MASTER THESIS | MASTER'S THESIS

Titel | Title

Risikomanagement im Datenschutz aus Sicht von Unternehmen

verfasst von | submitted by

Mag.rer.soc.oec. Manfred Lehner

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2025

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 999 083
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von | Supervisor:	Mag. Dr. Marcus Becka LL.M. MSc

Inhaltsverzeichnis

Abkürzungsverzeichnis

Anm	Anmerkung
Art	Artikel
Abs	Absatz
B2B	business-to-business
B2C	business-to-consumer
BIP	Bruttoinlandsprodukt
BSI	Deutsches Bundesamt für Sicherheit in der Informationstechnologie
bspw	Beispielsweise
bzgl	bezüglich
bzw	beziehungsweise
dh	das heißt
DSFA	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DSMS	Datenschutzmanagementsystem
EDPS	European Data Protection Supervisor
EMRK	Europäische Menschenrechtskonvention
ESG	Environmental, Social and Governance
EU	Europäische Union
EW	Einwohner
gem	gemäß
ggf	gegebenenfalls
GRC-System	Governance-, Risk- und Compliance-System
GRC	Charta der Grundrechte der Europäischen Union
Hrsg	Herausgeber
IAPP	International Association of Privacy Professionals
IKT	Informations- und Kommunikationstechnologie
inkl	inklusive
IoT	Internet of Things
ISO	Internationale Normungsorganisation
iSv	im Sinne von

IT	Informationstechnologie
Kap	Kapitel
mE	meines Erachtens
Mio	Million(en)
PIMS	Privacy Information Management System
RMS	Risiko-Management-System
SDM	Standard Datenschutzmodell
SWOT	Strengths, Weaknesses, Opportunities and Threats
TKG	Telekommunikationsgesetz
TOM	technische und organisatorische Maßnahmen
uvm	und viele mehr
VaR	Value at Risk
vgl	vergleiche
zB	zum Beispiel
zw	zwischen

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

In den letzten Jahren und Jahrzehnten hat sich die Unternehmenswelt massiv geändert. Um es Unternehmen zu ermöglichen, flexibler auf Umweltbedingungen zu reagieren, haben viele Unternehmen zumindest in Teilbereichen neue Organisationsmodelle wie bspw Selbstorganisation eingeführt. Diese Organisationsmodelle basieren oft auf zu einem großen Teil auf Vertrauen oder sind durch umfangreiche und komplexe Rollenbeschreibungen gekennzeichnet. In derartigen Systemen kommt es oft zu Informationsasymmetrien zwischen der Leitungsebene und den ausführenden Mitarbeitern. Gleichzeitig gibt es neue Regularien wie zB die EU Datenschutzgrundverordnung (DSGVO[1]), die neben zusätzlichen Anforderungen auch eine deutlich höhere Bußgelddrohung mit sich gebracht hat. In der Roadmap der EU finden sich weitere Regelungen wie AI Act, Data Act, Digital Markets Act, Digital Services Act etc. – viele davon mit hohen Bußgelddrohungen.

Diese Situation wirft verschiedene Fragen auf:

- Wie kann in Anbetracht dieser potentiellen Informationsasymmetrien in Verbindung mit gestiegenen Anforderungen dennoch eine effiziente Allokation von Ressourcen, die für effektiven Datenschutz sorgt, gelingen?
- Ist die Implementierung eines modernen Risikomanagementsystems für Datenschutz geeignet, um allfällige Informationsasymmetrien innerhalb der Unternehmen zu vermindern?
- Kann ein modernes Risikomanagementsystem für Datenschutz einen Beitrag zu einer wertorientierten Unternehmenssteuerung leisten?

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119.

2 Aufbau der Arbeit

Das Thema „Risikomanagement im Datenschutz“ ist ein interdisziplinäres Thema. Einerseits ist bereits Risikomanagement selbst interdisziplinär, da neben betriebswirtschaftlichen Aspekten auch Psychologie und Statistik eine wichtige Rolle spielen. Die Verknüpfung mit dem Thema Datenschutz bringt weitere Komplexität mit sich: Für effektiven Datenschutz ist neben der Berücksichtigung der rechtlichen Aspekte von Datenschutz auch eine Integration von Informationstechnologie und Organisation notwendig.[2]

Zur Einleitung stellt das Kapitel 3 „Motivation für Risikomanagement im Datenschutz“ Corporate Governance als Rahmenwerk für (unter anderem) Risiko Management vor.

Um die Entwicklung von Organisationen (bzw Organisationstheorien) besser zu verstehen wird im Kapitel 4 „Organisationstheorien und psychologische Konstrukte“ die Entwicklung von Organisationstheorien kurz beschrieben. Zusätzlich werden auch verschiedene psychologische Konstrukte, die zum Verständnis der Materie beitragen sollen, dargestellt. Aufgrund der Vielzahl an Theorien, Modellen und Konstrukten werden nur einige davon beispielhaft dargestellt. Eine einigermaßen erschöpfende Aufstellung würde den Rahmen dieser Arbeit sprengen.

Um die Einbettung von Datenschutz (und des dazugehörigen Risikomanagements) in die Organisationsstrategie und die sich daraus ergebenden Ziele besser zu verstehen, wird im danach folgenden Kapitel 5 „Strategisches Management“ eine knappe Einführung in wichtige Aspekte des strategischen Managements, die für die vorliegende Arbeit relevant sind, gegeben.

Im Kapitel 6 „Grundlagen Risikomanagement“ sollen die wichtigsten Grundlagen von Risikomanagement dargestellt werden. Dabei wird unter anderem das Teilgebiet „Risikoaggregation“ genauer beleuchtet, da erst dadurch eine Gesamtdarstellung der

[2] Vgl *Pachinger et al*, Datenschutz: Recht und Praxis: Verfahren & Behörden, Datenschutzbeauftragter, IT & Blockchain, Datenschutzverträge, Straf- & Arbeitsrecht, International, Strategie & Organisation, Sicherheit (Handbuch 2020) 369.

Risikoposition, und damit eine effiziente Ressourcenallokation und eine wertorientiere Unternehmensführung, möglich wird.

Im Kapitel 7 „Grundlagen Datenschutz“ werden Datenschutz und die dazugehörigen Teilgebiete Datenschutzmanagementsystem, Datenschutzstrategie und Datenschutzziele behandelt. Weiters wird der Begriff „Risiko“ in der DSGVO genauer betrachtet.

Kapitel 8 „Besonderheiten von Datenschutz im Risikomanagement“ schließlich führt die Erkenntnisse aus den vorangegangenen Kapiteln zusammen und versucht ein Gesamtbild zu zeichnen.

Das Kapitel 9 „Zusammenfassung der aufgestellten Thesen“ wiederum fasst die – hauptsächlich im vorangegangenen Kapitel aufgestellten – Hypothesen zusammen.

In den Anhängen findet sich noch Zusatzmaterial zu Wahrscheinlichkeits- und Dichtefunktionen, Beispiele von Monte-Carlo-Simulationen und eine Übersicht zu den bisher verhängten DSGVO-Bußgeldern.

Nachfolgend ist der Aufbau der Arbeit vereinfacht dargestellt:

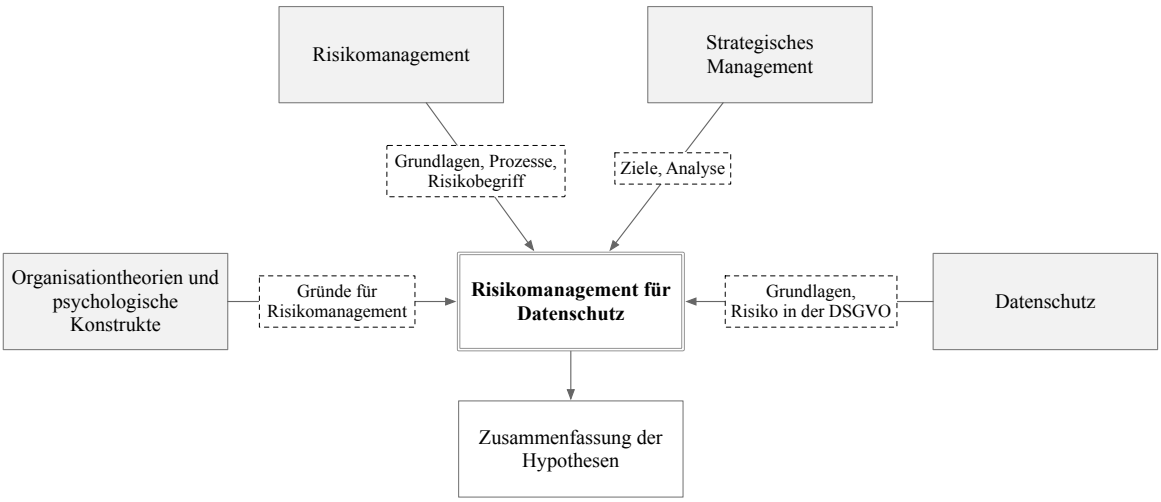


Abbildung 1: Aufbau der Arbeit (eigene Darstellung)

Geschlechtsneutrale Sprache

Der Autor versucht in der vorliegenden Arbeit eine geschlechtsneutrale Sprache zu verwenden. Sollte ausnahmsweise eine weibliche oder männliche Form verwendet werden, so sind Männer respektive Frauen immer mitgemeint.

3 Motivation für Risikomanagement im Datenschutz

Betrachtet man die rechtliche Seite von Datenschutz, ist einer der Gründe für die Einhaltung der Bestimmungen der DSGVO[3] die Androhung verhältnismäßig hoher Geldbußen bei Verstößen gegen diese EU Verordnung. Die DSGVO stellt dabei, neben dem Datenschutzgesetz[4] und dem Telekommunikationsgesetz[5] eine der wichtigsten rechtlichen Vorgaben im Bereich Datenschutz dar.

Die Einhaltung rechtlicher Vorgaben im Unternehmensumfeld wird üblicherweise unter dem Begriff „Compliance" zusammengefasst.[6] Compliance umfasst dabei neben Datenschutz noch weitere Bereiche:

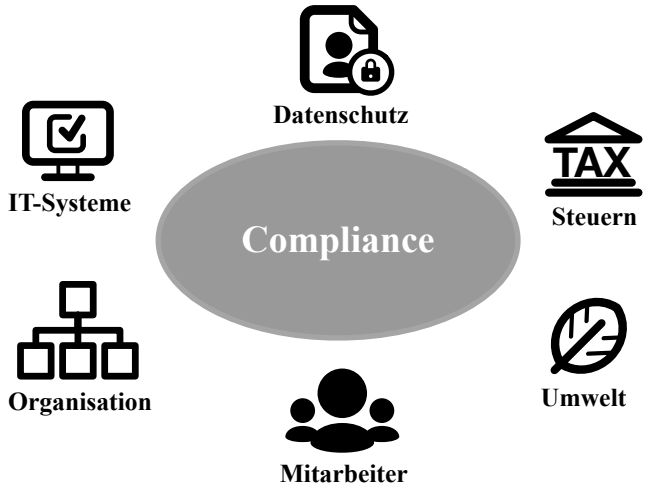


Abbildung 2: Wichtige Compliance Bereiche[7]

Der Vorstand ist dabei für die Compliance, d.h. für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Regelungen verantwortlich. Dafür werden im Rahmen von Compliance Management Systemen der Risikolage des Unternehmens

[3] DSGVO (EU) 679/2016.

[4] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF I 70/2024.

[5] Bundesgesetz, mit dem ein Telekommunikationsgesetz (Telekommunikationsgesetz 2021 – TKG 2021) erlassen wird, BGBl I 190/2021 idF I 75/2024.

[6] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance: Risikomanagement, Organisation, Compliance für Unternehmer (De gruyter praxishandbuch 2020) 2.

[7] *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 13.

entsprechende Maßnahmen implementiert.[8] Besonders wichtig ist das, weil Compliance-Risiken Unternehmen aufgrund des Geschäftseifers ihrer Führungskräfte und Mitarbeiter oft unerwartet und mit erheblichen Auswirkungen treffen.[9]

Compliance wiederum ist Teil der „Corporate Governance", die Leitplanken für das unternehmerische Handeln setzt. „*Corporate Governance umschreibt die vom Rechtsraum, von der Rechtsform, von der Branche, vom Kapitalmarktzugang abhängige und vom Unternehmen individuell selbst festgesetzte Unternehmensverfassung i.w.S.*"[10]

Zu einer gut ausgestalteten Corporate Governance gehört auch ein adäquates Risiko Management. Damit können Schwächen von Organisationen, wie beispielsweise Informationsasymmetrien (vgl Kapitel 4.2.3.1 „Neue Institutionenökonomik") zumindest teilweise mitigiert werden. Die nachfolgende Darstellung beschreibt die Zusammenhänge zwischen Compliance, Risiko Management, Corporate Governance und weiteren wichtigen Elementen im GRC-Ansatz (GRC = Governance, Risk, Compliance).

[8] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 10.

[9] Vgl *Schwieters*, Corporate Governance: verantwortliche Steuerung und Überwachung in Zeiten globaler Krisen (2023) 205.

[10] *Schwieters*, Corporate Governance, 5.

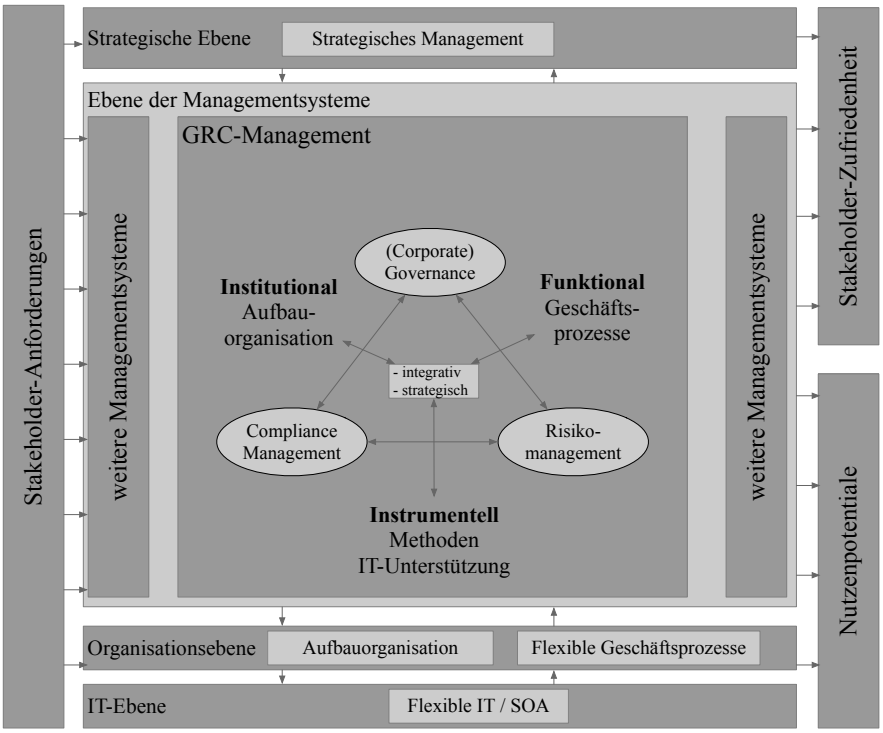


Abbildung 3: GRC-Ansatz[11]

Der GRC-Ansatz enthält nach Ansicht des Autors auch Schwächen – er betrachtet nur Risiken im engeren Sinne (dh negative Zielabweichungen). Nach herrschender Lehre können Risiken aber auch positive Abweichungen von Zielen darstellen: Während Zenke et al noch von einem Risikobegriff ausgehen, der primär ökonomische Nachteile betrachtet[12], wird der Risikobegriff heute üblicherweise breiter verstanden (vgl Kapitel 6 „Grundlagen Risikomanagement“).

Auch in der DSGVO wird der Begriff „Risiko“ an verschiedenen Stellen verwendet. Dabei ist aber immer das „Risiko für die Rechte und Freiheiten der Betroffenen“ gemeint (vgl auch Kapitel 7 „Grundlagen Datenschutz“ und 8 „Besonderheiten von Datenschutz im Risikomanagement“).
In diesem Werk soll aber primär das Risiko aus Unternehmenssicht, dh das betriebswirtschaftliche Risiko, das sich vom Risiko für die Rechte und Freiheiten der Betroffenen unterscheiden kann, behandelt werden.

[11] *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 6.

[12] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 2.

Aus Sicht des Autors ist das auch für den Bereich Datenschutz relevant. Während in vielen Fällen nur Verstöße gegen Datenschutzregularien (vgl Kapitel 7 „Grundlagen Datenschutz“) betrachtet werden, kann das Zielsystem im Datenschutz – natürlich abhängig von der jeweiligen Organisationsform des Unternehmens – neben Compliance Zielen auch andere Ziele enthalten. Beispielhaft wäre hier hohes Kunden-/Stakeholdervertrauen bzgl Datenschutz zu nennen (vgl Kap 8 „Besonderheiten von Datenschutz im Risikomanagement“).

4 Organisationstheorien und psychologische Konstrukte

4.1 Einleitung

Datenschutz effektiv umzusetzen, kann große, moderne Unternehmen mit vielfältigen und umfangreichen Verarbeitungen von personenbezogenen Daten vor große Herausforderungen stellen. Um die Herausforderungen für die Umsetzung von Datenschutz auf organisatorischer Ebene darzustellen, werden in diesem Kapitel verschiedene Organisationstheorien und psychologische Konstrukte beschrieben.

Nachfolgend wird die Entwicklung von Organisationstheorien kurz beschrieben. Aufgrund der Vielzahl werden nur einige Theorien beispielhaft dargestellt. Während die klassischen Ansätze „Bürokratie-Ansatz“, „Administrativer Ansatz“ und „Arbeitswissenschaftlicher Ansatz“ eher dem Gesamtverständnis der geschichtlichen Entwicklung dienen, und in der Praxis in ihrer Reinform wohl kaum mehr anzutreffen sind, sind die neoklassischen Ansätze „Human-Relations-Ansatz“ und „Anreiz-Beitrags-Theorie“ deutlich stärker verbreitet. Besonderes Augenmerk gilt in diesem Kapitel der „Neuen Institutionenökonomik“, speziell der „Principal-Agent-Theorie“ da sich dadurch organisatorische Probleme auch im Bereich Datenschutz erklären lassen.
Auch die „Lateralen Organisationsmodelle“, zu denen auch „Selbstorganisation“ zählt, sind für das Verständnis von organisatorischen Herausforderungen im Bereich Datenschutz wichtig. In den letzten Jahrzehnten haben Organisationsformen mit Aspekten von Selbstorganisation zunehmende Bedeutung erlangt. Einige dieser Modelle haben sehr weitreichende Bedeutung erlangt, bspw in der Softwareentwicklung, während andere Modelle eher die Ausnahme als die Regel darstellen.

Danach werden verschiedene psychologische Konstrukte, die zum Verständnis der Materie beitragen sollen, dargestellt. Während bei den klassischen Ansätzen der Organisationstheorien der Mensch als autopoietisches System keine Rolle spielte, bekam der „Faktor Mensch“ in den neoklassischen Organisationsmodellen einen deutlich höheren Stellenwert. In den modernen Ansätzen der Organisationstheorien spielt die Psychologie noch eine weit größere Rolle. Während bei lateralen Organisationsmodellen oft von einem sehr hohen Grad an Vertrauen zwischen Mitarbeitern und Unternehmen ausgegangen wird, unterstellt die Principal-Agent-Theorie den Akteuren Opportunismus. Das Konstrukt

„Vertrauen“ ist nicht nur für die Beziehung zwischen Mitarbeitern und Unternehmen relevant, sondern spielt auch in der Beziehung zwischen Kunden und einem Unternehmen eine bedeutende Rolle, bspw hinsichtlich Kundenbindung (vgl Kap 8 „Besonderheiten von Datenschutz im Risikomanagement“).

4.2 Entwicklung von Organisationen und Organisationstheorien

Organisationstheorien lassen sich nach verschiedenen Gesichtspunkten gliedern. Hier soll die historische Betrachtung behandelt werden.

4.2.1 Klassische Ansätze

4.2.1.1 Bürokratie-Ansatz

Wie auch beim Arbeitswissenschaftlichen Ansatz und beim Administrativen Ansatz beherrscht beim Bürokratie-Ansatz das Bild einer Maschine die Sicht auf die Organisation: Die einzelnen Stellen der Organisation bilden gleichsam Zahnräder, die möglichst gut geschmiert ineinandergreifen sollen. In diesem Verständnis ist die Organisationsstruktur gezielt gestaltbar, die einzelnen Elemente sollen so eingesetzt werden, dass möglichst geringe Reibungsverluste und ein hoher Wirkungsgrad entstehen. Diese Gestaltung ist Aufgabe der Führungskräfte und der Eigentümer.[13]

Wegen der fundamentalen wissenschaftlichen Kraft seiner Aussagen wird Max Weber (1864-1920) oft als „Vater der Organisationstheorie bezeichnet. Sein posthum veröffentlichtes Jahrhundertwerk „Wirtschaft und Gesellschaft“ bietet wichtige Grundlagen zum Verständnis der Funktionsweise moderner Großorganisationen. Weber will zeigen, dass und wie es in Großorganisationen gelingt, die Handlungen der Individuen zweckgeleitet aufeinander zu beziehen, regelhaft zu verstetigen und reibungslos zu einem Ganzen zu verbinden.[14]

[13] Vgl *Mayrhofer/Gurtmüller/Kasper* (Hrsg), Personalmanagement - Führung - Organisation (2023) 166.

[14] Vgl *Schreyögg/Geiger*, Organisation: Grundlagen moderner Organisationsgestaltung: mit Fallstudien (Lehrbuch 2016) 439f.

Als „Grundlage“ formulierte Weber dabei drei unterschiedliche Arten von Herrschaft und Autorität:[15]

- **charismatisch**: Legitimität der Herrschaft beruht auf außeralltägliche Hingabe, die Heldenkraft oder die Vorbildlichkeit einer Person.
- **traditionell**: Glaube an die Unverbrüchlichkeit von seit jeher geltenden Traditionen und der durch sie ausgezeichneten Personen; Diesen Personen wird „gedient“.
- **legal**: Während charismatische und traditionelle Herrschaft der Gehorsam ausgezeichneten Personen geschuldet wird, besteht bei der legalen Herrschaft der Glaube an eine rationale, legal gesetzte Ordnung; Wird von Weber als wichtigsten Herrschaftstyp für die Neuzeit gesehen.

Die bürokratische Organisation als rationale Form der legalen Herrschaft wird dabei durch folgende wesentliche Merkmale gekennzeichnet:

- strikte Regelgebundenheit der Amtsführung
- präzise Abgrenzung von Autorität und Verantwortung
- festgelegtes System von Über- und Unterordnungen mit genau umschriebener Befehlsgewalt (dh keine Willkür)
- Aktenmäßigkeit aller Verwaltungsvorgänge
- Strikt neutrale Amtsführung, sie hat nur der Sache nach zu erfolgen
- Spezielle, für die jeweilige Stelle ausgebildete „Fachleute“

Am Modell der bürokratischen Organisationen haben sich mehrere Kritikpunkte herausgebildet. Einerseits geht dieses Modell von einer stabilen Welt gleichförmiger Aufgaben aus. Andererseits bezieht sich die Kritik auch auf die Dysfunktionalitäten starrer Regeltreue und die verengte Perspektive organisationaler Beziehungen.[16]

4.2.1.2 Administrativer Ansatz

Das Ziel des Administrativen Ansatzes von Henri Fayol war eine rationale und effiziente Arbeitsbewältigung. Sein Organisationsmodell beschreibt ein Einliniensystem, d.h. jeder

[15] Vgl *Schreyögg/Geiger*, Organisation, 441f.

[16] Vgl *Schreyögg/Geiger*, Organisation, 442f.

Mitarbeiter hat genau einen Vorgesetzten. In seinem Modell soll ein Vorgesetzter "nicht zu viele" direkte Untergebene haben.
Fayol unterscheidet fünf Basiselemente guter Führung: Planung, Organisation, Befehl, Koordination und Kontrolle. Organisieren hat den Charakter einer Ingenieursaufgabe; er betrachtet eine Organisation als Maschine, die in zuverlässiger, effizienter und vorhersagbarer Weise die Anweisungen der Geschäftsleitung ausführt.[17]

4.2.1.3 Arbeitswissenschaftlicher Ansatz

Die zentralen Elemente des Arbeitswissenschaftlichen Ansatzes von Frederick W. Taylor sind die Analyse und Gestaltung konkreter Arbeitsabläufe in Organisationen. Im Mittelpunkt von Taylors Ansatz, den er selbst als "Scientific Management" bezeichnet hat, stehen die rationellste Arbeitsteilung und die Optimierung der Arbeitsvollzüge. Er löste die bis dahin übliche Einheit von Planung und Durchführung auf; Arbeit wird radikal in kleinste Teilverrichtungen aufgeteilt, um möglichst hohe Spezialisierungsgewinne zu erreichen. Da er Beschäftigten notorische "Drückebergerei" unterstellte, war ein weiteres Ziel deren Kontrollierbarkeit zu erhöhen.[18]

4.2.2 Neoklassische Ansätze

4.2.2.1 Human-Relations-Ansatz

Die Human Relations Bewegung geht auf Experimente, bei denen die Wirkung von Arbeitsbedingungen auf die Arbeitsleistung der Mitarbeiter untersucht werden sollten, zurück (Hawthorne Experimente). Dabei wurde festgestellt, dass die Arbeitsbedingungen geringeren Einfluss auf die Arbeitsleistung hatten als die Beziehung zwischen Unternehmen und den Mitarbeitern. Dadurch stellt der Human-Relations-Ansatz einen Paradigmenwechsel im Vergleich zu den oben beschriebenen klassischen Ansätzen dar.
Im Zentrum dieses Ansatzes steht daher, dass der Mensch ein soziales Wesen ist. Er funktioniert nach eigenen Gesetzen. Daraus folgt, dass bei den Mitgliedern der Organisation und den Vorgesetzten, eine positive Einstellung gegenüber der Arbeit zu einer hohen Zufriedenheit führt. Durch die hohe Zufriedenheit kann auch eine hohe Arbeitsleistung erreicht werden.[19]

[17] Vgl *Schreyögg/Geiger*, Organisation, 443f.

[18] Vgl *Schreyögg/Geiger*, Organisation, 446f.

[19] Vgl *Schreyögg/Geiger*, Organisation, 450f.

4.2.2.2 Anreiz-Beitrags-Theorie

Die Anreiz-Beitrags-Theorie ist eine Theorie der Arbeitsmotivation. Eine Organisation kann nur bestehen, in dem ein Gleichgewicht zwischen dem Anreiz (bspw Entlohnung, Prestige etc.) und dem Beitrag (Arbeitsleistung) hergestellt und aufrechterhalten wird. Das Unternehmen wird hier als kooperatives System verstanden.[20]

4.2.3 Moderne Ansätze

4.2.3.1 Neue Institutionenökonomik – Principal-Agent-Theorie

Grundsätzlich wendet die Neue Institutionenökonomik mikroökonomische Analytik auf organisatorische Fragestellungen an.[21] Sie bildet ein wichtiges Element der Organisationstheorien und stellt mittlerweile einen Grundpfeiler in der Organisations- und Strategieforschung dar.[22]

Die verschiedenen Ansätze der Neuen Institutionenökonomik haben eine individuellen Nutzenmaximierung ohne "moralische Skrupel" als Prämisse, gehen von unvollständiger Information aus und unterstellen die Kalkulierbarkeit aller Handlungsalternativen.[23]
Die aus der Neoklassik bekannten, idealisierten Annahmen eines vollkommenen und vollständigen Marktes werden kritisch hinterfragt und sukzessive aufgehoben. Dadurch wird eine explizite Berücksichtigung von Transaktionskosten und asymmetrischer Informationsverteilungen möglich. Verträge, bei denen zw relationalen, impliziten oder expliziten Verträgen unterschieden wird, stellen in der neuen Institutionenökonomik ein zentrales Konstrukt dar. [24]

Principal-Agent-Theorie
Die Principal-Agent-Theorie wohl der am meisten beachtete und für die vorliegende Arbeit der wichtigste Ansatz der Neuen Institutionenökonomik.

[20] Vgl *Schreyögg/Geiger*, Organisation, 454f.

[21] Vgl *Schreyögg/Geiger*, Organisation, 468.

[22] Vgl *Welge/Al-Laham/Eulerich*, Strategisches Management: Grundlagen - Prozess - Implementierung (Lehrbuch 2017) 43.

[23] Vgl *Schreyögg/Geiger*, Organisation, 468f.

[24] Vgl *Welge/Al-Laham/Eulerich*, Strategisches Management, 43f.

Der Grund dafür ist, dass die Behandlung von Principal-Agent-Fragen ein Problem jeder Vertragsbeziehung darstellen und daher von universaler Natur sind. Das Agency-Problem „[...] *ist grundlegend für jede Art der Organisation und ihre Innenbeziehungen, solche zwischen Aktionären und Management, den verschiedenen Ebenen des Managements ebenso wie solche zwischen den Aktionären und einem vorhandenen Aufsichtsorgan.*“[25]

Die Beziehungen zw Principal (Auftraggeberin) und Agent (Auftragnehmerin) sind dabei dadurch gekennzeichnet, dass die Auftraggeberin Entscheidungskompetenzen an die Auftragnehmerin delegiert, diese aber nicht unbedingt im Interesse der Auftraggeberin handelt. Die Auftragnehmerin verfolgt entsprechend der Annahmen ihre eigenen Interessen und wird den Auftrag deswegen nur optimal erfüllen, wenn sich ihre Interessen mit jenen der Auftraggeberin decken. Das Problem besteht dabei darin, dass die Principal aufgrund asymmetrisch verteilter Information weder vor Vertragsabschluss (Adverse-Selection-Problematik) noch nach Vertragsabschluss (Moral-Hazard- / Hold-up-Problematik) beurteilen kann, ob die Agentin in seinem Sinne handeln wird bzw gehandelt hat.[26]

Die nachfolgende Abbildung veranschaulicht das:

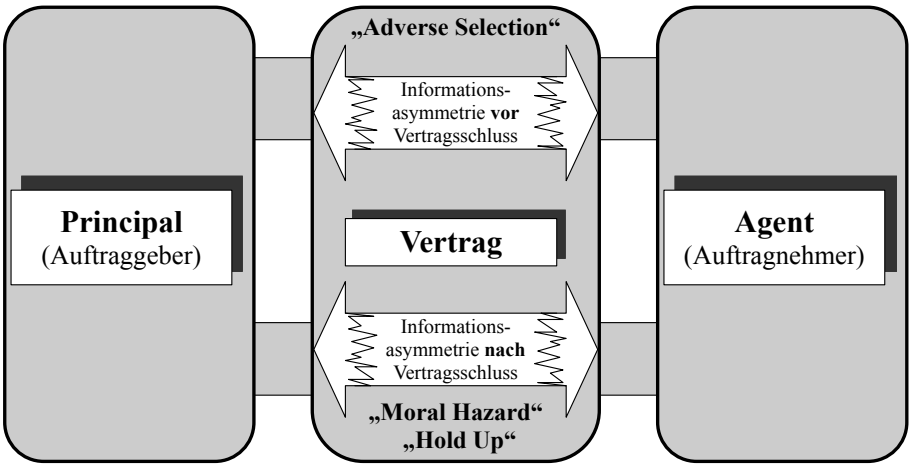


Abbildung 4: Darstellung der Principal-Agent-Problematik[27]

[25] *Schwieters*, Corporate Governance, 36.

[26] Vgl *Welge/Al-Laham/Eulerich*, Strategisches Management, 50f.

[27] *Welge/Al-Laham/Eulerich*, Strategisches Management, 50.

Die obige Darstellung betont auch, dass die Informationsasymmetrien vor oder nach dem Vertragsschluss auftreten können. Informationsasymmetrien, die vor dem Vertragsabschluss entstehen können, sind „hidden characteristics“ (die Agentin kennt die charakteristischen Eigenschaften der angebotenen Leistung, die Principal nicht) und „adverse selection“ (durch unterschiedlichen Informationsstand kommt es zu einer systematischen „Negativauswahl“, bspw sind Autofahrerinnen mit hoher Unfallgefahr eher geneigt, Versicherungen abzuschließen als Autofahrerinnen mit geringer Unfallgefahr) zu nennen. Die wesentlichen Informationsasymmetrien, die nach dem Vertragsabschluss vorkommen, sind „hidden action“ (verborgene Handlungen, bei denen die Principal kaum in der Lage ist, die Agentin zu kontrollieren), „hidden information“ (Principal kann zwar die erbrachte Leistung beurteilen, aber nicht deren Qualität) und „moral hazard“ (Agentin nutzt die ihr zugestandenen Handlungsspielräume aus „hidden action“ und „hidden information“ aus).[28]

Wie die nachstehende Tabelle beispielhaft veranschaulicht, gibt es die Principal-Agent-Problematik in verschiedensten Konstellationen.

Tabelle 1: Principal-Agent-Beziehungen[29]

Principal	**Agent**	**Aufgabe**
Vorgesetzte	Untergeordnete Mitarbeiterin	Engagierte Befolgung der Anordnung
Kreditgeberin	Aktionärinnen bzw Management	Umsichtige Verwendung der finanziellen Mittel
Vermieterin	Mieterin	Werterhaltende Instandsetzung des Hauses
Wählerin	Politikerin	Effiziente Bereitstellung öffentlicher Güter
Politikerin	Bürokratin	Effiziente verwaltungstechnische Umsetzung der politischen Entscheidungen

[28] Vgl *Welge/Al-Laham/Eulerich*, Strategisches Management, 51ff.

[29] *Erlei/Leschke/Sauerland*, Institutionenökonomik (2016) 72.

Für die vorliegende Arbeit sind die Principal-Agent-Beziehung innerhalb eines Unternehmens (und ggf jene zu den Aufsichtsorganen wie bspw den Aufsichtsrat in einer Aktiengesellschaft) am relevantesten.

4.2.3.2 Laterale Organisationsmodelle

Eine Reihe neuerer Konzepte setzt zentral an der formalen (bürokratischen) Ordnung als Symbol überkommener und in der Konsequenz demotivierender Organisationsstrukturen an. All diese Modelle haben ein hohes Maß an Mitarbeitermotivation, Kompetenz und Eigenverantwortung als Ausgangspunkt. Herzstück der meisten dieser Modelle ist die Einrichtung weitgehend selbständig agierender kohäsiver Teams, die sich aus hoch motivierten und kompetenten Individuen zusammensetzen. Viele Probleme, die vormals mit organisatorischen Regelungen gelöst wurden, sollen in die Hände kompetenter und intrinsisch motivierter Mitarbeiter und Teams gelegt werden - mit dem Ziel, dass die sich ergebenden Ordnungen effektiver sind als die formalen Ordnungsstrukturen.
Diese optimistischen Erwartungen decken sich nicht immer mit den empirischen Befunden - diese Modelle sind nur dann erfolgreich, wenn bestimmte Voraussetzungen gegeben sind.[30]
In der Literatur sind verschiedene laterale Organisationsmodelle zu finden, bspw Empowerment, horizontale Kooperation, Vernetzte Projektgruppen uvm zu finden. Auch im Teilbereich der "Selbstorganisation" haben sich verschiedene Modelle etabliert. Beispiele dafür sind Soziokratie, Holacracy, Teal Organisations und das Semco-Modell. Auch im agilen Projektmanagement wird Selbstorganisation eingesetzt.

Selbstorganisation

"*Wer hierarchische Strukturen abbaut ohne neue Regeln vorzugeben, landet im Chaos.*"

(Frederic Laloux)

Selbstorganisation – was ist das eigentlich?

Selbstorganisation bedeutet, dass ein Team Aufgaben übernimmt, die traditionell der Führungskraft vorbehalten sind. Die Teammitglieder organisieren sich selbst, gestalten

[30] Vgl *Schreyögg/Geiger*, Organisation, 167.

ihren Arbeitsalltag eigenständig, übernehmen Verantwortung und haben weitreichende Entscheidungsbefugnisse. Dabei entfallen klassische Hierarchien. Diese Organisationsform integriert Führungsaufgaben direkt in das Team. Selbstorganisation kann entweder auf Unternehmensebene, in einzelnen Teams oder in spezifischen Projekten umgesetzt werden.[31]

Als Beispiel wird häufig Morning Star, ein kalifornisches Unternehmen in der Lebensmittelindustrie, das auf Selbstorganisation setzt, angeführt. Es möchte laut seinem Leitbild ein Unternehmen schaffen, in dem alle Teammitglieder "*selbstbestimmte Beschäftigte sind, die Kommunikation und Koordination mit ihren Kollegen, Kunden Lieferanten und Branchenkollegen ohne Vorgaben von anderen selbst in die Hand nehmen.*"[32]

Wie aus den obigen Zitaten hervorgeht, gibt es unterschiedliche Ansätze zur Selbstorganisation.
Um Selbstorganisation erfolgreich umzusetzen, sind jedoch bestimmte Regeln erforderlich. Wer die Potenziale der Selbstorganisation wirklich nutzen möchte, braucht klar definierte und formalisierte Regeln, Rollen und Prozesse. Brinkmann und Lang betonen, dass Selbstorganisation nur dann gelingen kann, wenn auf drei Ebenen klare und widerspruchsfreie Rahmenbedingungen geschaffen werden: auf der Ebene der Architektur, die sich mit der Gestaltung von Räumen befasst, auf der Ebene der Aufbau- und Ablauforganisation, die die Strukturen regelt, und auf der Ebene der Kooperation, die die Kommunikation gestaltet.[33]

In einigen Formen der Selbstorganisation können Hierarchien in veränderter Form weiterhin bestehen. Ein Beispiel hierfür ist Holacracy, die als „Hierarchie der Kreise“

[31] Vgl *Knebel/Grätsch*, Selbstorganisation im Unternehmen: Was ist das? Wie funktioniert’s? <https://www.berlinerteam.de/magazin/so-funktioniert-selbstorganisation-im-unternehmen-die-10-grundlagen/>, zuletzt aufgerufen am 20.01.2025.

[32] *Hamel*, Schafft die Manager ab!, Harvard Business manager (2012) 27.

[33] Vgl *Lang/Brinkmann*, Selbstorganisation braucht klare Regeln, Frankfurter Allgemeine 2018, 18.

organisiert ist. Hier sind Hierarchien nicht vollständig abgeschafft, sondern werden in einer anderen Struktur umgesetzt, die dennoch Einfluss und Entscheidungsbefugnisse ordnet.[34]

Gründe für Selbstorganisation

Als Gründe für Selbstorganisation werden bspw eine Steigerung der Mitarbeitermotivation und eine schnellere Reaktionsfähigkeit angeführt.[35]

Vor allem die schnelle Reaktionsfähigkeit scheint in den letzten Jahrzehnten zunehmende Bedeutung zu erlangen. Eine Google-Suche nach dem Satz "Wir leben in einer immer komplexer werdenden Welt" bringt sehr viele Suchergebnisse. Auch wenn das wohl lediglich ein subjektives Gefühl darstellt, der Begriff "Komplexität" oftmals nicht genauer definiert ist, und die zunehmende Komplexität - und der damit verbundene Eindruck der stetig steigenden Dynamik - als Erscheinung der letzten Jahrzehnte bezweifelt wird[36], so könnte das dennoch mit ein Grund für den Einsatz von Selbstorganisation sein.

Holokratie – Holacracy

Holacracy basiert auf dem Ansatz, dass Stellenbeschreibungen durch Rollen ersetzt werden. Holacracy unterscheidet zwischen Rollen und den Menschen, die diese Rollen erfüllen. Eine Person kann zu einem bestimmten Zeitpunkt mehrere Rollen haben. Die Rollen werden von sogenannten Kreisen über einen kollektiven Governance-Prozess regelmäßig neu definiert, um sie den sich ständig ändernden Anforderungen des Unternehmens anzupassen. Holacracy strukturiert die verschiedenen Rollen im Unternehmen durch ein System von sich selbst organisierenden Kreisen, die hierarchisch angeordnet sind. Jeder Kreis ist einem klaren Zweck zugeordnet und dem über ihm liegenden größeren Kreis verantwortlich. Allerdings hat jeder Kreis die Befugnis, sich intern in der Art selbst zu organisieren, dass er seinen Zweck bestmöglich erfüllt.[37]

Dabei greift Holacracy mit seinem dritten Weg zwischen autokratischer und demokratischer Arbeitsorganisation stark in die Organisationsstrukturen eines

[34] Vgl Holacracy: Die Hierarchie der Kreise <https://www.zukunftsinstitut.de/zukunftsthemen/holacracy-die-hierarchie-der-kreise> (2024), zuletzt aufgerufen am 20.01.2025.

[35] Vgl *Knebel/Grätsch*, Selbstorganisation im Unternehmen: Was ist das? Wie funktioniert's?

[36] Vgl *Kühl*, Die agile Organisation ist kalter Kaffee <https://www.humanresourcesmanager.de/content/die-agile-organisation-ist-kalter-kaffee/> (2017), zuletzt aufgerufen am 20.01.2025.

[37] Vgl Holacracy: Die Hierarchie der Kreise.

Unternehmens ein. Während es bei agilen Methoden möglich ist, diese nur in Teilen eines Unternehmens einzusetzen, hat Holacracy in seiner Reinform den Anspruch, das gesamte Unternehmen diesem Prinzip unterzuordnen.[38]

4.3 Psychologische Konstrukte

4.3.1 Psychologischer Vertrag

Wenn sich jemand zu einer Arbeitsleistung für einen anderen verpflichtet, liegt ein Arbeitsvertrag vor. Darin werden die Rechte und Pflichten der Vertragspartner definiert. Üblicherweise versuchen beide Vertragspartner all ihre Erwartungen in den Verträgen zu definieren. Nicht zuletzt aufgrund des Wandels von Organisationen, und der damit einhergehenden Schwierigkeiten Anforderungen und Erwartungen exakt zu definieren, kann eine Unzahl an Erwartungen und Leistungen in diesen Verträgen nicht geregelt werden. Das führt dazu, dass die verbleibenden Lücken sowohl durch den Arbeitnehmer als auch durch den Arbeitgeber subjektiv interpretiert werden.

Zusätzlich zum rechtlichen Arbeitsvertrag (der natürlich formal gültig ist) entsteht daher ein psychologischer Arbeitsvertrag, der real den formalen Vertrag zu einem gewissen Teil verdrängt. Das Konzept des psychologischen Arbeitsvertrages beschreibt jene mehr oder weniger impliziten Erwartungen und Angebote, die über den juristischen Vertrag hinausgehen. Beispielsweise gehören die vom Arbeitnehmer tatsächlich erbrachte Arbeitsleistung, die Qualität dieser Leistung und das Engagement des Arbeitnehmers dazu. Die Verletzung des psychologischen Vertrags ist dabei wohl das wichtigste Element um zu verstehen, wie sich diese Verträge auf die Empfindungen, die Einstellung und das Verhalten von Mitarbeitern auswirkt. Abgeleitet vom Bruch eines rechtlichen Vertrages, tritt ein Bruch des psychologischen Vertrages dann auf, wenn aus Sicht einer der Vertragsparteien die Versprechungen der anderen Partei nicht erfüllt werden. Eine Verletzung des psychologischen Vertrages kann zu einer inneren Kündigung führen.[39]

[38] Vgl *Schermuly*, Holacracy: Die holokratische Organisation <https://www.haufe.de/personal/hr-management/new-work-moderne-formen-der-arbeitsgestaltung/holacracy-die-holokratische-organisation_80_406704.html> (2020), zuletzt aufgerufen am 22.01.2025.

[39] Vgl *Lehner*, Arbeitsplatzsicherheit, Organisationales Commitment, Organizational Citizenship Behavior sowie Radikales Value und Performancemanagement: Ergebnisse einer empirischen Studie bei der Telekom Austria (2011).

4.3.2 Organisationales Commitment

Über organisationales Commitment gibt es eine Vielzahl an wissenschaftlichen Arbeiten. Die meisten dieser Abhandlungen betrachten organisationales Commitment als eine Bestimmte Form der Bindung zwischen Mitarbeiter und einem Unternehmen, eine Art psychologisches Band.

Organisationales Commitment wird oft in drei verschiedene Formen unterteilt:

- Affektives Commitment: Die emotionale Verbindung zu einer Organisation
- Normatives Commitment: Die moralische Verpflichtung in einer Organisation zu verbleiben
- Kalkulatives (oder fortsetzungsbezogenes) Commitment: Entsteht aufgrund der Wechselkosten, die mit einem Austritt aus der Organisation verbunden sind.[40]

4.3.3 Organizational Citizenship Behaviour und Extra-Rollenverhalten

„Ein Mann, der nicht mehr leistet als das, wofür er bezahlt wird, leistet so wenig, dass er das nicht wert ist, was er bekommt."

(Abraham Lincoln)

Die Aufgaben in Organisationen sind nicht vorhersehbar und planbar, das Verhalten der Mitarbeiter in verschiedene Situationen ist nicht im Voraus erkennbar. Die Bedeutung der Zusatz-Handlungen, die für die Organisation „nutzbringender" sind, steigt. Diese Art von Handlungen, die als „Extra-Rollenverhalten" bezeichnet wird, bringt die Notwendigkeit des über die Norm hinausgehenden Arbeitsverhaltens mit sich. Organizational Citizenship Behaviour (OCB) ist eines der am meisten erforschte Konzepte des Extra-Rollenverhaltens. Organizational Citizenship Behaviour ist ein Konzept, das als freiwilliges, individuelles Arbeitsverhalten außerhalb von Rollenerwartungen und Arbeitsvertrag definiert wird. Ein Verhalten, das nicht vom formalen Entlohnungssystem erfasst wird, fördert die Leistungsfähigkeit der Organisation weiter.[41]

[40] Vgl *Lehner*, Arbeitsplatzsicherheit, Organisationales Commitment, Organizational Citizenship Behavior sowie Radikales Value und Performancemanagement: Ergebnisse einer empirischen Studie bei der Telekom Austria (2011).

[41] Vgl *Lehner*, Arbeitsplatzsicherheit, Organisationales Commitment, Organizational Citizenship Behavior sowie Radikales Value und Performancemanagement: Ergebnisse einer empirischen Studie bei der Telekom Austria (2011).

4.3.4 Vertrauen

In der Literatur sind verschiedene Definitionen von Vertrauen zu finden. Im Kern lässt sich Vertrauen als eine positive Erwartungshaltung gegenüber bestimmten Personen oder abstrakten Systemen definieren, selbst wenn die Möglichkeit besteht, dass diese Erwartungen enttäuscht werden. Ein Zeichen für Vertrauen ist die Bereitschaft, sich freiwillig in eine verletzliche Position zu begeben. Das bedeutet, dass die vertrauende Person oder Organisation dem Verhalten des Gegenübers ausgeliefert ist und potenziell erheblichen Schaden erleiden könnte, ohne dass Schutzmechanismen oder Sanktionen diesen Schaden verhindern würden.[42] Vertrauen kann Menschen ermöglichen, mit riskanten und unsicheren Situationen umzugehen. Es stellt eine Möglichkeit dar, Komplexität zu reduzieren da Menschen nicht mehr jede erdenkliche Möglichkeit in Betracht ziehen müssen.[43]

Betriebswirtschaftliche Überlegungen zur Gestaltung von Organisationen, bspw im Rahmen der Neuen Institutionenökonomie, basieren oft auf einer Opportunismusannahme. Selbst wenn eine Mehrheit der Akteure nicht opportunistisch handelt, so kann dennoch nicht ausgeschlossen werden, dass ein Teil der Akteure versuchen ihren eigenen Nutzen zu optimieren. In einer Organisation kann es deswegen notwendig sein, die Mehrheit der nicht-opportunistisch handelnden Akteure von der Minderheit der opportunistisch handelnden Akteure zu schützen. Vor allem bei jenen Akteuren, bei denen affektives Commitment (vgl oben) gering ausgeprägt ist und kalkulatives Commitment stark ausgeprägt ist. Hier muss der Rückgriff auf Vertrauen kritisch hinterfragt werden.
Dass Vertrauen als Organisationsparadigma zunehmend an Bedeutung gewinnt, zeigt auch folgender Satz von Laloux:

"Weil es kein mittleres Management und nur wenig Unterstützungsfunktionen gibt, verzichten evolutionäre Organisationen auf die gewohnten Kontrollmechanismen und arbeiten stattdessen aus einem geteilten Vertrauen."[44]

[42] Vgl *Eberl*, Vertrauen innerhalb von Organisationen – eine organisationstheoretische Betrachtung, in *Maring* (Hrsg), Vertrauen — zwischen sozialem Kitt und der Senkung von Transaktionskosten (KIT Scientific Publishing 2010) 239–255 (239).

[43] Vgl *Corritore/Kracher/Wiedenbeck*, On-line trust: concepts, evolving themes, a model, International journal of human-computer studies 2003, 737–758 (738).

[44] *Laloux*, Reinventing Organizations: ein Leitfaden zur Gestaltung sinnstiftender Formen der Zusammenarbeit (2015) 80.

Nicht nur bei zwischenmenschlichen Beziehungen und in der Gestaltung von Organisationen spielt Vertrauen eine Rolle. Auch bei der Gestaltung von Kundenbeziehungen ist Vertrauen einerseits für die Bindungsstärke relevant, andererseits kann es durch die Komplexitätsreduktion zu einer Verbesserung der Interaktionseffizienz kommen.[45]

Das Konstrukt Vertrauen ist daher in dieser Arbeit in zweierlei Hinsicht relevant. Einerseits in der Beziehung zwischen Mitarbeitern und dem Unternehmen bzw dessen Führungsebene(n), bei dem Vertrauen eine wichtige Determinante für die Ausgestaltung des Organisationssystems ist.
Andererseits ist Vertrauen in der Beziehung zwischen Kunden und dem Unternehmen wichtig, daher wird dieses Thema weiter unten (Kap 8.2 „Datenschutz als Produkteigenschaft“) nochmal aufgegriffen.

4.4 Zusammenfassung

Zunehmend wird die Maschinenmetapher von Organisationen abgelöst und neue Organisationsformen bilden sich. War es mit der Maschinenmetapher scheinbar einfach, Compliance in Organisationen umzusetzen (man musste ja nur die „Zahnräder“ gut schmieren), sind modernere Sichtweisen auf Organisationen komplexer. Moderne Organisationsformen verlassen sich zumindest teilweise auf Vertrauen zu allen Beteiligten. Es ist davon auszugehen, dass dieses Vertrauen in vielen Fällen gerechtfertigt ist. In manchen Fällen dürfte dieses Vertrauen aber erschüttert werden, bspw wenn der psychologische Vertrag gebrochen wird und sich dadurch das Commitment und das Organizational Citizenship Behaviour von Mitarbeitern ändert oder verloren geht. Hier setzt die Neue Institutionenökonomik, speziell mit der Principal-Agent-Theorie, an und unterstellt mit der Informationsasymmetrie bewusst Opportunismus. Eine von mehreren möglichen Methoden zur Verringerung dieser Informationsasymmetrie ist die Steigerung der Transparenz. Aus Sicht des Autors stellt ein Risikomanagementsystem eine wichtige Methode zur Transparenzsteigerung dar.

[45] Vgl *Bruhn*, Relationship Marketing: das Management von Kundenbeziehungen (Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften 2009) 77.

5 Strategisches Management

5.1 Einleitung

Die zentrale Frage im strategischen Management ist der nachhaltige Unternehmenserfolg. Dabei stehen die grundsätzliche Unternehmensentwicklung, die Ausrichtung des Unternehmens, der langfristige Erfolg und die Schaffung und Nutzung von Erfolgspotentialen und Wettbewerbsvorteilen im Fokus.[46]

Im klassischen Verständnis von Strategie wird eine Strategie als ein geplantes Maßnahmenbündel der Unternehmung zur Erreichung ihrer langfristigen Ziele definiert.

Laut *Welge* et al ist das klassische Strategieverständnis von folgenden Merkmalen geprägt:[47]

- Strategie bestehen aus einer Reihe miteinander verbundener Einzelentscheidungen
- Strategien sind ein hierarchisches Konstrukt
- Strategien treffen Aussagen zur Positionierung der Unternehmung
- Strategien treffen Aussagen zur Ressourcenallokation

Die Schule um Henry Mintzberg übt allerdings Kritik an dieser Rationalitätsprämisse. Für sie sind Strategien nicht notwendigerweise das Ergebnis formaler rationaler Planung. Dementsprechend können Strategien zwar auch als Pläne (Plan), aber auch als List (Ploy), als Muster (Pattern), als Positionierung (Position) oder Denkhaltung (Perspective) gesehen werden. Verdichtet man die Grundmuster der Strategietypen so ergeben sich beabsichtigte (geplante) Strategien, die realisiert wurden, beabsichtigte Strategien, die nicht realisiert wurden und realisierte Strategien, die nicht beabsichtigt waren. Das Konzept von Mintzberg bringt in der Praxis die Herausforderung mit sich, dass durch die konzeptionelle Offenheit wenig Aussagen darüber getroffen werden können, welche Phänomene aus dem Geltungsbereich ausgeschlossen werden können. Im Extremfall können alle Entscheidungen, die aus subjektiver Sicht bedeutend sind, als „strategisch“ bezeichnet werden.[48]

[46] Vgl *Reisinger/Gattringer/Strehl*, Strategisches Management: Grundlagen für Studium und Praxis (2017) 51.

[47] Vgl *Welge/Al-Laham/Eulerich*, Strategisches Management, 18ff.

[48] Vgl *Welge/Al-Laham/Eulerich*, Strategisches Management, 21ff.

5.2 Definition Strategisches Management

In diesem Werk soll der Begriff „Strategisches Management“ im klassischen Sinne verwendet werden und „*[...] als ein Prozess, in dessen Mittelpunkt die Formulierung und Umsetzung von Strategien in Unternehmungen steht*“[49] verstanden werden.

Auch wenn an der Erarbeitung einer Strategie viele Managementebenen und Unternehmensbereiche beteiligt sind, bleibt eine Strategie doch der Plan des Top-Managements um Unternehmensziele zu erreichen. Es kann dabei zwischen verschiedenen Ebenen unterschieden werden. Während Unternehmensstrategien auf der Ebene des Gesamtunternehmens definiert werden, sind auch Strategien auf der Ebene der strategischen Geschäftseinheiten möglich. Dabei sollte man laut Matzler et al Strategie in den Dimensionen Plan, Muster, Position, Perspektive und Manöver verstehen. Strategien werden dabei oft in jene auf Unternehmensebene und, bei Unternehmen mit mehreren strategischen Geschäftseinheiten, in solche auf der Ebene der strategischen Geschäftseinheiten unterteilt.[50]

5.3 Vision / Mission / Strategie

Vision

Die Vision beschreibt wie das Unternehmen in Zukunft aussehen soll, sie beschreibt eine auf die Zukunft ausgerichtete Leitidee. Sie legt damit die Richtungen fest, in die sich ein Unternehmen entwickeln will und stellt dadurch ein wichtiges Führungsinstrument dar, um Werte in einem Unternehmen zu vermitteln und zur Geltung zu bringen.[51]

Mission

Die Mission soll die Fragen nach dem Grund der Existenz des Unternehmens und seinem Grundzweck beantworten. Im Gegensatz zur Vision hat die Mission einen stärkeren Bezug zur Gegenwart und zu den Grundbedürfnissen der verschiedenen Stakeholder.[52]

[49] *Welge/Al-Laham/Eulerich*, Strategisches Management, 24.

[50] Vgl *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management: Konzepte und Methoden (2021) 5ff.

[51] Vgl *Kreikebaum/Gilbert/Behnam*, Strategisches Management (2018) 60ff.

[52] Vgl *Kreikebaum/Gilbert/Behnam*, Strategisches Management, 63.

Strategische und operative Ziele

Basierend auf der Vision, der Mission on den Leitbildern werden die strategischen Ziele erarbeitet. Bei strategischen Zielen handelt es sich um qualitative Ziele. Es soll dabei die Frage „Was soll erreicht werden?“ beantwortet werden. Außerdem werden hier Art und Richtung der Ziele festgelegt. Basierend auf den strategischen Zielen werden die operativen Ziele definiert. Operative Ziele sollten Zielausmaß, zeitlichen, räumlichen, personellen und Ressourcen Bezug aufweisen.[53] Die nachfolgende Grafik veranschaulicht das:

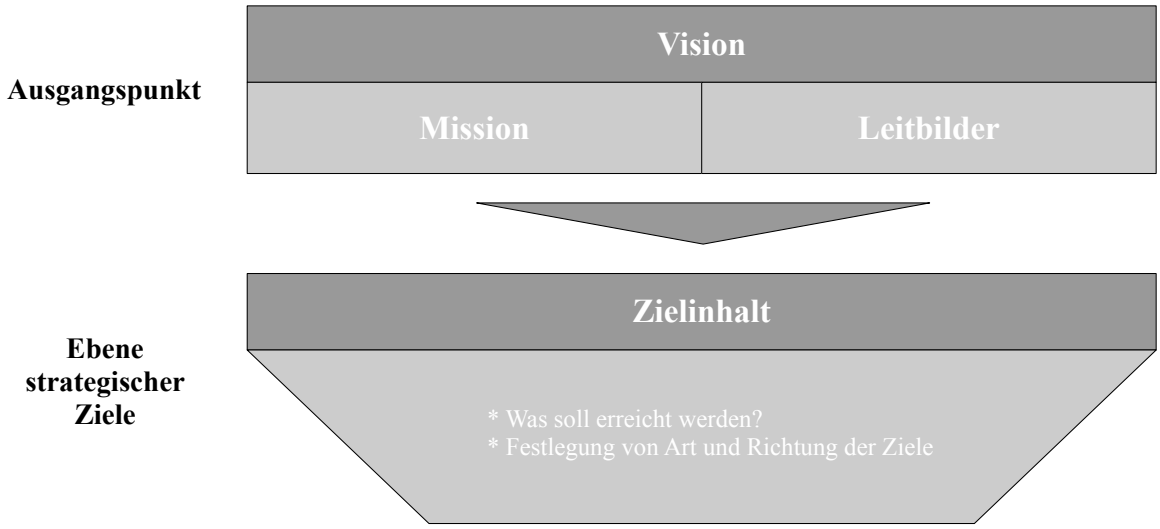


Abbildung 5: Zusammenhang von strategischen und operativen Zielen[54]

5.4 Strategieprozess

Passend zum oben beschriebenen Prozesscharakter des strategischen Managements (im Gegensatz zum Mintzberg’schen Modell) findet man in der Literatur werden verschiedene Prozessmodelle. Diese Modelle unterscheiden sich hauptsächlich hinsichtlich der

[53] Vgl *Kreikebaum/Gilbert/Behnam*, Strategisches Management, 73.

[54] *Kreikebaum/Gilbert/Behnam*, Strategisches Management, 73.

Gliederung der verschiedenen Prozessschritte. Manche dieser Prozessmodelle integrieren die Erarbeitung von Vision/Mission stärker in den Strategieprozess als andere.[55]

Hier sei beispielhaft ein sehr einfaches Prozessmodell beschrieben:

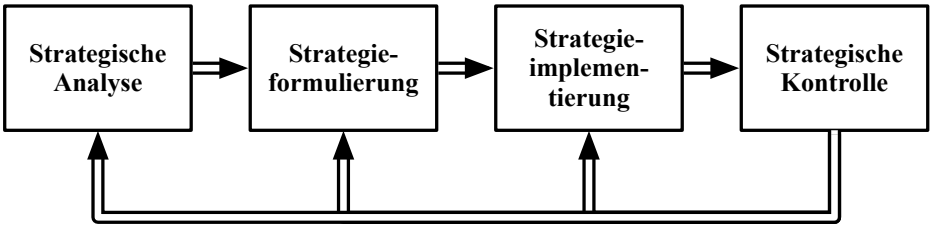


Abbildung 6: Ein einfaches Strategieprozessmodell[56]

Diesem Prozess folgend werden in den nächsten Kapiteln die einzelnen Schritte beschrieben. Entsprechend der Zielsetzung dieser Arbeit werden dabei verschiedene Prozessschritte umfangreicher, andere nur rudimentär beschrieben.

5.5 Strategische Analyse

Um strategische Entscheidungen treffen zu können, sind natürlich unternehmerisches Gespür und Kreativität notwendig. Zusätzlich ist es aber notwendig, ein möglichst umfassendes Verständnis über die Besonderheiten des Unternehmens und seiner Umwelt zu haben.[57] Deswegen ist für die Erarbeitung einer Strategie eine Positionsbestimmung, dh eine strategische Analyse der betrachteten Entität (bspw Gesamtunternehmen oder Geschäftsbereich), notwendig. Der strategische Handlungsspielraum ergibt sich aus dieser Analyse, dadurch wird das Terrain, auf dem das Unternehmen mit seinen Geschäftseinheiten in Zukunft operieren kann, bestimmt.[58]
Dazu sind in der Literatur verschiedenste Ansätze zu finden, bspw SWOT-Analyse (Strength-Weaknesses-Opportunities-Threats) oder PESTLE-Analyse (Political-

[55] Vgl *Kreikebaum/Gilbert/Behnam*, Strategisches Management; *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management; *Reisinger/Gattringer/Strehl*, Strategisches Management; *Welge/Al-Laham/Eulerich*, Strategisches Management.

[56] *Reisinger/Gattringer/Strehl*, Strategisches Management, 44.

[57] Vgl *Reisinger/Gattringer/Strehl*, Strategisches Management, 56.

[58] Vgl *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management, 7f.

Economic-Social-Technological-Legal-Environmental). Teil einer Analyse sollte immer auch eine Stakeholderanalyse sein.[59]

5.6 Strategieformulierung

Im Zuge der Strategieformulierung werden, basierend auf den Ergebnissen der Analysen, zunächst strategische Optionen entwickelt. Aus diesen Optionen werden jene ausgewählt, die versprechen, die Unternehmensziele am besten zu erreichen.[60]
Eine Geschäftsbereichsstrategie wollte dabei Antworten auf folgende Fragen geben:[61]
Wer: Wer sind unsere Kunden? Was sind unsere Produkte?
Wo: Wo sind unsere Zielmärkte?
Wie: Wie schaffen wir Mehrwert für unsere Kunden und wie differenzieren wir uns von den Konkurrenten?
Was: Was müssen wir dafür tun?
Wann: Was sind der Zeitplan und die Abfolge der einzelnen Schritte?
Warum: Warum verdienen wir damit Geld? Was ist unser Geschäftsmodell?

5.7 Strategieimplementierung

Basierend auf den im Zuge der Strategieformulierung definierten Optionen werden bei der Strategieimplementierung geeignete Maßnahmen umgesetzt.[62]

Eines von verschiedenen Werkzeugen für die Strategieimplementierung ist die Verwendung einer Balanced Scorecard. Dieses Werkzeug wird nachfolgend beschrieben da es aus Sicht des Autors für die Bestimmung der Ziele, und dadurch auch der Erkennung von Risiken diese Ziele nicht einzuhalten, ein wertvolles Werkzeug darstellt.

[59] Vgl *Kreikebaum/Gilbert/Behnam*, Strategisches Management; *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management; *Reisinger/Gattringer/Strehl*, Strategisches Management; *Welge/Al-Laham/Eulerich*, Strategisches Management.

[60] Vgl *Reisinger/Gattringer/Strehl*, Strategisches Management, 44.

[61] Vgl *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management, 137.

[62] Vgl *Reisinger/Gattringer/Strehl*, Strategisches Management, 44.

Balanced Scorecard

„Ein Unternehmen rein nach finanziellen Kennzahlen zu führen, ist vergleichbar mit dem Fahren von 100km/h auf einer Autobahn, nur mit Hilfe des Rückspiegels.“[63]

Die Balanced Scorecard entstand aus der Spannung zwischen dem Druck, Wettbewerbsvorteile zu schaffen, und der Treue zu einem traditionellen, auf historischen Werten basierenden Rechnungswesenmodell. Sie stellt eine Synthese dar, die es ermöglicht, beide Ansätze zu vereinen. Dieses Managementinstrument übersetzt die Vision und Strategie eines Unternehmens in ein kohärentes Set von Leistungskennzahlen. Es erweitert klassische finanzielle Kennzahlen, die vergangene Leistungen bewerten, um Faktoren, die zukünftige Erfolge beeinflussen. Dabei integriert die Balanced Scorecard strategische Maßnahmen und verbindet historische Finanzdaten mit zukünftigen Leistungstreibern. Die Kennzahlen der Balanced Scorecard decken neben den finanziellen Kennzahlen die Perspektiven Kunde, interne Geschäftsprozesse, Lernen und Wachstum ab. Sie basieren auf einer klaren und kompromisslosen Umsetzung der Unternehmensstrategie in konkrete Ziele und Maßnahmen, die die langfristige Entwicklung des Unternehmens fördern.[64]

In der folgenden Grafik werden die vier Ebenen der Balanced Scorecard beispielhaft dargestellt:

[63] *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management, 174.

[64] Vgl *Kaplan/Norton*, Balanced Scorecard: Strategien erfolgreich umsetzen (Management-Klassiker 2024).

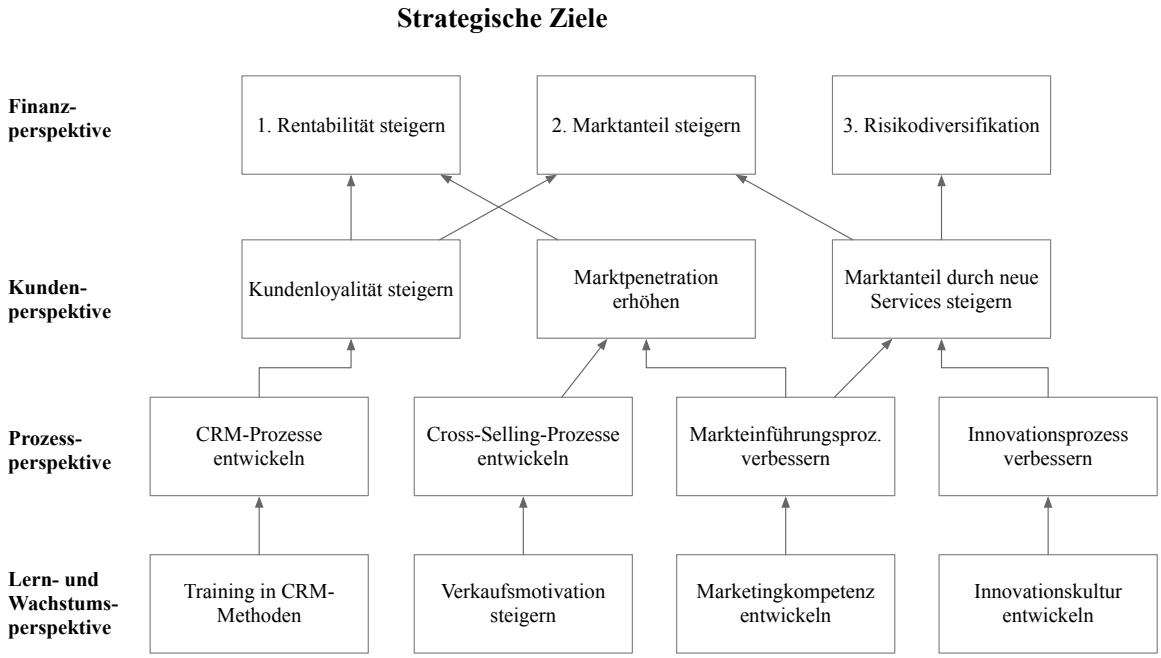


Abbildung 7: Strategiebaum[65]

Die Balanced Scorecard dient als Grundlage, um Unternehmensziele konkret umzusetzen. Sie übersetzt die Mission und Strategie einer Organisationseinheit in greifbare Ziele und messbare Kennzahlen. Nachdem die strategischen Ziele in den vier Perspektiven der Balanced Scorecard definiert wurden, erfolgt die Festlegung spezifischer Kennzahlen, messbarer Zielvorgaben und Projekte. Darüber hinaus spielt die Balanced Scorecard eine zentrale Rolle bei der Kommunikation: Sie schafft eine gemeinsame Basis, um die Strategie einer Organisationseinheit klar zu vermitteln und das Engagement sowie die Zustimmung auf der Führungsebene sicherzustellen.[66]

5.8 Strategische Kontrolle

Letztlich werden die implementierten Maßnahmen auf den Grad ihrer Umsetzung und ihre Wirksamkeit überprüft. Dadurch erhalten auch die Akteure Feedback und können entsprechende Anpassungen durchführen.[67]

[65] *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management, 176.

[66] *Kaplan/Norton*, Balanced Scorecard; Vgl *Matzler/Müller-Seeger/Hautz/Mooradian*, Strategisches Management.

[67] Vgl *Reisinger/Gattringer/Strehl*, Strategisches Management, 44.

5.9 Zusammenfassung

Genauso wie eine Strategie (und ein strategisches Management) auf Unternehmensebene wichtig ist, ist sie auch für den Teilbereich Datenschutz wichtig. Neben der Lenkungs- und Kommunikationsfunktion einer Strategie sind auch viele Methoden, die für die Entwicklung und Implementierung einer Unternehmensstrategie eingesetzt werden, wie bspw die Positionsbestimmung des Unternehmens und der Umwelt (inkl Stakeholder), in abgewandelter Form auch für die Entwicklung einer Datenschutzstrategie hilfreich. Auch die Balanced Score Card kann im Bereich Datenschutz gut eingesetzt werden. Einerseits hilft sie durch die vier verschiedenen Ebenen den Blick nach vorne zu richten anstatt nur in den „Rückspiegel“ zu schauen und bspw lediglich bereits über das Unternehmen verhängte Geldbußen zu berücksichtigen. Andererseits erweitert sie (unter anderem durch die Ebene der Kundenperspektive) auch das Blickfeld. Es können neben Compliance-Vorgaben auch andere für Datenschutz wichtige Faktoren wie bspw das Kundenvertrauen miteinbezogen werden. Die Balanced Score Card liefert dabei zusätzlich die Basis für die Definition operativer Ziele. Diese wiederum helfen bei der Steuerung und Kontrolle der Umsetzung – nicht nur auf Unternehmensebene, sondern auch im Bereich Datenschutz.

6 Grundlagen Risikomanagement

6.1 Einleitung

6.1.1 Entscheiden unter Unsicherheit

Da die Zukunft nie vollständig vorhersehbar ist, stehen Unternehmen oft vor Entscheidungen unter Unsicherheit. In solchen Situationen ist ein bewusster Umgang mit diesen Unsicherheiten von großer Bedeutung. Unternehmen sind immer sowohl Chancen als auch Gefahren ausgesetzt, die zu Abweichungen von geplanten Zielen führen können. Die Fähigkeit, mit diesen Risiken umzugehen, ist entscheidend für den Erfolg eines Unternehmens. Ein systematischer Ansatz, der sowohl Chancen als auch Risiken berücksichtigt, wird als Risikomanagement bezeichnet. Dabei handelt es sich um eine strukturierte Herangehensweise, um Unsicherheiten aktiv zu identifizieren, zu bewerten und entsprechend darauf zu reagieren.[68]

Ein strukturiertes Risikomanagement kann dazu beitragen, die Planungssicherheit zu verbessern. Da die Zukunft stets sowohl Risiken[69] als auch Chancen birgt, ermöglicht die Einführung eines Risikomanagementsystems (RMS), die strategische und operative Unternehmensplanung gezielter und sicherer zu gestalten.[70]

6.1.2 Risikomanagement als umfassende Aufgabe

Risikomanagement wird allgemein als eine sehr umfangreiche Aufgabe verstanden. Es geht dabei weit über die bloße Erfüllung gesetzlicher Vorgaben, den Abschluss von Versicherungen oder das Erstellen von Notfallplänen hinaus. Vielmehr umfasst Risikomanagement einen ganzheitlichen Prozess, der alle potenziellen Risiken identifiziert, bewertet, zusammenführt, überwacht und aktiv steuert, um Abweichungen von den gesetzten Zielen zu vermeiden. Infolge verschiedener Krisen, wie der Finanzkrise 2007-2008, ist der Druck auf Unternehmen deutlich gestiegen. Externe Akteure wie Gesetzgeber,

[68] Vgl *Gleißner*, Grundlagen des Risikomanagements: Handbuch für ein Management unter Unsicherheit (Management competence 2022); *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation: Schlüsseltechnologie für Risikomanagement und Controlling (Essentials 2019).

[69] Der Begriff "Risiken" ist hier als "Risiken im engeren Sinne" zu verstehen. Siehe dazu auch Kap 6.2 „Grundbegriffe".

[70] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 31.

Kapitalmärkte und Banken haben in den letzten Jahrzehnten erheblich dazu beigetragen, die Führungs- und Überwachungssysteme von Unternehmen zu verbessern. In Deutschland hat besonders das KonTraG dazu geführt, dass das Fehlen eines Risikomanagementsystems bei großen Kapitalgesellschaften erhebliche Konsequenzen haben kann, einschließlich einer möglichen persönlichen Haftung von Geschäftsführern oder Vorständen.[71]

6.1.3 Erreichung von Zielen

Viele Unternehmen sehen mittlerweile den Nutzen von Risikomanagement für die Erreichung ihrer strategischen Ziele. Statt es lediglich zur Erfüllung gesetzlicher Vorgaben zu verwenden, möchten sie Risikomanagement zunehmend als Werkzeug zur Verbesserung ihrer Führungs- und Steuerungsprozesse einsetzen. Ihr Ziel ist es, Risikomanagement nahtlos in die strategische Planung und das Performance Management zu integrieren.[72]

6.1.4 Dynamik der „Digitalisierung“

Die zunehmende Dynamik der Digitalisierung erhöht den Druck auf Unternehmen, ein effektives Risikomanagement sowohl strategisch als auch operativ zu etablieren. In einem immer schnelllebigeren Umfeld, in dem Digitalisierung und Disruption zentrale strategische Herausforderungen darstellen, verlagern viele Unternehmen ihren Fokus im Risikomanagement. Statt sich primär auf kurzfristige Risiken zu konzentrieren, richten sie ihre Aufmerksamkeit auf strategische Bedrohungen. Ihr Ziel ist es, das Risikomanagement eng in die strategischen und operativen Steuerungsprozesse und Methoden einzubinden.[73]

6.1.5 Vom Management von Einzelrisiken zur Gesamtrisikoposition

Die Herangehensweise im Risikomanagement wandelt sich: Statt ausschließlich einzelne Risiken isoliert zu betrachten, rückt zunehmend die Berücksichtigung von Abhängigkeiten zwischen Risiken und der gesamten Risikoposition in den Fokus. Fortschrittliche Unternehmen haben erkannt, dass das bisherige Management von Einzelrisiken aus

[71] *Gleißner*, Grundlagen des Risikomanagements; Vgl *Exner/Ruthner*, Corporate Risk Management: unternehmensweites Risikomanagement als Führungsaufgabe (Linde international 2019).

[72] Vgl *Exner/Ruthner*, Corporate Risk Management, V.

[73] Vgl *Exner/Ruthner*, Corporate Risk Management, V.

strategischer Perspektive nicht ausreicht, um Innovation und Wachstum zu fördern und gleichzeitig die Qualität der Unternehmensleistung zu sichern.[74]
Weitere Entwicklungsstufen werden in Kap 6.7 „Status und Zukunftsbild des Risikomanagements“ dargestellt.

6.1.6 Integration ins Führungssystem

Daraus folgt, dass Risikomanagement ein integraler Bestandteil des Führungssystems eines Unternehmens sein muss. Es zeigt sich immer deutlicher, dass ein ganzheitlicher, risikoorientierter Ansatz in der Unternehmensführung notwendig ist. Dies umfasst die Verknüpfung von Risikomanagement und Controlling, um unter anderem die Planungssicherheit zu erhöhen. Die Weiterentwicklung moderner Risikomanagement-Konzepte zielt darauf ab, alle unternehmerischen Risiken umfassend zu managen – einschließlich der Berücksichtigung von Wechselwirkungen zwischen Risiken – und das Risikomanagement nahtlos in das Führungssystem des Unternehmens zu integrieren.[75]

6.1.7 Risikomanagement als Querschnittsmaterie

Risikomanagement entwickelt sich zunehmend zu einer bereichsübergreifenden Aufgabe. Zu Beginn des 21. Jahrhunderts wird es als Querschnittsfunktion innerhalb von Unternehmen betrachtet. Seine theoretischen Grundlagen werden interdisziplinär erforscht und weiterentwickelt, wobei Disziplinen wie Statistik, Betriebswirtschaftslehre, Simulationsmethoden und Psychologie eine zentrale Rolle spielen.[76]

6.1.8 Vorteile von Risikomanagement

Risikomanagement bringt zahlreiche wirtschaftliche Vorteile mit sich, darunter die Reduzierung von Risikokosten und eine fundiertere Vorbereitung auf unternehmerische Entscheidungen. Gleißner führt folgende Vorteile für Risikomanagement an:[77]

- Transparenz über die Risikosituation
- Frühaufklärung und Krisenprävention
- Reduzierung der Risikokosten

[74] Vgl *Exner/Ruthner*, Corporate Risk Management, XIX.

[75] Vgl *Gleißner*, Grundlagen des Risikomanagements; *Exner/Ruthner*, Corporate Risk Management.

[76] Vgl *Gleißner*, Grundlagen des Risikomanagements, 3.

[77] Vgl *Gleißner*, Grundlagen des Risikomanagements, 4f.

- Bessere Informationsgrundlage bei Entscheidungen unter Unsicherheit
- Verbesserung der Robustheit des Unternehmens

6.1.9 Risikominimierung vs. Risiken als Werttreiber

Risiken werden bisher häufig nicht als potenzielle Wertschöpfungsfaktoren erkannt, sondern entweder ignoriert oder ausschließlich auf ihre Minimierung hin betrachtet. Versucht man jedoch, Risiken vollständig zu eliminieren, können die dafür entstehenden Kosten exponentiell ansteigen. Das Risikomanagement hingegen hilft Unternehmen, eine fundierte Balance zwischen erwarteten Erträgen und Risiken zu finden und so bei wichtigen Entscheidungen eine fundierte Bewertung vorzunehmen.[78]

6.2 Grundbegriffe

6.2.1 Risiko, Unsicherheit und Ungewissheit

Der Begriff "Unsicherheit" umfasst sowohl Risiko als auch Ungewissheit. Bei Entscheidungen unter Risiko sind die Wahrscheinlichkeiten für mögliche zukünftige Szenarien bekannt, während diese bei Entscheidungen unter Ungewissheit unbekannt sind. Dennoch können verschiedene Unsicherheitsgrade immer auf objektive Wahrscheinlichkeiten zurückgeführt werden. Fehlen beispielsweise konkrete Informationen über die Eintrittswahrscheinlichkeit, kann angenommen werden, dass alle Szenarien gleich wahrscheinlich sind. Daher ist eine detaillierte Unterscheidung zwischen Risiko und Ungewissheit oft nicht erforderlich.[79]

Im allgemeinen Sprachgebrauch wird der Begriff „Risiko" oft sowohl für die eigentliche Risikosituation als auch für die Ursache oder die Folgen eines schädlichen Ereignisses verwendet. Er kann sich somit auf jede Phase eines Ursache-Wirkungs-Zusammenhangs beziehen, wird jedoch meist mit einer negativen Entwicklung oder Gefahr in Verbindung gebracht. Die Psychologie beschäftigt sich mit dem Umgang mit Risiken und

[78] Vgl *Gleißner*, Grundlagen des Risikomanagements, 14; *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation, 9.

[79] Vgl *Gleißner*, Grundlagen des Risikomanagements, 20f.

Unsicherheiten, dabei wird der Risikobegriff oft als subjektiver Erwartungswert eines Nutzens oder Schadens definiert.[80]

Psychologische Studien zeigen, dass Menschen den Begriff „Risiko“ je nach Kontext unterschiedlich wahrnehmen und interpretieren. Dabei weicht ihr Verständnis häufig von der betriebswirtschaftlichen Definition ab. Gleißner unterscheidet dabei zw. folgenden Risiken:[81]

- Risiko als unmittelbare Bedrohung (techn. Risiken mit hohem Katastrophenpotential und geringer Eintrittswahrscheinlichkeit, bspw Kernkraftwerke, Staudämme, Chemieanlagen, Erdgaslager),
- Risiko als Schicksalsschlag (natürliche Gefahren mit geringer Eintrittswahrscheinlichkeit, bspw Überschwemmungen, Erdbeben, Vulkanausbrüchen etc.)
- Risiko als Herausforderung der eigenen Kräfte (Risiken, die man durch eigenes Verhalten steuern und meistern kann, bspw Extrembergsteigen, gefährliche Sport- und Freizeitaktivitäten)
- Risiko als Glücksspiel (Abwägung von Wahrscheinlichkeiten für Verlust und Gewinn, bspw Lotterien, Pferdewetten, Börsenspekulation, Abschließen von Versicherungen)
- Risiko als Frühindikator für schleichende Gefahren (Risiken, die man mit den eigenen Sinnesorganen nicht wahrnehmen und bewerten kann, bspw Lebensmittelzusätze, elektromagnetische Felder, ionisierende Strahlung, Pestizidrückstände, Innenraumbelastung, Feinstaub)

In der Wirtschaftswissenschaft wird der Begriff „Risiko“ sowohl in einem weiteren als auch in einem engeren Sinne verwendet. Grundsätzlich wird Risiko jedoch nicht als Erwartungswert, sondern als mögliche Abweichung vom Erwartungswert verstanden.[82]

[80] Vgl *Basel/Henrizi* (Hrsg), Psychologie von Risiko und Vertrauen: Wahrnehmung, Verhalten und Kommunikation (Lehrbuch 2023) 13ff.

[81] Vgl *Gleißner*, Grundlagen des Risikomanagements, 22f.

[82] Vgl *Basel/Henrizi* (Hrsg), Psychologie von Risiko und Vertrauen, 15.

In der Fachliteratur gibt es keine einheitliche Definition des Begriffs „Risiko“. Besonders in älteren Quellen wird Risiko häufig ausschließlich im Zusammenhang mit negativen Folgen betrachtet. Beispielsweise wird es als die Möglichkeit eines Schadens oder Verlusts beschrieben, der aus einem bestimmten Verhalten oder Ereignis resultieren kann. Diese Definition bezieht sich auf Gefahrensituationen, bei denen unerwünschte Konsequenzen auftreten können, aber nicht zwangsläufig müssen.[83]

Auch im Duden findet sich eine negative Definition von Risiko: „*möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind; mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis.*“[84]

Im Bankwesen wird der Begriff „Risiko“ häufig nur auf negative Abweichungen bezogen. Das operationelle Risiko wird dabei als die Gefahr von Verlusten definiert, die durch unzureichende oder fehlerhafte interne Prozesse, Systeme, menschliches Versagen oder externe Ereignisse entstehen. Diese Definition umfasst das Rechtsrisiko, schließt jedoch strategische und Reputationsrisiken aus. Kurz gesagt, beschreibt das operationelle Risiko mögliche Verluste aufgrund interner Schwächen oder äußerer Einflüsse.[85]

In der neueren Literatur wird zwischen Risiko im engeren und im weiteren Sinne unterschieden. Risiko im engeren Sinne bezieht sich ausschließlich auf negative Auswirkungen, während Risiko im weiteren Sinne allgemein Abweichungen von festgelegten Zielen umfasst – unabhängig davon, ob diese positiv oder negativ sind. Risiko wird hier als die Möglichkeit beschrieben, aufgrund unvorhersehbarer Störungen von den geplanten Zielen abzuweichen. Vanini und Rieg weisen ebenfalls darauf hin, dass das Risikomanagement sowohl positive als auch negative Abweichungen berücksichtigt.

[83] Vgl *Institut für Interne Revision Österreich - IIA Austria* (Hrsg), Das Risikomanagement aus der Sicht der Internen Revision: inkl. CD-ROM mit Checklisten! (Fachbuch Wirtschaft 2006) 13.

[84] Risiko - Rechtschreibung, Bedeutung, Definition, Herkunft | Duden <https://www.duden.de/rechtschreibung/Risiko>. Zuletzt aufgerufen am 13.01.2025.

[85] Vgl *Österreichische Nationalbank*, Leitfaden Management des operationellen Risikos, Leitfaden (2005), 9.

Positive Abweichungen werden dabei als Chancen, negative als Risiken im engeren Sinne bezeichnet. Ähnlich definieren Exner et al positive Auswirkungen als „upside risks“.[86]

Wenn, wie oben beschrieben, „Risiko“ eine positive oder negative Abweichung von Zielen darstellt, ist entscheidend, dass Risiko immer im Zusammenhang mit spezifischen, vorgegebenen Zielen betrachtet wird.[87]

6.2.2 Arten von Risiken

Grundsätzlich können drei unterschiedliche Kategorien von Risiken unterschieden werden:

- Vermeidbare Risiken
    - Risiken, die aus dem Unternehmen heraus entstehen und keinen strategischen Nutzen bringen
- Strategie Risiken
    - Werden bewusst in Kauf genommen („akzeptierte Risiken“)
- Externe Risiken
    - Entstehen außerhalb des Unternehmens, sind nicht beeinflussbar

[86] Vgl *Gleißner*, Grundlagen des Risikomanagements; *Exner/Ruthner*, Corporate Risk Management; *Vanini/Rieg*, Risikomanagement: Grundlagen - Instrumente - Unternehmenspraxis (Lehrbuch 2021).

[87] Vgl *Gleißner*, Grundlagen des Risikomanagements, 21.

Table 1: Risikokategorien[88]

Kategorie 1: Vermeidbare Risiken	**Kategorie 2: Strategische Risiken**	**Kategorie 3: Externe Risiken**
Risiken, die aus dem Unternehmen selbst resultieren und keinen strategischen Nutzen generieren	Risiken für höhere strategische Renditen	Externe, nicht kontrollierbare Risiken
Ziel der Risikominderung		
Integriertes Kultur- und Compliance-Modell: Entwicklung eines Leitbilds, von Werten und Glaubenssystemen, Regeln und Begrenzungssystemen, Standardarbeitsanweisungen, internen Kontrollen und interner Revision	Interaktive Diskussionen über Risiken für strategische Ziele unter Verwendung von Tools wie: - Karten zur Wahrscheinlichkeit und Auswirkung identifizierter Risiken - Scorecards für Schlüsselrisikoindikatoren (KRI) - Ressourcenzuweisung zur Eindämmung kritischer Risikoereignisse	„Voraussagen“ von Risiken durch: - Tail-Risk-Bewertungen und Stresstests - Szenarioplanung - War-Gaming
Rolle der Risikomanagement-Stellen		
- Koordinieren, überwachen und überarbeiten spezifische Risikokontrollen mit der internen Revisionsfunktion	- Leiten Risiko-Workshops und Risikoüberprüfungs-sitzungen	- Führen Stresstests, Szenarioplanungen und Kriegsspiele mit dem Managementteam durch

[88] Vgl *Kaplan/Mikes*, Managing Risks: A New Framework, HBR’s 10 Must Reads on Managing Risk (HBR’s 10 must reads series 2020) 1–20 (2); Übersetzung durch den Verfasser.

	- Helfen bei der Entwicklung eines Portfolios von Risikoinitiativen und deren Finanzierung - Fungieren als Advocatus Diaboli	- Fungieren als Advocatus Diaboli
Beziehung der Risikomanagementfunktion zu den Geschäftseinheiten		
Fungiert als unabhängige Aufsichtsstelle	Fungiert als unabhängige Expertenstelle oder als eingebettete Expertenstelle	Ergänzt das Strategieteam oder fungiert als unabhängige Moderatorenstelle bei Visualisierungsübungen

6.3 Aufbauorganisation und Rahmenbedingungen

Die Aufbauorganisation legt die grundlegenden Rahmenbedingungen für die Organisationsstruktur fest. Sie wird dabei stark von der Branche, der Art der Geschäftstätigkeit sowie deren Umfang und Komplexität beeinflusst.[89]

Die Gesamtverantwortung für das Risikomanagement liegt bei der Unternehmensführung. Allerdings werden zentrale Aufgaben, insbesondere die Koordination aller Risikomanagementprozesse, in der Regel einem „Risikomanager“ übertragen. Dieser ist auch dafür zuständig, alle relevanten Risikoinformationen zu bündeln und in einem Risikobericht zusammenzufassen.[90]

Im Rahmen der Aufbauorganisation müssen die Rollen und Zuständigkeiten im Risikomanagement klar definiert werden. Die Unternehmensleitung legt zentrale Aspekte wie Risikokultur, Risikostrategie und Risikoappetit fest und wird dabei häufig von einem Risikokomitee unterstützt.[91]

[89] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance.

[90] Vgl *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation, 9.

[91] Vgl *Schwieters*, Corporate Governance, 182.

6.4 Ablauforganisation

6.4.1 Überblick

Ein Risikomanagementsystem besteht nicht nur aus einer einmaligen Identifikation, Analyse und Steuerung von Risiken durch die Unternehmensleitung. Stattdessen erfordert es die Einführung eines kontinuierlichen Risikomanagementprozesses in allen Bereichen des Unternehmens. Dieser Prozess stellt sicher, dass Risiken fortlaufend erkannt, analysiert und gesteuert werden.

Die Ablauforganisation spielt dabei eine wichtige Rolle, da sie die Arbeitsabläufe innerhalb der bestehenden Organisationsstruktur optimal gestaltet. Sie sorgt dafür, dass der Risikomanagementprozess in die Unternehmensplanung einbezogen und nahtlos in die Geschäftsprozesse integriert wird.[92]

Nachfolgend eine veranschaulichende Darstellung der Prozessstruktur des Risikomanagements:

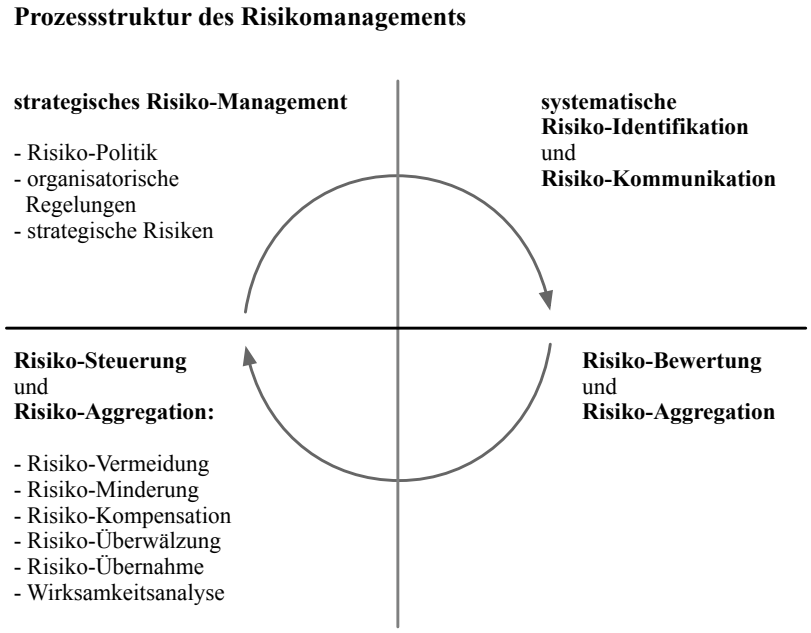


Abbildung 8: Prozessstruktur des Risikomanagements[93]

[92] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance.

[93] *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 42.

Die Ablauforganisation eines Risikomanagementsystems (RMS) umfasst den gesamten Prozess des Umgangs mit Risiken. Dazu gehören die systematische Erfassung und Kategorisierung von Risiken auf Unternehmensebene (Risikoidentifikation), ihre Bewertung nach Eintrittswahrscheinlichkeit und potenziellen Auswirkungen sowie ihre Priorisierung, insbesondere im Hinblick auf mögliche Bedrohungen für die Unternehmensfortführung (Risikobewertung).
Um ein Gesamtbild der Risikosituation des Unternehmens zu erhalten, werden die identifizierten Risiken in Kategorien wie finanzielle, operative, rechtliche, regulatorische, strategische oder ESG-Risiken (Umwelt, Soziales und Unternehmensführung) eingeteilt und über die verschiedenen Unternehmensbereiche hinweg zusammengeführt (Risikoaggregation). Die Risikosteuerung schließt sich an diesen Schritt an, da es ineffizient wäre, mögliche Wechselwirkungen innerhalb des Unternehmens zu ignorieren, wenn Maßnahmen wie Vermeidung, Reduktion, Teilung oder Übernahme von Risiken geplant werden.
Die laufende Überwachung und Berichterstattung der Risiken wird durch das Risikocontrolling gewährleistet. Dabei werden die Risiken auf Basis der Unternehmensziele, des verfügbaren Risikokapitals (wie Eigenkapital oder stille Reserven) und des definierten Risikoappetits geplant. Relevante Kennzahlen wie der Value at Risk (VaR) werden berechnet, Abweichungen zwischen geplanten und tatsächlichen Risiken analysiert und die Risikomessung sowie -steuerung zwischen Unternehmensbereichen, der Geschäftsleitung und externen Beteiligten koordiniert.
Die Risikoberichterstattung dient auch als Grundlage für die externe Kommunikation der Risikolage, insbesondere im Rahmen der Rechnungslegung.
Um sicherzustellen, dass das Risikomanagement stets wirksam bleibt, wird es kontinuierlich überwacht und an interne sowie externe Veränderungen angepasst.[94]

6.4.2 Risikoidentifikation

Es ist ratsam, zunächst geeignete Methoden zur Identifikation von Risiken zu definieren. Werden Risiken nur durch einfache Verfahren wie Mitarbeiterbefragungen (Risk Assessments) oder Brainstorming erfasst, besteht ein hohes Risiko, dass wichtige Gefahren übersehen werden. Psychologische Studien zeigen, dass Menschen dazu neigen, vor allem

[94] Vgl *Schwieters*, Corporate Governance, 184ff.

an auffällige oder kürzlich eingetretene Risiken zu denken, während andere potenziell bedeutsame Risiken häufig außer Acht gelassen werden.[95]

Zenke et al bezeichnen die folgenden Umsetzungshilfen und Methoden als typisch für die Risikoidentifikation in kleinen und mittleren Unternehmen:[96]

- Analyse der Geschäftsprozesse und Erkennen wesentlicher Risiken,
- Entscheidungsbäume und Entscheidungstabellen,
- prozessorientierte Risiko-Interviews und Brainstorming bzw Brainwriting,
- prozessorientierte Risikoerhebungsbögen und Checklisten,
- Szenariotechnik und Delphi-Methode sowie
- SWOT-Analyse (Strength Weaknesses Opportunities Threats).

6.4.3 Risikobewertung

Nach der Risikoidentifikation folgt die Risikoquantifizierung oder -bewertung. Dieser Prozess umfasst zwei wesentliche Schritte: Zum einen die quantitative Beschreibung des Risikos mithilfe geeigneter Wahrscheinlichkeitsverteilungen, zum anderen die Umrechnung dieser Daten in eine konkrete Zahl, das sogenannte Risikomaß.
Wichtig ist, dass Risikoanalysen als Grundlage für unternehmerische Entscheidungen dienen. Sie sollen verdeutlichen, wie sich der Umfang der Risiken des Unternehmens durch die Wahl einer bestimmten Handlungsoption verändern würde, zum Beispiel im Rahmen einer „Was-wäre-wenn-Analyse“.[97]

Die Quantifizierung von Risiken ist aus wirtschaftlicher Sicht notwendig, da nur so eine sinnvolle Priorisierung, Zusammenführung und Bewertung ihrer Gesamtwirkung auf das Unternehmen möglich ist. Ohne eine quantitative Erfassung können Risiken nicht effektiv aggregiert und in ihrer Bedeutung für das Unternehmen eingeschätzt werden.[98]

[95] Vgl *Gleißner*, Grundlagen des Risikomanagements, 128.

[96] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 45.

[97] Vgl *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation.

[98] Vgl *Klein* (Hrsg), Risikomanagement und Risiko-Controlling: Organisation und Dokumentation im Unternehmen, Datenerhebung und Risikobewertung, Integration in die Führungs- und Reportingsysteme, Umsetzungsbeispiele aus der Praxis (Haufe Fachpraxis 2011) 208.

Im Zukunftsbild des Risikomanagements sieht Gleißner hinsichtlich Risikoquantifizierung die Verwendung von sachgerechten Wahrscheinlichkeitsverteilungen statt Eintrittswahrscheinlichkeit und Schadenshöhe. Dementsprechend sollen bei der Risikoquantifizierung Risiken mithilfe passender Dichte- oder Verteilungsfunktionen beschrieben werden.[99]

Laut Gleißner können alle Risiken quantifiziert werden, selbst wenn keine oder nur wenige Informationen verfügbar sind. Allerdings zeigt sich, dass viele Menschen eine starke Abneigung gegenüber Zahlen und insbesondere komplexerer Mathematik haben. Dies führt häufig dazu, dass Risiken ungern quantifiziert und fälschlicherweise als nicht messbar dargestellt werden, was gerade im wertorientierten Unternehmensmanagement und Risikomanagement problematisch ist.
Quantifizierte Risiken lassen sich jedoch nicht einfach addieren, da Wechselwirkungen und Diversifikationseffekte berücksichtigt werden müssen. Dennoch ist die Quantifizierung von Risiken unerlässlich, um sie vergleichen, zusammenfassen und bei unternehmerischen Entscheidungen berücksichtigen zu können. Ein zentraler Grundsatz lautet: „Wenn man es nicht messen kann, kann man es nicht managen."
Um die Risiken verschiedener Geschäftsfelder zu vergleichen, müssen diese unter Berücksichtigung von Diversifikationseffekten aggregiert werden. Dies erfordert geeignete Methoden zur Risikoquantifizierung, die jedoch oft aufgrund von Datenmangel, fehlendem methodischen Wissen oder der Abneigung gegen Mathematik nicht angewendet werden.
Zusammenfassend ist es wichtig, Unsicherheiten über den Umfang eines Risikos sowie unzureichende Datenqualität explizit in die Bewertung einzubeziehen, da diese selbst das Risiko erhöhen können. Beispielsweise kann die Unsicherheit durch die Angabe von Parametervariabilität innerhalb einer Wahrscheinlichkeitsverteilung erfasst werden. Weder unzureichende Daten noch Unsicherheiten über die Höhe eines Risikos rechtfertigen es, auf dessen Quantifizierung zu verzichten.[100]

[99] Vgl *Gleißner*, Grundlagen des Risikomanagements.

[100] Vgl *Klein* (Hrsg), Risikomanagement und Risiko-Controlling, 208ff.

6.4.3.1 Wahrscheinlichkeits- und Dichtefunktionen

6.4.3.1.1 Einleitung

Für die Risikoquantifizierung ist es sinnvoll, Wahrscheinlichkeits- bzw Dichtefunktionen zu verwenden (siehe oben).

Bei der quantitativen Bewertung von Risiken ist es sinnvoll, die Wahrscheinlichkeitsverteilungen zu verwenden, die am besten zur Art des jeweiligen Risikos passen. Es ist weder sinnvoll noch erforderlich, für alle Risiken ausschließlich eine einzige Verteilungsart zu verwenden, wie beispielsweise die Binomialverteilung mit Schadenshöhe und Eintrittswahrscheinlichkeit. Moderne Methoden erlauben es, unterschiedliche Wahrscheinlichkeitsverteilungen zu kombinieren, um das Gesamtrisiko zu berechnen.[101]

Um diese Wahrscheinlichkeitsverteilungen zu veranschaulichen, werden daher nachfolgend einige derartige Funktionen beschrieben. Weiters finden sich unter „Anhang 1 – Wahrscheinlichkeits- und Dichtefunktionen“ grafische Darstellungen einiger ausgewählten Wahrscheinlichkeits- und Dichtefunktionen.

6.4.3.1.2 stetige Gleichverteilung

Bei einer stetigen Gleichverteilung sind alle Werte zwischen bestimmten Grenzen gleich wahrscheinlich.

[101] Vgl *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation, 16.

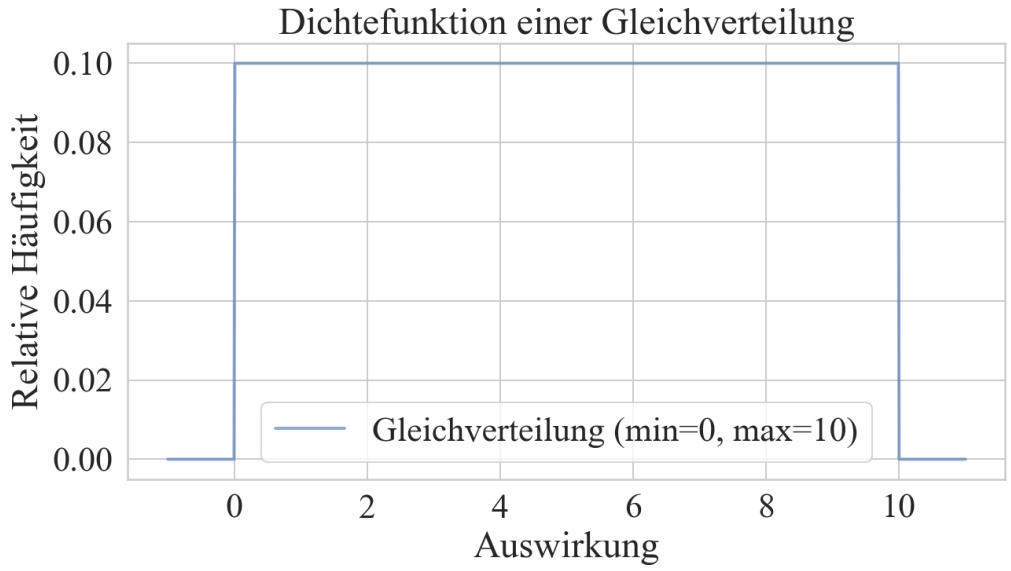


Abbildung 9: Dichtefunktion einer Gleichverteilung (eigene Darstellung)

Das Python-Script für die Generierung der obigen Darstellung findet sich in Anhang 1 („Python-Script zur Darstellung der stetigen Gleichverteilung“).

6.4.3.1.3 Dreiecksverteilung

Asymmetrische Risiken, bei denen entweder die Chancen oder die Gefahren dominieren, können besonders einfach mit der Dreiecksverteilung dargestellt werden, da sie intuitiv leicht verständlich ist. Diese Verteilung wird häufig verwendet, um Risiken von möglichen Kostenabweichungen in der Budgetplanung zu beschreiben. Dabei wird von einem Planwert ausgegangen, der als wahrscheinlichster Wert betrachtet wird, ergänzt durch die Angabe eines Mindestwerts und eines Maximalwerts. Diese drei Werte reichen aus, um das Risiko vollständig zu beschreiben, ohne dass Wahrscheinlichkeiten explizit angegeben werden müssen.[102]

Die Dreiecksverteilung ist durch ein Minimum (a), ein Maximum (b) und einen Modus bzw einen Punkt mit der höchsten Wahrscheinlichkeit (c) definiert.

[102] Vgl *Klein* (Hrsg), Risikomanagement und Risiko-Controlling, 212.

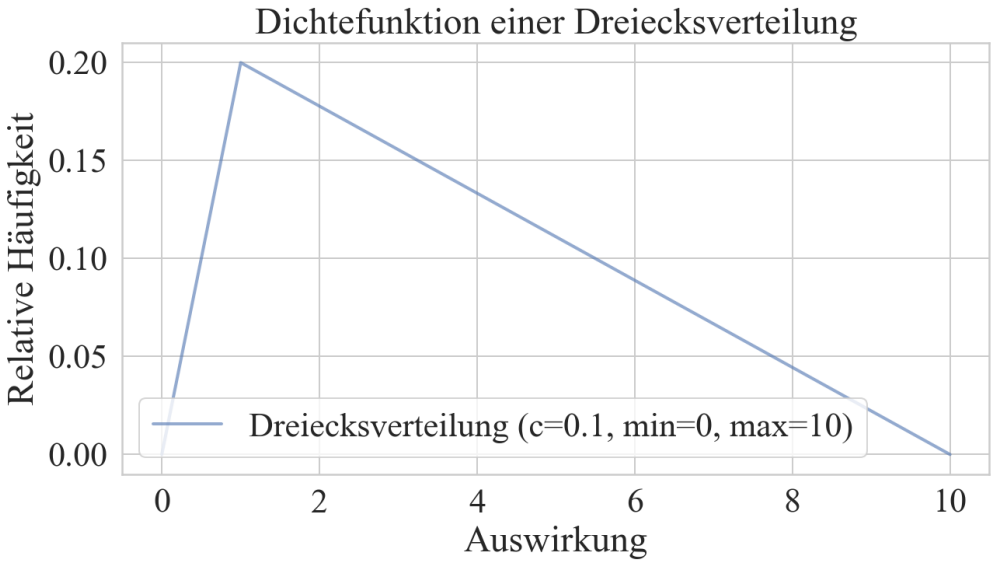


Abbildung 10: Dichtefunktion einer Dreiecksverteilung (eigene Darstellung)

Das Python-Script für die Generierung der obigen Darstellung findet sich in Anhang 1 („Python-Script für Darstellung der Dreiecksverteilung“).

6.4.3.1.4 Normalverteilung (Gauß-Verteilung)

Risiken, die sich auf stark zusammengefasste Größen beziehen, können oft gut mit der Normalverteilung, auch bekannt als Gaußsche Glockenkurve, beschrieben werden. Diese Verteilung eignet sich besonders für Risiken, die sich aus vielen kleinen Einzelfaktoren zusammensetzen und annähernd symmetrisch sind, das heißt, bei denen die positiven und negativen Abweichungen etwa gleich groß sind. Daher wird die Normalverteilung häufig verwendet, um Umsatzrisiken oder die meisten marktbezogenen Risiken zu beschreiben, wie zum Beispiel Schwankungen bei Rohstoffpreisen, Zinssätzen oder Wechselkursen.[103]

Die Normalverteilung ist eine symmetrische Verteilung, die durch den Mittelwert (μ) und die Standardabweichung (σ) beschrieben wird.

[103] Vgl *Klein* (Hrsg), Risikomanagement und Risiko-Controlling, 212.

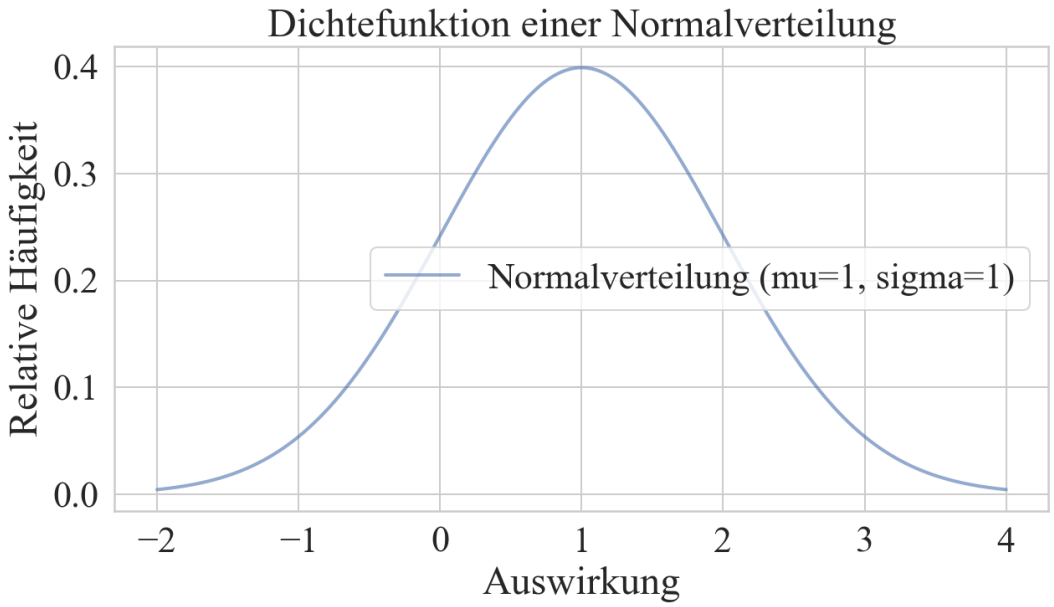


Abbildung 11: Dichtefunktion einer Normalverteilung (eigene Darstellung)

Das Python-Script für die Generierung der obigen Darstellung findet sich in Anhang 1 („Python-Script für Darstellung der Normalverteilung“).

6.4.3.1.5 Logarithmische Normalverteilung

Die logarithmische Normalverteilung ist – wie der Name schon vermuten lässt – von der Gauß-Verteilung abgeleitet.

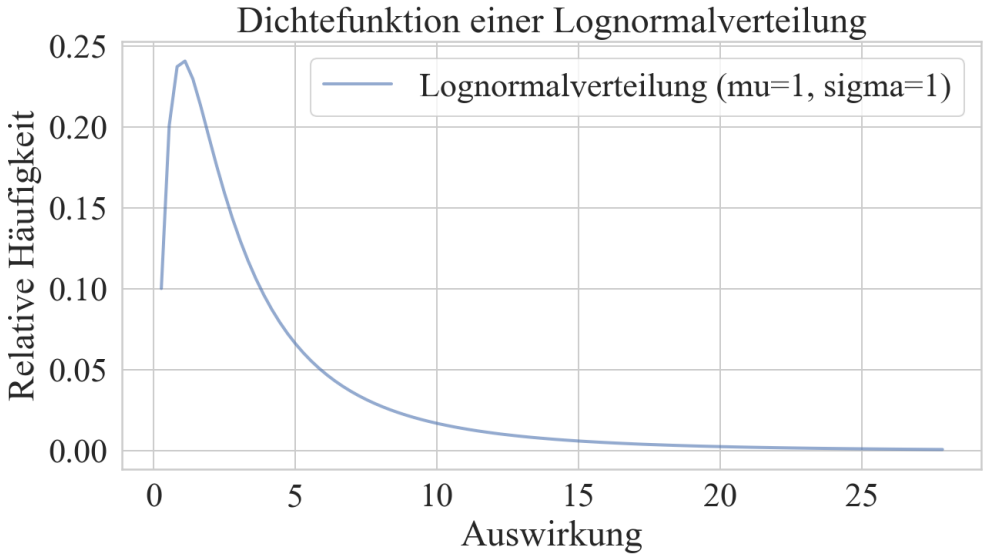


Abbildung 12: Dichtefunktion einer Lognormalverteilung (eigene Darstellung)

Das Python-Script für die Generierung der obigen Darstellung findet sich in Anhang 1 („Python-Script für Darstellung der Lognormalverteilung“).

6.4.3.1.6 Binomialverteilung

Die Binomialverteilung wird häufig für sogenannte ereignisorientierte Risiken verwendet, da sie sich gut eignet, um spezifische, klar definierte Ereignisse zu beschreiben. Ein Beispiel ist der mögliche Ausfall einer Maschine, der anhand zweier Parameter dargestellt werden kann: (a) der Wahrscheinlichkeit, dass der Ausfall eintritt, und (b) der Höhe des dadurch entstehenden Schadens. Die Binomialverteilung ist besonders dann passend, wenn die Schadenshöhe weitgehend sicher und feststeht.[104]

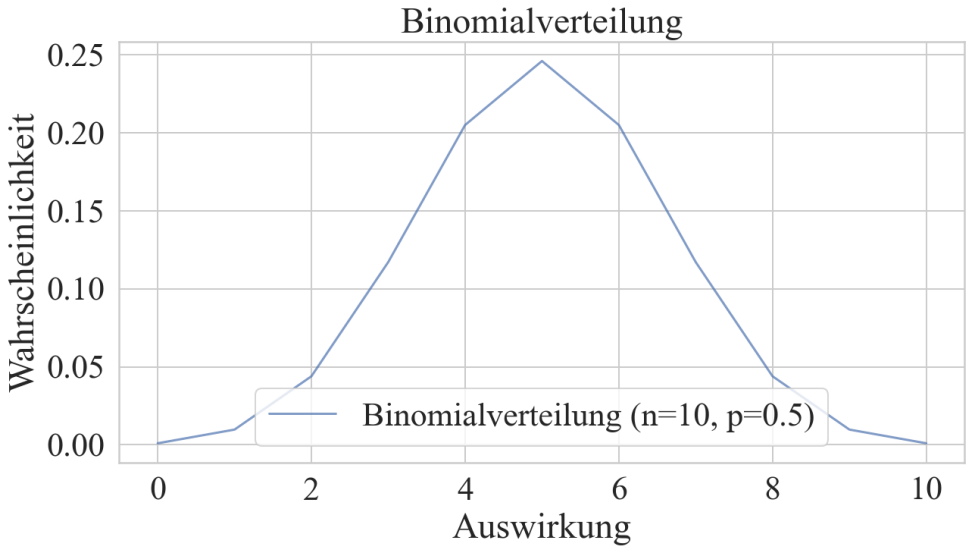


Abbildung 13: Binomialverteilung (eigene Darstellung)

Das Python-Script für die Generierung der obigen Darstellung findet sich in Anhang 1 („Python-Script zur Darstellung der Binomialverteilung“).

6.4.4 Risikoaggregation

Es sind in der Regel nicht einzelne Risiken, sondern die Kombination verschiedener Risiken, die potenziell existenzbedrohende Entwicklungen auslösen können. Daher spielt die Risikoaggregation eine zentrale Rolle im Risikomanagement. Sie ist entscheidend, um den Gesamtrisikoumfang zu berechnen und bildet die Grundlage, um Risikomanagement mit Controlling und einer wertorientierten Unternehmenssteuerung zu verknüpfen. Eine effektive Risikoaggregation ermöglicht es, erwartete Erträge und Risiken in Entscheidungsprozessen gegeneinander abzuwägen und so eine tatsächlich wertorientierte Unternehmensführung zu realisieren. Da Risiken nicht einfach addiert werden können und

[104] Vgl *Klein* (Hrsg), Risikomanagement und Risiko-Controlling, 213.

in der Regel keine analytischen Methoden zur Aggregation von Einzelrisiken zur Verfügung stehen, werden stochastische Simulationsverfahren wie die Monte-Carlo-Simulation eingesetzt. Ein zentrales Problem dabei ist, dass die Abhängigkeiten zwischen verschiedenen Risiken unbedingt berücksichtigt werden müssen.[105]

Monte-Carlo-Simulation

Gleißner sieht im Zukunftsbild des Risikomanagements bzgl. Risikoaggregation die Verwendung von Monte-Carlo-Simulationen anstatt dem Ignorieren von Kombinationseffekten von Risiken.[106]

Die Monte-Carlo-Simulation spielt eine zentrale Rolle bei der frühzeitigen Erkennung und Quantifizierung von Risiken. Sie hilft dabei, Risiken sichtbar und steuerbar zu machen. Dieses Verfahren verbindet das Risikomanagement eng mit dem Konzern-Controlling. Als computergestütztes Werkzeug ermöglicht die Monte-Carlo-Simulation die Berechnung einer großen Anzahl potenzieller Zukunftsszenarien, die durch Risiken beeinflusst werden. Sie erweitert die traditionelle, auf festen Werten basierende Unternehmensplanung, indem sie sowohl Chancen als auch Risiken einbezieht und dadurch realistische Entwicklungsspannen für die Zukunft aufzeigt (Bandbreitenplanung). Die Monte-Carlo-Simulation bildet somit die Grundlage für eine risikobewusste Unternehmensführung, etwa bei der Bewertung von Investitionen unter Berücksichtigung von Risiken. Sie kann vergleichsweise leicht in bestehende Planungstools wie Excel durch entsprechende Simulationssoftware integriert werden.[107]

Bei einer Monte-Carlo-Simulation werden anhand von Zufallszahlen viele Simulationsläufe durchgeführt – das ermöglicht das Gesamtrisiko zu schätzen. Hier ist beispielhaft die Aggregation eines Risikos mit Normalverteilung und eines Risikos mit Lognormalverteilung dargestellt:

[105] Vgl *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation.

[106] Vgl *Gleißner*, Grundlagen des Risikomanagements, 13.

[107] Vgl *Daume/Ernst*, Monte-Carlo-Simulation im Risiko-Controlling: am Beispiel eines Financial Models in Excel (2022); *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation.

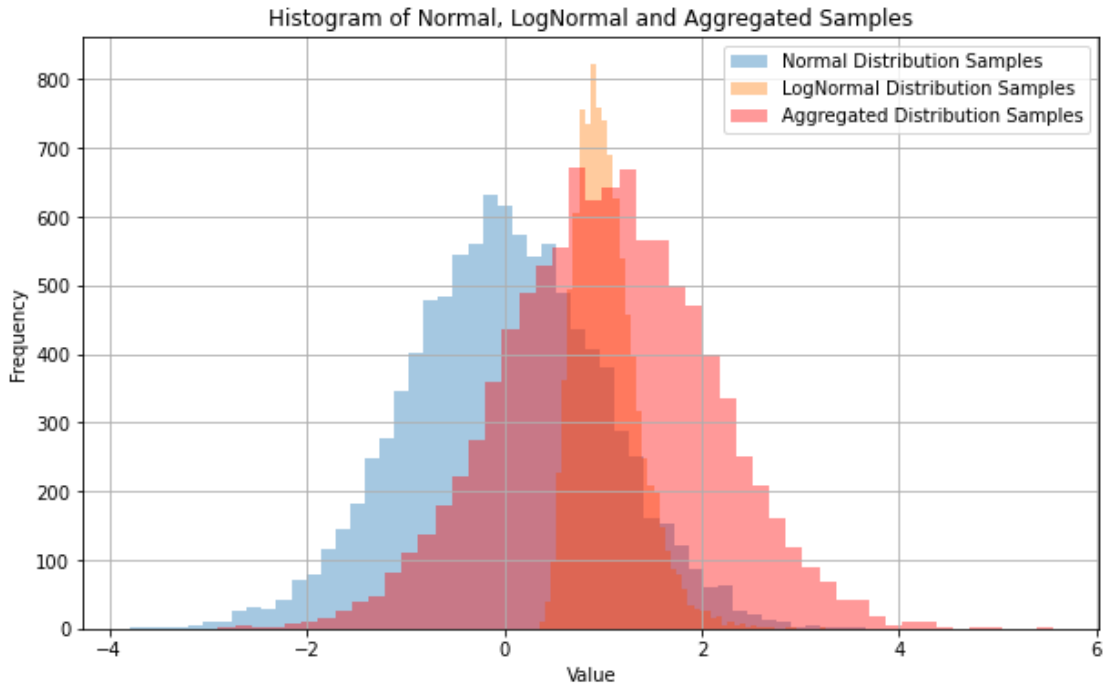


Abbildung 14: Aggregation eines normalverteilten Risikos und eines lognormalverteilten Risikos (eigene Darstellung)

Das Python-Script für die Generierung der obigen Darstellung findet sich in Anhang 2 („Python-Script für die Aggregation von Dichtefunktionen mittels Monte-Carlo-Simulation“).

Zur weiteren Veranschaulichung wird im „Anhang 2 – Monte-Carlo-Simulation“ eine vereinfachte Monte-Carlo-Simulation anhand der Schätzung der Kreiszahl π dargestellt.

6.4.5 Risikosteuerung und -überwachung

Die Risikosteuerung zielt darauf ab, erkannte und bewertete Risiken durch geeignete Maßnahmen zu beeinflussen, wobei die Risikostrategie, Risikoziele, Risikotragfähigkeit und Risikoneigung des Managements oder der Anteilseigner berücksichtigt werden. Zu den zentralen Aufgaben gehören die Entwicklung von Steuerungsstrategien, deren Umsetzung durch konkrete Maßnahmen sowie die kontinuierliche Überprüfung dieser Maßnahmen. Das Ziel der Risikosteuerung ist, die tatsächliche Risikosituation des Unternehmens mit der angestrebten Soll-Risikosituation in Einklang zu bringen. Die Begriffe Risikosteuerung und Risikobewältigung werden dabei oft synonym verwendet. Sie ist ein integraler

Bestandteil der Steuerungs- und Überwachungsprozesse in allen Bereichen des Unternehmens.[108]

Es gibt verschiedene Arten mit Risiken umzugehen.[109]

Riskoreduktion: Durch angemessene Maßnahmen wird der Risikograd vermindert.

Risikoübertragung: Das Risiko wird auf eine externe Partei verlagert, bspw durch Outsourcing.

Risikovermeidung: Das Risiko ist zu hoch und es gibt keine geeigneten Maßnahmen, um das Risiko zu vermindern. Um das Risiko zu vermeiden, kann bspw eine bestimmte Datenverarbeitung nicht durchgeführt werden.

Risikoakzeptanz: Liegt das Risiko unter einer definierten Schwelle, so kann es akzeptiert werden – weitere Maßnahmen sind dann nicht notwendig.

Bei Risikoakzeptanz ist zu beachten, dass die Gesetzeslage hier nur einen eingeschränkten Spielraum bietet.[110] Bei Normen, die mit Strafen oder Bußgeldern belegt sind, ist eine Risikoakzeptanz besonders problematisch. Der Staat akzeptiert in solchen Fällen keine wirtschaftliche Abwägung, die sich an Eintrittswahrscheinlichkeiten und möglichen Konsequenzen orientiert. Unternehmen, die solche Überlegungen anstellen und dies sogar in ihrer Risikoanalyse und Berichterstattung dokumentieren, laufen Gefahr, den Vorwurf zu erhalten, Rechtsverstöße fahrlässig oder bewusst in Kauf zu nehmen. Daher gibt es bei straf- oder bußgeldbewehrten Normen keinen Handlungsspielraum, wenn es darum geht, Vorschläge zur Minimierung von Compliance-Risiken umzusetzen.[111]

6.5 Herausforderungen im Risikomanagement

Einleitung

Das Risikomanagement steht vor zahlreichen Herausforderungen, die auf verschiedene Faktoren zurückzuführen sind. Eine davon ist, dass viele Unternehmen den Aufbau und die

[108] Vgl *Vanini/Rieg*, Risikomanagement, 311.

[109] Vgl *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden (Unternehmen und Wirtschaft 2017) 106.

[110] Vgl *Schäffter*, Datenschutzmanagement 2.0: EU-konformen Datenschutz effizient planen und umsetzen; Migration zu einem Datenschutzmanagement gemäß EU-Datenschutzgrundverordnung inklusive Verfahrensverzeichnis 2.0 (2017) 71.

[111] Vgl *Zenke/Schäfer/Brocke* (Hrsg), Corporate Governance, 19.

Weiterentwicklung von Risikomanagement-Prozessen und -Werkzeugen mit begrenzten internen Ressourcen bewältigen müssen.[112]

Psychologische Faktoren haben ebenfalls einen großen Einfluss auf das Risikomanagement. Studien zeigen, dass Menschen in komplexen Situationen häufig gravierende Fehler machen, unabhängig von ihrer Intelligenz oder fachlichen Kompetenz. Besonders schwierig ist es für sie, bestehende Risiken korrekt in ihre Entscheidungen einzubeziehen. Diese sogenannte Risikoblindheit hat tief verwurzelte psychologische Ursachen. Menschen zeigen eine starke Abneigung gegenüber Risiken und besonders gegenüber Verlusten. Zudem sind die Fähigkeiten, Chancen und Gefahren richtig einzuschätzen, in Unternehmen oft wenig ausgeprägt. Dies liegt unter anderem daran, dass Risiken gerne verdrängt werden (Kontrollillusion) und greifbare Risiken häufig falsch bewertet werden. Hinzu kommt, dass die Rahmenbedingungen oft problematisch sind: Menschen versäumen es häufig, sich vor Entscheidungen klar über ihre Ziele zu werden, sodass die angestrebten Zielgrößen nicht eindeutig definiert werden.[113]

Rumsfeld Matrix

Ähnlich einem Johari-Fenster[114] kann zwischen unterschiedlichen Graden des Wissens bzw Nicht-Wissens unterschieden werden. Benannt ist diese Matrix nach Donald Rumsfeld, dem damaligen US-Verteidigungsminister, der im Zuge einer Pressekonferenz 2002 folgende Aussage tätigte:

„[…] there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know.“[115]

[112] Vgl *Exner/Ruthner*, Corporate Risk Management, XX.

[113] Vgl *Gleißner*, Grundlagen des Risikomanagements, 64ff.

[114] Vgl Johari-Fenster <https://de.wikipedia.org/wiki/Johari-Fenster>, zuletzt aufgerufen am 23.01.2025.

[115] Donald Rumsfeld, Ausschnitt aus Pressekonferenz am 12.02.2002 <https://www.youtube.com/watch?v=REWeBzGuzCc> (2016); zuletzt aufgerufen am 14.01.2025.

Tabelle 2: Rumsfeld Matrix

	Wissen (Bekanntes, knowns)	**Unwissen** (Unbekanntes, unknowns)
bekanntes	bekanntes Wissen	bekanntes Unwissen
unbekanntes	unbekanntes Wissen	unbekanntes Unwissen

Persönliche Interessen

Auch wenn die durch ein Risikomanagement gesteigerte Transparenz im Sinne eines Unternehmens ist, und beispielsweise dazu beitragen kann, Informationsasymmetrien (vgl auch Kap 4.2.3.1 „Neue Institutionenökonomik“) zu vermindern, so muss diese Transparenz nicht unbedingt auch im persönlichen Interesse jedes Managers sein.[116]

Aus Sicht des Autors sollte man sich im Risikomanagement dieser Herausforderungen bewusst sein und ggf entsprechende Vorkehrungen treffen.

6.6 Rechtliche Rahmenbedingungen und Standards für Risikomanagement

Es gibt viele Vorschriften und Standards die Regelungen für Risikomanagement beinhalten. Beispiele dafür sind Rechnungslegungsänderungsgesetz 2004 (RelÄG), Unternehmensrechts-Änderungsgesetz 2008 (URÄG), Basel II, Solvency II, Sarbanes Oxley Act, der Österreichische Corporate Governance Kodex, COSO ERM, ISO 31000 / ÖNORM D 490x und in Deutschland das KonTraG.

ISO 31000 / ÖNORM D 490x

Die Norm ISO 31000[117] ist neben dem COSO ERM Modell eine wichtige Hilfestellung für die Implementierung eines Risikomanagementsystems. Die Normenreihe ÖNORM D 490x[118] konkretisieren die Vorgaben der ISO 31000 weiter.

[116] vgl *Gleißner*, Grundlagen des Risikomanagements, 18.

[117] *International Organization for Standardization (Hrsg)*, ISO 31000:2018, Risk management - Guidelines (02.2018).

[118] *Austrian Standards International (Hrsg)*, ÖNORM D 4900:2021, Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen (01.01.2021); *Austrian Standards International (Hrsg)*, ÖNORM D 4901:2021, Risikomanagement für Organisationen und Systeme - Anforderungen an das

Zentrale Gedanken der ISO 31000 sind beispielsweise die Forderungen zur klaren Formulierung der zu erfüllenden Aufgabe sowie die Zuordnung von Verantwortlichkeiten für Aufgaben und für die Aufgabenerfüllung notwendiger Ressourcen.[119]

Die Normenreihe ÖNORM D 490x besteht aus insgesamt sechs unterschiedlichen Normen, wie die nachfolgende Darstellung zeigt.

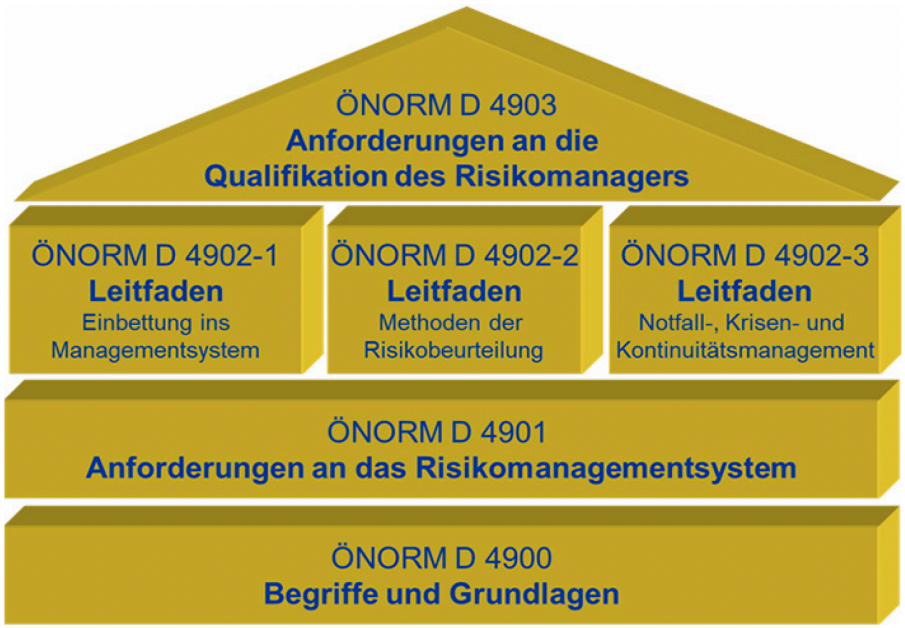


Abbildung 15: Risikomanagement für Organisationen und Systeme[120]

Risikomanagementsystem (01.01.2021); *Austrian Standards International (Hrsg)*, ÖNORM D 4902-1:2021, Risikomanagement für Organisationen und Systeme - Leitfaden Teil 1: Einbettung des Risikomanagements ins Managementsystem (01.01.2021); *Austrian Standards International (Hrsg)*, ÖNORM D 4902-2:2021, Risikomanagement für Organisationen und Systeme - Leitfaden Teil 2: Methoden der Risikobeurteilung (01.01.2021); *Austrian Standards International (Hrsg)*, ÖNORM D 4902-3:2021, Risikomanagement für Organisationen und Systeme - Leitfaden Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement (01.01.2021); *Austrian Standards International (Hrsg)*, ÖNORM D 4903:2021, Risikomanagement für Organisationen und Systeme - Anforderungen an die Qualifikation des Risikomanagers (01.01.2021).

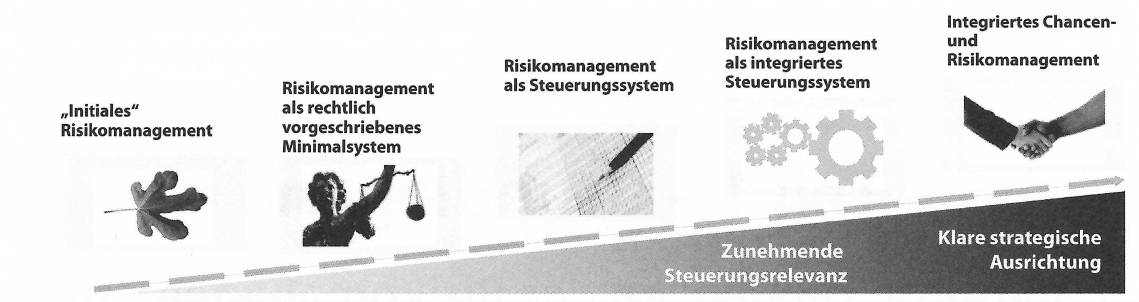
[119] Vgl *Gleißner*, Grundlagen des Risikomanagements, 110.

[120] *Austrian Standards International (Hrsg)*, ÖNORM D 4900:2021, Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen (01.01.2021) 4.

6.7 Status und Zukunftsbild des Risikomanagements

Viele der aktuell eingesetzten Risikomanagementsysteme erfüllen häufig nicht einmal die gesetzlichen Mindestanforderungen und tragen kaum oder gar nicht zur Wertschöpfung eines Unternehmens bei. Dies ist vor allem auf erhebliche methodische Schwächen zurückzuführen, wie etwa das Fehlen einer umfassenden Risikoaggregation und die mangelnde Integration des Risikomanagements in die Entscheidungsprozesse des Unternehmens.[121]

Unternehmen durchlaufen beim Einsatz von Risikomanagement oft einen typischen Entwicklungsprozess: Zunächst setzen sie eher einfache Systeme ein, die in erster Linie darauf abzielen, gesetzliche Vorgaben zu erfüllen. Im Laufe der Zeit entwickeln sie diese Systeme weiter zu komplexeren Ansätzen, die nicht nur den rechtlichen Anforderungen genügen, sondern auch zur operativen und strategischen Steuerung des Unternehmens beitragen sollen.[122]



Beschreibung				
Lediglich Großrisiken werden erfasst (qualitativ) und einzeln dargestellt („Risikobuchhaltung"). Die Risikoberichterstattung erfolgt anlassbezogen. Es dominieren Kollektionsmethoden.	Risiken und Chancen werden zuverlässig und vollständig erfasst (zumindest qualitativ) und dokumentiert. Die Berichterstattung erfolgt in zyklischen Intervallen.	Der Risikomanagement-Prozess folgt einer nachvollziehbar dokumentierten Methode. Hierbei werden auch analytische Methoden sowie Kreativitätsmethoden eingesetzt. Risiken werden quantifiziert und zusammengefasst (aggregiert). Maßnahmen werden erfasst und in ihrer Gesamtheit bewertet.	Chancen und Risiken werden als Korridor (mögliche Abweichungen) der Unternehmensplanung bewertet und aggregiert. Abhängigkeiten zwischen Risiken werden berücksichtigt. Maßnahmen werden sowohl mit ihrem Nutzen als auch ihren Kosten miteinbezogen.	Der risikoorientierte Planungsprozess ist integrierter Bestandteil der strategischen Unternehmensführung. Das RM-System ist direkt an die Steuerungssysteme des Unternehmens angebunden. Die Basis der Identifikation bilden analytische Methoden sowie Kreativitätsmethoden. Eine Risikokultur ist verankert.

Abbildung 16: Entwicklungsstufen des Risikomanagements[123]

[121] Vgl *Gleißner*, Grundlagen des Risikomanagements, 16.

[122] Vgl *Exner/Ruthner*, Corporate Risk Management, 1.

[123] *Exner/Ruthner*, Corporate Risk Management, 2.

Gleißner stellt die Entwicklungsstufen leicht unterschiedlich dar:

Abbildung 17: Die sechs Entwicklungsstufen des Risikomanagements[124]

Dementsprechend führt Gleißner hier die folgende Entwicklung an:[125]

- Risikoidentifikation: Stärkerer Fokus auf strategische und makroökonomische Risiken
- Risikoquantifizierung: Sachgerechte Wahrscheinlichkeitsverteilung statt Eintrittswahrscheinlichkeit und Schadenshöhe
- Risikoaggregation: Monte-Carlo-Simulation statt Ignorieren der Kombinationseffekte von Risiken
- Entscheidungsorientiertes Risikomanagement: Risikoanalysen für „unternehmerische Entscheidungen“ statt lediglich routinemäßiger Risikoreports
- Wertbeitrag: Risikoinformationen zur Steuerung der Werttreber „Kapitalkosten“ und „Insolvenzwahrscheinlichkeit“ statt Risikominimierung

[124] *Gleißner*, Grundlagen des Risikomanagements, 9.

[125] *Gleißner*, Grundlagen des Risikomanagements, 12 ff.

- Organisation des Risikomanagements: Integratives Risikomanagement statt Risikomanagement im „Silo“

Insgesamt ergibt sich daraus folgendes Bild:

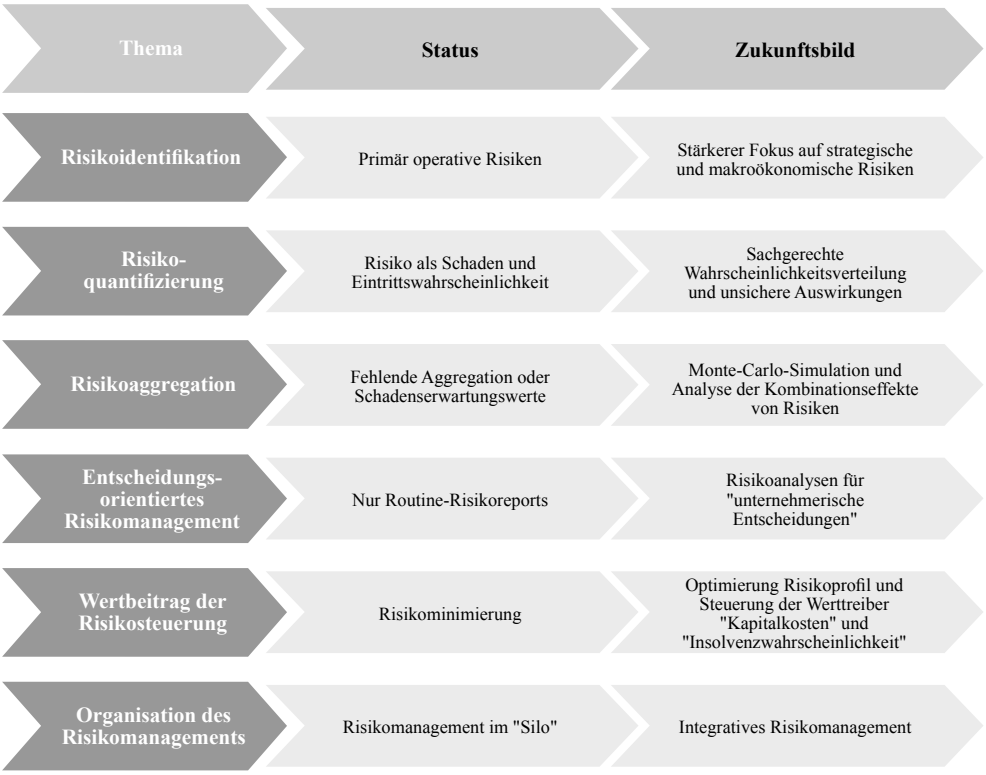


Abbildung 18: Risikomanagement: Status und Zukunftsbild[126]

Governance-, Risk- und Compliancesysteme (GRC)

In einigen Unternehmen verschiebt sich der Fokus von einem isolierten Risikomanagement hin zu einer Integration der Anforderungen aus Corporate Governance, Risikomanagement und Compliance-Systemen. Diese Verknüpfung wird als vorteilhaft angesehen, da sie Synergien schafft und die Qualität der Prozesse verbessert. Unabhängig voneinander arbeitende Kontroll- und Managementsysteme führen oft zu unkoordinierten oder sogar widersprüchlichen Informationen für die Unternehmensleitung. Wenn jedoch Governance-, Risiko- und Compliancemanagement als ein integriertes System betrachtet werden, können Aktivitäten und Informationen besser abgestimmt werden, was Redundanzen reduziert. Dies erhöht die Effizienz, verbessert die Transparenz und stärkt die Sicherheit der Steuerungs- und Kontrollmechanismen im Unternehmen. Bei genauerer

[126] *Gleißner*, Grundlagen des Risikomanagements, 16.

Betrachtung gibt es aber auch Nachteile dieser Integration. So beschäftigt sich Risikomanagement idealerweise auch mit Chancen, also positiven Abweichungen während GRC-Systeme meist nur Risiken im engeren Sinne betrachten. Weiters hat Risikomanagement nicht das Ziel der Risikovermeidung, sondern soll zur Transparenz beitragen. Governance- und Compliancesysteme zielen aber letztendlich auf die gänzliche Vermeidung von Bedrohungen ab. Außerdem sind die Synergien zwischen den Systemen oft nicht so groß, wie es auf den ersten Blick erscheinen mag. Zwar kann es im Bereich der Verwaltung von einzelnen Risiken große Synergien geben, bei der Risikobewertung, der Risikoaggregation und der Steuerung der Risikogesamtposition dürften diese aber deutlich geringer ausfallen.[127]

6.8 Zusammenfassung Risikomanagement

Risikomanagement kann eine Methode zur Steigerung der Transparenz und zur Verbesserung von Entscheidungen in Unternehmen sein. Dazu ist es notwendig, passende Strukturen im Unternehmen zu verankern und Risikomanagement als laufenden Prozess aufzusetzen.

Risiken entstehen durch die Unvorhersehbarkeit der Zukunft und beschreiben die Möglichkeit von Abweichungen von geplanten Zielen. Sie umfassen sowohl Chancen (positive Abweichungen) als auch Gefahren (negative Abweichungen). Das Risikomanagement hat die Aufgabe, Risiken systematisch zu identifizieren, zu bewerten, zu bündeln, zu steuern und zu überwachen. Ziel ist es, Transparenz über den gesamten Risikoumfang zu schaffen, um insbesondere existenzgefährdende Entwicklungen frühzeitig zu erkennen. Es unterstützt die Unternehmensführung dabei, die Unsicherheiten der Zukunft besser in ihre Entscheidungen einzubeziehen und somit den langfristigen Erfolg des Unternehmens zu sichern. Risikomanagement ist daher ein zentraler Bestandteil einer strategischen, risiko- und wertorientierten Unternehmensführung. Für fundierte Entscheidungen sind eine klare Strategie, eine darauf basierende operative Planung sowie eine gründliche Analyse von Chancen und Risiken unerlässlich. Da die Zukunft nie vollständig vorhersehbar ist, sollten alle Mitarbeiter – insbesondere die Führungskräfte – Risikomanagement als integralen Bestandteil ihrer Arbeit betrachten. Mit entsprechender Fachkompetenz können wesentliche Risiken durch passende Wahrscheinlichkeits-

[127] Vgl *Exner/Ruthner*, Corporate Risk Management, 3f.

verteilungen beschrieben werden. Die Risikoaggregation ermittelt den gesamten Risikoumfang, indem eine Vielzahl möglicher zukünftiger Szenarien mithilfe von Verfahren wie der Monte-Carlo-Simulation berechnet wird.[128]

Die Ermittlung des gesamten Risikoumfangs ermöglicht es entsprechende Entscheidungen zu treffen und so einen Wertschöpfungsbeitrag für das Unternehmen zu leisten.

Auch aus Datenschutzperspektive ist es aus Sicht des Autors dabei wichtig, dass Risiko in diesem Zusammenhang im weiteren Sinne begriffen wird, nämlich nicht nur als Gefahr, sondern auch als Chance. Während Compliance-Risiken oftmals nur als Gefahr wahrgenommen werden, ist es spätestens bei der Betrachtung der verschiedenen Perspektiven der Balanced Score Card hilfreich, auch Chancen erkennen und entsprechend verarbeiten zu können.

[128] Vgl *Gleißner/Wolfrum*, Risikoaggregation und Monte-Carlo-Simulation, 10ff.

7 Grundlagen Datenschutz

7.1 Begriff „Datenschutz“

In der öffentlichen Diskussion kommt es immer wieder zu Missverständnissen beim Begriff „Datenschutz“. Nicht zuletzt aufgrund begrifflicher Nähe werden die Begriffe Datenschutz und Datensicherheit oft verwechselt. Während Datenschutz den Schutz von Persönlichkeitsrechten von betroffenen Personen primär durch den Schutz vor Missbrauch durch Dritte zum Ziel hat, Bezieht sich Datensicherheit auf den Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität. Beim Datenschutz steht also nicht der Schutz der Daten im Vordergrund, sondern der Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen.[129]
Aus Sicht des Datenschutzes ist besonders das in Artikel 8 Absatz 1 der Europäischen Menschenrechtskonvention verankerte Recht auf Achtung des Privat- und Familienlebens hervorzuheben: „*Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.*“ Dementsprechend betont auch Forgó, dass unter Datenschutz der Schutz der rechtmäßigen Verwendung von personenbezogenen Daten zu verstehen ist und nicht der Schutz der personenbezogenen Daten an sich.[130]

Daher sollen auch die Vorschriften der DSGVO die Grundrechte und Grundfreiheiten natürlicher Personen und in diesem Zusammenhang deren Recht auf Schutz personenbezogener Daten gewährleisten. Ein weiteres Ziel der DSGVO ist es, sicherzustellen, dass der freie Verkehr personenbezogener Daten innerhalb der EU weder eingeschränkt noch verboten wird.[131]

[129] Vgl *Schäffter*, Datenschutzmanagement 2.0.

[130] Vgl *Forgó* (Hrsg), Grundriss Datenschutzrecht (Lehrbuch 2019) 2.

[131] Vgl *Forgó* (Hrsg), Grundriss Datenschutzrecht, 29.

7.2 Geschichtliche Entwicklung von Datenschutz

Nicht erst seit Facebook und Co die Weltbühne betraten, ist klar, dass bestimmte Informationen über Menschen privat bleiben sollten. So ist seit etwa 800 v.Chr. beispielsweise das ärztliche Schweigegebot bekannt.[132]

Dieser Gedanke wurde unter anderem auch in dem bekannten Aufsatz „The Right to Privacy" von Samuel D. Warren und Louis D. Brandeis aus dem Jahr 1890 festgehalten.[133] Als erstes spezifisches Datenschutzgesetz weltweit gilt das Hessische Datenschutzgesetz von 1970.[134] In Österreich wurde acht Jahre Später, mit dem DSG 1978, eine erste gesetzliche Grundlage für Datenschutz geschaffen. Der Europarat verabschiedete wenig später das erste international verbindliche Abkommen, das bis heute gültig ist: Das Übereinkommen 108[135], das den Schutz von Personen bei der automatischen Verarbeitung personenbezogener Daten regelt. Es wurde 1981 zur Unterzeichnung freigegeben und trat am 1. Oktober 1985 in Kraft. Dieses Abkommen gilt als der bedeutendste völkerrechtlich bindende Vertrag zum Schutz vor Missbrauch bei der elektronischen Verarbeitung persönlicher Daten. Im Laufe der Zeit wurden Datenschutzregelungen immer verbindlicher. Die EU Datenschutzrichtlinie[136] (1995) führte zum österreichischen Datenschutzgesetz 2000[137]. Die weitere Vereinheitlichung von Datenschutz in Europa und eine Stärkung der Rechte der Betroffenen (deren Daten verarbeitet werden) führte zur Datenschutzgrundverordnung (DSGVO), die 2018 wirksam wurde.

[132] Vgl *Rehborn*, Die ärztliche Schweigepflicht - ein schützenswertes Rechtsgut, GesR - Gesundheitsrecht 2017, 409 (410).

[133] Vgl *Forgó* (Hrsg), Grundriss Datenschutzrecht, 1.

[134] Vgl *Schäffter*, Datenschutzmanagement 2.0, 1.

[135] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108).

[136] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281.

[137] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl I 165/1999.

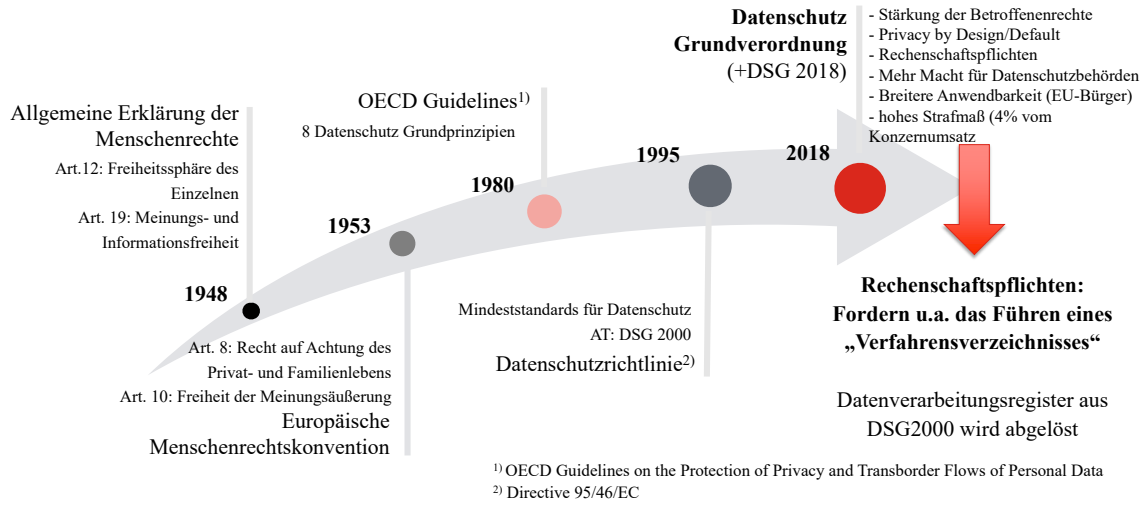


Abbildung 19: Meilensteine des Datenschutzes in Europa (eigene Darstellung)

Einer der wesentlichsten Punkte in der DSGVO war das - im Vergleich zum Datenschutzgesetz 2000 - hohe Strafmaß der DSGVO in der Höhe von bis zu 4% des weltweiten Konzernumsatzes. Diese Sanktionsandrohung stellt(e) einen hohen Anreiz dar, der viele Unternehmen nicht zu unterschätzende Aufwände auf sich nehmen ließ.

Eine weitere wichtige Änderung der DSGVO sind die Rechenschaftspflichten. Jeder Verantwortliche, der personenbezogene Daten verarbeitet, muss nachweisen können, dass diese Datenverarbeitungen den Regelungen der DSGVO entsprechen.

In der nebenstehenden Grafik sind die wesentlichen Grundprinzipien der DSGVO dargestellt - die Rechenschaftspflicht betrifft alle Regelungen der DSGVO.

Abbildung 20: DSGVO-Grundprinzipien (eigene Darstellung)

7.3 Datenschutzstrategie und Datenschutzkonzept

Die Datenschutzstrategie bildet den zentralen Orientierungspunkt des Datenschutzmanagements. Sie legt fest, wie wichtig der Datenschutz für die Organisation ist, integriert ihn in die Strukturen und definiert die Ziele sowie die wesentlichen Aufgaben des Datenschutzmanagements. Das Minimalziel ist dabei gesetzlich vorgegeben: Die

Einhaltung der Vorgaben der Europäischen Datenschutzgrundverordnung sowie der ergänzenden nationalen Gesetze und Verordnungen.[138]

Die wichtigsten nationalen Gesetze in Österreich sind derzeit das Datenschutzgesetz 2018 (DSG), und das Telekommunikationsgesetz 2021 (TKG 2021) in dem auch die ePrivacy Richtlinie[139] umgesetzt ist.

7.4 Datenschutzmanagement(-system)

Managementsystem

Der Begriff „Managementsystem" kann aus verschiedenen Blickwinkeln betrachtet werden. Bspw wird in der ISO/IEC 27000:2018 ein Managementsystem als ein Rahmenwerk von Leitlinien, Verfahren, Richtlinien und den zugehörigen Ressourcen, um Ziele der Institution zu erreichen, beschrieben.[140]

Aus systemtheoretischer Sicht werden Unternehmen als sozio-technische Systeme betrachtet. Obwohl physische Dinge wie Büroklammern, Stifte oder Druckerpatronen ebenfalls Teil eines Unternehmens sind, besteht das Unternehmen aus systemtheoretischer Sicht aus zwei Hauptkomponenten: den Menschen und den materiellen Ressourcen (wie Anlagen). Managementsysteme sind dabei arbeitsteilige soziale Systeme, die alle Personen im Unternehmen umfassen, die an der Erreichung der Unternehmensziele und -zwecke beteiligt sind. Diese Ziele können nur durch das koordinierte und arbeitsteilige Handeln dieser Personen verwirklicht werden. Im Kern ist ein Managementsystem daher ein Entscheidungssystem, das darauf abzielt, die Unternehmensziele effizient zu steuern.[141]

Die folgende Abbildung veranschaulicht das:

[138] Vgl *Schäffter*, Datenschutzmanagement 2.0, 19.

[139] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002 S 37 - 47.

[140] *International Organization for Standardization (Hrsg)*, ISO/IEC 27000:2018, Information technology - Security techniques — Information security management systems - Overview and vocabulary (02.2018).

[141] Vgl *Erk/Spoun*, Integrativ managen: Ein Modell für eine effektive Praxis der Unternehmensführung (2020) 273ff.

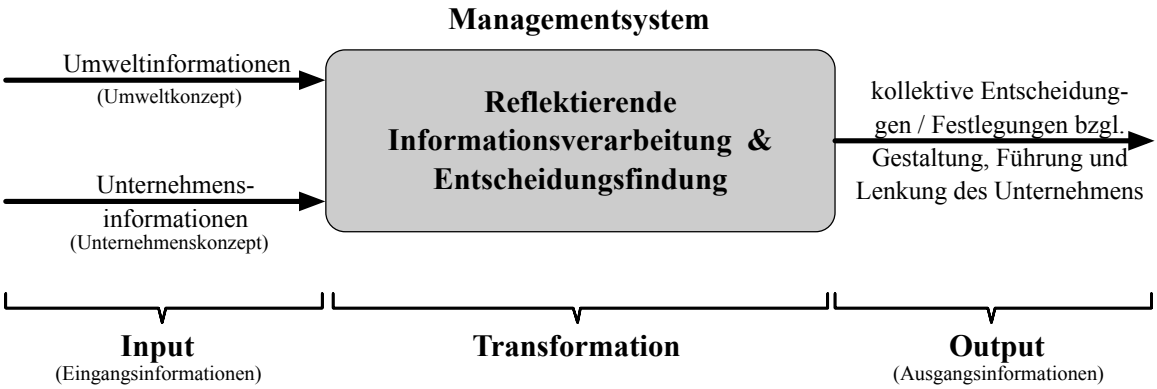


Abbildung 21: Managementsystem als Entscheidungssystem[142]

Managementsysteme werden auch häufig mit dem Konzept des „Orchestrierens" verglichen. Sie betrachten komplexe Themen ganzheitlich und beziehen dabei den gesamten „Lebenszyklus" mit ein. Grundsätzlich können sie als systematisches, zielgerichtetes und geplantes Vorgehen beschrieben werden, das auf die Umsetzung der Unternehmenspolitik und das Erreichen von Unternehmenszielen abzielt. Dies geschieht, indem sie betriebliche Prozesse steuern, eine strukturierte Prozessorganisation fördern und bestehende Abläufe im Unternehmen optimieren.[143]

Datenschutzmanagement

Datenschutzmanagement umfasst alle Maßnahmen zur Steuerung, Umsetzung und Überwachung der Datenschutzaktivitäten innerhalb eines Unternehmens oder einer Organisation. Dazu gehört auch die Kontrolle von Dienstleistern, Zulieferern und Geschäftspartnern, mit denen personenbezogene Daten ausgetauscht werden. Ein wichtiger Bestandteil des Datenschutzmanagements ist die Erstellung eines Datensicherheitskonzepts, das die Grundlage für den Schutz personenbezogener Daten bildet.[144]

[142] *Erk/Spoun*, Integrativ managen, 275.

[143] Vgl *Gaess*, Datenschutz mit bewährten Methoden des Risikomanagements: Handreichung (Datenschutzberater 2020) 11; Was ist ein Managementsystem & was zeichnet Managementsysteme aus? <https://www.din-iso-zertifizierung-qms-handbuch.de/was-ist-ein-managementsystem/>; zuletzt aufgerufen am 14.01.2025.

[144] Vgl *Schäffter*, Datenschutzmanagement 2.0.

Leicht abweichend von den oben beschriebenen Definitionen für Datenschutz definiert die ÖNORM 2017:2023 Datenschutzmanagementsystem als ein „*Managementsystem für Informationssicherheit, das sich mit dem Schutz der durch die Verarbeitung personenbezogener Daten möglicherweise beeinträchtigten Privatsphäre befasst.*“[145]

Beim Aufbau eines Datenschutzmanagementsystems sind verschiedene Aspekte zu berücksichtigen:[146]

- Managementauftrag
- Teilen der Verantwortung
- Unterrichten der Leitungsebene
- Einrichten der Datenschutzprozesse
- Erstellen von Richtlinien
- Beraten auf Fachebene
- Beraten auf Projektebene
- Durchführen von internen Kontrollen
- Durchführen von Schulungen
- Arbeiten zur Dokumentation
- Nachweisen der Ordnungsmäßigkeit
- Kontrollieren der Auftragsverarbeitungen
- Bewerten der wesentlichen Risiken
- Bearbeiten von Anfragen
- Zusammenarbeit mit der Aufsicht

Laut *Schäffter* gibt es folgende wichtige Aspekte und Ziele beim Datenschutz-management:[147]

- Vermeidung von Rechtsverletzungen und ihrer Folgen.
- Regelung der Verantwortlichkeiten im Datenschutz [...].
- Bestellung einer/eines Datenschutzbeauftragten (sofern erforderlich).

[145] *Austrian Standards International (Hrsg)*, ÖNORM A 2017:2023, Datenschutzmanagementsysteme (01.06.2023) 4.

[146] Vgl *Schäffter*, Datenschutzmanagement 2.0, 13f.

[147] *Schäffter*, Datenschutzmanagement 2.0, 16f.

- Trennung der Zuständigkeiten für den Datenschutz und die Informationssicherheit [...].
- Angemessene Beteiligung des betrieblichen bzw behördlichen Datenschutzbeauftragten in der Aufbau- und Ablauforganisation der verantwortlichen Stelle
- Angemessene Unterstützung des/der Datenschutzbeauftragten; Nachweis einer aktiven Tätigkeit
- Dokumentation und Verfahrensweise der Beteiligung des Bundes- oder Landesbeauftragten für Datenschutz oder Beteiligung der zuständigen Aufsichtsbehörde.
- Einhaltung der Datenschutzprinzipien, u.a. von Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung und Integrität und Vertraulichkeit
- Wahrung der Betroffenenrechte: Recht auf Auskunft, Berichtigung, Sperrung, Widerspruch, Schadenersatz.
- Verbot automatisierter Bewertungen (ohne manuelle Freigabe).

Auch im Standard-Datenschutzmodell (SDM) widmet sich ein Kapitel dem Thema Datenschutzmanagement.[148]

[148] Vgl *AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Das Standard Datenschutzmodell 3.1 - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (14.05.2024) 57ff.

Aufbau- und Ablauforganisation

Bei der Entwicklung einer Datenschutzorganisation ist sowohl die Aufbauorganisation als auch auf die Ablauforganisation („Prozesse“) zu entwickeln. Die nachfolgende Grafik zeigt eine vereinfachte Darstellung der Aufbau- und Ablauforganisation.

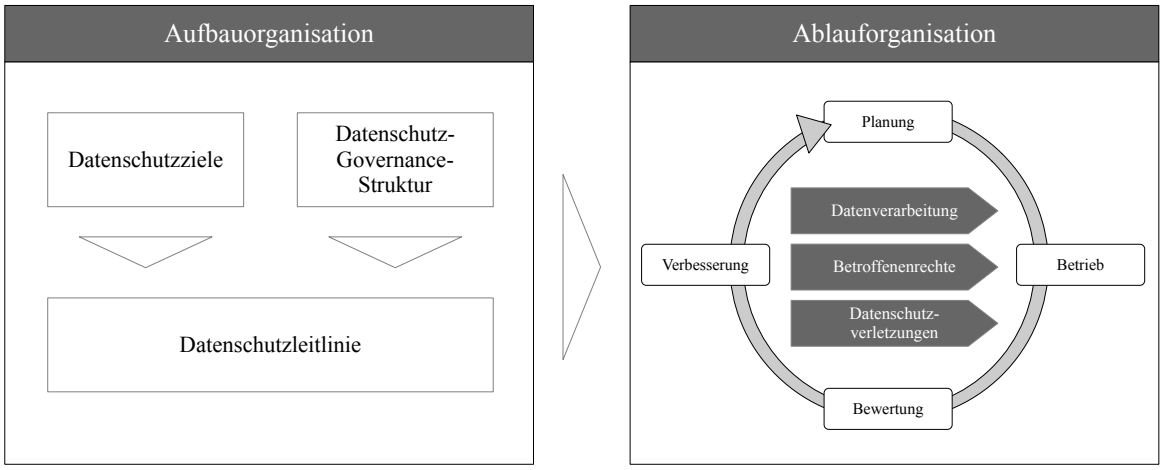


Abbildung 22: Datenschutzaufbau- und -ablauforganisation[149]

7.5 Datenschutzziele

7.5.1 Einleitung

Der Definition von Datenschutzzielen kommt im Zusammenhang mit Risikomanagement erhebliche Bedeutung zu, da „Risiko“ im Wesentlichen eine Zielabweichung bedeutet (vgl oben).

Für Kranig et al leiten sich die Datenschutzziele „*aus dem Sinngehalt der Datenschutzgesetze ab*“[150]. An anderer Stelle ist es eine Frage der strategischen Ausrichtung des Unternehmens, „*ob bei der Umsetzung von Datenschutz eine größtmögliche Compliance mit den gesetzlichen Vorschriften angestrebt werden soll (Compliance-Ansatz) oder möglicherweise über die gesetzlichen Vorschriften hinaus, z.B. aus Gründen von Wettbewerbsvorteilen, zusätzliche Anforderungen eingehalten werden sollen.*“[151]

Jedenfalls aber stellen die Datenschutzziele einen Teil der Unternehmensziele dar:

[149] *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 27.

[150] *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 27.

[151] *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 32f.

Abbildung 23: Datenschutz als Teil der Unternehmensziele[152]

Weiters stellt sich die Frage, wie einfach es ist, Ziele in konkrete funktionale Anforderungen umzuwandeln. Der Markt bietet nur wenige Modelle, die den Anspruch erheben, datenschutzrechtliche Vorgaben in solche konkreten Anforderungen zu übersetzen. Diese Umwandlung, die bei der Prüfung oder Gestaltung einer Verarbeitungstätigkeit unvermeidlich ist, ist dabei immer mit Verlusten verbunden – es bleibt immer ein gewisses Maß an Unschärfe oder Lücken bestehen.[153]

7.5.2 NIST Privacy Framework

Das NIST Privacy Framework ist ein Werkzeug, das entwickelt wurde, um Organisationen zu helfen, die Privatsphäre von Individuen durch ein umfassendes Risikomanagement zu verbessern. Dabei wird das Management von Datenschutzrisiken als organisationsübergreifender Prozess gesehen, der Unternehmen dabei unterstützt, zu verstehen, wie ihre Systeme, Produkte und Dienstleistungen potenzielle Probleme für Einzelpersonen verursachen können. Gleichzeitig hilft es, effektive Lösungen zu entwickeln, um diese Risiken zu bewältigen.[154]
Die nachstehende Grafik verdeutlicht den Zusammenhang zw Datenschutzrisiken und organisatorischem Risiko.

[152] *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 32.

[153] Vgl *Sowa/Rost*, Die ISO 27701 und das SDM-V2 im Lichte der Umsetzung der DSGVO, Datenschutz und Datensicherheit - DuD 2020, 659–662 (659).

[154] Vgl NIST privacy framework : a tool for improving privacy through enterprise risk management (2020) 4.

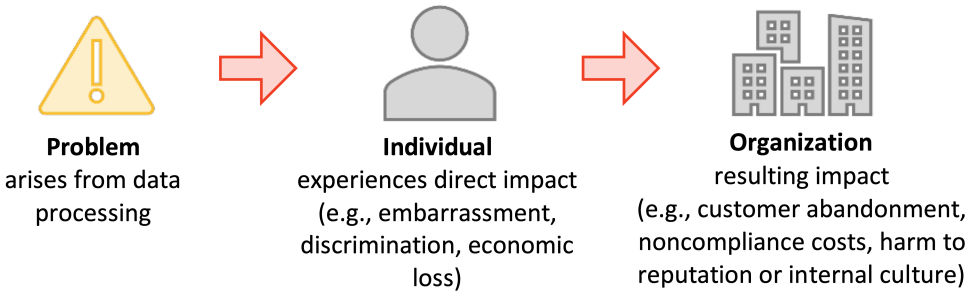


Abbildung 24: Relationship Between Privacy Risk and Organizational Risk[155]

Das Framework bietet zudem „Profile“, die es Organisationen ermöglichen, ihren aktuellen Datenschutzstatus zu bewerten und Ziele für Verbesserungen zu setzen. „Implementierungsebenen“ helfen dabei, den Reifegrad des Datenschutzmanagements einer Organisation einzuschätzen.
Das NIST Privacy Framework ist also ein flexibles und anpassbares Werkzeug, das Organisationen unterstützt, Datenschutzrisiken systematisch zu managen und dabei sowohl nationale als auch internationale Datenschutzvorschriften zu berücksichtigen.

7.5.3 Standard Datenschutzmodell

Das Standard Datenschutzmodell (SDM) des Arbeitskreises „Technik“ der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ist eine Hilfestellung für die Orientierung der europaweit geltenden Rechtsvorschriften.[156]
Seit dem Beschluss der DSK am 14. Mai 2024 liegt das Modell in der Version 3.1 vor.[157]

Das Standard-Datenschutzmodell (SDM) bietet effektive Methoden, um die rechtlichen Vorgaben der DSGVO in konkrete technische und organisatorische Maßnahmen umzusetzen. Dazu werden die rechtlichen Anforderungen zunächst identifiziert und den sogenannten Gewährleistungszielen wie Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit zugeordnet. Auf dieser Grundlage überführt das SDM die abstrakten rechtlichen Vorgaben in spezifische technische und organisatorische Maßnahmen, die im Referenzmaßnahmen-Katalog des

[155] NIST privacy framework : a tool for improving privacy through enterprise risk management, 4.

[156] Vgl *Schäffter*, Datenschutzmanagement 2.0, 34.

[157] Vgl *AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Das Standard Datenschutzmodell 3.1 - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (14.05.2024) 5.

SDM detailliert beschrieben sind. Dadurch erleichtert das SDM die systematische Umsetzung der DSGVO-Anforderungen und ermöglicht es, standardisiert zu überprüfen, ob die für die Datenverarbeitung vorgesehenen Maßnahmen den rechtlichen Anforderungen entsprechen.[158]

Schäffter beschreibt die Vorgangsweise für die Anwendung des SDMs wie folgt:[159]

1. **Erfassung der zentralen Verfahren**: Es werden die relevanten Daten, IT-Systeme und Prozesse beschrieben, wobei die Abgrenzung hauptsächlich durch die Zweckbindung erfolgt.
2. **Zuordnung der Datenschutzanforderungen**: Datenschutzrechtliche Anforderungen werden allgemeinen oder verfahrensspezifischen Gewährleistungszielen zugeordnet.
3. **Schutzbedarfsanalyse**: Basierend auf dem Stufenmodell des BSI wird der Schutzbedarf personenbezogener Daten ermittelt. Dieser Schutzbedarf wird anschließend auf die zugehörigen IT-Systeme und Prozesse übertragen.
4. **Ableitung von Schutzmaßnahmen**: Auf Grundlage standardisierter generischer Schutzmaßnahmen und eines zukünftigen Referenzkatalogs werden passende und wirksame technische und organisatorische Schutzmaßnahmen abgeleitet.
5. **Bewertung der Schutzmaßnahmen**: Die Wirksamkeit der umgesetzten Maßnahmen wird überprüft, gegebenenfalls durch eine Risikoanalyse verifiziert. Identifizierte Defizite können so erkannt und gezielt behoben werden.

Anmerkung des Autors: *Schäffter* bezieht sich hier auf eine sehr frühe Version des SDM – im Oktober 2017 war lediglich eine Erprobungsfassung des SDM Handbuchs verfügbar. Erst im April 2018 wurde die Version 1.1 des stark überarbeiteten SDM Handbuchs veröffentlicht.[160]

[158] Vgl *AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Das Standard Datenschutzmodell 3.1 - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (14.05.2024) 5f.

[159] Vgl *Schäffter*, Datenschutzmanagement 2.0, 35f.

[160] Vgl *AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*, Das Standard Datenschutzmodell 3.1 - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (14.05.2024) 71.

Daher ist auch nicht verwunderlich, dass zu diesem Zeitpunkt keine Maßnahmenkataloge zur Verfügung standen. Per Mitte August 2024 stehen folgende Bausteine des Maßnahmenkatalogs zur Verfügung:[161]

Tabelle 3: Bausteine aus dem Maßnahmenkatalog des SDM (eigene Darstellung)

Baustein 11	Aufbewahren
Baustein 41	Planen und Spezifizieren
Baustein 42	Dokumentieren
Baustein 43	Protokollieren
Baustein 50	Trennen
Baustein 51	Zugriffe auf Daten, Systeme und Prozesse regeln
Baustein 60	Löschen und Vernichten
Baustein 61	Berichtigen
Baustein 62	Einschränken der Verarbeitung

7.5.4 ISO 27701

Die Norm ISO 27701[162] hat das Ziel, Anforderungen und Leitlinien für die Einrichtung, Umsetzung, Wartung und kontinuierliche Verbesserung eines Datenschutz-Informationsmanagementsystems (Privacy Information Management System, PIMS) bereitzustellen. Sie verweist auf den bestehenden Standard ISO/IEC 27000[163] (Übersicht und Begriffe des ISMS) und ergänzt ISO/IEC 27001[164] (Anforderungen an das ISMS) und

[161] Vgl Standard-Datenschutzmodell - Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>, zuletzt aufgerufen am 22.01.2025.

[162] *International Organization for Standardization (Hrsg)*, ISO/IEC 27701:2019, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management Requirements and guidelines (2019).

[163] *International Organization for Standardization (Hrsg)*, ISO/IEC 27000:2018, Information technology - Security techniques — Information security management systems - Overview and vocabulary (02.2018).

[164] *International Organization for Standardization (Hrsg)*, ISO/IEC 27701:2019, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management Requirements and guidelines (2019).

ISO/IEC 27002[165] (Leitlinien für Sicherheitsmaßnahmen) und bietet zudem eine Zuordnung von Maßnahmen aus weiteren Standards (wie ISO/IEC 29100[166] (Rahmenwerk für Datenschutz), ISO/IEC 27018[167] (Datenschutz in Public-Cloud-Diensten) und ISO/IEC 29151[168] (Leitfaden zum Schutz personenbezogener Daten)) sowie zur DSGVO.
Die ISO/IEC 27701 stellt dabei keinen eigenständigen Standard dar, der unabhängig genutzt werden kann. Tatsächlich ist sie jedoch nur in Verbindung mit ISO 27001 anwendbar. Die Anforderungen an ein PIMS sind lediglich eine Erweiterung von ISO 27001. Der Standard passt die Terminologie von "Informationssicherheit" auf "Informationssicherheit und Datenschutz" an, wodurch der Fokus zusätzlich auf den Schutz personenbezogener Daten gelegt wird.
Schon die Einbettung in die ISO-Normenfamilie zeigt dabei, dass bei der ISO/IEC 27701 ein anderer Ansatz als bspw beim Standard-Datenschutzmodell gewählt wurde. Das SDM hat die grundrechtkonforme Gestaltung von Verarbeitungstätigkeiten im Fokus. Für die ISO/IEC 27701 hingegen ist es wichtig, einen praxisgerechten Kontakt zur Organisation und ihren Prozessen zu halten. Hinzu kommt, dass die ISO/IEC 27701 – im Gegensatz zum SDM – nicht spezifisch auf die DSGVO ausgerichtet ist.[169]

7.5.5 Datenschutz-Audit

Das Buch "Datenschutz-Audit" dient als umfassender Praxisleitfaden, der speziell darauf ausgerichtet ist, Organisationen bei der Einhaltung der Datenschutz-Grundverordnung (DSGVO) zu unterstützen. Es legt die aus der DSGVO resultierenden Pflichten auf die Kernbereiche Recht, Organisation, Prozess und IT um und bietet detaillierte Kontrollen, um die Einhaltung dieser Verpflichtungen effizient zu überprüfen. Dieses Kontrollset ist ein zentrales Element und übersetzt DSGVO (und, je nach Ausgabe auch nationalstaatliche

[165] *International Organization for Standardization (Hrsg)*, ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls (2013).

[166] *International Organization for Standardization (Hrsg)*, ISO/IEC 29100:2024, Information technology — Security techniques — Privacy framework (02.2024).

[167] *International Organization for Standardization (Hrsg)*, ISO/IEC 27018:2019, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (01.2019).

[168] *International Organization for Standardization (Hrsg)*, ISO/IEC 29151:2017, Information technology — Security techniques — Code of practice for personally identifiable information protection (08.2017).

[169] Vgl *Sowa/Rost*, Datenschutz und Datensicherheit - DuD 2020, 659–662 (659f).

Datenschutzregelungen) in prüfbare Kontrollen. Dadurch sollen Organisationen ihre Selbstverantwortung zur Einhaltung der datenschutzrechtlichen Pflichten besser wahrnehmen können.[170]

7.5.6 ÖNORM A 2017

Die ÖNORM A 2017[171] definiert Vorgaben für Datenschutzmanagementsysteme in Organisationen, die mit personenbezogenen Daten arbeiten. Ziel ist es, die Anforderungen der DSGVO umzusetzen, wobei sie sich an den Standards der ISO/IEC 27000-Reihe orientiert.[172]

Die ÖNORM A 2017 orientiert sich dabei an den Bedürfnissen kleinerer Organisationen. Sie soll dabei helfen, die Einhaltung der DSGVO-Vorschriften sicherzustellen, Datenschutzrisiken zu minimieren und das Vertrauen von Kunden und Behörden zu stärken. Dieser Standard ermöglicht die Einrichtung, Pflege und kontinuierliche Verbesserung von Datenschutzmanagementsystemen sowie die Beurteilung und Behandlung von Datenschutzrisiken. KMUs profitieren dabei von einer leistbaren und flexiblen Lösung, die entweder eigenständig oder integriert in bestehende Managementsysteme genutzt werden kann. Die ÖNORM A 2017 soll nicht nur rechtliche Sicherheit bringen, sondern auch dokumentieren, dass Unternehmen Datenschutz ernst nehmen und sich kontinuierlich verbessern.[173]

[170] Vgl *Pachinger* (Hrsg), Datenschutz-Audit: Recht - Organisation - Prozess - IT: der Praxisleitfaden zur Datenschutz-Grundverordnung (Rechtspraxis 2017).

[171] *Austrian Standards International (Hrsg)*, ÖNORM A 2017:2023, Datenschutzmanagementsysteme (01.06.2023).

[172] Vgl *Austrian Standards International (Hrsg)*, ÖNORM A 2017:2023, Datenschutzmanagementsysteme (01.06.2023).

[173] Vgl *Austrian Standards plus GmbH (Hrsg)*, Datenschutz-Management: So profitieren KMU von der neuen ÖNORM A 2017 <https://www.austrian-standards.at/de/newsroom/pressemeldungen/datenschutz-management-so-profitieren-kmu-von-der-neuen-oenorm-a-2017> (2023), zuletzt aufgerufen am 22.01.2025.

Um diese Ziele zu erreichen, stellt die ÖNORM A 2017 in den Anhängen A und B „Maßnahmenziele und Maßnahmen für Verantwortliche“ (respektive Auftragsverarbeiter in Anhang B) zur Verfügung. Dabei folgt die ÖNORM A 2017 hinsichtlich der Ziele folgender Struktur:[174]

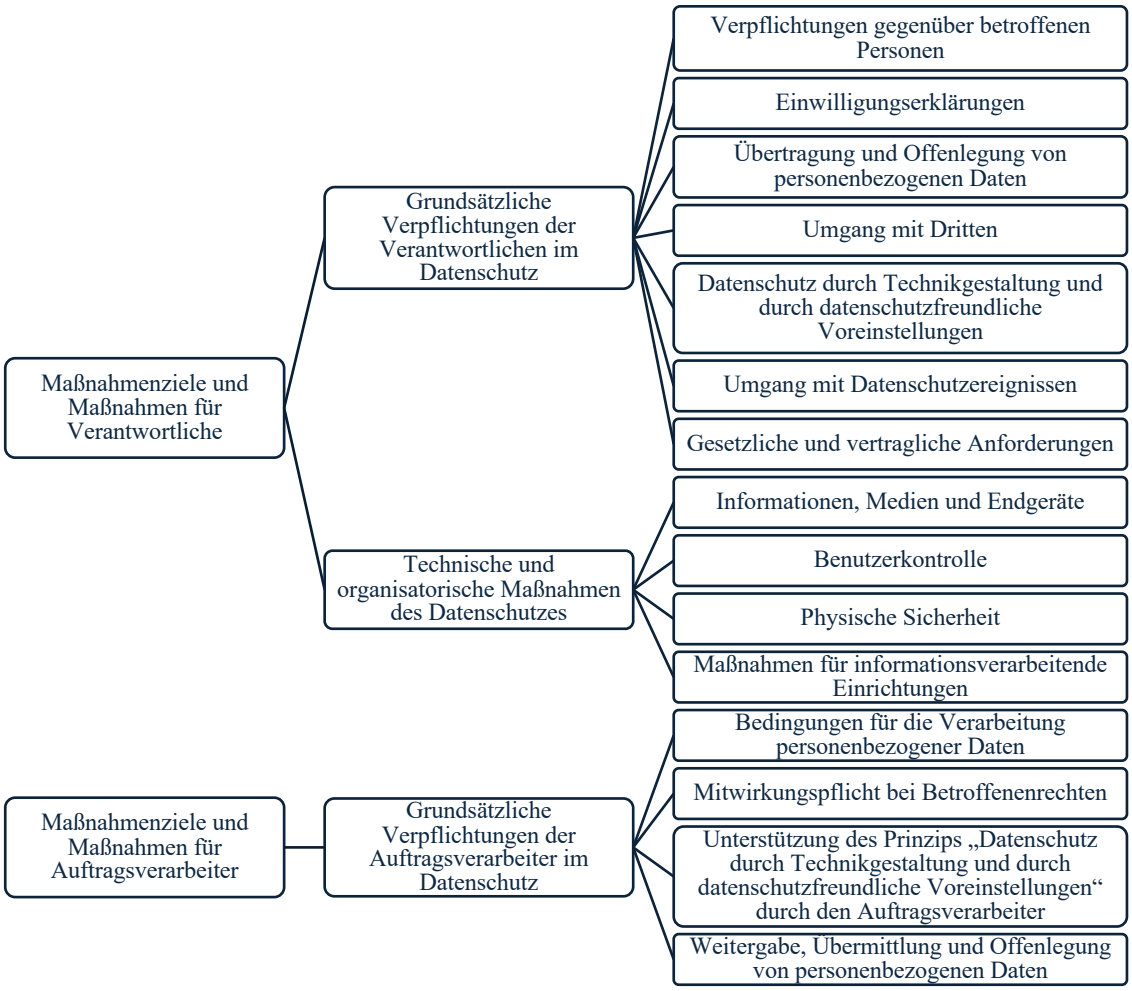


Abbildung 25: Zielestruktur ÖNORM A 2017 (eigene Darstellung)

In der ÖNORM A 2017 werden in einer weiteren Ebene Maßnahmen angeführt, um die oben beschriebenen Ziele zu erreichen. Für die beschriebenen Maßnahmen dürfte nach Ansicht des Autors weitere Operationalisierung notwendig sein, um sie bspw als Ziele für ein quantitatives Risikomanagement verwenden zu können.

[174] Vgl *Austrian Standards International (Hrsg)*, ÖNORM A 2017:2023, Datenschutzmanagementsysteme (01.06.2023) 21ff.

7.5.7 FIPPs – Fair Information Practice Principles

Die Fair Information Practice Principles (FIPPs) bilden die Grundlage vieler Datenschutzgesetze und -richtlinien weltweit und umfassen grundlegende Prinzipien, die den Umgang mit persönlichen Informationen regeln sollen. Ursprünglich wurden diese Prinzipien in den 1970er Jahren in einem Bericht des US-amerikanischen Department of Health, Education, and Welfare festgelegt. Die Kernprinzipien der FIPPs, die in verschiedenen Formulierungen bestehen, sind jedoch weitgehend konsistent und umfassen wichtige Aspekte wie Zugang und Berichtigung, Rechenschaftspflicht, Befugnis, Minimierung, Qualität und Integrität, individuelle Teilnahme, Zweckbestimmung und Nutzungsbegrenzung sowie Sicherheit und Transparenz.[175]
Vom National Institute of Standards and Technology wird auch eine Überleitung von den FIPPs zum NIST Privacy Framework zur Verfügung gestellt.[176]

7.5.8 Nissenbaum's "contextual integrity"

Die Theorie der "Contextual Integrity" von Helen Nissenbaum bietet einen innovativen Ansatz zum Verständnis von Datenschutz, indem sie die Bedeutung des Kontextes in den Vordergrund stellt. Nissenbaum argumentiert, dass der Schutz der Privatsphäre abhängig von den spezifischen Normen jedes sozialen Kontextes ist. Dabei betont sie, dass Informationen in einer Weise fließen sollten, die mit den Erwartungen und Normen dieses Kontextes übereinstimmt.
Ein zentraler Aspekt der Theorie ist, dass der Schutz der Privatsphäre nicht nur als eine Frage des individuellen Kontrollrechts über Informationen gesehen werden sollte. Vielmehr sollte die Angemessenheit des Informationsflusses innerhalb bestimmter sozialer Kontexte bewertet werden.[177]

7.5.9 Calo's Harm Dimensions

M. Ryan Calo's "The Boundaries of Privacy Harm" präsentiert eine differenzierte Betrachtung von Datenschutzverletzungen, indem er sie in zwei Hauptkategorien einteilt:

[175] Vgl *The Federal Privacy Council (FPC)*, Fair Information Practice Principles (FIPPs) <https://www.fpc.gov/resources/fipps/> (2016), zuletzt aufgerufen am 17.01.2025.

[176] Vgl *National Institute of Standards and Technology (Hrsg)*, Fair Information Practice Principles (FIPPs) Crosswalk <https://www.nist.gov/privacy-framework/fair-information-practice-principles-fipps-crosswalk> (2021), zuletzt aufgerufen am 22.01.2025.

[177] Vgl *Nissenbaum*, Privacy as Contextual Integrity, Washington Law Review 2004, 119ff.

subjektive und objektive Schäden. Subjektive Schäden beziehen sich auf die Wahrnehmung unerwünschter Beobachtung, die unangenehme mentale Zustände wie Angst, Peinlichkeit oder Furcht hervorrufen kann. Diese Kategorie umfasst alle Formen von Eingriffen in die Privatsphäre, die das Gefühl der Überwachung beim Betroffenen verursachen, von der Spionage durch den Vermieter bis hin zur umfassenden staatlichen Überwachung. Objektive Schäden entstehen hingegen durch die unerwartete oder erzwungene Verwendung von Informationen über eine Person, die gegen diese verwendet werden. Beispiele hierfür sind Identitätsdiebstahl, die Veröffentlichung klassifizierter Informationen, die einen verdeckten Agenten enttarnen, oder die Nutzung des Blutes eines betrunkenen Fahrers als Beweis gegen ihn. Diese Kategorie umfasst negative externe Handlungen, die durch persönliche Informationen gerechtfertigt werden. [178]

7.5.10 Factors Analysis in Information Risk (FAIR) Model

Das Modell "Factor Analysis of Information Risk" (FAIR) ist ein umfassendes Framework zur Quantifizierung und Analyse von Informationsrisiken. Es bietet einen strukturierten Ansatz, um die Wahrscheinlichkeit und das potenzielle Ausmaß von Verlusten zu bewerten, die aus Sicherheitsrisiken entstehen können.

FAIR unterscheidet sich von anderen Risikobewertungsmethoden durch seinen quantitativen Ansatz, der es ermöglicht, Risiken in finanziellen Begriffen auszudrücken. Dieser Ansatz unterstützt Organisationen dabei, ihre Risiken besser zu verstehen und fundierte Entscheidungen über Risikomanagementstrategien zu treffen.[179]

7.6 Datenschutz-Governance

Laut der EU-Datenschutzgrundverordnung teilen sich die Leitung, die Fachabteilungen und die Datenschutzbeauftragte die Verantwortung für den Datenschutz. Die Datenschutzbeauftragte übernimmt dabei vor allem eine beratende und überwachende Funktion.[180]

[178] Vgl *Calo*, The Boundaries of Privacy Harm, Indiana Law Journal(2011).

[179] Vgl *Jones*, An Introduction to Factor Analysis of Information Risk (FAIR), Norwich University Journal of Information Assurance (NUJIA) 2006, 1–66.

[180] Vgl *Schäffter*, Datenschutzmanagement 2.0, 84.

Die folgende Grafik zeigt die Verteilung der Aufgaben im Modell der „Three Lines of Defense“.

Das Modell der „Three Lines of Defense“

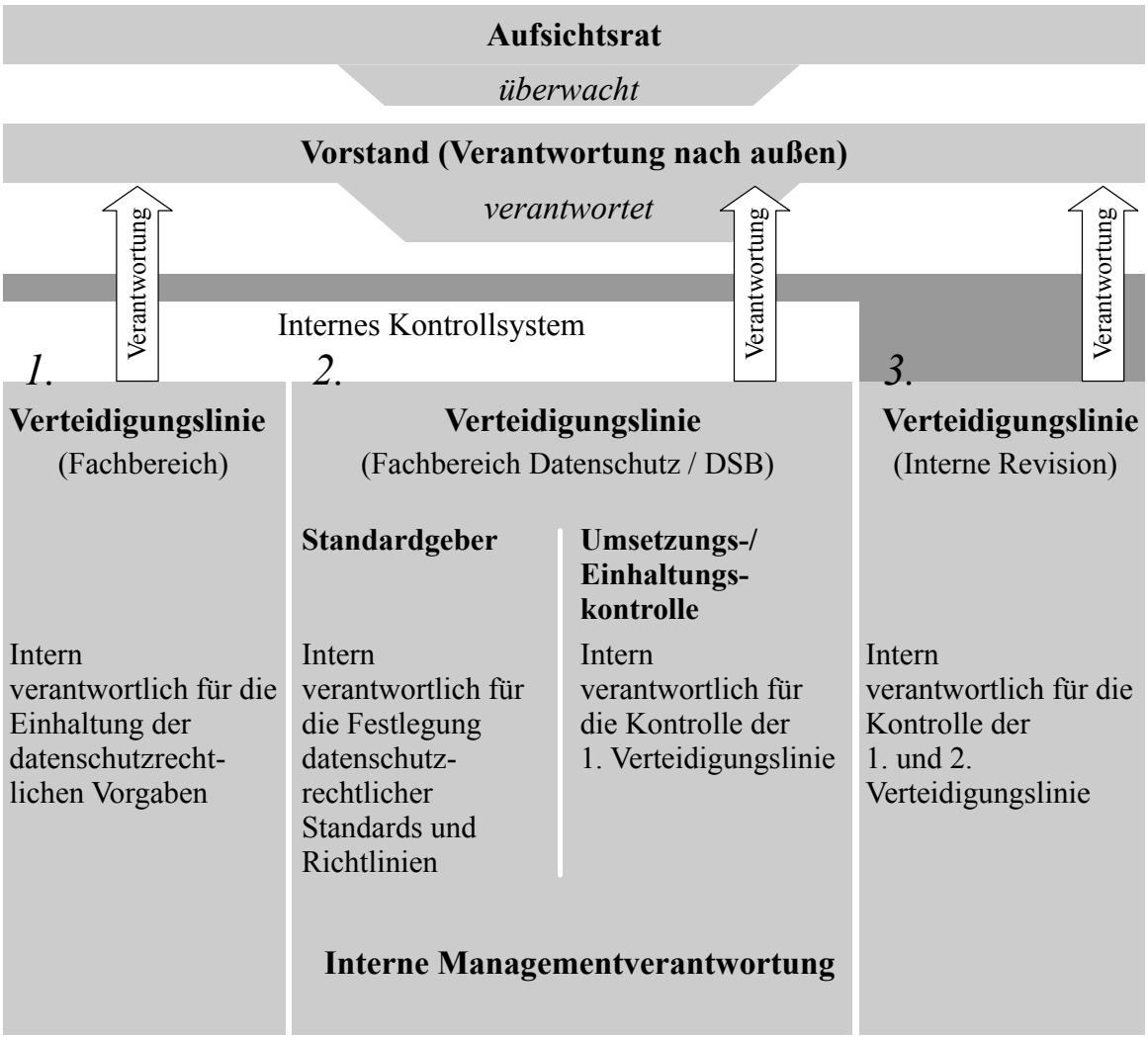


Abbildung 26: Modell der drei Verteidigungslinien[181]

Das Modell der „Three Lines of Defense” gliedert sich in 3 Verteidigungslinien. Diese Verteidigungslinien interagieren und sind folgendermaßen aufgebaut:[182]

Erste Verteidigungslinie:

Diese Verteidigungslinie wird von den operativ tätigen Fachbereichen gebildet und ist für die Arbeitsergebnisse wie auch für die daraus resultierenden Risiken verantwortlich.

[181] *Gaess*, Datenschutz mit bewährten Methoden des Risikomanagements, 6.

[182] Vgl *Gaess*, Datenschutz mit bewährten Methoden des Risikomanagements, 7.

Zweite Verteidigungslinie:
Die zweite Verteidigungslinie ist für die Steuerung und Überwachung der ersten Verteidigungslinie zuständig. Sie ist die standardgebende Instanz und wacht auch über die Einhaltung der gesetzten Vorgaben.

Dritte Verteidigungslinie:
Die dritte Verteidigungslinie in diesem Modell stellt eine unabhängige Prüfinstanz dar. Sie prüft die Zuständigkeitserfüllung der ersten und zweiten Verteidigungslinie.

Das Modell der „Three Lines of Defense“ findet sich auch im hybriden Datenschutz-Governance-Modell der International Association of Privacy Professionals (IAPP) wieder.[183]

Das „Three Lines of Defense” Modell spiegelt die Wichtigkeit der Verteilung von Aufgaben, Rollen und Verantwortlichkeiten wider. Während bspw die Fachbereiche Datenschutz oft im Organisationsbereich Datenschutz oder der IT-Abteilung sehen, versteht sich der Fachbereich Datenschutz in vielen Fällen wiederum nur als beratendes oder prüfendes Organ und sieht die Verantwortung für Datenschutzmanagement bei der Geschäftsführung. Die Geschäftsführung hingegen kann den Mehrwert von Datenschutz nicht erkennen und sieht darin lediglich ein Hindernis für die Geschäftsentwicklung.[184]

7.7 Risiko-Begriff in der DSGVO

Ein zentrales Ziel der DSGVO ist es, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen.[185] Dementsprechend zielt auch der Begriff Risiko, der sich in verschiedenen Erwägungsgründen der DSGVO findet auf die Rechte und Freiheiten natürlicher Personen ab.[186]

[183] Vgl *Densmore/International Association of Privacy Professionals* (Hrsg), Privacy program management: tools for managing privacy within your organization (2013) 20.

[184] Vgl *Gaess*, Datenschutz mit bewährten Methoden des Risikomanagements, 14f.

[185] Vgl Art 1 Abs 2 DSGVO (EU) 679/2016.

[186] Vgl ErwGr 74ff DSGVO (EU) 679/2016; ErwGr 94 DSGVO (EU) 679/2016.

Dementsprechend beschreibt ein Risiko im Sinne der DSGVO die Möglichkeit, dass ein Ereignis eintritt, welches entweder direkt Schaden verursacht (einschließlich der ungerechtfertigten Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) oder zu weiteren Schäden für eine oder mehrere Personen führen kann. Dabei gibt es zwei wesentliche Aspekte: Zum einen die Schwere des möglichen Schadens, und zum anderen die Wahrscheinlichkeit, dass das Ereignis und seine Folgen tatsächlich eintreten. Solche Schäden können sowohl aus der geplanten Verarbeitung von Daten selbst resultieren als auch aus Abweichungen, die entweder durch eigenes Verschulden oder durch Dritte verursacht werden.[187]

Zusammenfassend lässt sich sagen, dass der Begriff Risiko in der DSGVO sehr eingeschränkt verwendet wird. Es wird nur auf Risiko im engeren Sinne (also mit negativen Auswirkungen) abgezielt. Und selbst hier werden „nur“ die Rechte und Freiheiten natürlicher Personen berücksichtigt. Risiken für den Verantwortlichen iSv Compliance Risiken, werden nicht berücksichtigt. Es werden auch keine psychologischen Effekte für Betroffene, wie zB das Vertrauen in einen Verantwortlichen, behandelt.

7.8 DSGVO-Geldbußen

Geldbußen können – neben anderen Effekten - negative Auswirkungen von Datenschutz-Risiken sein. Dabei muss man zwischen den maximalen Geldbußen und den tatsächlich verhängten Geldbußen unterscheiden. Außerdem ist dabei zu beachten, dass Geldbußen nicht nur aufgrund von Verletzungen der DSGVO anfallen können, sondern auch aufgrund Verletzungen anderer Regelungen, bspw dem Telekommunikationsgesetz oder dem Datenschutzgesetz.
Als eine der Auswirkungen von Datenschutzrisiken sind Geldbußen ein wichtiges Instrument für die Risikoquantifizierung.

[187] Vgl *Datenschutzkonferenz (Hrsg)*, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf> (2018), zuletzt aufgerufen am 19.01.2025.

Im Art 83 DSGVO sind die maximalen Höhen der DSGVO-Geldbußen beschrieben[188]. Die nachstehende Tabelle gibt einen Überblick dazu.

Tabelle 4: Geldbußen gem Art 83 Abs 4 und Abs 5 DSGVO

Geldbuße	**Anwendung**
2% bzw 10 Millionen Euro	Die Pflichten der Verantwortlichen und der Auftragsverarbeiter gem den Artikeln 8, 11, 25 – 39, 42, 43
	Die Pflichten der Zertifizierungsstelle gem den Artikeln 42 und 43
	Die Pflichten der Überwachungsstelle gem Artikel 41 Abs 4
4% bzw 20 Millionen Euro	Die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gem den Artikeln 5, 6, 7 und 9
	Die Rechte der betroffenen Personen gem den Artikeln 12 – 22
	Die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gem den Artikeln 44 – 49
	Alle Pflichten gem den Rechtsvorschriften der Mitgliedsstaaten, die im Rahmen des Kapitels IX („Vorschriften für besondere Verarbeitungssituationen“) erlassen wurden
	Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gem Artikel 58 Abs 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Abs 1

[188] Art 83 DSGVO (EU) 679/2016.

Diese Regelung betrifft die maximalen DSGVO-Geldbußen. Die tatsächlich verhängten DSGVO-Geldbußen sind oft deutlich niedriger. Das lässt sich aus dem folgenden Diagramm ablesen. Es zeigt die Häufigkeitsverteilung von DSGVO-Geldbußen in Abhängigkeit der Höhe der Geldbuße. Zugrunde liegen dabei die Daten des „Enforcement Trackers“ mit Stand vom 25. Juli 2024.[189] Obwohl die im „Enforcement Tracker“ erfassten Geldbußen nicht vollständig sein dürften, ist es die umfangreichste Quelle für derartige Daten.

Um die große Bandbreite der Höhe von Geldbußen übersichtlich darzustellen, wurde dabei für die horizontale Achse (Höhe der Geldbuße) eine logarithmische Skalierung gewählt:

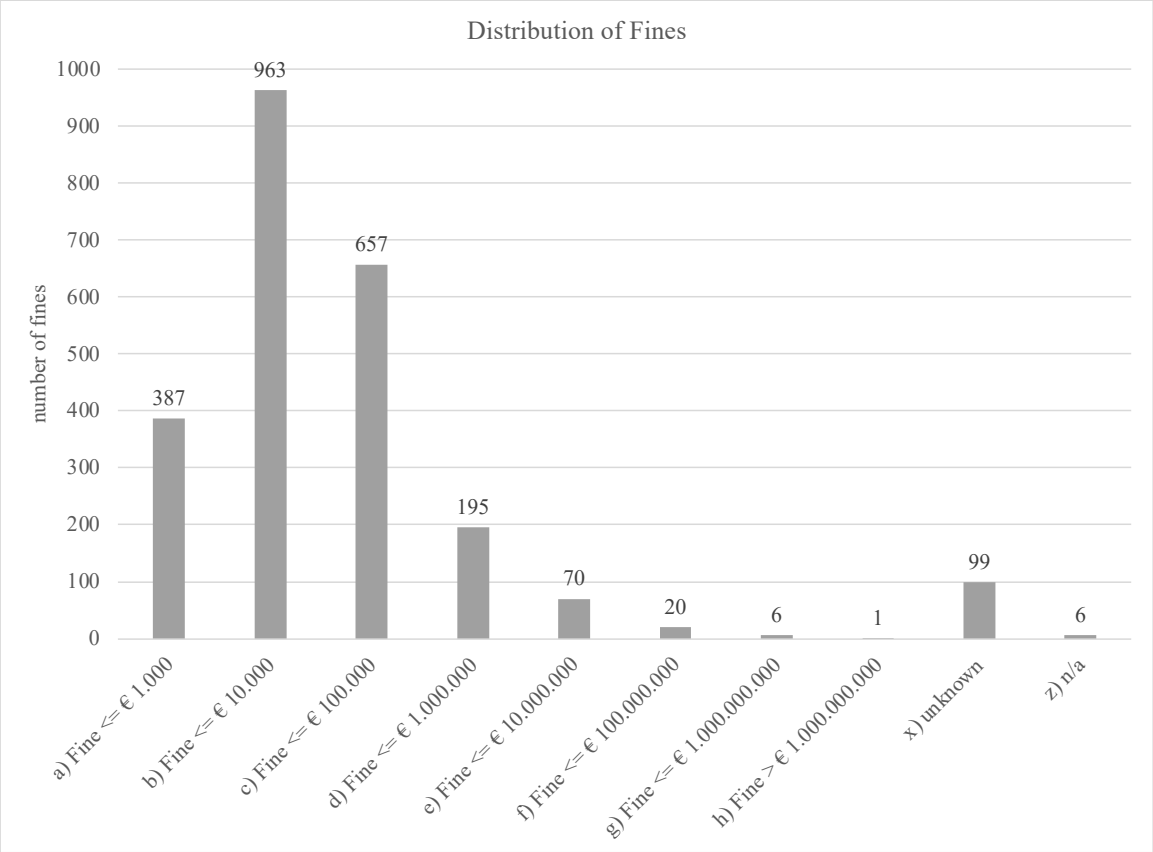


Abbildung 27: Häufigkeitsverteilung von DSGVO-Geldbußen gem „Enforcement Tracker“ (eigene Darstellung)

Diese Darstellung kann ggf. als Hilfestellung für die Quantifizierung eines Risikos herangezogen werden. Bspw dürfte diese Darstellung an eine Lognormal-Verteilung

[189] GDPR Enforcement Tracker - list of GDPR fines <https://www.enforcementtracker.com> Stand 25.07.2024, zuletzt aufgerufen am 19.01.2025.

hinweisen. Dabei ist zu berücksichtigen, dass in dieser Darstellung die Höhe des Bußgelds (x-Achse) logarithmisch skaliert ist.

Außerdem ist zu berücksichtigen, dass die Häufigkeitsverteilung der Höhe der Geldbußen vom Gebaren der jeweiligen Datenschutzbehörde abhängig ist. In der nachfolgenden Grafik ist deswegen der Anteil der Höhe von DSGVO-Bußgeldern auf Staaten aufgeteilt dargestellt. Aus Gründen der Übersichtlichkeit wurden dabei zusätzlich zu Österreich nur Länder, in denen laut Enforcement-Tracker per 25.07.2024 zumindest 25 DSGVO-Bußgelder verhängt wurden, dargestellt. Eine (absteigende) Reihung erfolgte nach dem Anteil der Bußgelder unter 10k€:

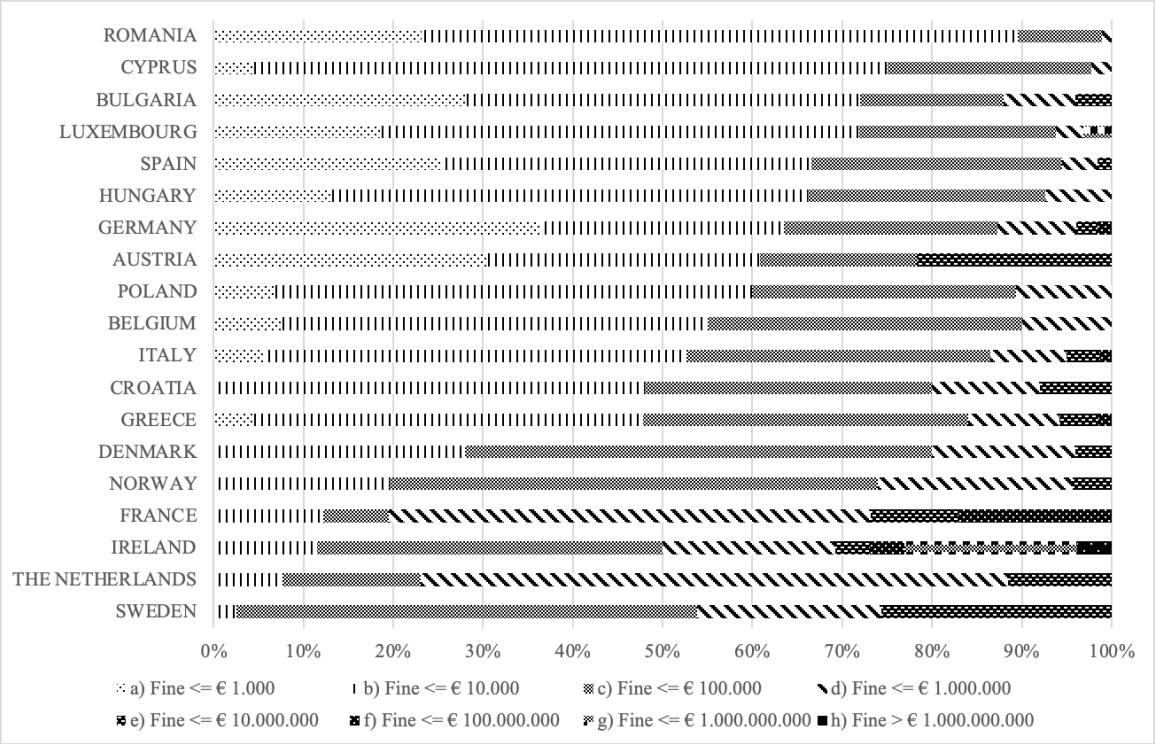


Abbildung 28: Höhe von DSGVO-Geldbußen nach Ländern gem "Enforcement-Tracker" (eigene Darstellung)

In der jeweiligen Kategorie werden dabei nur jene Bußgelder gezählt, die nicht bereits durch die nächstniedrigere Kategorie abgedeckt sind. Bspw werden in der Kategorie „b) Fine <= € 10.000“ nur die Bußgelder die größer als € 1.000 und kleiner gleich € 10.000 sind gezählt – jene Bußgelder die kleiner gleich € 1.000 sind, werde in der Kategorie „a) Fine <= € 1.000“ gezählt.

Bemerkenswert in dieser Grafik ist, dass in einigen Ländern mit einem hohen BIP/Kopf ein verhältnismäßig hoher Anteil an niedrigen Geldbußen verhängt wurde (zB Luxemburg, Deutschland, Österreich). Um diesen Umstand näher zu beleuchten, wurde in der folgenden

Tabelle die Anzahl der Bußgelder in Verhältnis zum BIP/Kopf und zur Bevölkerungsgröße der jeweiligen Länder gesetzt.

Tabelle 5: Verhältnis zw Anzahl der verhängten Bußgelder und der Bevölkerungsanzahl und dem BIP/Kopf (eigene Darstellung)

Land	Anzahl Bußgelder	Bevölkerung insgesamt 2024 [Mio EW]	BIP pro EW 2021 [US$]	Bußgelder pro Mio EW [1]	Bußgelder pro tausend USD BIP/Kopf [1/USD]
Belgien	40	11,8	51.875	3,4	0,77
Bulgarien	25	6,4	11.684	3,9	2,14
Dänemark	25	6	67.758	4,2	0,37
Deutschland	126	83,4	50.795	1,5	2,48
Frankreich	41	68,4	44.853	0,6	0,91
Griechenland	69	10,4	20.256	6,6	3,41
Irland	26	5,3	99.013	4,9	0,26
Italien	378	59	35.473	6,4	10,66
Kroatien	25	3,9	16.818	6,4	1,49
Luxemburg	32	0,7	136.701	45,7	0,23
Niederlande	26	17,9	58.292	1,5	0,45
Österreich	23	9,2	53.368	2,5	0,43
Polen	75	36,6	17.815	2,0	4,21
Rumänien	181	19,1	14.667	9,5	12,34
Schweden	39	10,6	60.029	3,7	0,65
Spanien	881	48,6	30.090	18,1	29,28
Ungarn	68	9,6	18.968	7,1	3,58
Zypern	44	0,9	30.846	48,9	1,43

Auch diese Darstellung weist auf unterschiedliches Verhalten der verschiedenen Datenschutzbehörden hin. Während bspw in Zypern pro Million Einwohner 48,9 Geldbußen verhängt wurden, wurden in Frankreich nur 0,6 Geldbußen pro Million Einwohnern verhängt. Da nicht klar ist, ob die Bevölkerungsanzahl ein relevantes Maß für die Anzahl der Datenschutzbußgeldern darstellt, wurde zusätzlich auch noch das BIP pro Kopf ins Verhältnis zur Anzahl der Bußgelder gesetzt. Aber auch hier ergibt sich ein uneinheitliches Bild. Spanien liegt hier mit über 29 Bußgeldern pro 1000 USD BIP/Kopf an der Spitze. Hingegen weißt Luxemburg mit 0,23 Bußgeldern pro 1000 USD BIP/Kopf den niedrigsten Wert auf – und das, obwohl es bei der Anzahl der Bußgelder pro Einwohner mit 45,7 Bußgelder pro Million Einwohner den zweithöchsten Wert aufweist. Länder wie Irland, in denen mutmaßlich viele Tech-Giganten ihre europäische Vertretung haben, zeigen sich in dieser Darstellung unauffällig.

Zusammenfassend kann hier festgestellt werden, dass sowohl die Verteilungen bzgl Höhe der Bußgelder als auch Kennzahlen wie Anzahl der Bußgelder pro Einwohner und Anzahl der Bußgelder pro BIP/Kopf zwar Unterschiede zw verschiedenen Ländern und dem Gebaren der Datenschutzbehörden zeigen, aber wenig Hinweise auf eine konkrete Quantifizierung des Bußgeldrisikos bieten.

7.9 Zusammenfassung

Der Begriff Datenschutz wird in der öffentlichen Diskussion oft mit Datensicherheit verwechselt. Während Datensicherheit die Vertraulichkeit, Integrität und Verfügbarkeit von (allen) Daten betrachtet, hat Datenschutz die ordnungsgemäße Verarbeitung von personenbezogenen Daten im Fokus, schützt also die betroffenen Personen.

Dementsprechend hat Datenschutz in den letzten Jahren eine stärkere Bedeutung bekommen. Die DSGVO hat, vor allem durch die Androhung verhältnismäßig hoher Bußgelder, wesentlich dazu beigetragen. In Anbetracht der immer umfassenderen Verarbeitungen von personenbezogenen Daten wird aus Sicht des Autors diese Bedeutung noch zunehmen – auch wenn die Datenschutzbehörden in den verschiedenen Ländern offenbar uneinheitliches Gebaren zeigen, und die maximale Höhe an Bußgeldern nicht immer ausschöpfen.

Im Zusammenhang mit Risikomanagement ist das Risiko als positive oder negative Abweichung von Zielen ein zentrales Element. Demzufolge ist auch die Definition der Datenschutzziele ein wichtiger Teil. Betrachtet man ausschließlich die DSGVO, so wird Risiko immer als Gefahr für die Rechte und Freiheiten natürlicher Personen beschrieben. Das entspricht einem der Ziele der DSGVO, stellt aber nur einen Teil der für eine ganzheitliche Betrachtung von Datenschutz notwendigen Ziele und Risiken dar. In der Literatur findet man weitere Modelle, für die Definition von Datenschutzzielen herangezogen werden können. Diese Modelle gehen oft weit über die „Risiken für Rechte und Freiheiten natürlicher Personen“ hinaus und folgen Compliance-Ansätzen oder auch Datenschutzmanagementsystemansätzen. Modelle die alle Ebenen (inkl Kundenebene) der Balanced Score Card berücksichtigen, konnte der Autor bisher nicht finden. Allen Modellen gemeinsam ist, dass sie an die Gegebenheiten des jeweiligen Unternehmens und seiner Umwelt individuell entwickelt oder zumindest angepasst werden müssen.

8 Besonderheiten von Datenschutz im Risikomanagement

8.1 Einleitung

Das Strafmaß der die seit 2018 in Kraft befindlichen Datenschutzgrundverordnung (DSGVO) hat mit bis zu 4% des weltweiten Konzernumsatzes eines Unternehmens eine nicht unerhebliche Größe erreicht. Dadurch legen Unternehmen naturgemäß hohes Augenmerk auf die Umsetzung der gesetzlichen Vorgaben. Gleichzeitig sind die inhaltlichen Anforderungen in Bezug auf die Umsetzung von effektivem Datenschutz mit der DSGVO gestiegen. Rechenschaftspflichten und Erfüllung von Betroffenenrechte seien hier nur als zwei Beispiele genannt. Diese Anforderungen stellen manche Unternehmen vor Herausforderungen.

Gleichzeitig etablieren sich in verschiedenen Bereichen immer häufiger Organisationsmodelle mit "Selbstorganisation". Beispielsweise werden im Bereich der Softwareentwicklung oder des Projektmanagements oft agile Methoden eingeführt. Auch ganze Unternehmen schwenken in Richtung Selbstorganisation.

Beim ersten Kontakt mit Organisationsmodellen der Selbstorganisation scheint es eine Diskrepanz zwischen den Stellen, die die Verantwortung für eine effektive Umsetzung des Datenschutzes tragen, und die mit einer allfälligen Geldbuße bei Nicht-Einhaltung der DSGVO belegt werden könnten (nämlich der Unternehmensvorstand), und jenen Stellen, die datenschutzrelevante Entscheidungen treffen - nämlich die Mitarbeiter des Unternehmens (oder Organisationseinheit) die die Datenverarbeitungen durchführen, zu geben.

Viele Organisationsmodelle im Bereich von Selbstorganisation basieren vorgeblich zu einem großen Teil auf Vertrauen.[190] *Schreyögg* bezeichnet diese Annahme als optimistisch (in Kombination mit der Kompetenz der Mitarbeiter)[191], *Kühl* bezeichnet Führung alleine durch Vertrauen als naiv.[192] Speziell wenn der psychologische Vertrag zwischen Mitarbeiter und Unternehmen nicht erfüllt wird, könnte das affektive Commitment von Mitarbeitern zu Gunsten von kalkulativem Commitment umschlagen und das Organisational Citizenship Behaviour könnte abnehmen.

[190] Vgl *Laloux*, Reinventing organizations, 80.

[191] Vgl *Schreyögg/Geiger*, Organisation.

[192] Vgl *Kühl*, Die agile Organisation ist kalter Kaffee.

Diese Erkenntnisse führen nicht dazu, große Hoffnungen in die Umsetzung von effektivem Datenschutz in selbstorganisierten Unternehmen (oder Organisationseinheiten) zu setzen - vor allem im Hinblick darauf, dass die Umsetzung von effektivem Datenschutz mit gewissen Aufwänden verbunden ist. Unterstellt man zumindest einem gewissen Anteil an Mitarbeitern Opportunismus, ist davon auszugehen, dass Datenschutz nicht in jedem Bereich korrekt umgesetzt wird. Ein Ökonom würde das wohl als externen Effekt bezeichnen: Das Risiko, das durch die mangelhafte Umsetzung von Datenschutz entsteht, liegt nicht beim Mitarbeiter, der die Entscheidung getroffen hat, die Umsetzung auf eine bestimmte Art durchzuführen, sondern beim Vorstand der Organisation. Nicht zuletzt dadurch, dass (zumindest in Teilen des Unternehmens) Selbstorganisation herrscht, ist auch davon auszugehen, dass dem Vorstand die mangelnde Umsetzung von Datenschutz verborgen bleibt. Dadurch herrscht eine Asymmetrie zwischen den für Datenschutz Verantwortlichen, dem Vorstand, und den handelnden Mitarbeitern - eine Situation, wie sie auch in der Neuen Institutionenökonomik, genauer gesagt der Prinzipal-Agent-Theorie, beschrieben wird.

Wie kann also Datenschutz (oder Compliance allgemein) in derartigen Organisationsmodellen gelingen?

Aus der Neuen Institutionenökonomik gibt es auch Gestaltungsempfehlungen zu den verschiedenen Themenfeldern bei Prinzipal-Agent-Problemen. Im Wesentlichen basieren diese Empfehlungen auf einer Verringerung der Informationsasymmetrien einerseits, auf einer Interessensangleichung andererseits.

Wie bereits festgestellt, ist für das Gelingen von Selbstorganisation ein gewisses Set an Regeln notwendig (vgl oben, Kap „Selbstorganisation“). Um Datenschutz wirksam über die gesamte (selbstorganisierte) Organisation umzusetzen, kann dieses Regelset entsprechend ausgestaltet werden. Im Sinne der Prinzipal-Agent-Theorie sollte dabei sowohl auf die Interessensangleichung zwischen Prinzipal (Vorstand) und den Agents (Mitarbeiterinnen) als auch auf eine Verringerung der Informationsasymmetrien geachtet werden.

Je nach zum Einsatz kommenden Selbstorganisationsmodell sind hier verschiedene Methoden denkbar:

Verringerung von Informationsasymmetrien:

- Einsatz von Risk-Management
- Datenschutz-Self-Assessments mit "Gütesiegel"
- Integration von Datenschutz in selbstorganisierte Abstimmungen

Interessensangleichung:

- Berücksichtigung von Datenschutz im Purpose des Unternehmens
- Definition von Datenschutz-Rollen in den operativen Teams
- Prozessdefinitionen zur Integration von Datenschutzanforderungen
- Entwicklung einer Datenschutz-Policy
- Integration von Datenschutz in selbstorganisierte Abstimmungen

Als eine von mehreren möglichen Methoden wird in diesem Werk der Einsatz von Risiko-Management näher beleuchtet.

8.2 Datenschutz als Produkteigenschaft

8.2.1 Einleitung

Oft wird Datenschutz nur als Erfüllung von rechtlichen Verpflichtungen gesehen, bspw jenen der DSGVO, des DSG oder des TKG. Betrachtet man aber den Produktbegriff aus dem Bereich Marketing, so kann das durchaus breiter verstanden werden:

„Produkt ist alles, was einer Person angeboten werden kann, um ein Bedürfnis oder einen Wunsch zu befriedigen.“[193]

Es ist wohl unzweifelhaft, dass der Schutz der „Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ ein Bedürfnis darstellt. Das wiederum erzeugt Nutzen für die Verbraucher.
Der Nutzen eines Produkts beschreibt, wie der Verbraucher dessen Fähigkeit einschätzt, seine Bedürfnisse zu erfüllen. Dabei ist der Umgang mit personenbezogenen Daten als eine relevante Produkteigenschaft zu betrachten. Jede Eigenschaft eines Produkts wird vom Konsumenten in Bezug auf ihren Beitrag zur Zufriedenheit bewertet. Diese Bewertung hängt davon ab, wie stark die jeweilige Eigenschaft die Bedürfnisse des Kunden erfüllt.

[193] *Kotler/Bliemel*, Marketing-Management (2001) 14.

Die Zufriedenheit entsteht aus dem Vergleich des tatsächlich wahrgenommenen Mehrwerts des Produkts nach dem Kauf mit den Erwartungen vor dem Kauf.
Frederick Herzbergs Zwei-Faktor-Theorie unterscheidet dabei zwischen „Dissatisfaktoren“, die Unzufriedenheit hervorrufen, und „Satisfaktoren“, die für Zufriedenheit sorgen. Daraus ergeben sich zwei wichtige Konsequenzen: Erstens sollten Hersteller und Vermarkter alles daransetzen, Unzufriedenheit auslösende Faktoren zu minimieren oder zu vermeiden. Zwar führen ausgeschaltete Dissatisfaktoren nicht automatisch zu einem Kauf, ihr Vorhandensein kann jedoch potenzielle Kunden abschrecken. Zweitens sollten die Faktoren, die tatsächlich Zufriedenheit und Kaufmotivation schaffen, für die jeweilige Zielgruppe sorgfältig identifiziert und zuverlässig in das Produkt integriert werden.[194]

Im Relationship Marketing, das der Beziehung zum Kunden noch größeren Stellenwert einräumt, geht man im Vergleich zum produktbezogenen Transaktionsmarketing noch weiter. Laut Bruhn ist die enge Definition des Leistungsangebots im Transaktionsmarketing, die sich ausschließlich auf das Produkt und dessen Vermarktung konzentriert, kritisch zu betrachten. In zahlreichen Branchen, insbesondere im Bereich von Industriegütern und Dienstleistungen, spielt auch die Interaktion zwischen Anbieter und Kunde eine zentrale Rolle als Bestandteil der erbrachten Leistung.[195]

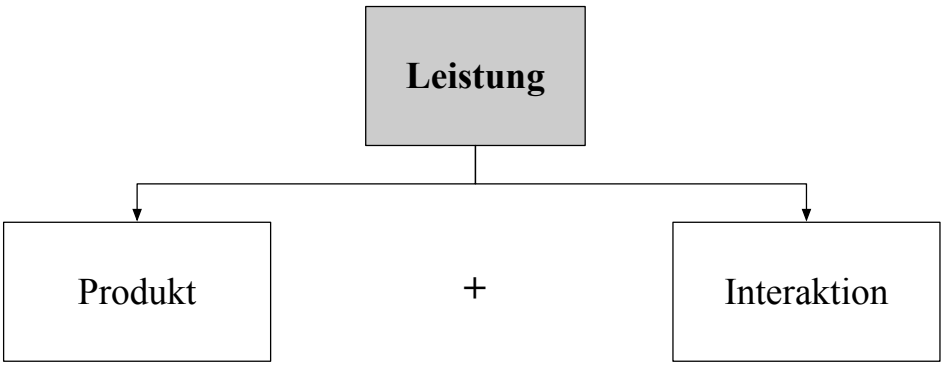


Abbildung 29. Leistungsangebot als Kombination von Produkt und Interaktion[196]

[194] Vgl *Kotler/Bliemel*, Marketing-Management.

[195] Vgl *Bruhn*, Relationship Marketing, 10.

[196] *Bruhn*, Relationship Marketing, 10.

Bruhn nennt neben verhaltensbezogenen und ökonomischen auch psychologische Faktoren als Indikatoren für die Intensität der Kundenbeziehung. Darunter fällt auch die Beziehungsqualität, zu der wiederum Vertrauen und Vertrautheit gehören.[197]

Die Wahrnehmung von Produkteigenschaften und Interaktionen beeinflusst auch das Markenimage. Verbraucher bilden ihre Meinung zu einer Marke oft durch den Vergleich der Eigenschaften verschiedener Marken. Das Markenimage entsteht dabei aus der Gesamtheit dieser Einschätzungen zu einer bestimmten Marke. Ein gutes Markenimage aufzubauen erfordert viel Zeit und sollte daher nicht leichtfertig gefährdet werden. Der Wert einer Marke basiert auf dem guten Ruf, den sie sich im Laufe der Zeit erarbeitet hat. Kunden entwickeln oft eine emotionale Bindung und Vertrauen darauf, dass eine Marke bestimmte Eigenschaften dauerhaft erfüllt. Dieses Vertrauen sollte nicht durch Handlungen untergraben werden, die nicht zum Charakter der Marke passen. Unternehmen, die kundenorientiert arbeiten, müssen die Wünsche und Bedürfnisse ihrer Kunden ernst nehmen und diese aus der Perspektive der Kunden verstehen – nicht aus der eigenen Sicht.[198]

Aus Sicht des Autors schließt dies ein, dass Datenschutz nicht als isolierte Compliance-Aufgabe betrachtet wird, sondern in Zusammenarbeit mit anderen Unternehmensbereichen integriert wird:

„Ganzheitliches Marketing entsteht, wenn alle Abteilungen eines Unternehmens bestrebt sind, im Interesse der Kunden zu wirken und sie zufriedenzustellen.“[199]

Einige Unternehmen haben diese Chance bereits erkannt. Beispielsweise startete das IT-Unternehmen Apple, das zeitweise das wertvollste Unternehmen weltweit war, 2014 eine Datenschutzoffensive.[200] Folgerichtig hat Apple Datenschutz auch in seine Marketing-

[197] Vgl *Bruhn*, Relationship Marketing, 60f.

[198] Vgl *Kotler/Bliemel*, Marketing-Management.

[199] *Kotler/Bliemel*, Marketing-Management, 37.

[200] Vgl *Schwan*, Apple-Chef Tim Cook startet Datenschutz-Offensive <https://www.heise.de/news/Apple-Chef-Tim-Cook-startet-Datenschutz-Offensive-2395243.html> (2014), zuletzt aufgerufen am 23.01.2025.

kommunikation integriert.[201] Während andere Unternehmen unter den Aufwänden, die mit der Umsetzung der DSGVO verbunden sind, stöhnen, fordert der CEO des U.S.-Unternehmens „DSGVO für alle“.[202]

Demensprechend preist Apple auch auf seiner Webseite Datenschutz an:

„Privacy is a fundamental human right. It’s also one of our core values. Which is why we design our products and services to protect it. That’s the kind of innovation we believe in.“[203]

8.2.2 Vertrauen: Digital- / Online-Trust

Wie bereits oben erwähnt, ist Vertrauen ein wesentlicher Baustein für eine Kundenbeziehung:

“In the world of business, trust is key to successful transactions and long-term relationships.”[204]

Während „Vertrauen“ in der Offline-Welt bereits seit den 1950ern Forschungsgegenstand in verschiedenen Disziplinen ist (vgl oben, Kap 4.3.4 „Vertrauen“), ist die Erforschung des Vertrauens in der Online-Welt, auch „digital trust“ oder „online trust“ genannt, noch ein verhältnismäßig junges Forschungsgebiet.

Ein Mangel an Vertrauen kann dazu führen, dass eine Austauschbeziehung gar nicht erst zustande kommt. Eine weltweite Umfrage ergab beispielsweise, dass fast die Hälfte der

[201] Vgl bspw *Andru Edwards*, Talking Privacy with Apple - Are Your Secrets Safe? <https://www.youtube.com/watch?v=1YOi0r3vptQ> (2024); *Apple*, Apple Intelligence | Privacy <https://www.youtube.com/watch?v=546ufMY7488> (2024); *Apple*, Privacy on iPhone | Flock | Apple <https://www.youtube.com/watch?v=0HjDpPnxcP0> (2024), zuletzt aufgerufen am 19.2025.

[202] Vgl *Cook*, 40th ICDPPC: Keynote Speech by Tim Cook, European Data Protection Law Review (2018).

[203] *Apple (Hrsg)*, Apple Privacy <https://www.apple.com/privacy/>, zuletzt aufgerufen am 19.01.2025.

[204] *Corritore/Kracher/Wiedenbeck*, International journal of human-computer studies 2003, 737–758 (738).

Internetnutzer, die nie online einkaufen, dies hauptsächlich auf fehlendes Vertrauen zurückführen.[205]

Vertrauen ist auch entscheidend für die Akzeptanz neuer Technologien. Digitales Vertrauen beschreibt die positive und überprüfbare Überzeugung, dass eine digitale Informationsquelle zuverlässig ist. Dieses Vertrauen beeinflusst die Bereitschaft, Technologien wie das Internet der Dinge, Cloud-Computing oder Big-Data-Analysen zu nutzen und anzunehmen.[206]

8.2.3 Marktforschung

Im B2C-Bereich gibt es in der Regel eine große Anzahl potenzieller Kunden. Ein Markt umfasst alle Personen mit einem bestimmten Bedürfnis oder Wunsch, die bereit und in der Lage sind, diesen durch einen Austauschprozess zu erfüllen. Wie bereits Sunzi in „Die Kunst des Krieges“ betonte, ist es essenziell, seinen „Gegner“ zu kennen. Im Marketing bedeutet dies, den Zielmarkt genau zu verstehen und zu wissen, wie man dessen Bedürfnisse erfüllen kann. Das Versäumnis dieser grundlegenden Marketingregel führt häufig zum Scheitern.[207]
Daraus ergibt sich die Notwendigkeit die Bedürfnisse der Kunden zu kennen. Die Marktforschung hält hierzu ein umfassendes Set an Methoden bereit.[208]
In der Praxis gibt es auch bereits Marktforschung im Datenschutzbereich. Hier sind bspw der „Privacy and Consumer Trust” von IAPP[209] oder das “Consumer Privacy Survey” von Cisco[210] zu nennen.

[205] Vgl *Zhang/Hassandoust/Auckland University of Technology/Williams/ICL Graduate Business School*, Online Customer Trust in the Context of the General Data Protection Regulation (GDPR), Pacific Asia Journal of the Association for Information Systems 2020, 86–122 (86).

[206] Vgl *Paliszkiewicz/Guerrero Cusumano/Gołuchowski*, Trust, Digital Business and Technology: Issues and Challenges (2022) 7.

[207] Vgl *Kotler/Bliemel*, Marketing-Management.

[208] Vgl *Scheuch*, Marketing (Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften 2007) 82ff.

[209] *International Association of Privacy Professionals (IAPP)*, Privacy and Consumer Trust (03.2023).

[210] Cisco 2022 Consumer Privacy Survey, (2022).

Aus Sicht des Autors sollten zusätzlich zu den Bedürfnissen der Betroffenen auch die jene von Auftragsverarbeitern eines Unternehmens berücksichtigt werden, bspw hinsichtlich der Gestaltung von datenschutzrelevanten Prozessen. Weiters sind auch relevante Bedürfnisse aller anderen Stakeholder (siehe auch Stakeholder-Analyse) erhoben werden und ggf in das Zielsystem einfließen. Auch hier kann der geschickte Einsatz von Methoden aus der empirischen Sozialforschung hilfreich sein.

8.3 Arten von Risikomanagement im Datenschutzbereich

In der Literatur wird an vielen Stellen nur zwischen Datenschutzrisiken (Risiken für die Rechte und Freiheiten natürlicher Personen) und datenschutzbezogene Compliance-Risiken (Verstoß gegen Datenschutzregularien) unterschieden.[211]

Nach Ansicht des Autors greift das für ein umfassendes Risikomanagement im Bereich Datenschutz aber zu kurz. Deswegen wurde zur Kategorisierung der Arten von Risikomanagement im Datenschutzbereich vier unterschiedliche Modelle entwickelt. Diese unterscheiden sich vor allem durch den verwendeten Risikobegriff als auch durch die Methodik.

Modell 1: Die DSGVO, und der darin verwendete Risikobegriff, fordern vom Verantwortlichen eine Identifikation, Bewertung und Behandlung von Risiken, die sich auf die Rechte und Freiheiten natürlicher Personen auswirken (Datenschutzrisiken).
Modell 2: Es ist unschwer zu erkennen, dass aus Unternehmenssicht im Modell 1 nur ein Teil der Risiken für das Unternehmen bzw für den Verantwortlichen abgedeckt sind. Es fehlen unter anderem sämtliche Risiken, die sich aus den Dokumentationspflichten der DSGVO (zB Nachweispflichten, Verfahrensverzeichnis) ergeben. Weiters ist es notwendig, zusätzlich zur DSGVO auch nationale Regelungen (wie bspw das DSG 2018) zu berücksichtigen. Werden im Risikomanagement alle datenschutzrechtlichen Vorgaben berücksichtigt, erfolgt ein Risikomanagement für datenschutzbezogene Compliance-Risiken.
Modell 3: Berücksichtigt man ausschließlich datenschutzrechtliche Vorgaben, besteht die Gefahr, dass die Verantwortliche im Zuge des Risikomanagements nicht schnell genug auf

[211] Vgl bspw *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 96.

sich ändernde Umweltbedingungen und Anforderungen reagieren kann. Daher ist es empfehlenswert, nicht nur datenschutzrechtliche Vorgaben zu berücksichtigen, sondern auch Strukturen, Prozesse und die Lernperspektive der Mitarbeiter, die zusammengenommen letztlich einen höheren Compliance-Level unterstützen sollen, in ein Risikomanagement miteinzubeziehen.

Modell 4: Für die Integration des Datenschutz-Risikomanagements in die Unternehmenssteuerung sollten nicht nur Risiken im engeren Sinne, sondern auch Chancen berücksichtigt werden. Dafür bietet sich, ausgehend von einer Datenschutzstrategie, die Abbildung der Datenschutz-Zielen (die auch positive Abweichungen haben können) auf einer Balanced Scorecard mit ihren vier Perspektiven (Finanzielle-Perspektive, Kunden-Perspektive, Prozess-Perspektive und Lern- und Entwicklungs-Perspektive) an. Diese Zieldefinition wiederum ist der Ausgangspunkt für das hier als „Ganzheitliches Datenschutz-Risikomanagement" bezeichnete Modell an.

Tabelle 6: Modelle des Risikomanagements im Datenschutz (eigene Darstellung)

Typ	**Zielsystem (Beispiele)**
Modell 1	Calo's Harms Dimensions, DSGVO, bspw DSFA
Modell 2	ÖNORM A 2017
Modell 3	IKS, GRC, „Das Datenschutz-Audit", NIST Privacy Framework, SDM
Modell 4	Gesamtheitliches Datenschutz-Risikomanagement

8.4 Datenschutzziele und Zielsysteme

8.4.1 Datenschutzkonzept und Datenschutzstrategie

In der Literatur findet sich keine einheitliche Beschreibung der Ziele von Datenschutz.
Bspw hat Datenschutz laut *Gaess* in erster Linie die Aufgabe, die Interessen der betroffenen Personen zu schützen, wie es der gesetzliche Auftrag vorsieht. Aus Unternehmenssicht würden diese Interessen jedoch oft als „Fremdziele" wahrgenommen, die mit den eigenen Unternehmenszielen in Konflikt geraten könnten.[212]
Andernorts stellt sich die Frage, ob der Datenschutz strategisch ausschließlich auf die umfassende Erfüllung gesetzlicher Vorgaben (Compliance-Ansatz) ausgerichtet sein solle

[212] Vgl *Gaess*, Datenschutz mit bewährten Methoden des Risikomanagements, 19f.

oder ob darüber hinaus zusätzliche Anforderungen eingehalten werden sollen, beispielsweise um Wettbewerbsvorteile zu erzielen.[213]

Es gibt dazu allerdings einige Hilfestellungen – siehe Kapitel 7.5 „Datenschutzziele".
Unstrittig dürfte sein, dass bei der Festlegung von Datenschutzzielen die zentralen datenschutzrechtlichen Risiken, die durch die Umsetzung dieser Ziele minimiert werden sollen (Compliance-Risiko), berücksichtigt werden müssen. Da sich die Risikosituation eines Unternehmens im Laufe der Zeit ändern kann, ist es wichtig, die Datenschutzziele regelmäßig – beispielsweise jährlich in Abstimmung mit der Geschäftsleitung – zu überprüfen. Datenschutz-Ziele können mit anderen Unternehmenszielen im Einklang stehen, sie ergänzen oder in Konkurrenz zueinander geraten, was zu Zielkonflikten führen kann. Ein typisches Beispiel ist der Konflikt zwischen den Datenschutzgrundsätzen wie Zweckbindung und Datenminimierung und den Marketinganforderungen, die eine umfassende Nutzung von Kundendaten für Segmentierung, Profilbildung und Analysen erfordern. Solche Konflikte lassen sich teilweise durch klare Prinzipien wie „Die Einhaltung rechtlicher Vorgaben hat Vorrang vor geschäftlichen Interessen" entschärfen oder lösen.[214]

Jedenfalls aber sollte das Zielsystem für Datenschutzziele Teil der Unternehmensstrategie sein. Dementsprechend muss es von jedem Unternehmen selbst entwickelt werden.

8.4.2 Balanced Scorecard

Angelehnt an das Balanced Scorecard System, das im strategischen Management verwendet wird, können auch Datenschutzziele auf verschiedenen Ebenen abgebildet werden. In der untenstehenden Grafik wird dieses System dargestellt. Die angeführten Ziele sind dabei als Beispiele zu verstehen – keinesfalls ist das eine taxative Aufzählung aller Datenschutzziele.

[213] Vgl *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 32f.

[214] Vgl *Sachs/Kranig/Gierschmann*, Datenschutz-Compliance nach der DS-GVO, 33.

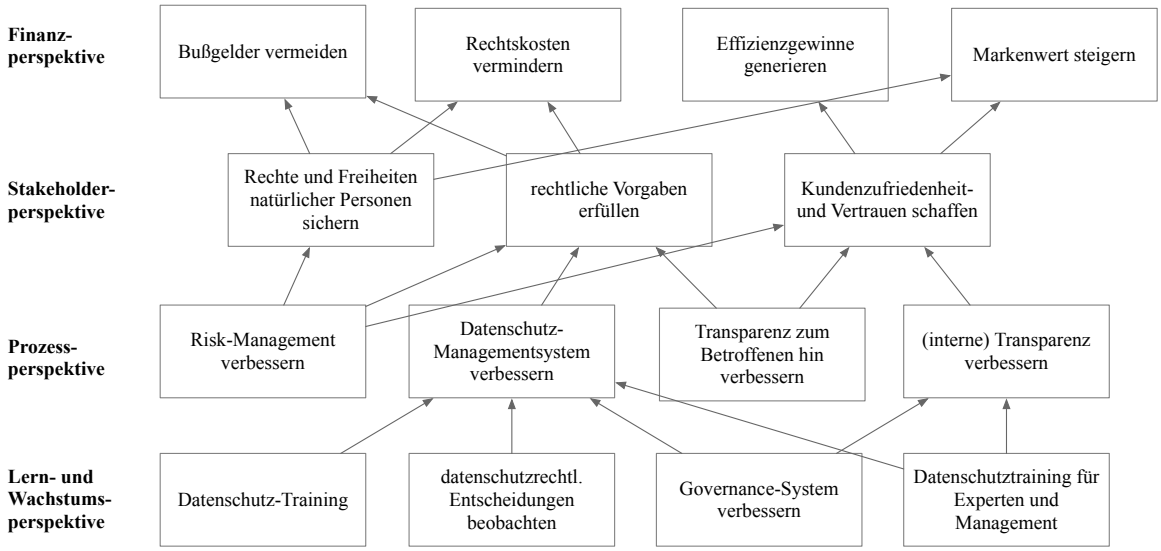


Abbildung 30: Datenschutzziele - Anlehnung an Balanced Scorecard (eigene Darstellung)

8.5 Zusammenfassung

Da es bei Datenschutz immer um den Schutz der Rechte und Freiheiten von natürlichen Personen geht, liegt es nahe, dass bei der Verarbeitung dieser Daten in vielen Fällen die betroffenen Personen in irgendeiner Form involviert sind. Dementsprechend sollten hier auch die Bedürfnisse dieser Personen (zB Vertrauen in ein Unternehmen oder ein Produkt) berücksichtigt und in ein Datenschutzrisikomanagement integriert werden. Ausgehend vom Grundsatz, dass Risiken positive oder negative Abweichungen von Zielen darstellen, ist es aus Sicht des Autors empfehlenswert, das Zielsystem entsprechend zu gestalten. Neben den in der DSGVO beschriebenen Verpflichtungen sollten daher auch andere datenschutzrechtlichen Compliance-Themen und Ziele für das Datenschutzmanagement-system in das Zielsystem integriert werden. Um die Bedürfnisse der Betroffenen zu berücksichtigen, kann es hilfreich sein auf die Methoden aus der empirischen Sozialforschung zurück zu greifen. Auch in der Zusammenarbeit mit Auftragsverarbeitern oder anderen (oder gemeinsamen) datenschutzrechtlich Verantwortlichen können diese Methoden gute Startpunkte bieten.

Weiters werden, ausgehend von den verschiedenen Arten von Zielen / Risiken, vier verschiedene Modelle von Datenschutzrisikomanagement dargestellt:

Modell 1: ausschließliche Berücksichtigung von Datenschutzrisiken (Risiken, die sich auf die Rechte und Freiheiten natürlicher Personen auswirken.
Modell 2: Risikomanagement für datenschutzbezogene Compliance-Risiken.
Modell 3: Zusätzlich zu Modell 2 Berücksichtigung von Strukturen, Prozessen und die Lernperspektive der Mitarbeiter
Modell 4: Zusätzlich zu Modell 3 werden hier auch Chancen berücksichtigt. Es werden alle Ebenen der Balanced Score Card berücksichtigt und es erfolgt eine quantitative Risikoaggregation als Grundlage für eine verbesserte Unternehmenssteuerung.

Während das Modell 1 primär für Datenschutzfolgenabschätzungen zum Einsatz kommen dürfte, scheinen Modell 2 und Modell 3 in der Praxis weit verbreitet zu sein. Passend auch zum Zukunftsbild von Risikomanagement ist aus Sicht des Autors Modell 4 anzustreben.

9 Zusammenfassung der aufgestellten Thesen

1. Risikomanagement im Datenschutzbereich kann, auch in Anbetracht moderner Organisationsformen wie Selbstmanagement, helfen, Informationsasymmetrien zu vermeiden.
2. Datenschutz sollte nicht nur als Risiko im engeren Sinne betrachtet werden, sondern auch als Chance
3. Modernes Risikomanagement mit quantitativer Bewertung von Risiken kann helfen, eine effizientere Ressourcenallokation in Unternehmen zu erreichen.
4. Ein Zielsystem, das aus Ausgangsbasis für die Identifikation von Risiken dient, sollte nicht nur Compliance-Risiken berücksichtigen, sondern Ziele auf verschiedenen Ebenen, bspw finanzielle Ebene, Stakeholder-Ebene, Prozess-Ebene und Lern- und Entwicklungsebene beinhalten.

10 Abstract

In der modernen Unternehmenslandschaft gewinnt das Risikomanagement im Datenschutz zunehmend an Bedeutung. Durch die fortschreitende Digitalisierung und den immer intensiveren Einsatz von Daten in geschäftlichen Prozessen stehen Unternehmen vor der Herausforderung, personenbezogene Informationen nicht nur gesetzeskonform, sondern auch im Einklang mit strategischen Zielen zu verarbeiten. Dieser Beitrag beleuchtet die zentralen Aspekte des Risikomanagements im Datenschutz aus unternehmerischer Perspektive und verknüpft dabei relevante Themen aus den Bereichen Organisationstheorien, psychologische Konstrukte, strategisches Management, Risikomanagement und Datenschutz. Besondere Aufmerksamkeit wird dabei quantitativen Methoden und der Möglichkeit des Beitrags von Risikomanagement zu einer wertbasierenden Unternehmensführung geschenkt.

Nach einer Einleitung werden verschiedene Organisationstheorien vorgestellt. Dabei wird ein Bogen von den klassischen Ansätzen, bei denen die Maschinenmetapher von Organisationen dominierend war, bis zu modernen Ansätzen des lateralen Managements und der Neuen Institutionenökonomik gespannt. Da Vertrauen vor allem bei modernen Ansätzen in verschiedener Hinsicht eine große Rolle spielt, wird dieses Konstrukt danach näher beleuchtet. Neben einer von vielen möglichen Ursachen für fehlendes Vertrauen, wird in diesem Zusammenhang auch der psychologische Vertrag behandelt. Auch die Auswirkungen von fehlendem Vertrauen, wie bspw fehlendes oder beeinträchtigtes organisationales Commitment und Organizational Citizenship Behaviour, werden kurz dargestellt.

Danach erfolgt eine Darstellung der für diese Arbeit relevanten Aspekte von strategischem Management. Aus Sicht des Verfassers ist es möglich, Werkzeuge aus dem strategischen Management in abgewandelter Form für Datenschutz und zur Erstellung einer Datenschutzstrategie zu verwenden. Speziell beleuchtet wird hier auch die „Balanced Score Card“ als Mittel zur Strategieimplementierung. Als Mittel zur umfassenden Zieldefinition ist sie, in Anbetracht der Definition von Risiko als Abweichung von Zielen, für Risikomanagement ein wichtiges Werkzeug – auch im Bereich Datenschutz.

Im nächsten Schritt erfolgt eine Darstellung der Grundlagen des Risikomanagements. Die Definition des Begriffes „Risiko“ als positive oder negative Abweichung von Zielen ist ein wichtiges Basiselement der vorliegenden Arbeit. Außerdem werden der Risikobewertung mit statistischen Wahrscheinlichkeits- bzw Dichtefunktionen und der Aggregation der so bewerteten Risiken mittels Monte-Carlos-Simulation großes Augenmerk geschenkt – diese Elemente stellen wichtige Grundvoraussetzungen dar um die Gesamtrisikoposition eines Unternehmens zu ermitteln, und dadurch einen Beitrag zu einer wertorientierten Unternehmenssteuerung zu leisten.

Danach werden einige für diese Arbeit relevanten Aspekte von Datenschutz betrachtet. Neben der Beleuchtung des Begriffes „Risiko“ wie er in der DSGVO verwendet wird, werden verschiedene „Zielsysteme“ vorgestellt. Ziele (und die Abweichungen davon) stellen die Grundlage für Risikomanagment dar.

Im nächsten Kapitel werden einige Besonderheiten im Datenschutz beschrieben. Hervorgehoben wird dabei die Betrachtung von Datenschutz als Produkteigenschaft, die geeignet ist das Kundenvertrauen zu stärken und dadurch mit Datenschutz einen Beitrag zur Wertschöpfung in Unternehmen zu leisten. Weiters werden vier verschiedene Modelle für Risikomanagement im Datenschutz skizziert. Sie basieren auf der Verwendung unterschiedlicher Zielmodelle und dem unterschiedlichen Einsatz von (quantitativen) Methoden.

Abschließend werden die aufgestellten Hypothesen zusammengefasst.

Diese Arbeit soll zeigen, dass ganzheitliches Risikomanagement im Datenschutz empfehlenswert ist, und bei Einsatz entsprechender Methoden helfen kann, eine effizientere Ressourcenallokation im Unternehmen zu unterstützen und letztlich einen Wertschöpfungsbeitrag für das Unternehmen zu leisten.

11 Abstract – English Version

In the modern corporate landscape, risk management in data protection is becoming increasingly important. Due to advancing digitization and the increasingly intensive use of data in business processes, companies are faced with the challenge of processing personal information not only in compliance with the law, but also in line with strategic goals. This article examines the key aspects of risk management in data protection from a business perspective, linking relevant topics from the areas of organizational theories, psychological constructs, strategic management, risk management and data protection. Particular attention is paid to quantitative methods and the possibility of risk management contributing to value-based corporate management.

After an introduction, various organizational theories are presented. This ranges from the classic approaches, in which the machine metaphor of organizations was dominant, to modern approaches of lateral management and New Institutional Economics. Since trust plays a major role in various respects, especially in modern approaches, this construct is then examined in more detail. In addition to one of many possible causes of a lack of trust, the psychological contract is also discussed in this context. The effects of a lack of trust, such as a lack of or impaired organizational commitment and organizational citizenship behavior, are also briefly presented.

This is followed by a presentation of the aspects of strategic management relevant to this work. From the author's point of view, it is possible to use tools from strategic management in a modified form for data protection and to create a data protection strategy. The "Balanced Score Card" is also particularly highlighted here as a means of strategy implementation. As a means of comprehensive goal definition, it is an important tool for risk management - also in the area of data protection - given the definition of risk as a deviation from goals.

The next step is a presentation of the basics of risk management. The definition of the term "risk" as a positive or negative deviation from goals is an important basic element of this work. In addition, great attention is paid to risk assessment using statistical probability or density functions and the aggregation of the risks assessed in this way using Monte Carlo simulation - these elements represent important basic requirements for determining the

overall risk position of a company and thereby making a contribution to value-oriented corporate management.

After that, some aspects of data protection relevant to this work are considered. In addition to highlighting the term "risk" as it is used in the GDPR, various "target systems" are presented. Targets (and deviations from them) form the basis for risk management.

The next chapter describes some special features of data protection. The emphasis is on considering data protection as a product feature that is suitable for strengthening customer trust and thus making a contribution to value creation in companies with data protection. Furthermore, four different models for risk management in data protection are outlined. They are based on the use of different target models and the different use of (quantitative) methods.

Finally, the hypotheses put forward are summarized.

This work aims to show that holistic risk management in data protection is advisable and, when appropriate methods are used, can help to support a more efficient allocation of resources within the company and ultimately make a contribution to value creation for the company.

12 Literaturverzeichnis

AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Das Standard Datenschutzmodell 3.1 - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, (2024)

Basel/Henrizi (Hrsg), Psychologie von Risiko und Vertrauen: Wahrnehmung, Verhalten und Kommunikation (Springer 2023)

Bruhn, Relationship Marketing: das Management von Kundenbeziehungen[2., vollst. überarb. Aufl] (Vahlen 2009)

Calo, The Boundaries of Privacy Harm, Indiana Law Journal, 2011

Cook, 40th ICDPPC: Keynote Speech by Tim Cook, European Data Protection Law Review (2018)

Corritore/Kracher/Wiedenbeck, On-line trust: concepts, evolving themes, a model, International journal of human-computer studies 2003, 737–758

Daume/Ernst, Monte-Carlo-Simulation im Risiko-Controlling: am Beispiel eines Financial Models in Exce[l1. Auflage] (UVK 2022)

Densmore/International Association of Privacy Professionals (Hrsg), Privacy program management: tools for managing privacy within your organization (International Association of Privacy Professionals 2013)

Erk/Spoun, Integrativ managen: Ein Modell für eine effektive Praxis der Unternehmensführung (Springer Fachmedien Wiesbaden 2020)

Erlei/Leschke/Sauerland, Institutionenökonomik[3., überarbeitete Auflage] (Schäffer-Poeschel Verlag 2016)

Exner/Ruthner, Corporate Risk Management: unternehmensweites Risikomanagement als Führungsaufgabe[3. Auflage] (Linde Verlag 2019)

Forgó (Hrsg), Grundriss Datenschutzrecht (LexisNexis 2019)

Gaess, Datenschutz mit bewährten Methoden des Risikomanagements: Handreichung[1] (Fachmedien Recht und Wirtschaft in Deutscher Fachverlag GmbH 2020)

Gleißner, Grundlagen des Risikomanagements: Handbuch für ein Management unter Unsicherheit[4., vollständig überarbeitete und erweiterte Auflage] (Verlag Franz Vahlen 2022)

Gleißner/Wolfrum, Risikoaggregation und Monte-Carlo-Simulation: Schlüsseltechnologie für Risikomanagement und Controlling (Springer 2019)

Hamel, Schafft die Manager ab!, Harvard Business manager, (2012)

Institut für Interne Revision Österreich - IIA Austria (Hrsg), Das Risikomanagement aus der Sicht der Internen Revision: inkl. CD-ROM mit Checklisten! (Linde 2006)

Jones, An Introduction to Factor Analysis of Information Risk (FAIR), Norwich University Journal of Information Assurance (NUJIA) 2006, 1–66

Kaplan/Mikes, HBR's 10 Must Reads on Managing Risk (Harvard Business Review Press 2020)

Kaplan/Norton, Balanced Scorecard: Strategien erfolgreich umsetzen[1. Auflage 1997, unveränderter Nachdruck Januar 2024] (Schäffer-Poeschel Verlag 2024)

Klein (Hrsg), Risikomanagement und Risiko-Controlling: Organisation und Dokumentation im Unternehmen, Datenerhebung und Risikobewertung, Integration in die Führungs- und Reportingsysteme, Umsetzungsbeispiele aus der Praxis[1. Aufl] (Haufe 2011)

Kotler/Bliemel, Marketing-Management[10., überarb. und aktualisierte Aufl] (Schaeffer-Poeschel 2001)

Kreikebaum/Gilbert/Behnam, Strategisches Management[8., überarbeitete Auflage] (Verlag W. Kohlhammer 2018)

Laloux, Reinventing Organizations: ein Leitfaden zur Gestaltung sinnstiftender Formen der Zusammenarbeit (Verlag Franz Vahlen 2015)

Lang/Brinkmann, Selbstorganisation braucht klare Regeln, Frankfurter Allgemeine 2018, 18

Lehner, Arbeitsplatzsicherheit, Organisationales Commitment, Organizational Citizenship Behavior sowie Radikales Value und Performancemanagement: Ergebnisse einer empirischen Studie bei der Telekom Austria (Diplomarbeit 2011)

Maring (Hrsg), Vertrauen — zwischen sozialem Kitt und der Senkung von Transaktionskosten (KIT Scientific Publishing container-title: Vertrauen — zwischen sozialem Kitt und der Senkung von Transaktionskosten) (KIT Scientific Publishing 2010)

Matzler/Müller-Seeger/Hautz/Mooradian, Strategisches Management: Konzepte und Methoden[3. Auflage] (Linde International 2021)

Mayrhofer/Gurtmüller/Kasper (Hrsg), Personalmanagement - Führung - Organisation[6. Auflage] (Linde Verlag Ges.m.b.H. 2023)

Nissenbaum, Privacy as Contextual Integrity, Washington Law Review 2004, 119ff

Österreichische Nationalbank, Leitfaden Management des operationellen Risikos, Leitfaden, 2005

Pachinger (Hrsg), Datenschutz-Audit: Recht - Organisation - Prozess - IT: der Praxisleitfaden zur Datenschutz-Grundverordnung[1. Auflage] (LexisNexis 2017)

Pachinger/Dobrauz/Grabinger/Heinrich/Jost/Meyer/Rosenauer/Schmidt/Schwaiger/Thiele/Warter, Datenschutz: Recht und Praxis: Verfahren & Behörden, Datenschutzbeauftragter, IT & Blockchain, Datenschutzverträge, Straf- & Arbeitsrecht, International, Strategie & Organisation, Sicherheit (LexisNexis 2020)

Paliszkiewicz/Guerrero/Gołuchowski, Trust, Digital Business and Technology: Issues and Challenges[1] (Routledge 2022)

Rehborn, Die ärztliche Schweigepflicht - ein schützenswertes Rechtsgut, GesR - Gesundheitsrecht 2017, 409

Reisinger/Gattringer/Strehl, Strategisches Management: Grundlagen für Studium und Praxis[2., aktualisierte und erweiterte Edition] (Pearson Studium ein Imprint von Pearson Deutschland 2017)

Sachs/Kranig/Gierschmann, Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden (Bundesanzeiger Verlag 2017)

Schäffter, Datenschutzmanagement 2.0: EU-konformen Datenschutz effizient planen und umsetzen; Migration zu einem Datenschutzmanagement gemäß EU-Datenschutzgrundverordnung inklusive Verfahrensverzeichnis 2.0[Erstausgabe Oktober 2017] (CreateSpace Independent Publishing Platform 2017)

Scheuch, Marketing[6., verb.erg. Aufl] (Vahlen 2007)

Schreyögg/Geiger, Organisation: Grundlagen moderner Organisationsgestaltung: mit Fallstudien[6., vollständig überarbeitete und erweiterte Auflage] (Springer Gabler 2016)

Schwieters, Corporate Governance: verantwortliche Steuerung und Überwachung in Zeiten globaler Krisen[1. Auflage] (Schäffer-Poeschel Verlag 2023)

Sowa/Rost, Die ISO 27701 und das SDM-V2 im Lichte der Umsetzung der DSGVO, Datenschutz und Datensicherheit - DuD 2020, 659–662

Vanini/Rieg, Risikomanagement: Grundlagen - Instrumente - Unternehmenspraxis[2., erweiterte Auflage] (Schäffer-Poeschel 2021)

Welge/Al-Laham/Eulerich, Strategisches Management: Grundlagen - Prozess - Implementierung[7., überarbeitete und aktualisierte Auflage] (Springer Gabler 2017)

Zhang/Hassandoust/Auckland University of Technology/Williams/ICL Graduate Business School, Online Customer Trust in the Context of the General Data Protection Regulation (GDPR), Pacific Asia Journal of the Association for Information Systems 2020, 86–122

Zenke/Schäfer/Brocke (Hrsg), Corporate Governance: Risikomanagement, Organisation, Compliance für Unternehmer[2nd ed] (De Gruyter 2020)

Internetquellen

Andru Edwards, Talking Privacy with Apple - Are Your Secrets Safe? <https://www.youtube.com/watch?v=1YOi0r3vptQ> (2024), zuletzt aufgerufen am 19.01.2025

Apple, Apple Intelligence | Privacy <https://www.youtube.com/watch?v=546ufMY7488> (2024), zuletzt aufgerufen am 19.01.2025

Apple, Privacy on iPhone | Flock | Apple <https://www.youtube.com/watch?v=0HjDpPnxcP0> (2024), zuletzt aufgerufen am 19.01.2025

Apple (Hrsg), Apple Privacy <https://www.apple.com/privacy/>, zuletzt aufgerufen am 19.01.2025

Austrian Standards plus GmbH (Hrsg), Datenschutz-Management: So profitieren KMU von der neuen ÖNORM A 2017 <https://www.austrian-standards.at/de/newsroom/pressemeldungen/datenschutz-management-so-profitieren-kmu-von-der-neuen-oenorm-a-2017> (2023), zuletzt aufgerufen am 22.01.2025

Cisco 2022 Consumer Privacy Survey, <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf> (2022), zuletzt aufgerufen am 23.01.2025

Datenschutzkonferenz (Hrsg), Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen <https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf> (2018), zuletzt aufgerufen am 23.01.2025

Donald Rumsfeld, Ausschnitt aus Pressekonferenz am 12.02.2002 <https://www.youtube.com/watch?v=REWeBzGuzCc> (2016), zuletzt aufgerufen am 14.01.2025

GDPR Enforcement Tracker - list of GDPR fines <https://www.enforcementtracker.com>

Holacracy: Die Hierarchie der Kreise <https://www.zukunftsinstitut.de/zukunftsthemen/holacracy-die-hierarchie-der-kreise> (2024), zuletzt aufgerufen am 20.01.2025

Johari-Fenster <https://de.wikipedia.org/wiki/Johari-Fenster>, zuletzt aufgerufen am 23.01.2025

International Association of Privacy Professionals (IAPP), Privacy and Consumer Trust, <https://iapp.org/media/pdf/resource_center/privacy_and_consumer_trust_report.pdf> (2023), zuletzt aufgerufen am 23.01.2025

Knebel/Grätsch, Selbstorganisation im Unternehmen: Was ist das? Wie funktioniert's? <https://www.berlinerteam.de/magazin/so-funktioniert-selbstorganisation-im-unternehmen-die-10-grundlagen/>, zuletzt aufgerufen am 20.01.2025

Kühl, Die agile Organisation ist kalter Kaffee <https://www.humanresourcesmanager.de/content/die-agile-organisation-ist-kalter-kaffee/> (2017), zuletzt aufgerufen am 20.01.2025

Risiko - Rechtschreibung, Bedeutung, Definition, Herkunft | Duden <https://www.duden.de/rechtschreibung/Risiko>, zuletzt aufgerufen am 13.01.2025

Schermuly, Holacracy: Die holokratische Organisation <https://www.haufe.de/personal/hr-management/new-work-moderne-formen-der-arbeitsgestaltung/holacracy-die-holokratische-organisation_80_406704.html> (2020), zuletzt aufgerufen am 22.01.2025

Schwan, Apple-Chef Tim Cook startet Datenschutz-Offensive <https://www.heise.de/news/Apple-Chef-Tim-Cook-startet-Datenschutz-Offensive-2395243.html> (2014), zuletzt aufgerufen am 23.01.2025

Standard-Datenschutzmodell - Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>, zuletzt aufgerufen am 23.01.2025

The Federal Privacy Council (FPC), Fair Information Practice Principles (FIPPs) <https://www.fpc.gov/resources/fipps/> (2016), zuletzt aufgerufen am 17.01.2025

Was ist ein Managementsystem & was zeichnet Managementsysteme aus? <https://www.din-iso-zertifizierung-qms-handbuch.de/was-ist-ein-managementsystem/>, zuletzt aufgerufen am 23.01.2025

Verwendete Rechtsnormen

Bundesgesetz, mit dem ein Telekommunikationsgesetz (Telekommunikationsgesetz 2021 – TKG 2021) erlassen wird, BGBl I 190/2021 idF I 75/2024

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl I 165/1999

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF I 70/2024

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.07.2002 S 37 - 47

Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108)

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119

Verwendete Standards und Normen

Austrian Standards International (Hrsg), ÖNORM A 2017:2023, Datenschutzmanagementsysteme, 01.06.2023

Austrian Standards International (Hrsg), ÖNORM D 4900:2021, Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen, 01.01.2021

Austrian Standards International (Hrsg), ÖNORM D 4901:2021, Risikomanagement für Organisationen und Systeme - Anforderungen an das Risikomanagementsystem, 01.01.2021

Austrian Standards International (Hrsg), ÖNORM D 4902-1:2021, Risikomanagement für Organisationen und Systeme - Leitfaden Teil 1: Einbettung des Risikomanagements ins Managementsystem, 01.01.2021

Austrian Standards International (Hrsg), ÖNORM D 4902-2:2021, Risikomanagement für Organisationen und Systeme - Leitfaden Teil 2: Methoden der Risikobeurteilung, 01.01.2021

Austrian Standards International (Hrsg), ÖNORM D 4902-3:2021, Risikomanagement für Organisationen und Systeme - Leitfaden Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement, 01.01.2021

Austrian Standards International (Hrsg), ÖNORM D 4903:2021, Risikomanagement für Organisationen und Systeme - Anforderungen an die Qualifikation des Risikomanagers, 01.01.2021

International Organization for Standardization (Hrsg), ISO/IEC 27000:2018, Information technology - Security techniques — Information security management systems - Overview and vocabulary, 02.2018

International Organization for Standardization (Hrsg), ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls, 2013

International Organization for Standardization (Hrsg), ISO/IEC 27018:2019, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, 01.2019

International Organization for Standardization (Hrsg), ISO/IEC 27701:2019, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management Requirements and guidelines, 2019

International Organization for Standardization (Hrsg), ISO/IEC 29100:2024, Information technology — Security techniques — Privacy framework, 02.2024

International Organization for Standardization (Hrsg), ISO/IEC 29151:2017, Information technology — Security techniques — Code of practice for personally identifiable information protection, 08.2017

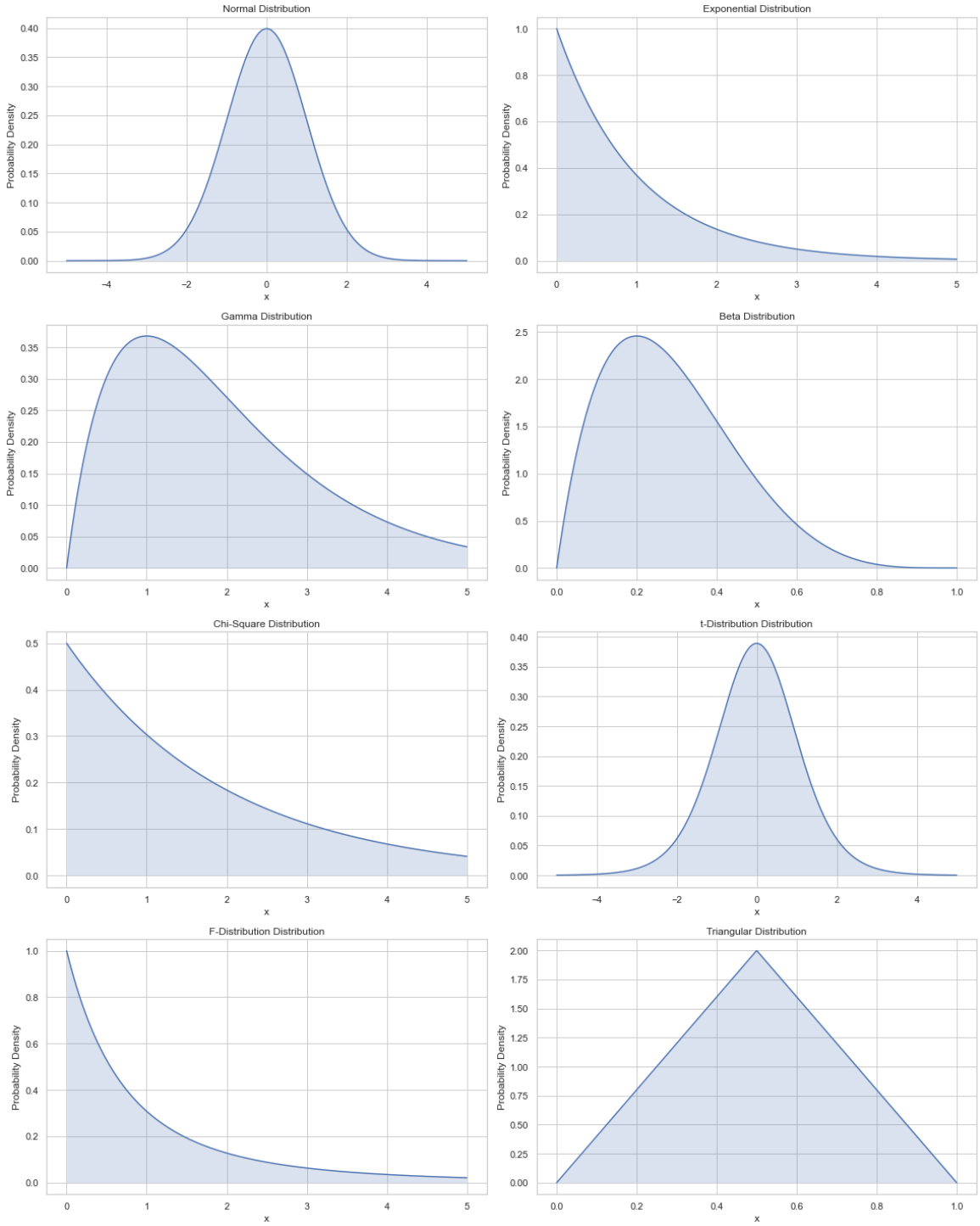
International Organization for Standardization (Hrsg), ISO 31000:2018, Risk management - Guidelines, 02.2018

National Institute of Standards and Technology (Hrsg), Fair Information Practice Principles (FIPPs) Crosswalk <https://www.nist.gov/privacy-framework/fair-information-practice-principles-fipps-crosswalk> (2021)

NIST privacy framework: a tool for improving privacy through enterprise risk management[Version 1.0]. (National Institute of Standards and Technology, U.S. Department of Commerce, 2020)

13 Anhang 1 – Wahrscheinlichkeits- und Dichtefunktionen

13.1 Ergebnisse – Überblick



13.2 Python Script für Überblicksdarstellung

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Created on Mon Jul 15 06:04:46 2024

@author: Manfred Lehner
"""

## Erforderliche Bibliotheken importieren

import numpy as np
import seaborn as sns
import matplotlib.pyplot as plt
from scipy.stats import norm, expon, gamma, beta, chi2, t, f, triang

# Der Stil für "seaborn" Diagramme wird festgelegt
sns.set(style="whitegrid")

# Ein Bereich von x-Werten wird definiert, der für die meisten
Verteilungen geeignet ist.
x = np.linspace(-5, 5, 1000)

# Ein Wörterbuch mit den Namen der Verteilungen und ihren entsprechenden
scipy.stats-Objekten wird erstellt.
distributions = {
    'Normal': norm(loc=0, scale=1),
    'Exponential': expon(scale=1),
    'Gamma': gamma(a=2, scale=1),
    'Beta': beta(a=2, b=5),
    'Chi-Square': chi2(df=2),
    't-Distribution': t(df=10),
    'F-Distribution': f(dfn=2, dfd=5),
    'Triangular': triang(c=0.5, loc=0, scale=1)
}

# Mit plt.subplots wird eine Gitteranordnung von Unterdiagrammen
erstellt.
fig, axs = plt.subplots(4, 2, figsize=(16, 20))
```

```
# Flatten the array of axes for easy iteration
axs = axs.flatten()

# Für jede Verteilung wird das PDF (Probability Density Function)
berechnet und geplottet. Die fill_between-Methode füllt den Bereich
unter der Kurve, um die Dichte anzuzeigen.
for ax, (name, distribution) in zip(axs, distributions.items()):
    # Adjust the x range for specific distributions
    if name in ['Exponential', 'Gamma', 'Chi-Square', 'F-Distribution']:
        x = np.linspace(0, 5, 1000)
    elif name == 'Beta':
        x = np.linspace(0, 1, 1000)
    elif name == 'Triangular':
        x = np.linspace(0, 1, 1000)
    else:
        x = np.linspace(-5, 5, 1000)

    # Plot the distribution
    y = distribution.pdf(x)
    sns.lineplot(x=x, y=y, ax=ax)
    ax.fill_between(x, y, alpha=0.2)
    ax.set_title(f'{name} Distribution')
    ax.set_xlabel('x')
    ax.set_ylabel('Probability Density')

# Mit plt.tight_layout wird das Layout der Diagramme angepasst, um
Überlappungen zu vermeiden.
plt.tight_layout()
plt.show()
```

13.3 Python-Script zur Darstellung der stetigen Gleichverteilung

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Created on 2024-08-20

@author: Manfred Lehner
```

```
Erstellt eine grafische Darstellung einer Gleich-Verteilung
Als Parameter werden der Minimalwert und der Maximalwert verwendet

Parameter:
- a (float): Minimalwert der Verteilung.
- b (float): Maximalwert der Verteilung.
"""

# Libraries importieren
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import uniform

# Beispielparameter für eine Gleich-Verteilung
a = 0  # Minimalwert der Verteilung
b = 10  # Maximalwert der Verteilung


# Werte der X-Achse (Auswirkung) generieren
x = np.linspace(a-1, b+1, 1000)

# Dichtefunktion für jeden X-Wert berechnen
pdf = uniform.pdf(x, loc=a, scale = b-a)

# Diagramm ausgeben
plt.figure(figsize=(10, 5))
plt.plot(x, pdf, 'b-', lw=2, alpha=0.6, label=f'Gleichverteilung
(min={a}, max={b})')
plt.title('Dichtefunktion einer Gleichverteilung')
plt.xlabel('Auswirkung')
plt.ylabel('Relative Häufigkeit')
plt.legend()
plt.grid(True)
plt.show()
```

13.4 Python-Script für Darstellung der Dreiecksverteilung

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
```

```
"""
Created on 2024-08-20

@author: Manfred Lehner

Erstellt eine grafische Darstellung einer Dreiecks-Verteilung
Als Parameter werden der Minimalwert, der Maximalwert und die Stelle des
wahrscheinlichsten Wertes verwendet

Parameter:
- c (float): Stelle des wahrscheinlichsten Wertes. Ist c = 0, fällt der
wahrscheinlichste Wert mit dem Minimalwert zusammen,
wenn c = 1, fällt der wahrscheinlichste Wert mit dem Maximalwert
zusammen.
- a (float): Minimalwert der Verteilung.
- b (float): Maximalwert der Verteilung.
"""


# Libraries importieren
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import triang

# Beispielparameter für eine Dreieck-Verteilung
c = 0.1  # Stelle des wahrscheinlichsten Wertes
a = 0  # Minimalwert der Verteilung
b = 10  # Maximalwert der Verteilung


# Werte der X-Achse (Auswirkung) generieren
x = np.linspace(a, b, 1000)

# Dichtefunktion für jeden X-Wert berechnen
pdf = triang.pdf(x, c, a, b-a)

# Diagramm ausgeben
plt.figure(figsize=(10, 5))
plt.plot(x, pdf, 'b-', lw=2, alpha=0.6, label=f'Dreiecksverteilung
(c={c}, min={a}, max={b})')
plt.title('Dichtefunktion einer Dreiecksverteilung')
```

```
plt.xlabel('Auswirkung')
plt.ylabel('Relative Häufigkeit')
plt.legend()
plt.grid(True)
plt.show()
```

13.5 Python-Script für Darstellung der Normalverteilung

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Created on 2024-08-20

@author: Manfred Lehner

Erstellt eine grafische Darstellung einer Normalverteilung
Als Parameter werden Mittelwert und Standardabweichung der
Normalverteilung verwendet

Parameter:
- mu (float): Mittelwert
- sigma (float): Standardabweichung
"""

# Libraries importieren
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import norm

# Beispielparameter für eine Normalverteilung
mu = 1  # Mittelwert
sigma = 1  # Standardabweichung


# Werte der X-Achse (Auswirkung) generieren
x = np.linspace(mu - 3*sigma, mu + 3*sigma, 1000)

# Dichtefunktion für jeden X-Wert berechnen
pdf = norm.pdf(x, mu, sigma)
```

```
# Diagramm ausgeben
plt.figure(figsize=(10, 5))
plt.plot(x, pdf, 'b-', lw=2, alpha=0.6, label=f'Normalverteilung
(mu={mu}, sigma={sigma})')
plt.title('Dichtefunktion einer Normalverteilung')
plt.xlabel('Auswirkung')
plt.ylabel('Relative Häufigkeit')
plt.legend()
plt.grid(True)
plt.show()
```

13.6 Python-Script für Darstellung der Lognormalverteilung

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Created on 2024-08-20

@author: Manfred Lehner

Erstellt eine grafische Darstellung einer Lognormal-Verteilung
Als Parameter werden Mittelwert und Standardabweichung der
zugrundeliegenden Normalverteilung verwendet

Parameter:
- mu (float): Mittelwert der zugrundeliegenden Normalverteilung
- sigma (float): Standardabweichung  der zugrundeliegenden
Normalverteilung
"""

# Libraries importieren
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import lognorm

# Beispielparameter für eine Lognormal-Verteilung
mu = 1  # Mittelwert der zugrundeliegenden Normal-Verteilung
sigma = 1  # Standardabweichung der zugrundeliegenden Normal-Verteilung
```

```
# Werte der X-Achse (Auswirkung) generieren
x = np.linspace(lognorm.ppf(0.01, sigma, scale=np.exp(mu)),
                lognorm.ppf(0.99, sigma, scale=np.exp(mu)), 100)

# Dichtefunktion für jeden X-Wert berechnen
pdf = lognorm.pdf(x, sigma, scale=np.exp(mu))

# Diagramm ausgeben
plt.figure(figsize=(10, 5))
plt.plot(x, pdf, 'b-', lw=2, alpha=0.6, label=f'Lognormalverteilung
(mu={mu}, sigma={sigma})')
plt.title('Dichtefunktion einer Lognormalverteilung')
plt.xlabel('Auswirkung')
plt.ylabel('Relative Häufigkeit')
plt.legend()
plt.grid(True)
plt.show()
```

13.7 Python-Script zur Darstellung der Binomialverteilung

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
"""
Created on 2024-08-20

@author: Manfred Lehner

Erstellt eine grafische Darstellung einer Binomial-Verteilung
Als Parameter werden die Anzahl der Versuche und die
Erfolgswahrscheinlichkeit für die einzelnen Versuche verwendet

Parameter:
- n (int): Anzahl der Versuche.
- p (float): Erfolgswahrscheinlichkeit für die einzelnen Versuche.
"""



# Libraries importieren
import numpy as np
```

```
import matplotlib.pyplot as plt
from scipy.stats import binom

# Beispielparameter für eine Gleich-Verteilung
n = 10   # Anzahl der Versuche
p = 0.5  # Erfolgswahrscheinlichkeit

# Werte der X-Achse (Auswirkung) generieren
x = np.arange(0, n+1)

# Dichtefunktion für jeden X-Wert berechnen
pmf = binom.pmf(x, n, p)

# Diagramm ausgeben
plt.figure(figsize=(10, 5))
plt.plot(x, pmf, color = 'b', alpha=0.7, label=f'Binomialverteilung
(n={n}, p={p})')
plt.title('Binomialverteilung')
plt.xlabel('Auswirkung')
plt.ylabel('Wahrscheinlichkeit')
plt.legend()
plt.grid(True)
plt.show()
```

14 Anhang 2 – Monte-Carlo-Simulation

14.1 Ergebnisse der Monte-Carlo-Simulation für PI

Als Beispiel für eine Monte-Carlo-Simulation wurde mit der Scriptsprache Python ein einfaches Modell für die Schätzung der Kreiszahl π entwickelt. In diesem Beispiel werden zuerst 20.000 Zufallszahlen für X und Y im Bereich von null bis eins generiert. Mit der Formel $x^2 + y^2 \leq 1$ wird errechnet, ob sich die jeweilige Zufallszahl innerhalb des Kreises befindet. Das Verhältnis der Zahlen innerhalb des Kreises zur Anzahl der erzeugten Zufallszahlen ergibt den geschätzten Wert von π.
In diesem Fall lieferte das Programm folgendes Ergebnis:

```
Geschätzter Wert für Pi: 3.1344
```

Dass das Ergebnis nur ein relativ ungenauer Schätzwert der tatsächlichen Kreiszahl (π = 3,14159265...) ist, liegt an der verhältnismäßig niedrigen Anzahl der Simulationsläufe (20.000). Erhöht man die Anzahl an Simulationsläufen, nähert sich das Ergebnis der Schätzung dem tatsächlichen π an.

In der grafischen Darstellung des Ergebnisses wird diese Ungenauigkeit noch deutlicher. Hier gibt es viele weiße „Flecken“ – diese vermindern die Genauigkeit:

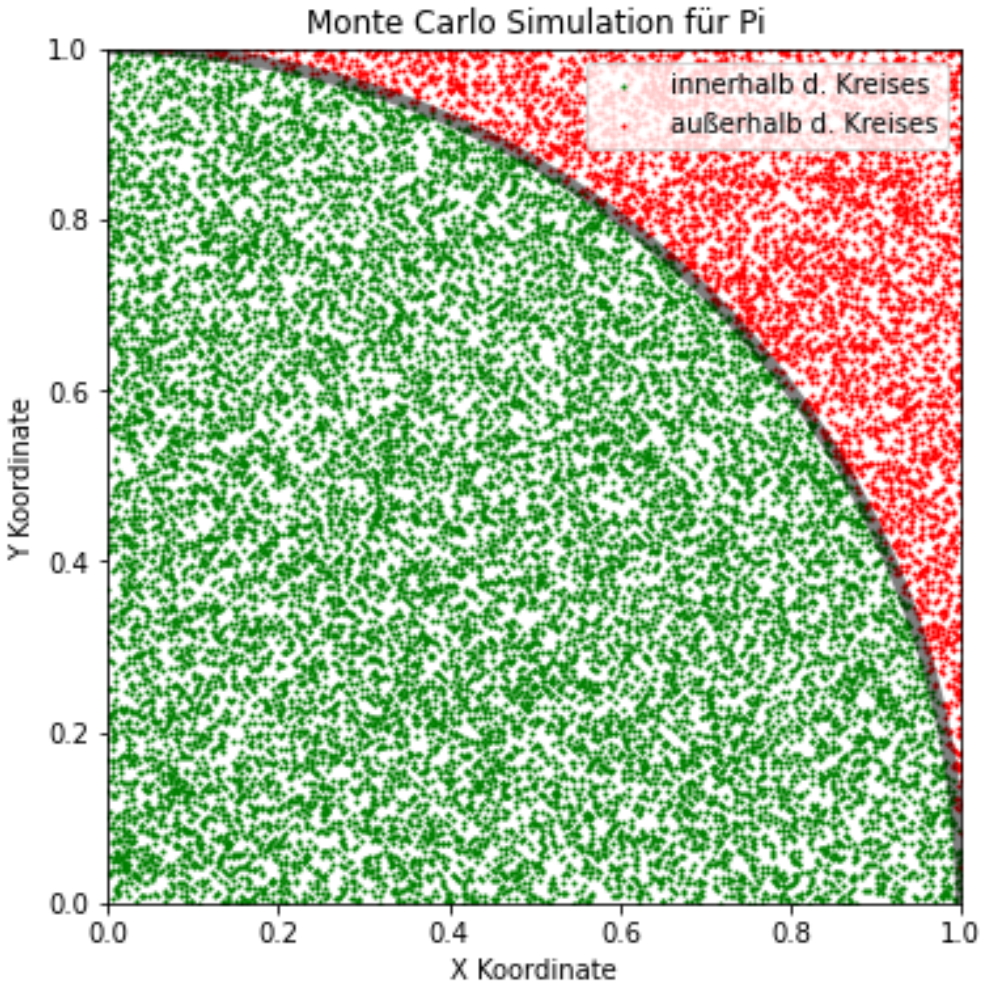


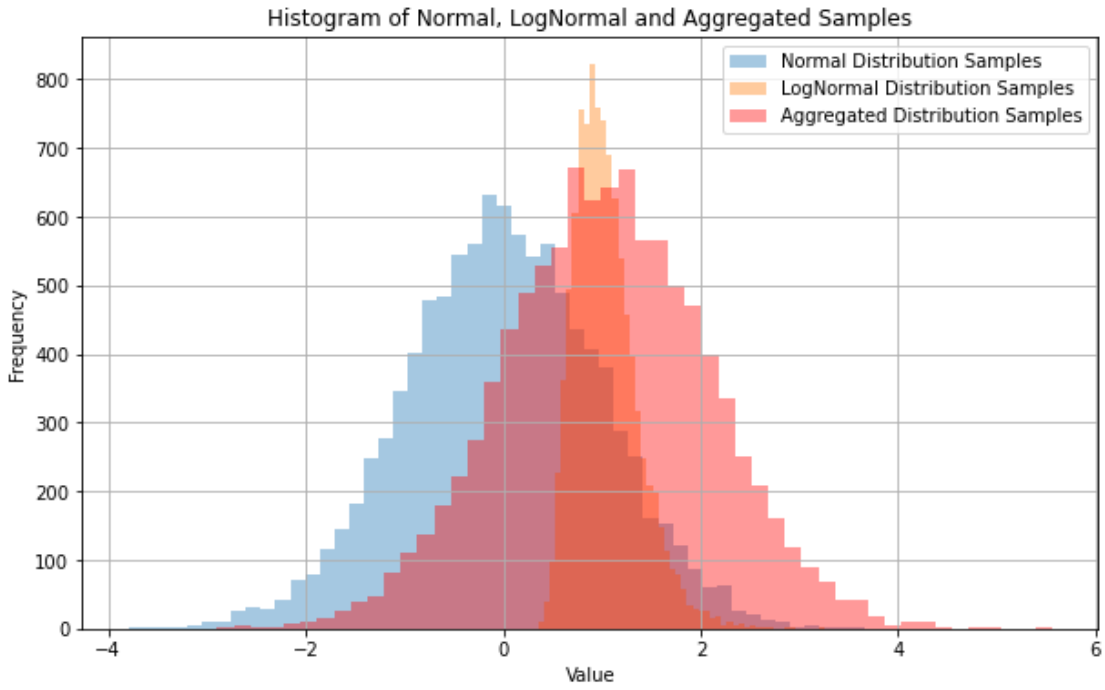
Abbildung 31: Monte-Carlo-Simulation zur Schätzung von Pi mittels Python Script. Eigene Darstellung.

14.2 Python Script für die Monte-Carlo-Simulation für PI

```
Created on Thu Jun 13 21:38:36 2024

@author: Manfred Lehner
"""
# Benötigte Libraries importieren
import numpy as np
import matplotlib.pyplot as plt

############################################################
#   Unterprogramm für die Monte-Carlo-Simulation           #
############################################################
def monte_carlo_pi(num_samples):
    # Zufallszahlen für X und Y erzeugen
    x = np.random.uniform(0, 1, num_samples)
    y = np.random.uniform(0, 1, num_samples)

    # Abstand der Zufallspunkte vom Ursprung berechnen, um
festzustellen, ob sie innerhalb des Kreises liegen
    # Punkte liegen innerhalb des Kreises, wenn x^2 + y^2 <= 1
    inside_circle = x**2 + y**2 <= 1

    # Pi schätzen: Anteil der Punkte, der innerhalb des Kreises liegt
    pi_estimate = 4 * np.sum(inside_circle) / num_samples

    # Errechnete Ergebnisse an das Hauptprogramm zurückgeben
    return x, y, inside_circle, pi_estimate

############################################################
#   Unterprogramm für grafische Ausgabe der Simulation     #
############################################################
def plot_monte_carlo(x, y, inside_circle):
    # Zufallspunkte ausgeben
    plt.figure(figsize=(6, 6))
    plt.scatter(x[inside_circle], y[inside_circle], color='green', s=1,
label='innerhalb d. Kreises')
    plt.scatter(x[~inside_circle], y[~inside_circle], color='red', s=1,
label='außerhalb d. Kreises')
```

```
    # Kreissegment ausgeben
    circle = plt.Circle((0, 0), 1, edgecolor='black', facecolor='none',
linewidth=5, alpha=0.5)
    plt.gca().add_artist(circle)

    # Beschriftung und Konfiguration der Darstellung
    plt.xlim(0, 1)
    plt.ylim(0, 1)
    plt.gca().set_aspect('equal', adjustable='box')
    plt.xlabel('X Koordinate')
    plt.ylabel('Y Koordinate')
    plt.legend()
    plt.title('Monte Carlo Simulation für Pi')
    plt.show()


############################################################
#   Hauptprogramm                                          #
############################################################

def main():
    # Anzahl der Simulationsläufe (= Anzahl der zu berechnenden Punkte)
setzen
    num_samples = 20000

    # Monte-Carlo-Simulation durchführen
    x, y, inside_circle, pi_estimate = monte_carlo_pi(num_samples)

    # Ergebnis der Schätzung von Pi ausgeben (im Prompt, nicht Grafik)
    print(f"Geschätzter Wert für Pi: {pi_estimate}")

    # Grafische Darstellung der Monte-Carlo-Simulation
    plot_monte_carlo(x, y, inside_circle)

############################################################
#   Rumpf zum Aufruf des Hauptprogramms                    #
############################################################
if __name__ == "__main__":
    main()
```

14.3 Ergebnis der Aggregation von Dichtefunktionen mittels Monte-Carlo-Simulation



14.4 Python-Script für die Aggregation von Dichtefunktionen mittels Monte-Carlo-Simulation

```
import numpy as np
import matplotlib.pyplot as plt
from scipy.stats import norm, lognorm

def monte_carlo_aggregation(mu_normal, sigma_normal, mu_lognormal,
sigma_lognormal, num_samples):
    """
    Performs a Monte Carlo simulation to aggregate samples from a normal
distribution and a lognormal distribution.

    Parameters:
    - mu_normal (float): Mean of the normal distribution.
    - sigma_normal (float): Standard deviation of the normal
distribution.
    - mu_lognormal (float): Mean of the underlying normal distribution
for the lognormal distribution.
    - sigma_lognormal (float): Standard deviation of the underlying
normal distribution for the lognormal distribution.
```

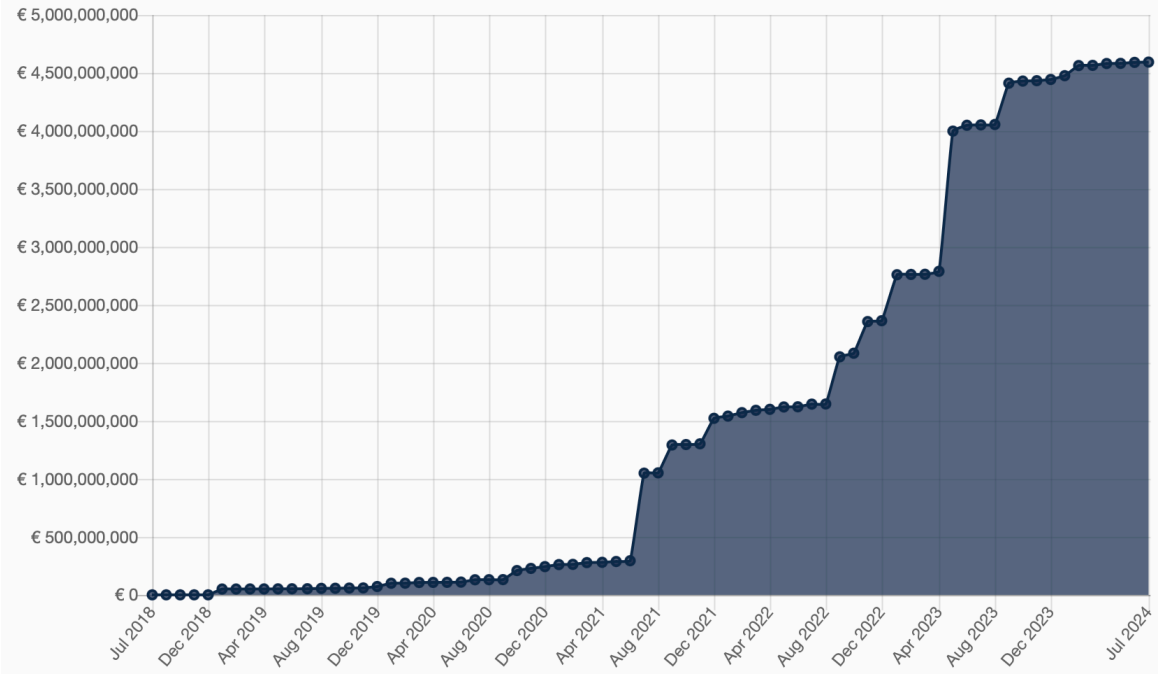
```
    - num_samples (int): Number of samples to generate for the
simulation.
    """
    # Generate samples from a normal distribution
    normal_samples = norm.rvs(size=num_samples, loc=mu_normal,
scale=sigma_normal)

    # Generate samples from a lognormal distribution
    s = sigma_lognormal  # Shape parameter for lognorm
    scale = np.exp(mu_lognormal)  # Scale parameter for lognorm
    lognormal_samples = lognorm.rvs(s=s, scale=scale, size=num_samples)

    # Aggregate the samples from both distributions
    aggregated_samples = normal_samples + lognormal_samples

    # Plotting the results
    plt.figure(figsize=(10, 6))
    plt.hist(normal_samples, bins=50, alpha=0.4, label='Normal
Distribution Samples')
    plt.hist(lognormal_samples, bins=50, alpha=0.4, label='LogNormal
Distribution Samples')
    plt.hist(aggregated_samples, bins=50, alpha=0.4, label='Aggregated
Distribution Samples', color='red')
    plt.title('Histogram of Normal, LogNormal and Aggregated Samples')
    plt.xlabel('Value')
    plt.ylabel('Frequency')
    plt.legend()
    plt.grid(True)
    plt.show()

# Parameters for the distributions
mu_normal = 0
sigma_normal = 1
mu_lognormal = 0
sigma_lognormal = 0.3
num_samples = 10000

# Call the function with the specified parameters
monte_carlo_aggregation(mu_normal, sigma_normal, mu_lognormal,
sigma_lognormal, num_samples)
```

15 Anhang 3 – DSGVO-Geldbußen

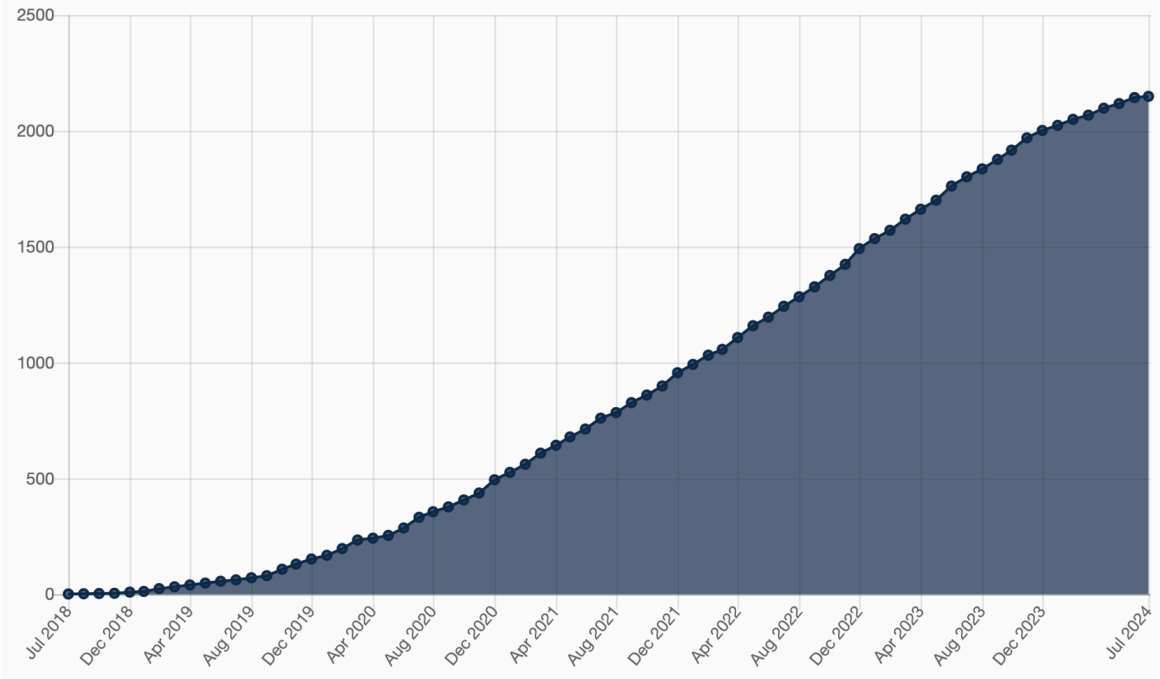
Quelle: https://www.enforcementtracker.com (Stand 25. Juli 2024)

1. Course of overall sum and number of fines (cumulative):

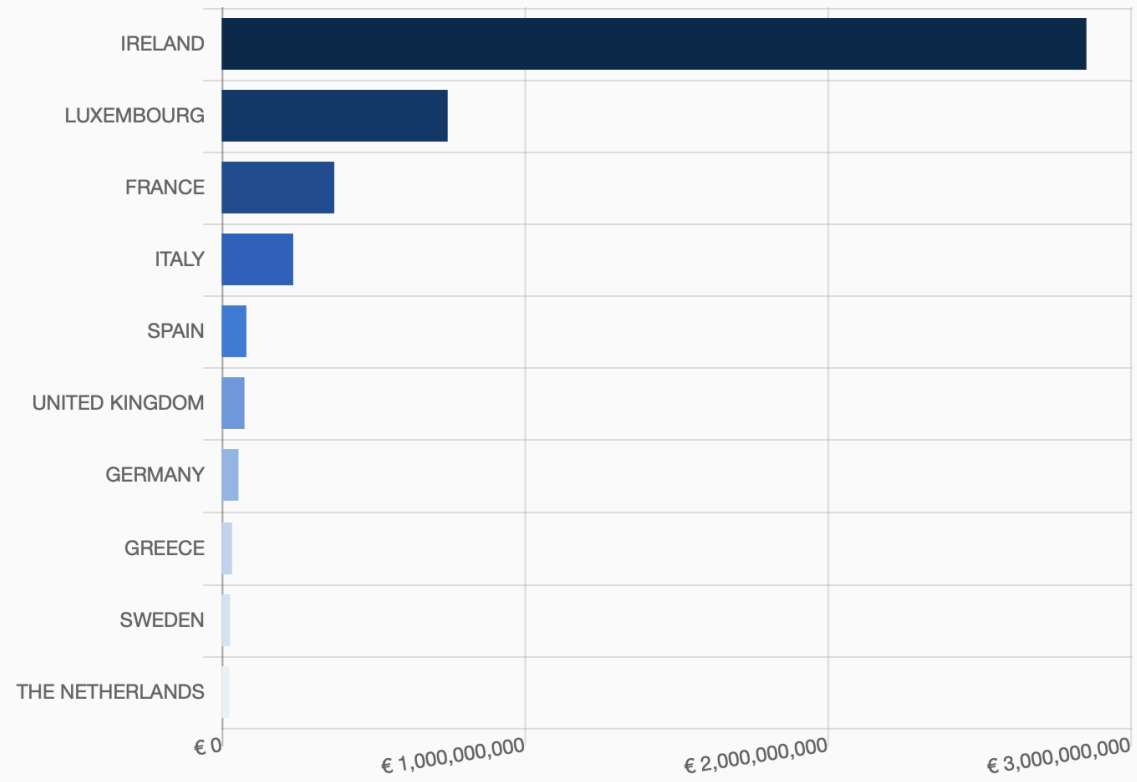
a) Course of overall sum of fines (cumulative):



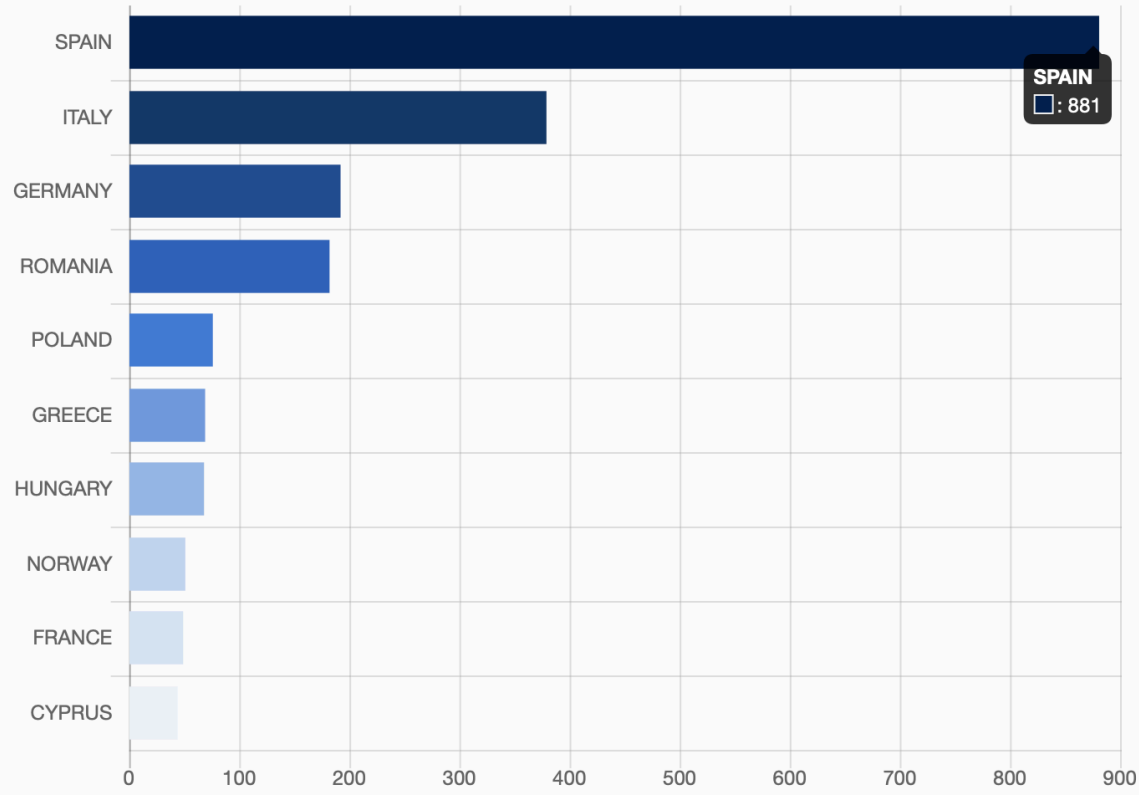
b) Course of overall number of fines (cumulative):



1. By total sum of fines:



2. By total number of fines:



Violation	Sum of Fines
Non-compliance with general data processing principles	**€ 2,089,112,250** (at 602 fines)
Insufficient legal basis for data processing	**€ 1,652,782,712** (at 650 fines)
Insufficient technical and organisational measures to ensure information security	**€ 475,707,615** (at 387 fines)
Insufficient fulfilment of information obligations	**€ 247,854,260** (at 195 fines)
Insufficient fulfilment of data subjects rights	**€ 100,942,646** (at 212 fines)
Unknown	**€ 23,200,700** (at 11 fines)
Insufficient cooperation with supervisory authority	**€ 6,633,329** (at 120 fines)
Insufficient fulfilment of data breach notification obligations	**€ 3,031,392** (at 44 fines)
Insufficient data processing agreement	**€ 1,117,110** (at 12 fines)
Insufficient involvement of data protection officer	**€ 961,300** (at 21 fines)

Violation	Number of Fines
Insufficient legal basis for data processing	**650** (with total € 1,652,782,712)
Non-compliance with general data processing principles	**602** (with total € 2,089,112,250)
Insufficient technical and organisational measures to ensure information security	**387** (with total € 475,707,615)
Insufficient fulfilment of data subjects rights	**212** (with total € 100,942,646)
Insufficient fulfilment of information obligations	**195** (with total € 247,854,260)
Insufficient cooperation with supervisory authority	**120** (with total € 6,633,329)
Insufficient fulfilment of data breach notification obligations	**44** (with total € 3,031,392)
Insufficient involvement of data protection officer	**21** (with total € 961,300)
Insufficient data processing agreement	**12** (with total € 1,117,110)
Unknown	**11** (with total € 23,200,700)

Sector	Sum of Fines
Media, Telecoms and Broadcasting	**€ 3,313,891,366** (at 296 fines)
Industry and Commerce	**€ 916,360,577** (at 461 fines)
Transportation and Energy	**€ 173,509,941** (at 119 fines)
Finance, Insurance and Consulting	**€ 63,966,758** (at 225 fines)
Employment	**€ 59,718,777** (at 141 fines)
Public Sector and Education	**€ 27,852,063** (at 245 fines)
Accomodation and Hospitalty	**€ 22,574,648** (at 71 fines)
Health Care	**€ 17,075,309** (at 206 fines)
Real Estate	**€ 2,685,831** (at 63 fines)
Individuals and Private Associations	**€ 1,892,856** (at 293 fines)
Not assigned	**€ 1,815,188** (at 134 fines)

Sector	Number of Fines
Industry and Commerce	**461** (with total € 916,360,577)
Media, Telecoms and Broadcasting	**296** (with total € 3,313,891,366)
Individuals and Private Associations	**293** (with total € 1,892,856)
Public Sector and Education	**245** (with total € 27,852,063)
Finance, Insurance and Consulting	**225** (with total € 63,966,758)
Health Care	**206** (with total € 17,075,309)
Employment	**141** (with total € 59,718,777)
Not assigned	**134** (with total € 1,815,188)
Transportation and Energy	**119** (with total € 173,509,941)
Accomodation and Hospitalty	**71** (with total € 22,574,648)
Real Estate	**63** (with total € 2,685,831)

#	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	1.200.000.000	Insufficient legal basis for data processing	2023-05-12
2	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEM-BOURG	746.000.000	Non-compliance with general data processing principles	2021-07-16
3	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405.000.000	Non-compliance with general data processing principles	2022-09-05
4	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	390.000.000	Non-compliance with general data processing principles	2023-01-04
5	TikTok Limited	Media, Telecoms and Broadcasting	IRELAND	345.000.000	Non-compliance with general data processing principles	2023-09-01
6	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	265.000.000	Insufficient technical and organisational measures to ensure information security	2022-11-25
7	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225.000.000	Insufficient fulfilment of information obligations	2021-09-02
8	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90.000.000	Insufficient legal basis for data processing	2021-12-31
9	Enel Energia SpA	Transportation and Energy	ITALY	79.100.000	Insufficient technical and organisational measures to ensure information security	2024-02-08
10	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60.000.000	Insufficient legal basis for data processing	2021-12-31