Checkliste

Ad hoc Krisen-PR

Was Unternehmen in den ersten 24 Stunden tun müssen

Ein praxisorientierter Leitfaden für Kommunikation, Unternehmensleitung, Strategie und Risikomanagement – mit Sofort-Checklisten, Fristen und den neuen Anforderungen aus NIS-2, DSGVO und KI-Zeitalter.

consense communications GmbH (GPRA)
Krisen-PR München • Stand: April 2026

Inhalt

1. Herausforderungen an die Krisenkommunikation in 2026

Krisen werden schneller, lauter und technischer. Was früher vier bis sechs Stunden Reaktionszeit ließ, entscheidet sich 2026 oft in den ersten 30 bis 90 Minuten. Ein einziger Clip auf TikTok, ein manipuliertes Video des CEO, ein Kommentar im falschen Ton – und ein Vorfall wird zur Reputationsfrage.

Gleichzeitig verlangt der Gesetzgeber mehr: Seit der Umsetzung der NIS-2-Richtlinie in Deutschland müssen Unternehmen aus vielen Branchen erhebliche Sicherheitsvorfälle innerhalb von 24 Stunden an das BSI melden. Bei personenbezogenen Daten greift parallel die 72-Stunden-Frist der DSGVO. Die Geschäftsleitung haftet persönlich, wenn Prozesse fehlen.

Diese Checkliste fasst auf rund zehn Seiten zusammen, was Kommunikationsverantwortliche, Vorstände, Strategieabteilungen und Risikomanager heute wissen müssen. Sie ist bewusst kein Handbuch, sondern eine Arbeitsunterlage: zum Mitnehmen in den Krisenstab, zum Abarbeiten Schritt für Schritt.

Die drei Grundregeln, die sich nicht verändert haben

1. Schweigen wird als Schuldeingeständnis gelesen.
2. Wer intern zuletzt erfährt, redet extern am lautesten.
3. Vertrauen entsteht vor der Krise – in der Krise wird es nur getestet.

2. Bevor es brennt: Vorbereitung in fünf Schritten

Der wichtigste Teil jeder Krisenkommunikation findet statt, bevor eine Krise eintritt. Unternehmen, die im Ernstfall souverän wirken, haben meist dieselben fünf Dinge vorbereitet.

2.1 Risiken kartieren und Szenarien vordenken

Listen Sie die fünf bis zehn Szenarien, die Ihr Unternehmen tatsächlich treffen könnten: Produktrückruf, Arbeitsunfall, Cyberangriff, Datenleck, Vorwurf gegen Führungskraft, Lieferkettenproblem, Shitstorm, behördliche Ermittlung. Halten Sie je Szenario eine halbe Seite fest: wer ist betroffen, welche Kanäle sind kritisch, welche Aussage ist in der ersten Stunde verantwortbar.

- ☐ Fünf bis zehn realistische Szenarien sind schriftlich durchdacht.
- ☐ Zu jedem Szenario existieren ein Faktengerüst und drei bis fünf Kernbotschaften in Entwurfsform.
- ☐ Jede Szenarien-Seite wird mindestens einmal jährlich aktualisiert.

2.2 Krisenstab besetzen und Rollen verteilen

Ein arbeitsfähiger Krisenstab hat sechs bis acht Rollen, nicht mehr: Leitung, Kommunikation, Recht, IT/Sicherheit, HR, Operations, Protokoll, Kontakt zu Behörden. Für jede Rolle braucht es eine Vertretung. Entscheidend ist nicht die Hierarchie, sondern Entscheidungsrahmen und schnelles Handeln unter Druck.

- ☐ Krisenstab und Stellvertretungen sind benannt, erreichbar und geschult.
- ☐ Entscheidungskompetenzen sind schriftlich geregelt – wer darf was freigeben, wer spricht mit Medien.
- ☐ Eine alternative Kommunikationswege-Liste existiert für den Fall, dass interne Systeme ausfallen.

2.3 Krisenhandbuch lebendig halten

Ein Krisenhandbuch ist nur so viel wert wie seine letzte Aktualisierung. Kontaktdaten, Sprecherregelung, Freigabewege, Mustertexte, Darksite-Zugänge, Passwörter für Social-Media-Accounts – all das veraltet schneller, als die meisten Unternehmen denken. Zwei feste Review-Termine pro Jahr sind das Minimum.

- ☐ Das Handbuch liegt als PDF und als ausgedruckte Notfallmappe außerhalb der IT-Infrastruktur bereit.
- ☐ Alle Kontakte sind in den letzten sechs Monaten verifiziert worden.
- ☐ Eine Darksite oder Krisen-Landingpage ist technisch einsatzbereit.

2.4 Stakeholder-Landkarte pflegen

Wer ruft Sie als Erstes an, wenn etwas passiert? Wem müssen Sie als Erstes antworten? Eine gepflegte Stakeholder-Karte beantwortet beides. Sie umfasst Mitarbeitende, Betriebsrat, Kunden, Geschäftspartner, Investoren, Behörden, Verbände, Leitmedien, Fachpresse, relevante Influencer:innen und Bewertungsplattformen.

- ☐ Pro Stakeholdergruppe sind Kanal, Informationsbedarf und Ansprechperson festgelegt.
- ☐ Zu wichtigen Journalistinnen und Journalisten besteht ein tragfähiger Kontakt, nicht erst im Ernstfall.
- ☐ Social-Listening läuft im Normalbetrieb, nicht erst ab dem ersten negativen Post.

2.5 Trainieren, nicht nur dokumentieren

Pläne ohne Übung versagen in der Krise. Eine halbtägige Simulation pro Jahr – gerne mit realistischem Medien-Druck durch externe Coaches – zeigt mehr Schwachstellen als jede Analyse. Wer einmal unter Stress vor der Kamera gestanden hat, trifft in der echten Krise bessere Entscheidungen.

- ☐ Mindestens eine vollständige Krisensimulation pro Jahr findet statt.
- ☐ Sprecher:innen haben ein aktuelles Medientraining absolviert (nicht älter als 18 Monate).
- ☐ Nach jeder Übung wird ein kurzer Maßnahmenkatalog abgeleitet und umgesetzt.

3. Die ersten 60 Minuten: Lage erfassen

In der ersten Stunde werden die meisten Kommunikationsfehler gemacht. Das Ziel ist nicht, sofort zu sprechen, sondern sofort zu verstehen – und dann schnell und ehrlich Position zu beziehen. Die bewährten sieben W-Fragen strukturieren diese Phase.

3.1 Die sieben W-Fragen der Lagebewertung

Frage	Worauf es ankommt
Was	Art, Schwere und Umfang des Vorfalls. Nur gesicherte Fakten, keine Annahmen.
Wann	Genauer Zeitpunkt, Dauer, ist der Vorfall noch aktiv oder abgeschlossen.
Wo	Standorte, betroffene Regionen oder Systeme, geografische Reichweite.
Wer ist betroffen	Mitarbeitende, Kundinnen und Kunden, Partner, Anwohner, Behörden – nach Dringlichkeit sortiert.
Wie ist es passiert	Ablauf, ausgelöste Ursachen, Eskalationspfad. Wenn unklar: offen so benennen.
Warum	Hintergründe, mögliche Motive, strukturelle Ursachen. In dieser Phase häufig noch unklar.
Wer sagt es	Quelle der Erstmeldung: interne Kenntnis, Whistleblower, Medien, Behörde, Social Media.

3.2 Parallel: den digitalen Puls nehmen

Zeitgleich zur Faktensammlung läuft das Monitoring. 2026 ist das mehr als klassische Medienbeobachtung: Social Listening umfasst auch Kurzvideos, Audio-Inhalte und Bewegungen in halböffentlichen Kanälen wie WhatsApp-Statusmeldungen, Telegram-Gruppen oder Discord-Servern. Gerade bei TikTok und Instagram Reels entsteht Stimmung innerhalb von Minuten.

- ☐ Monitoring-Tool ist aktiviert und deckt X, LinkedIn, TikTok, Instagram, YouTube, Bewertungsportale und Leitmedien ab.
- ☐ Ein Teammitglied verfolgt Sentiment, Reichweite und auffällige Accounts kontinuierlich.
- ☐ Screenshots und Links werden systematisch dokumentiert – inklusive Zeitstempel.

3.3 Entscheidungspunkt nach 30 bis 60 Minuten

Nach spätestens einer Stunde fällt eine Drei-Wege-Entscheidung: Stufe 1 – Issue, beobachten und intern prüfen. Stufe 2 – Krise, Krisenstab aktivieren, erste Stellungnahme vorbereiten. Stufe 3 – existenzielle Krise, sofortige Public Statements, Vorstand einbinden, Behördenmeldungen vorbereiten.

Merksatz für die erste Stunde

Lieber schnell sagen, dass man informiert und prüft, als langsam schweigen. Eine kurze, ehrliche Holding Statement schlägt jede spekulative Lücke, die andere füllen.

4. Krisenstab aktivieren und intern kommunizieren

4.1 Krisenstab einberufen

Ein Krisenstab arbeitet am besten in festen Rhythmen: kurze Briefings alle 60 bis 90 Minuten, klare Agenda, protokollierte Entscheidungen. Wer redet, wer entscheidet, wer dokumentiert – das muss in den ersten zehn Minuten geklärt sein.

- ☐ Krisenstab ist physisch oder digital aktiviert – im Idealfall trifft er sich in einem dafür frei gehaltenen Raum
- ☐ Leitung, Kommunikation, Recht, IT, HR und Protokoll sind besetzt.
- ☐ Ein einziger, fortlaufend gepflegter Lagebericht existiert – nicht drei konkurrierende Dokumente.
- ☐ Besprechungstakt (z. B. stundengenau) ist festgelegt.

4.2 Mitarbeitende zuerst informieren

Der teuerste Kommunikationsfehler lautet: Mitarbeitende lesen in der Presse, was in ihrem Unternehmen passiert ist. Sie sind die ersten Botschafter – ob gewollt oder nicht. Eine Multi-Channel-Information über Intranet, Mitarbeiter-App, E-Mail und gegebenenfalls Townhall gehört in die erste Stunde. Ausnahme: kapitalmarktrelevante Informationen börsennotierter Unternehmen, die gleichzeitig extern veröffentlicht werden müssen.

- ☐ Eine erste Information an Mitarbeitende ist zeitnah versendet (Stand der Dinge, was bekannt ist, was nicht).
- ☐ Führungskräfte haben ein Sprachregelungs-Briefing bekommen – inklusive der Frage, was sie privat posten dürfen.
- ☐ Eine interne Rückkanal-Möglichkeit besteht (Postfach, Hotline, HR-Kontakt).

4.3 Besonders sensibel: wenn Menschen betroffen sind

Bei Unfällen, Todesfällen oder schweren Personenschäden gelten eigene Regeln. Angehörige werden niemals über die Presse informiert. Empathie ist kein optionaler Tonfall, sondern Pflicht. Abgestimmtes Vorgehen mit Polizei, Notfallseelsorge und ggf. Betriebsarzt ist Voraussetzung für jede öffentliche Aussage.

5. Botschaften, Sprecher, Kanäle

5.1 Kernbotschaften in drei Sätzen

Gute Krisenkommunikation kommt mit drei Sätzen aus: Was ist passiert. Was unternehmen wir. Was bedeutet das für die Betroffenen. Alles andere ist Kontext, den die Zielgruppe von sich aus abruft – oder nicht.

- Klarheit vor Stil: kurze Sätze, aktive Verben, keine Juristen-Formulierungen.
- Verantwortung statt Ausflucht: niemand verlangt Selbstanklage, aber Ausweichen wird sofort entlarvt.
- Empathie zeigen: zuerst die Menschen, dann das Unternehmen.
- Konkrete nächste Schritte nennen: was das Unternehmen jetzt tut, bis wann es nächste Informationen gibt.

5.2 One-Voice-Prinzip ohne starre Skripte

Ein Unternehmen spricht in der Krise mit einer Stimme – aber nicht mit einem einzigen Wortlaut. Sprecher:innen bekommen Leitplanken (zugelassene Kernbotschaften, rote Linien, offene Fragen), nicht Drehbücher. Der Grat zwischen Konsistenz und Roboterhaftigkeit ist schmal; Stakeholder spüren sofort, wenn Menschen sich verlesen.

- ☐ Q&A-Dokument ist aktuell, enthält auch die unangenehmen Fragen und wird stundengenau nachgepflegt.
- ☐ Nur geschulte Sprecherinnen und Sprecher treten auf – intern wie extern.
- ☐ Bei Kamera-Auftritten stehen Setting, Kleidung, Hintergrund fest (keine Improvisation am Schreibtisch).

5.3 Kanäle: wo Ihre Zielgruppen 2026 zuhören

Zielgruppe	Primäre Kanäle in der Krise
Mitarbeitende	Mitarbeiter-App, Intranet, E-Mail, Townhall, direkte Führungskraft.
Kunden / B2B-Partner	Direkte E-Mail vom Ansprechpartner, Service-Hotline, Kunden-Login-Seite, ggf. LinkedIn-Post.
Medien	Pressemitteilung, Darksite, kurze O-Töne für TV und Hintergrundgespräche mit Leitmedien.
Breite Öffentlichkeit	Unternehmenswebsite (Statement oben), LinkedIn, Instagram, bei Bedarf kurze TikTok-Antwort.
Behörden	Schriftliche Meldung über den vorgesehenen Kanal (BSI-Meldeportal, Datenschutzaufsicht), benannter Einzelkontakt.
Investoren (börsennotiert)	Ad-hoc-Mitteilung gemäß MAR, IR-Call, Analysten-Info – zeitgleich mit öffentlicher Kommunikation.

6. Rechtliche Pflichten und Fristen

Krisenkommunikation endet nicht bei der PR. 2026 sind mehrere Meldepflichten parallel zu bedienen. Wer sie verpasst, riskiert Bußgelder, Haftungsfragen für die Geschäftsleitung und den schwerwiegendsten Schaden von allen: den Vorwurf der Vertuschung.

6.1 Die wichtigsten Fristen auf einen Blick

Frist	Anlass	Wohin und was
24 Stunden	Erhebliche Cyber-Sicherheitsvorfälle (NIS-2)	Frühwarnung an das BSI über das Meldeportal. Noch keine abschließende Bewertung nötig.
72 Stunden	Datenschutzverletzung (DSGVO, Art. 33)	Meldung an die zuständige Datenschutzaufsicht (in Bayern: BayLDA bzw. BayDSB). Betroffene ggf. gem. Art. 34 informieren.
72 Stunden	NIS-2: vertiefte Meldung	Aktualisierter Bericht an das BSI mit erster Bewertung, Ursachen und Auswirkungen.
1 Monat	NIS-2: Abschlussbericht	Detaillierter Bericht mit Maßnahmen, Lessons Learned, ggf. verbleibenden Risiken.
Unverzüglich	Kursrelevanz bei börsennotierten Unternehmen	Ad-hoc-Mitteilung nach Art. 17 MAR. Prüfung gemeinsam mit IR und Rechtsabteilung.

6.2 Haftung, Transparenz, anwaltliche Abstimmung

Seit der deutschen NIS-2-Umsetzung haftet die Geschäftsleitung persönlich, wenn Risikomanagement und Meldeprozesse fehlen. Die Kommunikationsabteilung sollte deshalb niemals alleine entscheiden, welche Informationen wann nach draußen gehen – aber sie muss die Prozesse kennen. Enge Abstimmung mit Rechtsabteilung und externen Anwaltskanzleien gehört in den Krisenstab, nicht erst danach.

- ☐ Meldepflichten und Zuständigkeiten sind im Krisenhandbuch benannt.
- ☐ Vor öffentlichen Statements erfolgt ein kurzer Legal-Review – mit festem SLA (z. B. 30 Minuten).
- ☐ Für Datenschutz- und Cybervorfälle liegt ein vorbereiteter Meldetext mit Lücken zum Füllen bereit.

7. Umgang mit Deepfakes, Fake News und KI-Manipulation

Ein gefälschtes Video der Geschäftsführung, eine manipulierte Sprachnachricht, ein scheinbar interner Chatverlauf – KI-generierte Inhalte werden 2026 zu einem regulären Krisenauslöser. Die gute Nachricht: gegen gezielte Manipulation hilft genau das, was ohnehin gute Krisenkommunikation ausmacht – Tempo, Transparenz, verifizierbare Quellen.

- Authentizität absichern: offizielle Kanäle klar markieren, verifizierte Accounts pflegen, Pressekontakte mit direkter Durchwahl statt anonymer Mailadressen.
- Schnelle Faktenseite: bei Verdacht auf Deepfake eine Landingpage online stellen, die den Sachverhalt nachvollziehbar richtigstellt – mit Zeitstempel und benannter verantwortlicher Person.
- Technische Prüfung: forensische Analyse von Bild-, Ton- und Videoquellen beauftragen. Das Ergebnis fließt in die Kommunikation ein, ersetzt sie aber nicht.
- Plattformen einbinden: Meldewege zu Meta, TikTok, YouTube, X und LinkedIn kennen und dokumentiert haben. Entfernung manipulierter Inhalte aktiv einfordern.
- Mitarbeitende sensibilisieren: Schulungen zu CEO-Fraud, Voice-Cloning und Phishing mit KI sind heute so selbstverständlich wie Brandschutzübungen.

> *Wer Manipulation transparent aufklärt, gewinnt mehr Vertrauen, als sie ihm genommen hat. Schweigen dagegen verstärkt das fälschende Narrativ.*

8. Nach der Krise: Auswerten, Lernen, Reputation zurückgewinnen

Die Post-Krisenphase entscheidet, ob aus einem Vorfall eine Narbe oder eine Lerngeschichte wird. Zwei bis vier Wochen nach dem akuten Ereignis sollte ein strukturierter Review vorliegen – nicht länger warten, sonst verblassen Eindrücke und Verantwortlichkeiten.

8.1 Strukturierte Nachbereitung

- ☐ Protokoll und Zeitachse sind sauber dokumentiert (Entscheidungen, Botschaften, Kanäle, Zeitpunkte).
- ☐ Alle Beteiligten – auch Beobachter:innen – werden befragt; schriftlich und in kurzen Interviews.
- ☐ Kennzahlen liegen vor: Reichweite, Sentiment-Verlauf, Medienberichterstattung, interne Zufriedenheit.
- ☐ Lessons Learned fließen konkret in Handbuch, Trainings und Risikokatalog ein, nicht nur in ein PDF.

8.2 Reputation aktiv zurückgewinnen

Reputation erholt sich nicht durch Schweigen, sondern durch sichtbares Handeln. Wer die Ursachen konkret adressiert, Veränderungen belegt und mit Betroffenen im Dialog bleibt, baut schneller wieder Vertrauen auf als Unternehmen, die sich wegducken.

- Fortschrittsberichte: in Abständen von vier bis acht Wochen nachvollziehbar berichten, was sich verändert hat.
- Unabhängige Validierung: Prüfungen durch externe Gutachter:innen oder Zertifizierer schaffen Glaubwürdigkeit.
- Betroffene einbinden: Kundenpanels, Mitarbeiterumfragen, Community-Formate. Zuhören zeigt mehr als senden.
- Proaktive Kommunikation bzw. Positivkommunikation in ruhigen Zeiten: regelmäßige Storys zu Qualität, Sicherheit, Verantwortung wirken als reputationsstärkend für den nächsten Ernstfall.

9. Quellen und weiterführende Literatur

Diese Checkliste basiert auf eigener Beratungs- und Trainingspraxis sowie auf öffentlich zugänglichen Studien, Richtlinien und Fachbeiträgen. Für weiterführende Recherche empfehlen wir insbesondere:

- Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden Krisenkommunikation. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.pdf
- secjur: NIS-2-Meldepflichten – Fristen und Ablauf 2026. https://www.secjur.com/blog/nis2-meldepflicht-cybervorfaelle-deutschland
- secjur: Krisenkommunikation bei Cybervorfällen nach NIS-2. https://www.secjur.com/blog/nis2-krisenkommunikation-cybervorfaelle-meldepflichten
- BDO Security: Cyberangriff – Meldepflichten in Deutschland. https://www.bdosecurity.de/de-de/insights/security-kolumne/cyberangriff-diese-meldepflichten-gelten-in-deutschland
- Transferstelle Cybersicherheit: Cyberangriff – So gelingt Krisenkommunikation im Notfall. https://transferstelle-cybersicherheit.de/cyberangriff-so-gelingt-die-krisenkommunikation-im-notfall/
- ASW Bundesverband: Leitblatt Krisenkommunikation. https://www.asw-bundesverband.de/wp-content/uploads/24-07-09_Leitblatt-Krisenkommunikation.pdf
- DKKV: Risiko- und Krisenkommunikation (Newsletter). https://dkkv.org/wp-content/uploads/2023/01/DKKV_NL_Juni.pdf
- IHK München: Krisenkommunikation für Unternehmen. https://www.ihk-muenchen.de/de/Service/Krisenmanagement-neu/Krisenkommunikation/
- Bundesministerium des Innern: Leitfaden Krisenkommunikation (Langfassung). https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.pdf
- famefact: Shitstorm-Management 2025 – Krisenkommunikation in sozialen Medien. https://famefact.com/2025/06/21/shitstorm-management-2025-krisenkommunikation-in-sozialen-medien/
- Meltwater: Social-Listening-Guide 2026. https://www.meltwater.com/de/blog/der-ultimative-social-listening-guide
- Influencer Marketing Hub: Social Media Listening Report 2025. https://influencermarketinghub.com/social-media-listening-report/
- connect: Deepfake-Bedrohungen für Unternehmen. https://www.connect.de/ratgeber/deepfake-bedrohungen-unternehmen-sicherheitskonzept-technik-sensibilisierung-ratgeber-3212262.html
- Proliance: Cybersecurity & Datenschutz-Trends 2026 (NIS-2, KI, DSGVO). https://www.proliance.ai/blog/cybersecurity-datenschutz-trends-2026
- Security-Insider: Warum viele Unternehmen 2026 bei NIS-2 scheitern werden. https://www.security-insider.de/nis-2-umsetzung-transparenz-2026-a-69be65b566369f3ff916f60a6f6ffe58/
- Itwelt: Wie Deepfakes das Unternehmensrisiko neu definieren. https://itwelt.at/news/digitales-vertrauen-in-gefahr-wie-deepfakes-das-unternehmensrisiko-neu-definieren/
- Artikel 33 und 34 DSGVO – Meldung von Datenschutzverletzungen. https://dsgvo-gesetz.de/art-33-dsgvo/

Hinweis zur Methodik: Der Text wurde auf Basis des langjährigen Fachwissens von consense communications verfasst und mit KI-Unterstützung (Claude Opus 4.7) redigiert. Das Titelbild wurde von Gemini erstellt.

Autorin: Claudia Thaler · consense communications · München · Stand: April 2026 · überarbeitete und aktualisierte Fassung der Erstausgabe Juli 2025.