

# Datenschutz für Führungskräfte in Marketing, Sales und Vertrieb

Der kompakte Praxisleitfaden –  
mit Checklisten und Vorlagen  
für den Führungsalltag

von

Karlheinz Ferenz

Alle im Buch verwendeten Begriffe verstehen sich geschlechterneutral. Aus Gründen der besseren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet – entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat lediglich redaktionelle Gründe und beinhaltet keine Wertung.

**Bibliografische Information der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

ISBN 978-3-8005-2001-5

**dfv** Mediengruppe

© 2026 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main  
[www.ruw.de](http://www.ruw.de)

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Satzkonvertierung: Lichtsatz Michael Glaese GmbH, 69502 Hemsbach

Druck und Verarbeitung: Beltz Bad Langensalza GmbH, 99947 Bad Langensalza

## Vorwort

Datenschutz ist kein Blockierer, sondern ein starkes Profilierungsmerkmal. Im dynamischen Ringen um Marktanteile und Kundenaufmerksamkeit wird Vertrauen zur härtesten Währung. Während viele Marktteilnehmer Datenschutz primär als administrative Hürde wahrnehmen, integrieren vorausschauende Führungskräfte Datenschutz als festen Bestandteil ihrer Vertriebsstrategie – als Beleg für Verlässlichkeit, nicht als juristische Fußnote.

Kunden, die sich sicher fühlen, entscheiden schneller, binden sich länger und teilen bereitwilliger die Daten, die Sie wirklich brauchen. Die Intuition vieler Führungskräfte wird durch harte Fakten gedeckt: Datenschutz ist ein ökonomischer Beschleuniger. Die aktuelle Cisco 2025 Data Privacy Benchmark Study<sup>1</sup> zeigt, dass Unternehmen, die Datenschutz nicht als Compliance-Last, sondern als strategisches Asset begreifen, messbare Vorteile erzielen. 96% der befragten Organisationen berichten, dass die Erträge ihrer Datenschutzinvestitionen die Kosten übersteigen – mit einem durchschnittlichen ROI-Faktor von 1,6.

Noch gravierender ist die Kehrseite: In einer Zeit, in der KI-gestützte Datenverarbeitung zum Standard wird, ist Vertrauen der zentrale Erfolgsfaktor. Die Studie belegt, dass 95% der befragten Organisationen der Aussage zustimmen, dass Kunden einen Kaufprozess abbrechen würden, wenn sie Zweifel an der Sicherheit ihrer Daten haben. Datenschutz ist damit keine bloße Pflichtaufgabe mehr, sondern die Eintrittskarte für den Pitch. Wer hier patzt, verliert nicht nur Daten, sondern Deals.

Wer Datenschutz als gelebtes Qualitätsversprechen führt, sendet eine klare Botschaft: „Hier sind Sie in guten Händen. Hier behalten Sie die Kontrolle über Ihre Daten.“ In einer Zeit, in der Datenmissbrauch zum Markenschaden wird, avanciert Ihr Unternehmen zum vertrauenswürdigen Partner – und damit zur bevorzugten Wahl.

Dieses Buch richtet sich an Führungskräfte in Marketing, Sales und Vertrieb, die Verantwortung für Kundendaten tragen – ohne selbst Datenschutzjuristen oder IT-Sicherheitsprofis zu sein. Es übersetzt die Vorgaben der DSGVO und der ein-

---

<sup>1</sup> Cisco Systems, Inc., 2025 Data Privacy Benchmark Study, „The Privacy Advantage: Building Trust in a Digital World“, S. 4 ff.; die Studie analysiert Daten von über 2.600 Sicherheits- und Datenschutzexperten aus 12 Ländern und weist nach, dass Datenschutzinvestitionen den Verkaufszyklus glätten und operative Reibungsverluste minimieren, abrufbar unter: <https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html>, sowie <https://blogs.cisco.com/security/unlocking-the-privacy-advantage-to-build-trust-in-the-age-of-ai>, Stand 12/2025.

schlägigen Spezialgesetze in konkrete Entscheidungen, Prozesse und Checklisten für den Alltag: von Kampagnenplanung und CRM über Agentursteuerung bis hin zu internationalen Kooperationen.

Besonderes Herzstück ist das Kapitel „Incident in 60 Minuten“. Es zeigt Schritt für Schritt, wie Sie bei einer Datenpanne in Ihrem Bereich innerhalb der ersten Stunde richtig reagieren – auch dann, wenn die Faktenlage unvollständig ist, der Druck hoch und die Geschäftsleitung schnelle Antworten erwartet. Alle übrigen Kapitel zahlen auf dieses zentrale Szenario ein: Sie helfen, typische Vorfälle zu vermeiden, Incidents professionell zu managen und aus ihnen zu lernen.

Sie müssen dieses Buch nicht von vorne bis hinten lesen. Viele Lesende werden mit dem Incident-Kapitel beginnen und erst danach die Grundlagen vertiefen. Andere steigen mit den Kapiteln zu Kampagnen, CRM oder internationalen Datentransfers ein. Die Struktur ist bewusst so gewählt, dass Sie entlang Ihrer aktuellen Herausforderungen navigieren können – und dennoch jederzeit den roten Faden behalten.

Ich wünsche Ihnen beim Lesen viele konkrete Aha-Momente – und vor allem die Sicherheit, in kritischen Situationen schnell, professionell und auditfest handeln zu können.

Wiesbaden, im Februar 2026

*Karlheinz Ferenz*

## Inhaltsverzeichnis

Vorwort .....	V
Einleitung – Wie Sie dieses Buch nutzen .....	1
Warum Datenschutz in Marketing, Sales und Vertrieb Chefsache ist .....	1
Drei Perspektiven dieses Buches .....	2
Wie die Teile und Kapitel zusammenhängen .....	2
Lese- und Arbeitsempfehlung .....	3
Kompass: Datenschutz ist mehr als Compliance – er ist der Schutzraum der Freiheit .....	4

### TEIL I – Vor der Datenpanne: Alltag der Führungskraft

<b>1. Rolle der Führungskraft im Datenschutz .....</b>	<b>7</b>
Praxisfall – „Delegiert – und trotzdem verantwortlich“ .....	7
1.1 Verantwortung, Delegation und Rechenschaftspflicht .....	7
1.2 Abgrenzung zu Datenschutzbeauftragten, IT, HR, Legal .....	9
1.3 Persönliche Haftung vs. Unternehmensrisiko .....	10
1.3.1 Externes Risiko – gegenüber Aufsicht und Betroffenen .....	10
1.3.2 Internes Risiko – gegenüber Ihrem Arbeitgeber .....	10
1.4 Typische Fehlannahmen von Führungskräften .....	11
Exkurs: Datenschutz als Umsatz- und Effizienzhebel für Marketing und Vertrieb .....	12
(1) Datenschutz als „Sales Accelerator“ (weniger Reibung, kürzere Zyklen) .....	12
(2) Vertrauen als kaufentscheidender Faktor (Marke, Abschlussquote, Retention) .....	14
(3) Datenschutz als Marketing-Performance-Faktor: bessere Daten statt „mehr Daten“ .....	15
(4) Datenschutzinvestitionen rechnen sich: ROI, Effizienz, Schadensvermeidung .....	17
(5) Die Kosten der Nicht-Compliance: Bußgelder, Nacharbeiten, Reputationsschäden .....	18

## Inhaltsverzeichnis

---

(6) Praktische Auswirkung auf Governance und Beweisfähigkeit . . . .	18
(7) Fazit . . . . .	19
1.5 Praxisfall mit Risikoindikator-Logik – „Die Fanpage macht doch Facebook“ . . . . .	19
1.6 Fallakte: „Leadlisten, Callcenter, Vertrieb – und am Ende 79 Millionen“ .	20
<b>2. Rechtsgrundlagen in 20 Minuten . . . . .</b>	<b>23</b>
Praxisfall – „Nur ein kurzer Reminder“ . . . . .	23
2.1 DSGVO-/BDSG-Basics – in der Sprache von Marketing und Vertrieb .	24
2.2 Typische Rechtsgrundlagen im Geschäftsalltag (Vertrag, berechtigtes Interesse, Einwilligung, § 7 UWG, § 25 TDDDGD) . . . . .	25
2.2.1 Vertrag – alles, was zur Leistung gehört (Art. 6 Abs. 1 lit. b DSGVO) . . . . .	25
2.2.2 Rechtliche Pflicht (Art. 6 Abs. 1 lit. c DSGVO) . . . . .	25
2.2.3 Berechtigtes Interesse – der flexible Standard (Art. 6 Abs. 1 lit. f DSGVO) . . . . .	26
2.2.4 Einwilligung – wenn Sie eindeutig werben oder tracken (Art. 6 Abs. 1 lit. a DSGVO) . . . . .	26
2.2.5 Zusatzebene: § 25 TDDDGD (Endgerätezugriff) – Cookies, Pixel, SDKs . . . . .	27
2.2.6 § 7 UWG – wann Werbung „zumutbar“ ist . . . . .	27
2.3 Praktische Beispiele für zulässige und unzulässige Verarbeitung . . . . .	28
2.3.1 Beispiel 1 – Transaktionsmail vs. versteckte Werbung . . . . .	28
2.3.2 Beispiel 2 – Newsletter an Messe- und LinkedIn-Kontakte . . . . .	28
2.3.3 Beispiel 3 – Bestandskundenwerbung per E-Mail . . . . .	29
2.4 Faustregeln für die tägliche Praxis . . . . .	30
2.5 Fallakte: „Werbung wie eine E-Mail – und am Ende 325 Millionen“ . . .	31
<b>3. Datenlandkarte Marketing, Sales und Vertrieb . . . . .</b>	<b>33</b>
Praxisfall – „Wo liegen die Daten eigentlich?“ . . . . .	33
3.1 Typische Prozesse: Kampagnen, CRM, Portale, Lead-Management, Loyalty, B2B-Verträge . . . . .	34
3.1.1 Prozess: Kampagnen (E-Mail, Social Media, Direct Mail, Online-Anzeigen) . . . . .	34
3.1.2 Prozess: CRM (Customer Relationship Management) . . . . .	34
3.1.3 Prozess: Portale (B2B- und Self-Service-Portale) . . . . .	34

3.1.4	Prozess: Lead-Management (Online und Offline) . . . . .	35
3.1.5	Prozess: Loyalty-Programme (B2B und B2C) . . . . .	35
3.1.6	Prozess: B2B-Verträge und Key-Account-Steuerung . . . . .	36
3.2	Welche Daten wo entstehen (Bestandskunden, Leads, Tracking-Daten, B2B-Kontakte) . . . . .	36
3.2.1	Personengruppen . . . . .	36
3.2.2	Tracking- und Profildaten . . . . .	37
3.2.3	B2B-Kontakte . . . . .	37
3.2.4	Datenarten . . . . .	37
3.3	Datenquellen, Schnittstellen und „blinde Flecken“ . . . . .	38
3.3.1	Typische Datenquellen und Schnittstellen . . . . .	38
3.3.2	Typische „blinde Flecken“ . . . . .	38
3.4	Warum eine aktuelle Landkarte im Incident-Fall entscheidend ist . . . . .	39
3.5	Risikoindikator-Logik: Reifegrad Ihrer Datenlandkarte . . . . .	40
3.6	Fallakte: „Loyalty, Online-Shop, Pass-Karte – und plötzlich sind 5–10 Jahre ‚inaktiv‘ ein Problem“ . . . . .	41
	Exkurs: Social Selling und Datenanreicherung – Chancen, Grenzen, Abmahnrisiken . . . . .	42
	(1) Die Analyse . . . . .	43
	(2) Quick-Box: Social Selling (Do’s und Don’ts) . . . . .	44
<b>4.</b>	<b>Kommunikation und Kampagnenorganisation . . . . .</b>	<b>45</b>
	Praxisfall – „Nur ein interner Test“ . . . . .	45
4.1	E-Mail, Newsletter, CC/BCC, Verteiler, Zielgruppen . . . . .	45
4.1.1	Was technisch simpel wirkt – und rechtlich heikel ist . . . . .	46
4.1.2	CC, BCC und Verteiler – einfache Regeln . . . . .	46
4.1.3	Zielgruppen und Segmentierung – weniger ist oft sicherer . . . . .	47
4.2	Kampagnen-Workflows: Briefing, Freigaben, Tests, Go-Live . . . . .	48
4.2.1	Der Kampagnen-Workflow in vier Phasen . . . . .	48
4.2.2	Rolle der Führungskraft im Workflow . . . . .	49
4.3	Wo und wie aus organisatorischen Fehlern Datenpannen werden . . . . .	49
4.3.1	Fehlende oder lückenhafte Prozesse . . . . .	50
4.3.2	Key-Person-Risiko: Abhängigkeit von Einzelpersonen . . . . .	50
4.3.3	Dauerhafte Workarounds und Schattenprozesse . . . . .	50
4.3.4	Keine oder unzureichende Schulung . . . . .	50
4.3.5	Ungenutzte Alarmzeichen . . . . .	50

## Inhaltsverzeichnis

---

4.4	Einfache Regeln, um klassische Pannen zu vermeiden	51
4.4.1	Risikoindikator-Logik: Kommunikationsrisiken im Überblick	51
4.4.2	Mini-Checkliste „Pre-Send-Check“	52
4.5	Fallakte: „Namensvetter im CRM, falsche E-Mail – und am Ende 10.000 Euro“	53
<b>5.</b>	<b>Beschäftigtendaten im Team</b>	<b>55</b>
	Praxisfall – „Nur ein Test“ mit echten Personaldaten	55
	Die Lehre aus dem Fall	55
5.1	Umgang mit Leistungsdaten, Zielen, Feedback und Krankheitsinformationen	56
5.1.1	Was alles Leistungs- und Verhaltensdaten sind	56
5.1.2	Zielvereinbarungen und variable Vergütung	56
5.1.3	Feedback, Kritik und „Schattenakten“	57
5.1.4	Krankheitsinformationen: besonders sensible Daten	57
5.2	Sichtbarkeiten in Tools und Berichten	58
5.2.1	Leitfrage: Wer sieht was, wozu und wie lange?	58
5.2.2	Typische Fehler bei Sichtbarkeiten	59
5.3	Grenzen der Transparenz im Team	59
5.3.1	Erlaubte Transparenz	59
5.3.2	Problematische Transparenz	60
5.3.3	Umgang mit sensiblen Situationen	60
5.4	Do's and Don'ts für Führungskräfte im Umgang mit Beschäftigtendaten	60
5.4.1	Risikoindikator-Logik für Beschäftigtendaten	61
5.4.2	Konkrete Do's und Don'ts	62
5.5	Fallakte: „Welcome Back Talk, Notizen, Rankings – und am Ende 35,3 Millionen“	63
<b>6.</b>	<b>Geräte, Schatten-IT und mobile Arbeit</b>	<b>65</b>
	Praxisfall – „Das Whiteboard im Messenger“	65
	Die Lehre aus dem Fall	66
6.1	Dienstgeräte, private Geräte, Messenger, Cloud-Speicher	66
6.1.1	Dienstgeräte – wofür sie gedacht sind	66
6.1.2	Private Geräte und BYOD – Segen oder Risiko?	67

6.1.3	Messenger und Kollaborationstools .....	68
6.1.4	Cloud-Speicher und Sync-Funktionen .....	68
6.2	Datei-Sharing, Screenshots, Fotos von Whiteboards .....	69
6.2.1	Datei-Sharing in Projekten und mit Agenturen .....	69
6.2.2	Screenshots und Fotos von Whiteboards.....	70
6.2.3	Schutzmaßnahmen: weniger ist mehr .....	70
6.3	Schatten-IT erkennen und in geordnete Bahnen lenken .....	71
6.3.1	Was ist Schatten-IT?.....	71
6.3.2	Warum gerade Ihr Bereich anfällig ist.....	71
6.3.3	Vom Schatten zur geordneten Lösung.....	71
6.4	Minimale, aber wirksame Regeln für den Bereich .....	72
6.4.1	Risikoindikator-Logik: Geräte und Tools.....	73
6.4.2	Mini-Checkliste „Mobiles Arbeiten und Geräte-Einsatz“.....	74
6.5	Fallakte: „USB-Stick im Rucksack – und plötzlich 145.000 EUR“ .....	74
	Exkurs: Der neue Kollege KI – Prompting ohne Daten-Striptease .....	76
	(1) Der Praxisfall (Narrativ).....	76
	(2) Die Analyse (Kompakt & Rechtlich).....	76
	(3) Quick-Box: KI im Marketing (Do’s und Don’ts).....	77
	(4) Achtung Zeitplan AI Act.....	77
<b>7.</b>	<b>Foto, Video und Social Media .....</b>	<b>78</b>
	Praxisfall – „Das Sommerfest auf LinkedIn“.....	78
	Die Lehre aus dem Fall .....	79
7.1	Interne und externe Bildnutzung: Einwilligungen und Widerspruchsrechte .....	79
7.1.1	Wann Fotos personenbezogene Daten sind.....	79
7.1.2	Interne Nutzung: berechtigtes Interesse mit Grenzen .....	80
7.1.3	Externe Nutzung: Einwilligung als Regelfall.....	80
7.1.4	Widerspruch und Widerruf: Wie Sie fair reagieren .....	81
7.2	Event-Fotografie, Teamfotos, Referenzen .....	82
7.2.1	Event-Fotografie – von der Einladung bis zur Auswahl .....	82
7.2.2	Teamfotos und Mitarbeiterportraits.....	82
7.2.3	Referenzen mit Kunden- und Partnerlogos.....	83
7.3	Social-Media-Posts aus Ihrem Bereich: Chancen und Risiken .....	84
7.3.1	Offizielle Unternehmenskanäle.....	84
7.3.2	Private Accounts von Mitarbeitenden.....	84
7.3.3	Besondere Risiken: Kinder, sensible Kontexte, Notfälle.....	85

## Inhaltsverzeichnis

---

7.4	Typische Fehler – und wie Sie sie vermeiden . . . . .	85
7.5	Fallakte: „Teamfoto, Website, Instagram – und am Ende 9.000 Euro“ . . .	87
	Exkurs: Conversion-Optimierung vs. Dark Patterns – Wenn UX toxisch wird . . . . .	89
	(1) Der Praxisfall . . . . .	89
	(2) Die Analyse (Kompakt & Rechtlich) . . . . .	89
	(3) Quick-Box: Design-Check (Fairness vs. Täuschung) . . . . .	90
	(4) Mustertext (Briefing für UX-Agentur/Web-Team) . . . . .	90
<b>8.</b>	<b>Dienstleister und Agenturen . . . . .</b>	<b>91</b>
	Praxisfall – „Die Agentur kümmert sich um alles“ . . . . .	91
	Die Lehre aus dem Fall . . . . .	92
8.1	Warum Dienstleister und Agenturen im Datenschutz Chefsache sind . .	92
8.2	Auftragsverarbeitung vs. gemeinsame Verantwortlichkeit . . . . .	93
	8.2.1 Klare Auftragsverarbeitung – typische Fälle . . . . .	93
	8.2.2 Gemeinsame Verantwortlichkeit – wann sie vorliegt. . . . .	94
	8.2.3 Praktische Entscheidungsfragen für die Rollenklärung. . . . .	94
8.3	Typische Vertragsbausteine und „rote Flaggen“ . . . . .	95
	8.3.1 Was in jeden guten Vertrag mit Dienstleistern gehört . . . . .	95
	8.3.2 „Rote Flaggen“ in Agentur- und Dienstleisterverträgen . . . . .	96
8.4	Wie Agenturen zu Ausgangspunkten von Incidents werden . . . . .	97
8.5	Praktische Checkliste zur Agenturauswahl und -steuerung . . . . .	98
	8.5.1 Vor der Auswahl – strategische Fragen . . . . .	98
	8.5.2 In der Vertragsphase – Fragen an potenzielle Dienstleister . . . .	99
	8.5.3 Im laufenden Betrieb – Steuerung und Kontrolle. . . . .	99
	8.5.4 Offboarding – wenn die Zusammenarbeit endet. . . . .	100
8.6	Fallakte: „Consent-Banner von der Stange, Mediaagentur unter Druck – und am Ende 250.000 Euro“ . . . . .	101
<b>9.</b>	<b>Frühwarnsystem und Meldewege . . . . .</b>	<b>104</b>
	Praxisfall – „Scraping? Das ist doch kein richtiger Hack ...“ . . . . .	104
	Die Lehre aus dem Fall . . . . .	104
9.1	Wie Datenpannen in Marketing/Sales typischerweise auffallen . . . . .	105
9.2	Interne Meldewege: Wer informiert wen, wie schnell und mit welchen Mindestinformationen? . . . . .	106

9.2.1	Grundprinzip: Jeder Verdacht darf (und soll) gemeldet werden .	108
9.2.2	Wer informiert wen – ein pragmatisches Modell . . . . .	108
9.2.3	Wie schnell muss gemeldet werden? . . . . .	108
9.2.4	Welche Mindestinformationen müssen in der Erstmeldung stehen? . . . . .	109
9.3	Kultur der offenen Fehlerkommunikation statt „Wegdrücken“ . . . . .	109
9.3.1	Warum Wegdrücken gefährlicher ist als der Fehler selbst. . . . .	110
9.3.2	Was Sie als Führungskraft konkret tun können . . . . .	110
9.3.3	„Do und Don’t“ für Führungskräfte. . . . .	111
9.4	Vorbereitung auf Kapitel 10: Was eine Meldung enthalten sollte . . . . .	111
9.4.1	Drei Stufen der Incident-Information . . . . .	111
9.4.2	Welche Inhalte Sie vorab festlegen sollten . . . . .	111
9.4.3	Kurz-Check: Ist Ihr Frühwarnsystem einsatzbereit? . . . . .	112
9.5	Fallakte: „Der Alarm kam aus dem Callcenter – und 22 Tage später wurde es teuer“ . . . . .	113

TEIL II – Im Ernstfall:  
„Incident in 60 Minuten“

<b>10.</b>	<b>Incident in 60 Minuten – Muster-Notfallplan für Datenpannen in Marketing, Sales und Vertrieb . . . . .</b>	<b>117</b>
10.1	Der 60-Minuten-Rahmen auf einen Blick . . . . .	117
	Praxisfall – „Freitag, 16:05 Uhr“ . . . . .	117
	Die Lehre aus dem Fall . . . . .	118
	Fünf universelle Schritte für alle Vorfälle . . . . .	118
	Visueller One-Pager als Orientierung. . . . .	122
10.2	Typische Eskalationswege in Marketing, Sales und Vertrieb. . . . .	122
10.2.1	Wo Vorfälle typischerweise aufschlagen . . . . .	123
10.2.2	Von der Meldung zum passenden Szenario . . . . .	123
10.2.3	Wann eine Führungskraft persönlich gefragt ist. . . . .	124
10.2.4	Kurzbox: Konzern-Scope in 5–15 Minuten klären (auditfest) . .	125
10.3	Szenario A – Kampagne schiefgelaufen . . . . .	126
10.3.1	Startsignal: Woran Sie es erkennen . . . . .	126
10.3.2	T0–15 Minuten: Alarm annehmen und stoppen. . . . .	127
10.3.3	T15–30 Minuten: Sichern und erste Bewertung. . . . .	128
10.3.4	T30–60 Minuten: Entscheidung und Eskalation . . . . .	129
10.3.5	Typische Fehler und Best Practices . . . . .	130

## Inhaltsverzeichnis

---

10.4 Szenario B – Agentur-/Dienstleister-Fehler . . . . .	130
10.4.1 Startsignal: „Die Agentur hat Mist gebaut“ . . . . .	131
10.4.2 T0–15 Minuten: Klare Rollen und Sofortstopp . . . . .	131
10.4.3 T15–30 Minuten: Informationsbeschaffung bei der Agentur . . .	132
10.4.4 T30–60 Minuten: Bewertung und Eskalation . . . . .	132
10.4.5 Typische Fehler und Best Practices . . . . .	133
10.5 Szenario C – Tool-/Plattform-Leak (CRM, Kampagnentool, Cloud, Data Clean Room) . . . . .	134
10.5.1 Startsignal: Meldung des Toolanbieters oder der IT . . . . .	134
10.5.2 T0–15 Minuten: Zugang sichern und Scope eingrenzen . . . . .	135
10.5.3 T15–30 Minuten: Informationen vom Toolanbieter/der IT einholen . . . . .	135
10.5.4 T30–60 Minuten: Bewertung, Meldepflicht und Kommunikationslinie . . . . .	136
10.5.5 Typische Fehler und Best Practices . . . . .	137
10.6 Szenario: Szenarioübergreifende Werkzeuge . . . . .	138
10.6.1 Risikoindikator-Logik für Führungskräfte . . . . .	138
10.6.2 Incident-Log und Dokumentation . . . . .	139
10.6.3 Textbausteine für interne Kommunikation . . . . .	140
10.6.4 One-Pager: „Incident in 60 Minuten“ . . . . .	141
10.7 Fallakte: „Checkout, Cyberangriff – und am Ende 20 Millionen Pfund“ . . . . .	141

### TEIL III – Nach der Datenpanne: Verstetigung und Auditfestigkeit

<b>11. Kampagnen, CRM und Einwilligungen nachschärfen . . . . .</b>	<b>145</b>
11.1 Erkenntnisse aus dem Incident für Zielgruppen, Einwilligungen und Datenqualität . . . . .	145
Praxisfall – „Der Verteiler, der nie sterben wollte“ . . . . .	145
11.2 Typische Korrekturen in Kampagnen-Setups und CRM-Konfigurationen . . . . .	146
11.3 Checklisten für zukünftige Kampagnen . . . . .	147
11.4 30-Tage-Plan nach dem Incident . . . . .	148
11.4.1 Woche 1 – Stabilisieren (Sofortmaßnahmen, die ab jetzt Standard sind) . . . . .	148

11.4.2	Woche 2 – Nachweisfähigkeit herstellen	149
11.4.3	Woche 3 – Prozess und Tool-Guardrails	149
11.4.4	Woche 4 – Verankern (ohne dass es zum „Großprojekt“ wird)	149
11.5	Fallakte: „Fast eine Million SMS – ohne Consent“	150
<b>12.</b>	<b>Betroffenenrechte und Beschwerden pragmatisch abarbeiten</b>	<b>152</b>
	Praxisfall – „Schicken Sie mir alles. Wirklich alles.“	153
12.1	Auskunfts-, Lösch- und Widerspruchsrechte im Bereich Marketing/Sales	153
12.2	Was bedeutet das konkret für Führungskräfte?	154
12.3	Risikoindikator-Logik – so steuern Sie Aufwand und Risiko	154
12.4	Entscheidungsbaum – in 7 Fragen	155
12.5	Kurz-Checkliste für Ihren Bereich (ohne Anhang-Overkill)	155
12.6	Umgang mit Beschwerden nach einer Panne	156
12.7	Standardantworten, Abstimmung mit DSB/Legal, interne Dokumentation	157
12.7.1	Lehre/Regel – Standard schlägt Spontanität	157
12.7.2	Praktische Führungsregel – „3 Ebenen der Antwort“	158
12.7.3	Mini-Standard für interne Abstimmung (DSB/Legal)	158
12.8	Fallakte: „An ausgewählte Partner“ – und dann mussten Namen auf den Tisch	158
<b>13.</b>	<b>Internationalität und Konzernstruktur</b>	<b>161</b>
	Praxisfall – „SCC unterschrieben, Problem gelöst?“	161
13.1	Internationale Datentransfers, Konzernkonstellationen und Joint Controllershship einfach erklärt	161
13.2	Zusammenarbeit mit ausländischen Gesellschaften und Dienstleistern im Incident-Fall	163
13.3	Minimalanforderungen an Verträge und Dokumentation	164
13.4	Fallakte: „EU-Region, US-Support – und am Ende 1,2 Milliarden“	165
<b>14.</b>	<b>Selbst-Audit ohne Panik</b>	<b>168</b>
	Praxisfall – „Der unscheinbare Consent-Code“	168

## Inhaltsverzeichnis

---

14.1 Einfache Audit-Checkliste für Führungskräfte in Marketing, Sales und Vertrieb . . . . .	169
14.1.1 Was ein Selbst-Audit leisten muss – und was nicht . . . . .	169
14.1.2 Die „20-Minuten-Audit-Checkliste“ . . . . .	169
14.1.3 Risikoindikator-Logik „Audit-Fitness“ . . . . .	170
14.2 Stichproben, Interviews, Maßnahmenplanung . . . . .	171
14.2.1 Warum Stichproben besser sind als die Vollständigkeits- Illusion . . . . .	171
14.2.2 Der Stichprobenplan „10 × 3“ . . . . .	171
14.2.3 Interviewleitfaden (15 Minuten je Rolle) . . . . .	171
14.2.4 Maßnahmenplanung: Befund → Maßnahme → Owner → Termin → Nachweis . . . . .	172
14.3 Vorbereitung auf die interne Revision und Aufsichtsbehörden . . . . .	173
14.3.1 Internes Audit/Revision: Was typischerweise wirklich gefragt wird . . . . .	173
14.3.2 Aufsichtsbehörde: ruhig bleiben – aber strukturiert. . . . .	173
14.3.3 Typische Prüffelder der Aufsicht in Marketing/Sales (Praxis-Radar). . . . .	174
14.3.4 Checkliste: „Selbst-Audit in 60 Minuten“ . . . . .	175
14.4 Fallakte: „Excel mit Geheimfach – und am Ende £ 750.000“ . . . . .	175
<b>Audit-Simulation: 14 Stress-Test-Module für Marketing, Sales und Vertrieb . . . . .</b>	<b>178</b>
Executive Summary: Die neue Härte der Datenschutzprüfungen . . . . .	178
Methodik der Audit-Simulation . . . . .	178
Modul 1: Verantwortung und Delegation (Kapitel 1) . . . . .	179
(1) Die Stress-Frage . . . . .	179
(2) Analyse des Prüfungshintergrunds . . . . .	179
(3) Auditfeste Antwortstrategie . . . . .	180
(4) Begründung der Antwort . . . . .	180
(5) Erforderliche Nachweise (Die „Akte“) . . . . .	181
(6) Sofortmaßnahmen . . . . .	181
Modul 2: Rechtsgrundlagen und Zweckbindung (Kapitel 2) . . . . .	181
(1) Die Stress-Frage . . . . .	181
(2) Analyse des Prüfungshintergrunds . . . . .	181
(3) Auditfeste Antwortstrategie . . . . .	182
(4) Begründung der Antwort . . . . .	183

(5) Erforderliche Nachweise. ....	183
(6) Sofortmaßnahmen. ....	183
Modul 3: Datenlandkarte und Ransomware-Resilienz (Kapitel 3) .....	183
(1) Die Stress-Frage. ....	183
(2) Analyse des Prüfungshintergrunds. ....	183
(3) Auditfeste Antwortstrategie .....	184
(4) Erforderliche Nachweise (Die „Akte“) .....	184
(5) Sofortmaßnahmen. ....	185
Modul 4: Kommunikation und Datensicherheit (Kapitel 4) .....	185
(1) Die Stress-Frage. ....	185
(2) Analyse des Prüfungshintergrunds. ....	185
(3) Auditfeste Antwortstrategie .....	185
(4) Erforderliche Nachweise. ....	186
Modul 5: Beschäftigtendaten & Team-Transparenz (Kapitel 5) .....	186
(1) Die Stress-Frage. ....	186
(2) Analyse des Prüfungshintergrunds. ....	186
(3) Auditfeste Antwortstrategie .....	186
(4) Erforderliche Nachweise. ....	187
Modul 6: Geräte, BYOD & Schatten-IT (Kapitel 6) .....	187
(1) Die Stress-Frage. ....	187
(2) Analyse des Prüfungshintergrunds. ....	187
(3) Auditfeste Antwortstrategie .....	187
(4) Erforderliche Nachweise. ....	188
Modul 7: Dienstleister & Auftragsverarbeitung (Kapitel 7/8) .....	188
(1) Die Stress-Frage. ....	188
(2) Analyse des Prüfungshintergrunds. ....	188
(3) Auditfeste Antwortstrategie .....	189
(4) Erforderliche Nachweise. ....	189
Modul 8: Foto, Video und Events (Kapitel 7) .....	189
(1) Die Stress-Frage. ....	189
(2) Analyse des Prüfungshintergrunds. ....	189
(3) Auditfeste Antwortstrategie .....	190
(4) Erforderliche Nachweise. ....	190
Modul 9: KI und Automatisierung (Kapitel 6, Exkurs). ....	190
(1) Die Stress-Frage. ....	190
(2) Analyse des Prüfungshintergrunds. ....	190
(3) Auditfeste Antwortstrategie .....	191
(4) Erforderliche Nachweise. ....	192

## Inhaltsverzeichnis

---

Modul 10: Incident Management (Kapitel 10) .....	192
(1) Die Stress-Frage .....	192
(2) Analyse des Prüfungshintergrunds .....	192
(3) Auditfeste Antwortstrategie .....	192
(4) Erforderliche Nachweise .....	193
Modul 11: Kampagnen-Hygiene und CRM (Kapitel 11) .....	193
(1) Die Stress-Frage .....	193
(2) Analyse des Prüfungshintergrunds .....	193
(3) Auditfeste Antwortstrategie .....	193
(4) Erforderliche Nachweise .....	194
Modul 12: Betroffenenrechte (Kapitel 12) .....	194
(1) Die Stress-Frage .....	194
(2) Analyse des Prüfungshintergrunds .....	194
(3) Auditfeste Antwortstrategie .....	194
(4) Erforderliche Nachweise .....	195
Modul 13: Internationaler Datentransfer (Kapitel 13) .....	195
(1) Die Stress-Frage .....	195
(2) Analyse des Prüfungshintergrunds .....	195
(3) Auditfeste Antwortstrategie .....	195
(4) Erforderliche Nachweise .....	196
Modul 14: Der „30-Tage-Plan“ und Selbst-Audit (Kapitel 14) .....	196
(1) Die Stress-Frage .....	196
(2) Analyse des Prüfungshintergrunds .....	196
(3) Auditfeste Antwortstrategie .....	196
(4) Erforderliche Nachweise .....	197
Fazit: Von der Angst zur Routine .....	197
<b>Epilog</b> .....	198
Vom Bremsklotz zum Wettbewerbsvorteil – Ein neues Mindset für Vertrieb, Marketing und Sales .....	198
Das strategische Fundament der digitalen Ökonomie heißt Vertrauen .....	198
Datenschutz als knallhartes Qualitätsmanagement .....	199
Rechtssicherheit als Innovationsmotor .....	200
Fazit: Agieren statt Reagieren .....	200

Anhänge

**Anhang 1 – Muster-Checklisten** ..... 203

A1.1 Checkliste „Rolle der Führungskraft im Datenschutz“ ..... 203

A1.2 Checkliste „Was gehört in die Akte?“ – prüffeste Dokumentation ... 204

A1.3 Checkliste „Was gehört in die Akte?“ – prüffeste Dokumentation für Rechtsgrundlagen, Einwilligungen, UWG, TDDDG ..... 206

A1.4 Checkliste „Ihre Datenlandkarte in 10 Schritten“ ..... 209

A1.5 Checkliste „Was gehört in die Akte?“ – prüffeste Dokumentation zur Datenlandkarte ..... 210

A1.6 Checkliste „Was gehört in die Akte?“ – prüffeste Dokumentation zur Kommunikation ..... 211

A1.7 Checkliste „Was gehört in die Akte?“ – Beschäftigtendaten im Team ..... 212

A1.8 Checkliste „Was gehört in die Akte?“ – Geräte, Schatten-IT und mobile Arbeit ..... 215

A1.9 „Was gehört in die Akte?“ – Foto, Video und Social Media ..... 218

A1.10 „Was gehört in die Akte?“ – Dienstleister und Agenturen ..... 220

A1.11 Checkliste „Was gehört in die Akte?“ – Frühwarnsystem und Meldewege ..... 222

A1.12 Checkliste „Was gehört in die Akte?“ – Incident in 60 Minuten ..... 225

A1.13 „Was gehört in die Akte?“ – Kampagnen, CRM und Einwilligungen (nach dem Incident) ..... 228

A1.14 Checkliste „Pre-Send 2.0“ (für Kampagnen nach einem Incident) ... 229

A1.15 Checkliste „Was gehört in die Akte?“ – Betroffenenrechte und Beschwerden“ ..... 231

A1.16 Checkliste „Was gehört in die Akte?“ – Internationalität und Konzernstruktur“ ..... 233

A1.17 Checkliste „Was gehört in die Akte?“ – Selbst-Audit ohne Panik ... 235

**Anhang 2 – Muster-Formulare und Textbausteine** ..... 239

A2.1 Muster-E-Mail/Bereichs-Memo – „Zuständigkeiten und Meldewege im Datenschutz“ ..... 239

## Inhaltsverzeichnis

---

A2.2	Muster – Kurzvermerk zur Rechtsgrundlage (intern) für Kampagnen, CRM-Maßnahmen, Tools und Tracking . . . . .	240
A2.3	Muster – Einwilligung für Newsletter/E-Mail-Kommunikation . . . . .	242
A2.4	Mustertext: Einladung zur „Datenlandkarte“ im Bereich . . . . .	243
A2.5	Musterformulierung „Information über Abwesenheiten im Team“ . . . . .	244
A2.6	Musterformulierung „Einladung zu Feedback- und Zielgesprächen“ . . . . .	245
A2.7	Mustertext „Hinweis auf Nutzung von Leistungs- und Feedbackdaten“ . . . . .	245
A2.8	Muster-Memo/E-Mail „Regeln für Geräte, Tools und mobile Arbeit im Bereich“ . . . . .	246
A2.9	Kurz-Hinweise für Workshops, Tools und Screenshots . . . . .	248
A2.10	Mustertexte – Foto- und Video-Hinweise bei Events . . . . .	248
A2.11	Muster-Einwilligung für Mitarbeitenden-Fotos . . . . .	249
A2.12	Standard-Hinweise für Social-Media-Guidelines . . . . .	250
A2.13	Muster-Memo/E-Mail „Grundsätze für den Einsatz von Dienstleistern und Agenturen“ . . . . .	251
A2.14	Muster – Kurz-Check „Dienstleister/Agentur“ (intern) . . . . .	252
A2.15	Musterklausel „Datenschutz und Vertraulichkeit“ für Leistungsbeschreibungen mit Dienstleistern/Agenturen . . . . .	253
A2.16	Muster – Kurzmeldung bei Verdacht auf Datenpanne (E-Mail/Chat) . . . . .	254
A2.17	Musterformular – Incident-Log (Kurzprotokoll, „60-Minuten-tauglich“) . . . . .	255
A2.18	Mustertext – Kurzstatus (Erstmeldung/Update, intern) . . . . .	256
A2.19	Mustertext – Kampagnen-Freigabevermerk „Consent und Audience“ (auditfest, 1 Seite) . . . . .	257
A2.20	Muster – Eingangsbestätigung Betroffenenanfrage (Auskunft, Löschung, Widerspruch) . . . . .	259
A2.21	Muster – Bestätigung Widerspruch gegen Direktwerbung (Art. 21 Abs. 2 DSGVO) . . . . .	259
A2.22	Muster – Antwort auf Beschwerde nach einer Panne (kurz, belastbar, ohne Vorfestlegung) . . . . .	260
A2.23	Muster – Faktenabfrage an ausländische Konzerngesellschaft oder Dienstleister im Incident-Fall . . . . .	260

A2.24	Muster – Kurzvermerk „Rollen- und Transfer-Check“ (Art. 26/28 und Kapitel V DSGVO) – 1 Seite .....	261
A2.25	Mustertext – Team-Ansage „Selbst-Audit in 30 Tagen“ (E-Mail/Teams-Post).....	262
A2.26	Mustertext – Erstreaktion an interne Revision oder Aufsichtsbehörde.....	263
<b>Anhang 3 – Glossar der wichtigsten Begriffe für Führungskräfte .....</b>		<b>264</b>
<b>Anhang 4 – Abkürzungsverzeichnis .....</b>		<b>287</b>
<b>Anhang 5 – „Die zwölf Quellen, die Sie im Stress wirklich brauchen“ ...</b>		<b>293</b>
<b>Anhang 6 – Literatur- und Quellenverzeichnis.....</b>		<b>294</b>

## **Einleitung – Wie Sie dieses Buch nutzen**

Ein falscher Verteiler, ein Screenshot im Chat, eine hastig freigegebene Kampagne – und plötzlich steht die Frage im Raum: „Ist das noch in Ordnung oder schon ein Datenschutzvorfall?“ Vermutlich hat Ihr Unternehmen bereits eine Datenschutzorganisation und ein Justizariat etabliert, aber in diesem Moment sitzt niemand von ihnen mit am Tisch.

Die Entscheidung liegt bei Ihnen als Führungskraft.

Dieses Buch unterstützt Sie genau in solchen Situationen: kurz, klar und auditfest, damit Sie in heiklen Situationen nicht erst lange suchen müssen. Es ersetzt keine Rechtsabteilung, gibt Ihnen aber genug Orientierung, um in Marketing, Sales und Vertrieb zügig begründete Entscheidungen zu treffen – ohne Gutachten, mit tragfähigen Leitplanken.

## **Warum Datenschutz in Marketing, Sales und Vertrieb Chefsache ist**

In Ihrem Bereich wird mit Kundendaten gearbeitet: Kampagnen, CRM, Portale, Loyalty-Programme, internationale Kooperationen. Hier entsteht Umsatz und – langfristig – Vertrauen. Umgekehrt gilt: Fehlender Datenschutz vernichtet Umsatzchancen, noch bevor sie entstehen. Aktuelle Erhebungen zeigen, dass bis zu 95% der Kunden einen Kaufprozess abbrechen würden, wenn sie Zweifel an der Datensicherheit haben.<sup>2</sup> In der digitalen Ökonomie ist ein robustes Datenschutzkonzept somit die Eintrittskarte zum Pitch – ohne sie findet kein Geschäft statt. Ein verantwortungsvoller Umgang mit Kundendaten ist folglich die Grundlage für deren Loyalität und für Ihre Marktposition.

Als Führungskraft kommt es vor allem auf drei Punkte an:

- Sie müssen Risiken erkennen, bevor sie zu handfesten Problemen werden.
- Sie müssen im Incident-Fall handlungsfähig bleiben – gerade dann, wenn wenig Zeit bleibt.
- Sie müssen gegenüber Ihren Kunden, der Geschäftsleitung und der Datenschutzaufsicht nachweisen, dass Ihr Bereich verlässlich organisiert ist.

---

<sup>2</sup> Vgl. Fn. 1, 2025 Cisco Privacy Benchmark Study, Infographic „The Privacy Advantage“; 95% der Konsumenten stimmen der Aussage zu: „Customers won't buy if data isn't protected“. Datenschutz avanciert damit zum Hygienefaktor für den Marktzugang.

## Wie die Teile und Kapitel zusammenhängen

Dieses Buch will Ihnen dafür ein praktisches Grundverständnis geben – nicht jedes Detail der DSGVO, aber das, was Sie für sichere Entscheidungen im Alltag brauchen.



Abbildung 1: Warum DS in MSV Chefsache ist

## Drei Perspektiven dieses Buches

Das Buch ist aus drei Blickwinkeln aufgebaut, die sich durch alle Teile ziehen:

- Prävention – Wie organisieren Sie Kampagnen, Vertrieb, Tools und Dienstleister so, dass typische Fehler gar nicht erst passieren?
- Incident – Was tun Sie, wenn doch einmal etwas schiefgeht? Insbesondere im zentralen Kapitel „Incident in 60 Minuten“.
- Lernen und Audit – Wie ziehen Sie aus Vorfällen die richtigen Konsequenzen – und wie stellen Sie sicher, dass Ihr Bereich prüffest organisiert ist?

Zu jedem dieser Blickwinkel finden Sie klare Regeln, eine Risikoindikator-Logik, Checklisten und kurze Mustertexte.

## Wie die Teile und Kapitel zusammenhängen

TEIL I (Kapitel 1–9) kartographiert das Terrain: Ihre Rolle als Führungskraft, die wichtigsten Rechtsgrundlagen in verständlicher Sprache, typische Prozesse in Marketing und Vertrieb, Zusammenarbeit mit Dienstleistern, Umgang mit Be-

schäftigendaten, Geräten, KI und Kommunikation. Ziel: Eine stabile Basis schaffen und Incidents vermeiden.

TEIL II (Kapitel 10) sichert die Notfallrouten: „Incident in 60 Minuten“. Hier finden Sie Schritt-für-Schritt-Anleitungen für die erste Stunde nach einer Datenpanne, mit Risikoindikator-Logiken, Fragenlisten und Textbausteinen – so, dass Sie auch unter Zeitdruck strukturiert und sicher navigieren können.




TEIL III (Kapitel 11–14) ebnet den Weg nach vorn: Verbesserung von Kampagnen und CRM, pragmatische Bearbeitung von Betroffenenrechten, Umgang mit internationalen Konstellationen, ein einfacher 30-Tage-Plan und ein kompaktes Selbst-Audit für Ihren Bereich. Die Anhänge enthalten Checklisten, Musterformulare, kurze Protokollvorlagen und ein Glossar – als Routenplaner für den Alltag.

## Lese- und Arbeitsempfehlung

Sie müssen dieses Buch nicht linear lesen. Nutzen Sie es situationsbezogen:

- Wenn Sie Ihre Organisation verbessern wollen: beginnen Sie mit TEIL I und springen Sie danach in TEIL III.
- Wenn gerade etwas passiert ist oder Sie einen Fall nachbesprechen möchten: gehen Sie direkt zu Kapitel 10.
- Wenn Sie eine Prüfung oder ein kritisches Managementgespräch erwarten: Nutzen Sie TEIL III und die Anhänge.

In diesem Buch finden Sie zahlreiche Handlungsempfehlungen, Entscheidungsbäume und Checklisten mit Risikoindikator-Codes:

Form-Code	Bedeutung	Praxisbedeutung
STOP 	Hohes Risiko, zum Beispiel unzulässige Datenübermittlung	Vorgang sofort stoppen.
PRÜFEN 	Klärungsbedarf	Prüfen, Rückfrage einholen.
OK 	Standardfall	Vorgehen zulässig, übliche Dokumentation.

Arbeiten Sie mit diesem Buch wie mit einem praktischen Handbuch: Kapitel nach Bedarf aufschlagen, Checkliste durchgehen, Kernaussagen markieren, die vorgeschlagenen Dokumentationspunkte übernehmen. So bauen Sie Schritt für Schritt ein robustes, nachvollziehbares Datenschutz-Niveau in Ihrem Verantwor-

tungsbereich auf – ohne den Anspruch, selbst Jurist oder Datenschutzberater sein zu müssen.

## **Kompass: Datenschutz ist mehr als Compliance – er ist der Schutzraum der Freiheit**

Wie im Vorwort postuliert, ist Datenschutz der Schlüssel zu echten Kundenbeziehungen. Doch warum ist das so? Die Antwort liefert nicht die Betriebswirtschaftslehre, sondern das Verfassungsrecht.

Das Bundesverfassungsgericht hat diesen Mechanismus bereits im visionären Volkszählungsurteil von 1983 definiert. Es warnte vor einer Gesellschaft, in der Menschen ihr Verhalten vorsorglich anpassen, weil sie sich überwacht fühlen. Wer nicht weiß, ob seine Neugier registriert und bewertet wird, verzichtet auf Abweichung und Innovation – er konsumiert „sicher“, statt frei. Das Gericht formulierte dazu eine Kernaussage, die heute für jede Marke überlebenswichtig ist:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung [...] nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“<sup>3</sup>

Für Ihr Marketing bedeutet das: Tracking ohne Transparenz erzeugt Misstrauen. Ein Kunde, der sich im „digitalen Panoptikum“ wähnt, verhält sich defensiv. Er nutzt Adblocker, gibt falsche Daten an oder bricht den Kauf ab – ein ökonomischer „Chilling Effect“, der Umsätze einfriert. Datenschutz durchbricht diesen Zirkel. Er schafft den „Right to be let alone“ – jenes „Recht, in Ruhe gelassen zu werden“, das der US-Richter *Louis Brandeis* schon 1890 als das „umfassendste Recht zivilisierter Menschen“ bezeichnete.<sup>4</sup> Es ist das Recht auf einen inneren Freiraum, ohne den der Mensch zum bloßen Objekt von Profiling und Steuerung degradiert wird.

Indem Sie als Führungskraft Datenschutz proaktiv als Qualitätsmerkmal leben, signalisieren Sie: „Hier bist du sicher. Hier darfst du dich frei entscheiden.“ Sie verwandeln die gesetzliche Pflicht in einen Vertrauensfaktor, der nachweislich Verkaufszyklen verkürzt und Kundenloyalität stärkt. In einer Ära, in der Daten

---

<sup>3</sup> BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 („Volkszählung“), BVerfGE 65, 1 ff., insb. Leitsatz 2 und Rn. 148. Die Aussage begründet das Verbot eines diffusen Überwachungsgefühls, das zu konformistischem und defensivem Kundenverhalten führt.

<sup>4</sup> *Louis Brandeis*, Dissens in *Olmstead v. United States*, 277 U.S. 438 (1928). Marketing-Übersetzung: Respektieren Sie die Privatsphäre als den „inneren Freiraum“. Nur wer sich unbeobachtet fühlt, entwickelt echte Bedürfnisse jenseits der Norm.

## Kompass: Datenschutz ist mehr als Compliance

als „toxisch“ gelten können, wenn sie missbraucht werden, wird Ihre Marke zum sicheren Hafen. *Michel Foucault* warnte: „Sichtbarkeit ist eine Falle“.<sup>5</sup> Befreien Sie Ihre Kunden aus dieser Falle durch Transparenz.

Datenschutz ist damit die Bremse am Rennwagen: Sie existiert nicht, damit Sie langsam fahren, sondern damit Sie sicher Höchstgeschwindigkeit erreichen können, ohne aus der Kurve zu fliegen.

Der „Schutzraum der Freiheit“ ist somit nicht nur ein verfassungsrechtliches Ideal, sondern der marktwirtschaftliche Markt der Zukunft. Wer diesen Schutzraum garantiert, sichert sich den Zugang zum wertvollsten Gut der digitalen Ökonomie: dem echten, unmanipulierten Vertrauen des Kunden.



Abbildung 2: Kompass DS ist mehr als Compliance

<sup>5</sup> *Michel Foucault*, Überwachen und Strafen. Die Geburt des Gefängnisses, aus dem Französischen von Walter Seitter, Frankfurt a. M.: Suhrkamp 1976, S. 257 (Kapitel „Der Panoptismus“): „Die Sichtbarkeit ist eine Falle.“ (Das ist der Mechanismus, vor dem das BVerfG praktisch warnt: Wenn Beobachtung möglich scheint, wird Verhalten vorsorglich angepasst).

## 4. Kommunikation und Kampagnenorganisation

Damit Kampagnen wirken, müssen sie zur richtigen Zeit die richtigen Menschen erreichen. Genau dort passieren die klassischen Datenschutzpannen: falsche Zielgruppe, veraltete Verteiler, offenes CC statt BCC, Tests mit Echtdateien, hektische Freigaben kurz vor dem Versand. In diesem Kapitel geht es nicht um die Rechtsgrundlagen – die kennen Sie aus Kapitel 2 – sondern um Organisation und Kommunikation: Wie Sie Ihren E-Mail- und Kampagnenalltag so aufsetzen, dass Fehler seltener passieren und im Ernstfall nicht als Organisationsversagen gewertet werden.

► Viele Datenschutzpannen im Marketing sind keine IT-Probleme, sondern Organisationsfehler.

### *Praxisfall – „Nur ein interner Test“*

In einem internationalen Konzern soll ein neuer Newsletter getestet werden. Die Kampagne wird von einer Agentur vorbereitet, das Kampagnentool von der IT betrieben, die Zielgruppenliste kommt aus dem CRM. Kurz vor Feierabend bittet die Projektleitung: „Schick doch bitte mal einen Test an den Verteiler, der im Tool hinterlegt ist – ist nur intern.“

Was niemand mehr prüft: Im Tool ist noch der Live-Verteiler der letzten Kampagne hinterlegt. Statt an zwölf interne Tester geht der „Test“ an 18.000 externe Kunden – einige davon haben der Werbung widersprochen oder den Newsletter längst abbestellt. Zudem sind im Text interne Formulierungen und Platzhalter („XY-Rabatt für Problemkunden“) sichtbar.

Die Aufsichtsbehörde bewertet den Vorfall nicht als einmaligen Flüchtigkeitsfehler, sondern als Folge mangelnder Organisation: kein sauberer Testverteiler, keine Freigabeprozesse, keine klaren Regeln für CC/BCC und Zielgruppen. Der Bereich muss nicht nur den Vorfall, sondern seine gesamte Kampagnenorganisation nachschärfen.

### *4.1 E-Mail, Newsletter, CC/BCC, Verteiler, Zielgruppen*

E-Mail ist im Geschäftsalltag der wichtigste Kommunikationskanal – und zugleich einer der häufigsten Auslöser für Datenpannen. Das gilt für klassische Massenmailings ebenso wie für „nur kurz“ zusammengestellte Verteiler im Team.

#### 4.1.1 Was technisch simpel wirkt – und rechtlich heikel ist

Einige typische Konstellationen aus dem Alltag von Marketing, Sales und Vertrieb:

- Offene Verteiler: Adressen im „An“- oder „CC“-Feld statt im „BCC“-Feld; alle Empfänger sehen alle anderen E-Mail-Adressen.
- Veraltete Verteiler: Excel-Listen oder Tool-Listen mit Personen, die längst kein Kunde, Partner oder Mitarbeitender mehr sind oder die Werbung abbestellt haben.
- Mischverteiler: interne und externe Adressen, verschiedene Zielgruppen oder Gesellschaften in einem Verteiler.
- „Sammelpostfächer“: Adressen wie „sales@...“, hinter denen mehrere Personen oder externe Dienstleister stehen, ohne klare Steuerung.
- „Private“ Verteiler von Mitarbeitenden: persönlich geführte Kontaktlisten, die an der offiziellen CRM-Logik vorbeigehen.

Rechtlich berühren Sie damit vor allem Art. 5 DSGVO – insbesondere die Datenminimierung und Vertraulichkeit, Art. 32 DSGVO (Sicherheit der Verarbeitung) – angemessene technische und organisatorische Maßnahmen, § 7 UWG und § 25 TDDDG – ob und wie Sie überhaupt Werbung per E-Mail versenden dürfen (vgl. Kapitel 2.2 und 2.3).

► Ein offener CC-Verteiler bei externen Empfängern ist keine Kleinigkeit, sondern eine Verletzung von Vertraulichkeit und Datensicherheit.

#### 4.1.2 CC, BCC und Verteiler – einfache Regeln

Als Führungskraft müssen Sie die technischen Details nicht selbst konfigurieren, aber Sie sollten einige Regeln setzen:

- BCC ist für Rundmails an externe Empfänger Pflicht. Für Kampagnen sind professionelle Tools mit Einzelversand zwingend.
- CC mit Augenmaß: CC sollte nur genutzt werden, wenn die Empfänger gegenseitig sichtbar sein sollen und dies sachlich gerechtfertigt ist (zum Beispiel kleines Projektteam, alle intern, keine sensiblen Daten).
- Keine „manuell gepflegten Mega-Verteiler“ in Outlook und Co. für Kampagnen – dafür sind dedizierte Tools mit sauberer Zielgruppenlogik und Sperrlisten vorgesehen.
- Newsletter und Kampagnenmails laufen über definierte Systeme, nicht über individuelle Postfächer.

- Zielgruppen gehören ins CRM, nicht in lose Excel-Listen auf Laufwerken oder in Agenturordnern.

### Was bedeutet das konkret für Sie?

Sie machen in Ihrem Bereich klar: Massenmailings über persönliche Postfächer sind unzulässig. Sie sorgen dafür, dass Newsletter und Serienmailings nur über freigegebene Tools laufen (zum Beispiel Kampagnentool, CRM-Modul). Sie lassen sich erklären, wie Sperrlisten (Opt-out) technisch berücksichtigt werden – und lassen das stichprobenartig prüfen. Sie machen „BCC statt CC“ für externe Verteiler zur verbindlichen Teamregel.

### 4.1.3 Zielgruppen und Segmentierung – weniger ist oft sicherer

Zielgruppen sind der Kern jeder Kampagne – und häufig Quelle von Fehlern:

- Zu breite Zielgruppen: „Alle, die wir haben“, ohne Rücksicht auf Einwilligungen, Widersprüche oder Produktrelevanz.
- Fehlende Aktualität: Abmeldungen, Bounce-Adressen und Widersprüche werden nicht konsequent ausgesteuert.
- „Kreative“ Segmente: Zielgruppen werden nach Kriterien gebildet, die sensibel sein können (zum Beispiel Gesundheitsstatus, Ethnie, sexuelle Orientierung, politische Einstellung, Religionszugehörigkeit) – oft ohne Bewusstsein dafür, dass damit besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) berührt werden können.
- Der EuGH hat 2024 den Begriff „Gesundheitsdaten“ bewusst weit gezogen: Schon ein Kontext, der typischerweise Rückschlüsse auf den Gesundheitszustand zulässt, kann Art. 9 DSGVO auslösen.<sup>39</sup> Für das Marketing heißt das: Segmentierungen wie „Assistenzbedarf“, „medizinische Sonderwünsche“, „besondere Betreuung“, oder ähnliche Proxy-Merkmale sind rechtlich kein „kreatives Targeting“, sondern potenziell besondere Kategorien – mit erheblich höherem Risiko.

Ihre Leitfragen als Führungskraft: Worauf beruht diese Zielgruppe? (Kaufhistorie, Einwilligung, Bestandskundenprivileg, Interessenprofil?). Wie wird sichergestellt, dass Abmeldungen und Widersprüche automatisch berücksichtigt werden? Gibt es Segmente, die faktisch Rückschlüsse auf besonders sensible Merkmale ermöglichen?

► Je konkreter und nachvollziehbarer die Zielgruppendefinition, desto leichter können Sie sie im Incident-Fall erklären und verteidigen.

---

<sup>39</sup> EuGH, Urt. v. 4.10.2024 – C-21/23, *ND/DR (Lindenapotheke)*, ECLI:EU:C:2024:846.

#### 4.2 Kampagnen-Workflows: Briefing, Freigaben, Tests, Go-Live

Technik, Agentur, Fachbereich, CRM – ohne klare Kampagnenorganisation droht Chaos. Ein strukturierter Workflow reduziert nicht nur operative Fehler, sondern ist auch eine „Technisch-Organisatorische Maßnahme“ im Sinne des Art. 32 DSGVO.

##### 4.2.1 Der Kampagnen-Workflow in vier Phasen

###### 1. Briefing

Hier werden die Weichen gestellt. Ein gutes Briefing enthält mindestens:

- Den Zweck der Kampagne (Absicht, Zielgrößen).
- Eine Zielgruppenbeschreibung (inklusive Herkunft der Daten, Einwilligungs-/ Rechtsgrundlage, Länder/Regionen).
- Die Kanäle (E-Mail, SMS, App, Portal, Social Media, Offline).
- Die Inhalte (Angebote, Tonalität, besondere Hinweise).
- Die beteiligten Systeme und Dienstleister (Kampagnentool, CRM, Agentur, Plattformen).

Verweis: Die rechtlichen Grundlagen hierzu finden Sie in Kapitel 2; für die Dokumentation siehe Checkliste zu Rechtsgrundlagen im Anhang 1 (A1.3).

###### 2. Setup und Tests

In dieser Phase wird es häufig kritisch:

- Verwendung von Testdaten: wenn möglich synthetische Testdaten oder belastbar anonymisierte Daten. Wenn das nicht möglich ist: pseudonymisierte Testkopien (Minimalfelder!), enges Berechtigungskonzept, kurze Speicherdauer, Logging; Echtdatei nur, wenn das zwingend erforderlich ist und mit klaren Schutzmaßnahmen.
- Testzielgruppen: Nutzung eines klar abgegrenzten Testverteilers (zum Beispiel interne Adressen, Testkunden), niemals „versehentlich“ der Live-Verteiler einer früheren Kampagne.
- Mehr-Augen-Prinzip: mindestens ein zweites Paar Augen prüft Betreff, Inhalt, Zielgruppe, Abmeldeinformationen und Links.

###### 3. Freigaben

Vor dem Go-Live sollte ein transparenter Freigabepunkt stehen:

- Fachliche Freigabe durch die verantwortliche Führungskraft oder Kampagnenverantwortliche.

## 4. Kommunikation und Kampagnenorganisation

---

- Datenschutz-/Legal-Freigabeempfehlung bei besonderen Risiken (neue Datenquelle, neue Zielgruppe, neue Partner, sensible Inhalte).
- Dokumentation: Wer hat wann was freigegeben? (kurzer Eintrag im Kampagnensteckbrief oder Tool.)

### 4. Go-Live und Monitoring

Nach dem Versand ist vor der Auswertung:

- Monitoring der ersten Reaktionen (Bounces, Beschwerden, Abmeldungen).
- Schnelle Stop-Möglichkeit („Kill Switch“ – Not-Aus/Sofort-Stopp-Regel) bei erkannten Fehlern.
- Kurzer Nachbericht mit Lessons Learned – insbesondere, wenn es Auffälligkeiten oder Incidents gab.

► Ein klarer Kampagnen-Workflow ist Ihre wichtigste „Versicherung“ gegen den Vorwurf, Sie hätten Organisation und Kontrolle vernachlässigt.

### 4.2.2 Rolle der Führungskraft im Workflow

Sie müssen nicht jeden Newsletter selbst freigeben. Ihre Aufgabe ist es, den Rahmen zu setzen: Sie entscheiden, ab welcher Größenordnung oder Risikoqualität (zum Beispiel neue Datenquellen, sensible Zielgruppe, internationale Partner) eine explizite Führungskräftefreigabe erforderlich ist.

Sie benennen Kampagnenverantwortliche („Campaign Leads“) und legen fest, welche Freigaben diese selbst erteilen dürfen und wo sie eskalieren müssen.

Sie sorgen dafür, dass der Kampagnen-Workflow dokumentiert und kommuniziert ist (zum Beispiel in einem Bereichsleitfaden oder Intranet-Artikel).

Sie verknüpfen den Workflow mit dem Incident-Prozess in Teil II (Kapitel 10): Wer informiert wen, wenn trotz aller Vorsicht etwas schiefgeht?

### 4.3 *Wo und wie aus organisatorischen Fehlern Datenpannen werden*

Nicht jede Panne ist ein Zeichen schlechter Organisation. Wiederholte oder strukturelle Fehler dagegen schon. Aus Sicht von Aufsichtsbehörden zählen vor allem folgende Muster:

#### 4.3.1 Fehlende oder lückenhafte Prozesse

Es gibt keinen definierten Kampagnen-Workflow, keine klaren Verantwortlichkeiten, keine Checklisten. Test- und Live-Verteiler werden nicht getrennt, Abmeldungen nicht konsequent berücksichtigt.

#### 4.3.2 Key-Person-Risiko: Abhängigkeit von Einzelpersonen

Wissen steckt in Köpfen einzelner Mitarbeitender („Frau X weiß das alles“). Fällt diese Person aus, bricht die Kontrolle zusammen.

#### 4.3.3 Dauerhafte Workarounds und Schattenprozesse

Agenturen pflegen eigene Verteiler, die nicht mit dem CRM synchronisiert werden. Teams arbeiten mit Excel-Exporte „auf Zuruf“, ohne Löschkonzept (vgl. Kapitel 3).

#### 4.3.4 Keine oder unzureichende Schulung

Neue Mitarbeitende im Campaign-Team oder in Agenturen erhalten keine Einweisung in CC/BCC-Regeln, Meldewege und Sperrlisten.

#### 4.3.5 Ungenutzte Alarmzeichen

Beschwerden von Kunden („Ich bekomme Ihre E-Mails trotz Abmeldung“) werden als Einzelfälle abgetan. Bounce-Raten oder hohe Abmelderaten werden nicht als Hinweis auf strukturelle Probleme verstanden.

Im Ergebnis bewerten Aufsichtsbehörden solche Konstellationen als Verstoß gegen die Pflicht, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu ergreifen (Art. 24, 32 DSGVO). Gerade fehlende oder lückenhafte Prozesse im Kampagnen-Setup werden dabei als Organisationsmangel gewertet.

#### **Was bedeutet das konkret für Sie?**

Sie sollten nicht nur einzelne Fehler korrigieren, sondern immer fragen: „Was sagt uns das über unseren Prozess?“ Sie nutzen Incidents als Anlass, den Kampagnen-Workflow, die Rollen und die Checklisten zu schärfen – und dokumentieren das. Sie verankern im Team die Kultur: Fehler werden früh und offen gemeldet, nicht versteckt oder „still korrigiert“.