Datenschutz für Führungskräfte in Marketing, Sales und Vertrieb

Der kompakte Praxisleitfaden – mit Checklisten und Vorlagen für den Führungsalltag

von
Karlheinz Ferenz

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

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

www.ruw.de

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[1] 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-

---

1 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

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

TEIL III – Nach der Datenpanne: Verstetigung und Auditfestigkeit

Anhänge

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 Justiziariat 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.[2] 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.

2 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.

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-

schäftigtendaten, 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."[3]

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.[4] 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

3 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.

4 *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.

als „toxisch“ gelten können, wenn sie missbraucht werden, wird Ihre Marke zum sicheren Hafen. *Michel Foucault* warnte: „Sichtbarkeit ist eine Falle“.[5] 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 Marktplatz 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

5 *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 Echtdaten, 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.[39] 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.

39 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; Echtdaten 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.

- 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".