu Kollegen bei der Personalaktenführung bevorzugt/benachteiligt werden (für jeden AN sind die gleichen Daten zu erfassen).
- Alle Personalvorgänge sind digital zu erfassen und müssen jederzeit aufgerufen werden können.
- u.U. ist Aufbewahrung der Originale geboten: z.B. sozialversicherungspflichtige Nachweise (§ 28f Abs. 1 S. 1 SGB IV)

10.4.3 Transparenz

- § 26 Abs. 5 BDSG/Art. 13 DSGVO: Unterrichtung des AN über digitale Personalaktenführung
- § 83 BetrVG/nebenvertragliche Pflicht: Einsichtsrecht des AN
- § 34 Abs. 1 Nr. 1 BDSG/Art. 15 Abs. 3 DSGVO: schriftliches Auskunftsrecht des AN über die zu seiner Person gespeicherten Daten

10.4.4 Vertraulichkeit

- Zugriffsbefugnisse sind in differenzierten Berechtigungskonzept festzulegen
- Zugriffsarten können sein: Leseberechtigung, Lese- und Speicherberechtigung, Veränderungsberechtigung)
- Anzahl der Zugriffsrechte ist festzulegen
- besonders sensible Vorgänge sind zu verschlüsseln
- lediglich vorgangsbezogene Zugriffe sind zuzulassen
- Zugriffskontrollen mit regelmäßiger Überprüfung sind einzurichten
- verbindliche Verfahrensanweisungen für Systemnutzer sind zu erstellen

10.5 Checkliste für die Umsetzung der digitalen Personalakte

Die Datenschutzbeauftragten des Bundes und der Länder hat eine Handlungsempfehlung zum Datenschutz bei technisch unterstützten Verfahren der Personal- und Haushaltsbewirtschaftung entworfen. Diese kann als Checkliste für die Umsetzung der elektronischen Personalakte verstanden werden.

(1) Personenbezogene Daten der Beschäftigten dürfen in technikgestützten Verfahren nur in dem Umfang gespeichert, übermittelt und genutzt werden, in dem dies

rechtlich zulässig und im Rahmen der festgelegten Zwecke zur Durchführung der der jeweiligen Stelle obliegenden personalwirtschaftlichen, organisatorischen und sozialen Aufgaben erforderlich ist (Grundsatz der Zulässigkeit, Zweckbindung und Erforderlichkeit).

(2) In einem Berechtigungskonzept ist festzulegen, welche Stellen und/oder Funktionsträgerinnen oder Funktionsträger im Rahmen der ihnen übertragenen Aufgaben für welche Zwecke und in welcher Form (lesend/verändernd) befugt sind, auf Daten zuzugreifen oder Auswertungen vorzunehmen. Das Berechtigungskonzept ist fortzuschreiben und mindestens so lange zu speichern wie die zugehörigen Protokolldaten.

(3) Es ist schon im Vorfeld bei der Auswahl und Gestaltung der automatisierten Verfahren darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden (Grundsatz der Datenvermeidung und Datensparsamkeit).

(4) Die Betroffenen sind über ihren persönlichen Datenbestand, die Zwecke der Verarbeitung und Zugriffsberechtigungen zu unterrichten. Ihre Rechte auf Auskunft, Sperrung und Löschung sind zu wahren (Transparenzgebot und Betroffenenrechte).

(5) Arbeits- und dienstrechtliche Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient (Verbot der automatisierten Einzelentscheidung).

(6) Zulässige dienststellenübergreifende Auswertungen der in den Verfahren verarbeiteten Personaldaten sollten soweit möglich anonym oder pseudonym erfolgen; dies gilt nicht für Auswertungen, Abgleiche oder Zusammenführungen, die sich auf die in der Anlage aufgeführten Merkmale (Informationen zur dienstlichen Funktion und Erreichbarkeit = sog. Funktionsträgerdaten) beschränken.

(7) Die Sicherungsziele Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit sind – ausgerichtet am Schutzbedarf der Daten – durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

(8) Protokolldaten von Anwendern sowie Administratoren, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert werden, dürfen grundsätzlich nicht für andere Zwecke, insbesondere nicht für eine Verhaltens- und Leistungskontrolle, verarbeitet werden. Die Zweckbindung muss daher technisch und organisatorisch (z.B. durch Dienstanweisung) sichergestellt werden. Für Art, Umfang und Aufbewahrung der Protokollierung gilt der Grundsatz der Erforderlichkeit. Soweit technisch

möglich und ausreichend, sollte auf personenbezogene Daten verzichtet werden. Die Beteiligungsrechte des Personalrates sind zu beachten.

(9) Vor der Einführung und Anwendung neuer Verfahren oder im Falle einer wesentlichen Veränderung der Verfahren ist eine Vorabkontrolle (auch „Technikfolgenabschätzung“ genannt) durchzuführen, wenn dies durch eine Rechtsvorschrift vorgesehen ist.

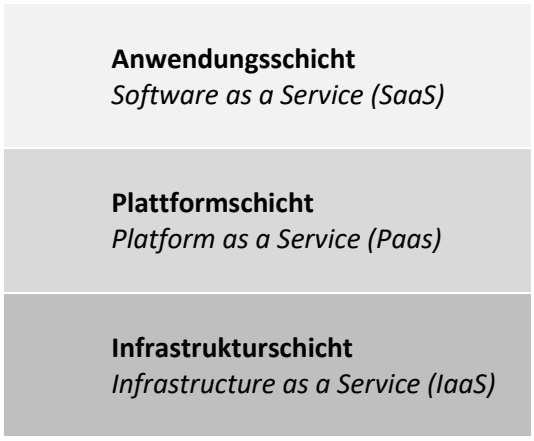
(10) Die Verfahren sind in inhaltlicher und technischer Hinsicht ausreichend und nachvollziehbar zu dokumentieren.

(11) Um die Akzeptanz zu fördern, wird empfohlen, über Einführung und Anwendung der Verfahren eine Dienstvereinbarung mit dem Betriebsrat abzuschließen, in der insbesondere die Fragen der Zugriffsberechtigungen, der Zulässigkeit und Zweckbestimmung von Auswertungen und die Durchführung von Kontrollen für alle Beteiligten eindeutig und klar geregelt werden. Soweit die Verfahren geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sind die Mitbestimmungs- bzw. Mitwirkungsrechte der Personalvertretung zu berücksichtigen.

11 Rechtssicherheit in der Cloud

11.1 Arten des Cloud Computing

Eine Unterscheidung lässt sich anhand der Cloud Computing-Architektur vornehmen, diese besteht aus drei Schichten:



11.1.1 Infrastructure as a Service (IaaS)

- unterste Schicht des Cloud Computing
- Angeboten wird lediglich die zur Umsetzung bestimmter Anwendungen notwendige Hardware (befindet sich im Rechenzentrum und wird dort betreut).
- Cloud-Anwender erhalten Zugriff auf virtualisierte Komponenten zur Datenverarbeitung, zum Datentransport und zur Datenspeicherung und können somit beliebige Anwendungsprogramme und Betriebssysteme einsetzen und installieren.

>> Zwischenfazit: Man mietet sich IT-Infrastruktur und Wartung.

11.1.2 Platform as a Service (Paas)

- mittlere Schicht des Cloud Computing
- Auf der angebotenen Infrastruktur werden mittels Schnittstellen eigene Programme entwickelt und ausgeführt.
- PaaS-Anbieter stellt Entwicklungsumgebungen in Form von Frameworks bereit
- Entwickler hat keine Möglichkeit, auf die zur Bereitstellung des Diensts genutzte Infrastruktur administrativ oder kontrollierend zuzugreifen. Er kann lediglich die selbst eingebrachten Programme und Daten kontrollieren.

11.1.3 Software as a Service (SaaS)

- oberste Schicht des Cloud Computing – baut auf vorhergehenden Schichten auf
- Kunde bekommt Software-Anwendung als Dienstleistung gegen Entgelt zur Verfügung gestellt. Software und IT-Infrastruktur werden bei externem Dienstleister betrieben.

>> Software wird nicht lizenziert und auf eigener Hardware installiert, sondern nur als Service „angemietet“ und kann überall mit jedem Internetbrowser genutzt werden.

11.2 Zulässigkeit des Cloud Computing

11.2.1 Geltende Rechtslage

Grundsatz: Verarbeitung personenbezogener Daten steht unter Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO).

- Rechtfertigungstatbestände, explizit genannt in Art. 6 DSGVO; gesetzliche Vorschriften (z.B. § 26 BDSG), Einwilligung des Betroffenen; Betriebsvereinbarungen

- Auslagerung an Cloud-Anbieter entbinden datenverarbeitende Stelle nicht vom Verbot mit Erlaubnisvorbehalt: Verantwortlicher ist jede Person oder Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Ziffer 7 DSGVO)

- Verantwortlicher trägt auch weiterhin eine Auswahlverantwortung hinsichtlich des Auftragsverarbeiters, der strikt den Weisungen des Verantwortlichen unterliegt, vgl. Art. 29 DSGVO

- Verantwortlicher hat zu prüfen, ob der Auftragsverarbeiter entsprechende Garantien im Hinblick auf Einhaltung der Vorgaben der Verordnung bieten kann. Da Garantien den gesamten Zeitraum der Datenverarbeitung abdecken müssen, muss Verantwortlicher fortlaufend kontrollieren, ob bspw. Zertifikate erneuert wurden, vgl. Art. 24, 32 DSGVO.

Begriffsdefinitionen:

- Verantwortlicher (Auftraggeber): „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen

über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet […]“, vgl. Art. 4 Nr. 7 DSGVO

- Auftragsverarbeiter (Auftragnehmer): „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“, vgl. Art. 4 Nr. 8 DSGVO

Räumlicher Anwendungsbereich:

- Anwendung dann, wenn Verarbeitung im Rahmen einer Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet

>> Hat Auftragsverarbeiter seinen Sitz in der Union, verarbeitet die Daten aber außerhalb der Union, sind dennoch die Pflichten der DSGVO anwendbar.

Anforderungen an die Auftragsverarbeitung nach der DSGVO:

- Vertrag oder anderes Rechtsinstrument zwischen Verantwortlichem und Auftragsverarbeiter
- schriftliches oder elektronisches Format nunmehr ebenfalls zulässig, vgl. Art. 28 Abs. 9 DSGVO

>> Schriftliche Abfassung stets erforderlich; elektronisches Format muss Echtheit der im Dokument genannten Verpflichtungen sicherstellen, einfache E-Mail genügt dieser Anforderung regelmäßig nicht.

Vertrag/anderes Rechtsinstrument muss gem. Art. 28 Abs. 3 DSGVO folgende Mindestinhalt besitzen:

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten
- Kategorien betroffener Personen
- Verarbeitung nur auf dokumentierte Weise
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Person zur Vertraulichkeit

- Sicherstellung technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus
- Unterstützung des Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des Verantwortlichen bei der Meldepflicht von Datenschutzverletzungen
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung
- Einschaltung eines Subunternehmers durch den Auftragnehmer nur nach Zustimmung des Auftraggebers

11.2.2 Übermittlung personenbezogener Daten in Drittländer

Die Übermittlung personenbezogener Daten in Drittländer ist nach der DSGVO in einem Verzeichnis zu dokumentieren, s.u. und vgl. Art. 44 ff. DSGVO mit den vier Grundaussagen:

- Übermittlungen personenbezogener Daten an Empfänger in Drittländern müssen die Zulässigkeitsvoraussetzungen der DSGVO erfüllen, insbes. jene des Kapitels II (u.a.: Zweckbindung, Datenminimierung, Richtigkeit, Rechtmäßigkeit der Verarbeitung, vgl. Art. 5 ff. DSGVO).
- Übermittlungen personenbezogener Daten an Empfänger in Drittländern sind nur erlaubt, wenn sie in Einklang mit mind. einem der in Kapitel V genannten Erlaubnistatbestände (z.B. Angemessenheitsbeschluss der Kommission, vgl. Art. 45 Abs. 3 DSGVO) stehen.
- Die DSGVO findet auch auf Weiterübermittlungen an Empfänger in Drittländern Anwendung.
- Die Regelungen sind immer unter der Prämisse anzuwenden, dass das von der DSGVO dem Betroffenen garantierte Schutzniveau nicht unterschritten wird.

Angemessenes Schutzniveau kann festgestellt werden durch:

- Angemessenheitsbeschluss der Kommission, Art. 45 Abs. 3 DSGVO (hier kommt EU-US-Privacy-Shield zum Tragen)
- Verbindliche interne Datenschutzvorschriften, Art. 46 Abs. 2 lit. b i.V.m Art. 47 DSGVO
- Standarddatenschutzklauseln, Art. 46 Abs. 2 lit. c. und d DSGVO
- genehmigte Verhaltensregeln, Art. 46 Abs. 2 lit. e i.V.m. Art. 40 DSGVO
- genehmigte Zertifizierungsmechanismen, Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DSGVO
- sonstige Maßnahmen, Art. 46 Abs. 2 lit. a, Abs. 3 lit. a und b DSGVO

11.3 Arbeitnehmerdaten in der Cloud

11.3.1 Möglichkeiten der externen Datenverarbeitung im Inland

- zwei Möglichkeiten: Auftragsdatenverarbeitung oder Funktionsübertragung (Letzteres weist hohe Datenschutzrisiken auf und ist daher nicht zu empfehlen)
- Weiterleitung von Beschäftigtendaten an Cloud-Anbieter i.R.d. Auftragsdatenverarbeitung bedarf keiner zusätzlichen Erlaubnis
- AG muss sicherstellen, dass der Cloud-Anbieter ausschließlich auf der Basis relativ engmaschiger Weisungen handelt.
- Anforderungen der Auftragsverarbeitung (s.o. unter Ziffer 12.2.1)

11.3.2 Möglichkeiten der Datenverarbeitung im Ausland

- Bei besonders sensiblen Daten sollte auf nationale Anbieter zurückgegriffen werden.
- Cloud-Anbieter innerhalb der EU/EWR: Vorgaben der DSGVO sind einzuhalten
- Cloud-Anbieter in Drittstaaten: Beschäftigtendaten-Übermittlung nur bei Gewährleistung eines angemessenen Datenschutzniveaus
- Übermittlung in unsichere Drittstaaten: Hürden zur Übermittlung sind hoch, da es üblicherweise an der Erforderlichkeit einer Übermittlung in einen Drittstaat fehlt; mit Einwilligung des AN, Art. 6 Abs. 1 lit. a DSGVO, Art. 7 DSGVO, § 26 BDSG

11.3.3 Einbindung des Betriebsrates

Unterrichtungs- und Beratungspflicht

- AG ist vor Einführung der Cloud-Anwendungen verpflichtet, die Auswirkungen der Cloud-Nutzung auf die AN mit dem Betriebsrat zu beraten, § 90 Abs. 2 S. 1 BetrVG
- Überwachungspflicht des Betriebsrates, § 80 Abs. 1 Nr. 1 BetrVG

Mitbestimmungsrecht

- vgl. § 87 Abs. 1 Nr. 5 BetrVG
- Die meisten Cloud-Dienste zur Verwaltung von Beschäftigtendaten ermöglichen AG, umfassende Leistungs- und Verhaltensdaten durchzuführen.

>> Empfohlen wird der Abschluss einer Betriebsvereinbarung über die Einführung und Nutzung von Cloud-Diensten zur Verwaltung von Beschäftigtendaten - kann auch als Erlaubnisnorm nach Art. 6 DSGVO zur Rechtfertigung des Umgangs von Beschäftigtendaten in der Cloud dienen.

11.4 Allgemeine Checkliste für die Auswahl eines externen Cloud-Anbieters

- Welche Arbeitsbereiche sollen in die Cloud ausgelagert werden?
- Welche Chancen und Risiken bestehen dabei?
- In welchem Land werden die Daten gespeichert?
- Behalten Sie die Kontrolle über die Daten und bleiben sie in Ihrem Besitz?
- Wer kann die Daten einsehen?
- Welche Zugangs- und Zugriffssicherung bietet der Provider?
- Verarbeitet der Provider Daten verschiedener Nutzer getrennt auf dem Server?
- Informiert Sie der Provider über Änderungen und können Sie rechtzeitig darauf reagieren?
- Werden Ihnen weit reichende Service-Levels zugesichert?

12 Informationspflichten (Impressum)

Impressumspflichten können sich aus TMG, DL-InfoV, Fernabsatz- und Presserecht ergeben.

12.1 § 5 Telemediengesetz (TMG)

12.1.1 Anwendungsbereich

Wer ist von der Norm erfasst? Diensteanbieter, die geschäftsmäßig in der Regel gegen Entgelt Telemedien anbieten:

- Telemedien: Informations- und Kommunikationsdienste. Von anderen Diensten unterscheiden sie sich vor allem dadurch, dass sie nicht-linear ausgestrahlt werden und sich nicht in der Übertragung von Signalen über Telekommunikationsnetze erschöpfen, vgl. § 1 Abs. 1 S. 1 TMG. Neben Webseiten können auch E-Mail-Newsletter und RSS-Newsfeeds Telemedien sein.

- Diensteanbieter: Jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Erfasst sind damit u.a. Anbieter von Websites und Newslettern, auch wenn sie lediglich Werbung für Waren ohne unmittelbare Bestellmöglichkeit und sonstige Interaktionsmöglichkeiten betreiben, vgl. § 2 Nr. 1 TMG

- Geschäftsmäßigkeit/Entgeltlichkeit: Nur geringe Anforderungen. Allein das nachhaltige Angebot von Telekommunikation mit oder ohne Gewinnerzielungsabsicht genügt. Gemeinnützige Websites ebenso wie Angebote von Bildungseinrichtungen und selbst rein private Homepages sind von dieser Definition erfasst, da jede auf Dauer angelegte Internetseite das Merkmal der Nachhaltigkeit erfüllt.

>> Praktisch jeder, der eine Internetseite bereithält, ist von den Pflichten aus § 5 TMG erfasst.

12.1.2 Gestalterische Anforderungen

Welche gestalterischen Anforderungen ergeben sich aus § 5 TMG? Pflichtangaben müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar gehalten werden.

Leicht erkennbar heißt:

- gut/effektiv optisch wahrnehmbare Stelle; ohne langes Suchen auffindbar

- nicht unter den Allgemeinen Geschäftsbedingungen, in einer Datenschutzerklärung oder unter den Frequently Asked Questions
- gut lesbar = Verwendung entsprechender Schriftgröße und einer sich vom Hintergrund abhebenden Schriftfarbe
- Verwendung eines Dateiformats, das mit den Standardeinstellungen der gängigen Browser sichtbar ist
- Bezeichnung ist nicht vorgeschrieben. Das Wort Impressum muss nicht zwingend verwendet werden. Als genügend anzusehen sind etwa die Bezeichnungen „Anbieterkennzeichnung", „Über uns" oder „Kontakt" (das ist in Rechtsprechung/Literatur allerdings umstritten)

Unmittelbar erreichbar heißt:

- Zugangsmöglichkeit ohne wesentliche Zwischenschritte
- Literatur/BGH: 2-Klick-Regelung, wonach ein Nutzer in der Regel nicht mehr als zwei Schritte benötigen darf, um zu den Pflichtangaben zu gelangen

Ständig verfügbar heißt:

- Zugriff auf Pflichtangaben muss jederzeit gewährleistet sein
- Möglichkeit einer dauerhaften Archivierung durch den Nutzer muss gegeben sein

>> Pflichtangaben müssen ausdruckbar sein.

Handelt es sich um ein kostenpflichtiges Telemedium, muss die Anbieterkennzeichnung schon vor dem Login aufrufbar sein.

12.1.3 Erforderliche Angaben

Welche Angaben müssen aufgrund von § 5 TMG im Impressum enthalten sein?

§ 5 Abs. 1 Nr. 1 TMG

- Name: Vor- und Nachname (Pseudonym nur bei hohem Bekanntheitsgrad ausreichend)

- Adresse: Straße, Hausnummer, PLZ, Ort (Postfachadresse nicht ausreichend)

- besitzt Anbieter mehrere Niederlassungen, muss Anschrift derjenigen Niederlassung genannt werden, bei der organisatorische Ressourcen für den Betrieb der Telemedien gebündelt sind (im Zweifel: Hauptniederlassung)

- juristische Personen: Rechtsform (korrekt und vollständig, Abkürzungen [AG, GmbH etc.] zulässig), Vertretungsberechtigte + sofern Angaben über das Kapital der Gesellschaft gemacht werden: Angabe von Stamm- oder Grundkapital sowie, wenn nicht alle in Geld zu leistenden Einlagen eingezahlt sind, den Gesamtbetrag der ausstehenden Einlagen. Ausreichend, wenn Kapital irgendwo auf der Webseite (z.B. im Zusammenhang mit einem Geschäftsbericht), erwähnt ist

§ 5 Abs. 1 Nr. 2 TMG

- Angabe einer E-Mail-Adresse ist zwingend!
- daneben mindestens eine weitere Kontaktmöglichkeit (nicht unbedingt Telefonnummer)

§ 5 Abs. 1 Nr. 3 TMG

- zuständige Aufsichtsbehörde (falls vorhanden)
- Zulassungsbehörde muss nicht genannt werden
- Mitteilung der Behördenadresse nicht erforderlich, Nutzer soll gleichwohl einfache Kontaktaufnahme ermöglicht werden (z.B. durch Link auf Aufsichtsbehörde)

§ 5 Abs. 1 Nr. 4 TMG

- Nennung der Registernummer (falls vorhanden) und die das Register führende Stelle

§ 5 Abs. 1 Nr. 5 TMG

- Angabe der zuständigen Kammer (bei Pflichtmitgliedschaft)
- gesetzliche Berufsbezeichnung
- Staat, in dem Berufsbezeichnung verliehen worden ist
- Nennung der berufsrechtlichen Regelungen (Fundstelle im Bundesgesetzblatt oder andere öffentlich zugängliche Sammlung oder Link auf andere Webseite wie etwa Kammer)

§ 5 Abs. 1 Nr. 6 TMG

- Umsatzsteuer-Identifikationsnummer i.S.d. § 27a UStG (soweit vorhanden)
- Ist nur Wirtschafts-Identifikationsnummer nach § 139c AO vorhanden, ist diese anzugeben. Sind beide vorhanden, besteht Wahlrecht.
- „Normale“ Steuernummer ist nicht im Impressum anzugeben!

§ 5 Abs. 1 Nr. 7 TMG

- Abwicklung oder Liquidation von Kapitalgesellschaften
- Angaben zum Liquidator/Insolvenzverwalter nicht erforderlich
- entsprechende Anwendung auf Personengesellschaften ist angezeigt

12.2 Dienstleistungs-Informationspflichten-Verordnung (DL-InfoV)

12.2.1 Anwendungsbereich

Wer ist von der DL-InfoV erfasst?

- Gilt für alle Personen, die Dienstleistungen erbringen, die in den Anwendungsbereich des Art. 2 der RL 2006/123/EG fallen.

- Auf folgende Tätigkeiten findet die Richtlinie keine Anwendung (Auswahl): nicht-wirtschaftliche Dienstleistungen von allgemein-wirtschaftlichem Interesse, Finanzdienstleistungen, Gesundheitsdienstleistungen, Tätigkeiten von Notaren oder Gerichtsvollziehern

- Für das Impressum dann anwendbar, wenn Dienstleistung über Webseite erbracht wird.

- Gilt auch, wenn im Inland niedergelassener Dienstleistungserbringer Dienstleistung im EU-/EWR-Ausland erbringt.

12.2.2 Gestalterische Vorgaben

Welche gestalterischen Anforderungen ergeben sich aus der DL-InfoV?

- deutsche Sprache
- rechtzeitig: Müssen vor Abschluss eines schriftlichen Vertrages, oder sofern kein schriftlicher Vertrag geschlossen wird, vor Erbringung der Dienstleistung zur Verfügung gestellt werden

>> Der Leistungsempfänger muss sich noch entscheiden können, ob er Dienstleistung in Anspruch nimmt.

- klare und verständliche Form (abzustellen ist auf den durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Dienstleistungsempfänger)

12.2.3 Erforderliche Angaben

Welche Angaben müssen vorgehalten werden?

- DL-InfoV unterscheidet zwischen stets zur Verfügung zu stellenden Informationen und solchen, die auf Anfrage zur Verfügung zu stellen sind
- Stets zur Verfügung zu stellenden Informationen sind teilweise mit jenen aus § 5 TMG identisch. Darüber hinaus:
- Angaben über verwendete AGB (falls vorhanden)
- verwendete Vertragsklauseln über das auf den Vertrag anwendbare Recht oder über den Gerichtsstand
- gegebenenfalls bestehende Garantien, die über die gesetzlichen Gewährleistungsrechte hinausgehen
- wesentliche Merkmale der Dienstleistung, soweit sich diese nicht bereits aus dem Zusammenhang ergeben
- Angaben zur Berufshaftpflichtversicherung (falls vorhanden), insbesondere Name und Anschrift des Versicherers und räumlicher Geltungsbereich

12.3 Umsatzsteuergesetz

- Angabe der Umsatzsteuer-Identifikationsnummer (vgl. § 27a UStG)

12.4 Fernabsatzrecht (§§ 312b ff. BGB)

- Informationspflichten gem. Art. 246a EGBGB (vgl. § 312d Abs. 1 BGB)
- Verträge über Finanzdienstleistungen: Art. 246b EGBGB (vgl. § 312d Abs. 2 BGB)
- § 312e BGB: Fracht-, Liefer-, Versand- oder sonstige Kosten

12.5 Presserecht/Rundfunkstaatsvertrag

- Presserecht: Jeweiliges Landesrecht beachten! Vgl. etwa § 8 Niedersächsisches Pressegesetz (u.a.: Name/Firma, Anschrift des Druckers und Verlegers, bei Selbstverlagen Name und Anschrift des Verfassers/Herausgebers)

- Rundfunkstaatsvertrag (RStV): § 55 RStV (für Anbieter, die keine Telemedien im Sinne des § 5 TMG bereithalten) (Name, Anschrift, bei juristischen Personen Name und Anschrift des Vertretungsberechtigten)

12.6 Fernunterrichtsschutzgesetz

- Fernunterricht: auf vertraglicher Grundlage erfolgende, entgeltliche (unentgeltlich, soweit ausdrücklich vorgesehen) Vermittlung von Kenntnissen und Fähigkeiten, bei der der Lehrende und der Lernende ausschließlich oder überwiegend räumlich getrennt sind und der Lehrende oder sein Beauftragter den Lernerfolg überwachen

- § 3 Abs. 2 FernUSG: Informationspflichten des § 312d BGB geltend entsprechend

13 Anlagen

13.1 Mustervertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO

Auftragsdatenvereinbarung

zwischen

.....
(Verantwortlicher - nachstehend bezeichnet als **Auftraggeber**)

und

.....
- Auftragsverarbeiter - nachstehend bezeichnet als **Auftragnehmer**)

.....]
[ggf.: Vertreter gemäß Art. 27 DSGVO:

Hinweis

„Die einzelnen Festlegungen nach Art. 28 Abs. 3 DSGVO sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden.

Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden.

Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen.

Vergütungs- und Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers sollten im Hauptvertrag vereinbart werden.“

>> Dieses Muster dient der Veranschaulichung und ersetzt nicht die rechtliche Beratung.

1. Gegenstand und Dauer des Auftrags

1.1. Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/..... vom ....., auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

Oder:

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: …… (Definition der Aufgaben)

1.2. Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

2.1. Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom .....

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: .....

Die Erbringung der vertraglich vereinbarten Datenverarbeitung 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. DSGVO erfüllt sind. Das angemessene Schutzniveau in …….

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DSGVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e i.V.m. 40 DSGVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).

☐ wird hergestellt durch sonstige Maßnahmen: ……. (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DSGVO)

2.2. Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ ...

2.3. Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ ...

3. Technisch-organisatorische Maßnahmen

3.1. Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen 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.

3.2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in Anlage 1].

3.3. Die 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.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.

(2) Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(3) Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(4) Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(5) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

(6) Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

(7) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten

einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(8) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

(9) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(10) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(11) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(12) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird

(13) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(1) ☐ Eine Unterbeauftragung ist unzulässig.
(2) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Leistung

(3) ☐ Die Auslagerung auf Unterauftragnehmer oder
☐ der Wechsel des bestehenden Unterauftragnehmers
sind zulässig, soweit:
a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
b) der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

6.3. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

6.5. Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;
☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

7.1. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem 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.

7.2. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.4. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

(1) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
(2) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

(3) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
(4) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
(5) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

9.1. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.2. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

10.3. Kopien oder Duplikate der Daten 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.

10.4. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten 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.

10.5. 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.

++++

13.2 Technisch-organisatorische Maßnahmen

	Kontrolle	*Maßnahme*
1.	**Vertraulichkeit**	*(Art. 32 Abs. 1 lit. b DSGVO*)
	Zutrittskontrolle	Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
	Zugangskontrolle	Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
	Zugriffskontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
	Trennungskontrolle	Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
	Pseudonymisierung	(Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)/Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;
2.	**Integrität**	*(Art. 32 Abs. 1 lit. b DSGVO)*
	Weitergabekontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
	Eingabekontrolle	Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

	Kontrolle	*Maßnahme*
3.	**Verfügbarkeit und Belastbarkeit**	*(Art. 32 Abs. 1 lit. b DSGVO)*
	Verfügbarkeits-kontrolle	Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
	Rasche Wiederherstellbarkeit	*(Art. 32 Abs. 1 lit. c DSGVO)*
4.	**Überprüfung**	*Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)*
	Datenschutz-Management	Incident-Response-Management; Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO); Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

+++