Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Studierendenprojekt

Integrität in der direkten Demokratie: Manipulationsprävention bei Unterschriftensammlungen

Ein sicherheitsorientierter Bezugsrahmen für Bundeskanzlei, Komitees und Sammelnde

Bachelorarbeit 2025

Auftraggeberschaft	Schweizerische Bundeskanzlei (BK)
Autor	Patrick Vontobel
Dozierende	Prof. Dr. Petra Maria Asprion
Ort, Datum	Schöftland, 09.01.2026

Integrität in der direkten Demokratie:
Manipulationsprävention bei
Unterschriftensammlungen
Ein sicherheitsorientierter Bezugsrahmen für
Bundeskanzlei, Komitees und Sammelnde

Autor
Patrick Vontobel
Rütiweg 6
5040 Schöftland
+41 79 740 71 17
patrick.vontobel@students.fhnw.ch

Dozierende
Prof. Dr. Petra Maria Asprion
Fachhochschule Nordwestschweiz
petra.asprion@fhnw.ch

Auftraggeberschaft
Schweizerische Bundeskanzlei (BK)
Herr Steven Sohn
Bundeshaus West
3003 Bern
+41 58 464 77 04
steven.sohn@bk.admin.ch

Schöftland, Januar 2026

Eigenständigkeitserklärung

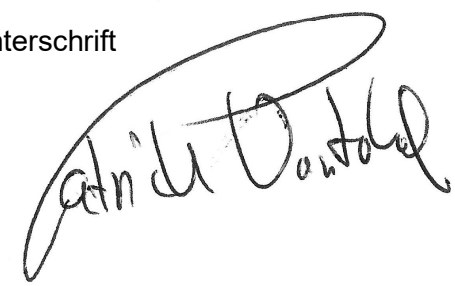
Ich erkläre hiermit,

- dass ich sämtliche nicht von mir selbst stammenden Textstellen gemäss gängigen wissenschaftlichen Zitierregeln korrekt zitiert und die verwendeten Quellen gut sichtbar erwähnt habe;
- dass ich in einem Verzeichnis alle verwendeten Hilfsmittel (z. B. KI-Assistenzsysteme, wie Chatbots [z. B. ChatGPT], Übersetzungs-, Paraphrasier-Tools) oder Programmierapplikationen [z. B. Github Copilot], deklariert und ihre Verwendung bei den entsprechenden Textstellen angegeben habe;
- dass ich sämtliche immateriellen Rechte an von mir allfällig verwendeten Materialien, wie Bildern oder Grafiken, erworben habe oder dass diese Materialien von mir selbst erstellt wurden;
- dass das Thema, die Arbeit oder Teile davon nicht bei einem Leistungsnachweis eines anderen Moduls verwendet wurden, sofern dies nicht ausdrücklich mit der Dozentin oder dem Dozenten im Voraus vereinbart wurde und in der Arbeit ausgewiesen wird;
- dass ich mir bewusst bin, dass meine Arbeit auf Plagiate und auf Drittautorschaft menschlichen oder technischen Ursprungs (künstliche Intelligenz) überprüft werden kann;
- dass ich mir bewusst bin, dass die Hochschule für Wirtschaft FHNW einen Verstoss gegen diese Eigenständigkeitserklärung, bzw. die ihr zugrundeliegenden Pflichten der Studien- und Prüfungsordnung der Hochschule für Wirtschaft FHNW, verfolgt. Zu den Pflichten gehört insbesondere die Wahrung von Urheberrechten und das Unterlassen von Plagiaten (§ 29 Abs. 1 lit. d StuPO). Ein diesbezüglicher Verstoss wird mit der Note 1 bewertet, und es können zusätzlich disziplinarische Folgen (Verweis/Ausschluss aus dem Studiengang) resultieren.

Ort, Datum

Schöftland, 09.01.2026

Unterschrift



Vorwort

Diese Bachelorarbeit ist im Rahmen einer Zusammenarbeit zwischen der Hochschule für Wirtschaft FHNW und der Schweizerischen Bundeskanzlei (BK), Sektion Politische Rechte, entstanden. Ich danke der Auftraggeberschaft, insbesondere Barbara Perriard und Steven Sohn, für den konstruktiven Austausch, die offenen Einblicke in die Praxis und die zur Verfügung gestellten Unterlagen.

Ebenso danke ich meiner Betreuerin, Prof. Dr. Petra Maria Asprion, für die fachliche Begleitung, die kritischen und zugleich ermutigenden Rückmeldungen sowie das Vertrauen in dieses Projekt und meine eigene Entwicklung.

Mein Dank gilt auch allen Personen, die mit Rückmeldungen und fachlichen Hinweisen ihre Zeit und Erfahrung eingebracht und damit zum Gelingen dieser Arbeit beigetragen haben.

Management Summary

Die Unterschriftensammlung für eidgenössische Volksinitiativen und fakultative Referenden ist ein Kernprozess der politischen Rechte in der Schweiz. In den vergangenen Jahren sind im Zusammenhang mit professionellen, gegen Entgelt tätigen Sammelorganisationen einzelne Verdachtsfälle bekannt geworden, in denen Unterschriften mutmasslich gefälscht oder unter problematischen Umständen zustande gekommen sein könnten. Solche Vorkommnisse gefährden nicht nur die formale Rechtmässigkeit, sondern auch die wahrgenommene Integrität des Verfahrens und damit das Vertrauen in die direkte Demokratie. Vor diesem Hintergrund stellt sich für die Schweizerische Bundeskanzlei (BK) die Frage, wie Komitees und Sammelnde gezielt für Integritätsrisiken sensibilisiert werden können, ohne die politische Handlungsfreiheit einzuschränken.

Die Arbeit verfolgt das Ziel, ein evidenzbasiertes, prozessorientiertes Sensibilisierungskonzept für Komitees und Sammelnde zu entwickeln, das zur Rolle und zum Handlungsspielraum der BK passt. Drei Forschungsfragen strukturieren die Arbeit: (1) Welche typischen Integritätsrisiken, Verdachtsfälle und kritischen Situationen treten im Sammelprozess auf? (2) Welche Merkmale von Sensibilisierungsmassnahmen (Awareness) sowie von Massnahmen zum Umgang mit menschlichen Faktoren (Human Factor) gelten als verhaltensnah wirksam und sind auf diesen Kontext übertragbar? (3) Wie kann auf dieser Grundlage ein Sensibilisierungskonzept ausgestaltet werden, das Integritätsrisiken gezielt adressiert und zugleich realistisch umsetzbar ist?

Methodisch folgt die Arbeit einem qualitativ dominierten Mixed-Methods-Ansatz mit Triangulation verschiedener Datenquellen. Die Basis bildet ein theoretischer Bezugsrahmen, der Integrität als sicherheitsrelevantes Ziel in der direkten Demokratie versteht und vier Dimensionen verknüpft: Steuerungs- und Verantwortungsrahmen (Governance; z. B. formelle und informelle Regeln, Rollen und Zuständigkeiten), Prozesse (z. B. Abläufe und Kontrollen), Human Factor (z. B. Verhalten, Drucksituationen und Anreize der Beteiligten) sowie Awareness- und Unterstützungsinstrumente (z. B. Sensibilisierungsmassnahmen, Informationsmaterialien und praktische Hilfsmittel). Darauf aufbauend werden eine systematische Literaturrecherche zu Awareness- und Human-Factor-Massnahmen (Fokus 2020–2025), zentrale Dokumente und Prozessbeschreibungen der BK zur Unterschriftensammlung sowie vier schriftliche Rückmeldungen von Fachpersonen aus Politik, digitaler Demokratie und IT-Sicherheit (zwei Kommunalpolitiker, ein Unternehmer im Bereich Software- und IT-Sicherheit, ein im Feld digitaler Demokratie und digitale Unterschriftensammlung (E-Collecting) tätiger Unternehmer) mit einer inhaltlich strukturierenden qualitativen Inhaltsanalyse ausgewertet und verdichtet. Als analytische Linse dienen die Integritätshebel: «Situationen, Strukturen, Signale».

Die Ergebnisse zeigen erstens, dass Integritätsrisiken weniger an einem einzelnen «kritischen Punkt» entstehen, sondern aus dem Zusammenspiel von konkreten Situationen (z. B. Einsatz

externer Sammelorganisationen, Sammeln unter Zeitdruck, Umgang mit vulnerablen Personen), unklaren Strukturen (Rollen, Vorgaben, Meldewege) und widersprüchlichen Signalen (implizite und explizite Botschaften zum gewünschten Verhalten). Integrität in der Unterschriftensammlung erweist sich damit als eigenständiges Sicherheitsziel, das über die Einhaltung formaler Anforderungen hinausgeht. Zweitens macht die Auswertung der Awareness- und Human-Factor-Literatur deutlich, dass klassische, stark wissensorientierte Schulungsformate unter Bedingungen knapper Ressourcen und hoher Fluktuation nur begrenzt verhaltensnahe Wirkung entfalten. Wirksamer erscheinen kurze, kontextspezifische Lernimpulse, die mit konkreten Handlungsoptionen in typischen Situationen verknüpft sind, in bestehende Prozesse eingebettet werden und sich wiederholen, ohne die Zielgruppen zu überfordern.

Drittens überführt die Arbeit diese Befunde in ein zweistufiges Sensibilisierungskonzept. Paket A stärkt die BK-seitige Verankerung von Integrität, indem an ausgewählten Prozesspunkten – etwa in Leitfäden, Schreiben an Komitees oder internen Checklisten – Integritätsanforderungen sichtbarer gemacht und Ansprechstellen klarer definiert werden. Paket B richtet sich unmittelbar an Komitees und Sammelnde und besteht aus drei leichtgewichtigen Bausteinen: einem einseitigen Integritäts-Check für Komitees, einem Einseiter «Faires Sammeln» für Sammelnde sowie einer Kurz-Checkliste für heikle Situationen. Alle Elemente folgen fünf Designprinzipien: evidenzbasiert und pragmatisch, prozessorientiert und situationsbezogen, rollen- und freiheitskompatibel, radikal einfach und ressourcenschonend sowie anschlussfähig und beobachtbar.

Die Arbeit liefert damit keine statistisch generalisierbaren Aussagen, sondern kontextbezogene, theoretisch und empirisch abgestützte Vorschläge für den Umgang mit Integritätsrisiken in der Unterschriftensammlung und für die Rolle der BK in diesem Prozess. Für die Praxis eröffnet das Sensibilisierungskonzept die Möglichkeit, Integrität als Teil eines sicherheitsorientierten Governance-Verständnisses systematisch in bestehende Abläufe einzubetten und Komitees sowie Sammelnde mit einfachen, freiwillig nutzbaren Hilfsmitteln zu unterstützen. Für weitere Forschung bietet die Arbeit Ansatzpunkte, die Nutzung und Wirkung der vorgeschlagenen Bausteine im Rahmen von Pilotierungen – etwa im Kontext künftiger Arbeiten der BK zu E-Collecting – empirisch zu evaluieren und den Bezugsrahmen auf andere Formen politischer Beteiligung zu übertragen.

Inhaltsverzeichnis

Eigenständigkeitserklärung II

Vorwort III

Management Summary IV

Inhaltsverzeichnis VI

1 Einleitung 1

1.1 Ausgangslage und Kontext 1

1.2 Problemstellung 1

1.3 Zielsetzung und Forschungsfragen 2

1.4 Auftraggeberschaft und Rahmenbedingungen 3

1.5 Vorgehen und Aufbau der Arbeit 3

2 Kontext: Direkte Demokratie, Unterschriftensammlung und Integrität 6

2.1 Politische Rechte und rechtlicher Rahmen 6

2.2 Ablauf einer Volksinitiative und eines fakultativen Referendums 7

2.3 Rollen und Verantwortlichkeiten 8

2.4 Integritätsrisiken 10

2.5 Zwischenfazit 11

3 Theoretischer Bezugsrahmen: Integrität, Governance, Informationssicherheit, Awareness-Programme und Human Factor 13

3.1 Governance und Rollenverständnis 13

3.2 Informationssicherheit 15

3.3 Awareness-Programme und verhaltensnahe Wirksamkeit 18

3.4 Human Factor 22

3.5 Zusammenfassung 25

4 Methodik und Forschungsdesign 29

4.1 Forschungsansatz 29

4.2 Literaturrecherche 30

4.2.1 Geltungsbereich 31
4.2.2 Datenbasis und Suchstrategie 31
4.2.3 Kategorien 31
4.2.4 Einschluss- und Ausschlusskriterien 32
4.2.5 Evidenzlogik 32
4.2.6 Analyseschritte und Verknüpfung mit dem theoretischen Bezugsrahmen 33
4.3 Dokumenten- und Prozessanalyse 33
4.3.1 Ziel und Funktion der Analyse 33
4.3.2 Datenbasis: Leitfäden, Prozessbeschreibungen und Konzeptentwürfe der BK 34
4.3.3 Analyseschritte und Verknüpfung mit dem theoretischen Bezugsrahmen 35
4.3.4 Prozessorientierte Verdichtung: Situationen, Strukturen, Signale 35
4.3.5 Beitrag zur Beantwortung der Forschungsfragen 36
4.4 Interviews mit Fachpersonen 37
4.4.1 Zielsetzung und Einbettung 37
4.4.2 Auswahl der Fachpersonen 37
4.4.3 Erhebungsdesign und Durchführung 39
4.4.4 Datenschutz und Vertraulichkeit 39
4.5 Auswertungsverfahren 40
4.5.1 Auswertungslogik und analytischer Bezugsrahmen 40
4.5.2 Auswertung der Literatur- und Dokumentenbasis 41
4.5.3 Auswertung der Interviews mit Fachpersonen und Triangulation 42
4.6 Gütekriterien und Limitationen 43
4.6.1 Gütekriterien des Forschungsdesigns 43
4.6.2 Limitationen des Forschungsdesigns 44
4.6.3 Umgang mit Limitationen 45
5 Ergebnisse der Literatur- und Dokumentenanalyse 46

5.1 Evidenzübersicht 2020–2025 46
5.2 Zentrale Wirkungshebel der Awareness-Literatur 47
5.3 Governance-Schicht und Messlücke 49
5.4 Übertragung auf Bundeskanzlei, Komitees und Sammelnde 50
5.5 Zwischenfazit und Implikationen für die Konzeptphase 52
6 Ergebnisse der empirischen Erhebung 53
6.1 Datengrundlage und Einordnung 53
6.2 Wahrnehmung der Integrität im Schweizer Kontext 54
6.3 Grenze zwischen legitimer Überzeugungsarbeit und Manipulation 55
6.4 Einordnung entlang des Bezugsrahmens 56
6.5 Zwischenfazit und Implikationen für das Sensibilisierungskonzept 57
7 Entwicklung des Sensibilisierungskonzepts 59
7.1 Designprinzipien 59
7.2 Paket A – BK-seitiger Rahmen 61
7.3 Paket B – Minimal Viable Awareness-Paket für Komitees und Sammelnde 62
7.4 Wirkungslogik und Indikatoren 64
7.5 Abgrenzung zu weiteren Massnahmen 65
8 Diskussion 67
8.1 Beantwortung der Forschungsfragen 67
8.2 Einordnung in Forschung (Awareness/Human Factor) und Verwaltungspraxis 68
8.3 Implikationen für BK und andere Behörden 69
8.4 Stärken, Limitationen, Forschungsbedarf 70
9 Schlussfolgerung 72
9.1 Zusammenfassung der zentralen Ergebnisse 72
9.2 Reflexion des Mixed-Methods-Ansatzes 73
9.3 Ausblick: Pilotierung, Evaluation und Transfer 74
Literaturverzeichnis 76

Hilfsmittelverzeichnis 80

Abbildungsverzeichnis 81

Tabellenverzeichnis 82

Abkürzungsverzeichnis 83

Anhang A – Evidenztabelle Awareness- und Human-Factor-Literatur (2020–2025) 84

Anhang B – Interviewleitfaden und schriftliche Befragung 138

Anhang C – Prototypische Sensibilisierungsmaterialien (Paket B) 149

1 Einleitung

1.1 Ausgangslage und Kontext

Die direkte Demokratie ist ein zentrales Merkmal der politischen Ordnung der Schweiz. Auf Bundesebene ermöglichen eidgenössische Volksinitiativen und fakultative Referenden, dass Stimmberechtigte politische Anliegen mittels Unterschriftensammlung auf die nationale Agenda bringen (BV, 2000). Die Sammlung, Bescheinigung und Einreichung von Unterschriften bildet dabei einen Kernprozess der politischen Rechte: Sie entscheidet darüber, ob ein Volksbegehren überhaupt zustande kommt und in den politischen Entscheidungsprozess eintritt (BPR, 1978).

In den vergangenen Jahren sind im Zusammenhang mit professionellen, gegen Entgelt tätigen Sammelorganisationen einzelne Verdachtsfälle bekannt geworden, in denen Unterschriften mutmasslich gefälscht oder unter problematischen Umständen zustande gekommen sein könnten (Bundeskanzlei, 2025a). Solche Vorkommnisse berühren nicht nur die formale Rechtmässigkeit, sondern auch die wahrgenommene Integrität der Unterschriftensammlung. Sie können das Vertrauen in den Prozess beeinträchtigen und werfen Fragen danach auf, welche Verantwortung Komitees und Sammelnde bei der Organisation und Durchführung von Sammelaktionen tragen.

Die Schweizerische Bundeskanzlei (BK) hat vor diesem Hintergrund verschiedene Massnahmen ergriffen, um die Integrität der Unterschriftensammlung zu stärken (Bundeskanzlei, 2025a). Dazu zählen insbesondere Anpassungen von Formularen und Abläufen, kommunikative Hinweise in Leitfäden sowie der gezielte Austausch mit der Wissenschaft (Bundeskanzlei, 2025b, 2025c). In diesem Rahmen wurde die Sensibilisierung von Initiativ- und Referendumskomitees als eine mögliche Massnahme identifiziert. Die vorliegende Arbeit ist in diesen Kontext eingebettet: Sie untersucht aus einer informationssicherheitsorientierten Perspektive, wie Komitees und Sammelnde für Integrität, Manipulationsprävention und verantwortungsbewusstes Handeln im Sammelprozess sensibilisiert werden können.

1.2 Problemstellung

Die rechtlichen Grundlagen und die von der BK bereitgestellten Leitfäden definieren zentrale Anforderungen an die Unterschriftensammlung – etwa die eigenhändige und datierte Unterschrift, die Bescheinigung der Stimmberechtigung durch die Gemeinden und die fristgerechte Einreichung der Unterschriftenlisten (BPR, 1978; BV, 2000; VPR, 1978; Bundeskanzlei, 2025b, 2025c). Diese Vorgaben schaffen einen normativen Rahmen, gewährleisten aber allein noch nicht, dass alle Beteiligten in kritischen Situationen integritätskonform handeln. Insbesondere im Zusammenspiel von Zeitdruck,

finanziellen Anreizen, politischer Überzeugung und unklaren Zuständigkeiten können Graubereiche entstehen, in denen Fehlverhalten wahrscheinlicher wird.

Komitees und Sammelnde sind häufig temporär organisierte Strukturen mit begrenzten Ressourcen und hoher Fluktuation, wie sich auch in den Rückmeldungen der befragten Fachpersonen zeigt (vgl. Abschnitte 5.2 und 5.3). Neue Sammelnde werden teils nur kurz instruiert, externe Sammelorganisationen sind schwerer zu steuern, und im Alltag gibt es wenig Raum für vertiefte Schulungen. Gleichzeitig verfügt die BK nur über indirekte Einflussmöglichkeiten: Sie kann Rahmenbedingungen setzen und informieren, hat aber keine Weisungsbefugnis gegenüber Komitees und ihren Sammelnden. Daraus ergibt sich eine doppelte Herausforderung: Sensibilisierungsmassnahmen müssen einerseits Integritätsrisiken realistisch adressieren und konkrete Orientierung bieten, andererseits zum Ressourcen- und Handlungsspielraum der BK und der Komitees passen und die politische Handlungsfreiheit respektieren.

Vor diesem Hintergrund stellt sich die Frage, wie Sensibilisierung so gestaltet werden kann, dass sie an typischen Risikosituationen im Sammelprozess ansetzt, die Eigenverantwortung von Komitees und Sammelnden stärkt und gleichzeitig mit den bestehenden Prozessen und Kommunikationskanälen der BK kompatibel bleibt.

1.3 Zielsetzung und Forschungsfragen

Ausgangspunkt der Arbeit ist die Zielsetzung der Auftraggeberschaft, Initiativ- und Referendumskomitees sowie Sammelnde wirksamer für Integritätsrisiken in der Unterschriftensammlung zu sensibilisieren. Die Arbeit verfolgt das übergeordnete Ziel, ein evidenzbasiertes, prozessorientiertes Sensibilisierungskonzept zu entwickeln, das sowohl zur Rolle der BK als auch zu den praktischen Rahmenbedingungen von Komitees und Sammelnden passt.

Daraus leiten sich drei Forschungsfragen ab, die den weiteren Aufbau der Arbeit strukturieren und in den Kapiteln 5–7 beantwortet werden:

1. **F1 – Integritätsrisiken und kritische Situationen:** Welche typischen Integritätsrisiken, Verdachtsfälle und kritischen Situationen treten im Prozess der Unterschriftensammlung aus Sicht der BK, der Komitees und der Sammelnden auf (BPR, 1978; VPR, 1978; Bundeskanzlei, 2025b, 2025c)?
2. **F2 – Wirksame Awareness-Ansätze:** Welche Merkmale von Awareness (Sensibilisierung) und Human-Factor-Massnahmen (menschliche Faktoren) gelten in der aktuellen Forschung als verhaltensnah wirksam, und inwiefern lassen sie sich auf den Kontext von Komitees und Sammelnden bei eidgenössischen Volksbegehren übertragen (ENISA, 2021, S. 25–26, 30; Hu et al., 2022, S. 754–757)?

3. **F3 – Sensibilisierungskonzept für die BK und Komitees:** Wie kann auf Basis dieser Evidenz und der bestehenden Prozess- und Dokumentenlandschaft der BK ein Sensibilisierungskonzept ausgestaltet werden, das Integritätsrisiken gezielt adressiert und gleichzeitig zum Ressourcen- und Handlungsspielraum von BK, Komitees und Sammelnden passt (Bundeskanzlei, 2025b, 2025c)?

Die Forschungsfragen verbinden damit die Analyse von Integritätsrisiken (F1), die Auswertung bestehender Evidenz zu wirksamer Sensibilisierung (F2) und die Entwicklung eines konkret umsetzbaren Sensibilisierungskonzepts (F3).

1.4 Auftraggeberschaft und Rahmenbedingungen

Die vorliegende Arbeit entsteht im Rahmen des Bachelor-Studiums an der Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz (FHNW). Auftraggeberschaft ist die Schweizerische Bundeskanzlei, Sektion Politische Rechte. Die Arbeit ist Teil des von der BK initiierten Formats «Austausch mit der Wissenschaft» und fokussiert auf die Integrität der Unterschriftensammlung bei eidgenössischen Volksinitiativen und fakultativen Referenden.

Der Bearbeitungszeitraum liegt im Herbstsemester 2025. Inhaltlich liegt der Schwerpunkt auf der Sensibilisierung von Komitees und Sammelnden. Andere Formen politischer Beteiligung sowie kantonale und kommunale Prozesse werden nicht systematisch untersucht. Die Arbeit benennt rechtliche Grundlagen – insbesondere Bundesverfassung (BV), Bundesgesetz über die politischen Rechte (BPR), Verordnung über die politischen Rechte (VPR) und Datenschutzgesetz (DSG) – interpretiert oder bewertet sie jedoch nicht im Sinne einer rechtswissenschaftlichen Analyse.

1.5 Vorgehen und Aufbau der Arbeit

Diese Arbeit ist als qualitativ ausgerichtete explorative Fallstudie mit Fokus auf die BK und den Prozess der Unterschriftensammlung auf Bundesebene konzipiert. Das Forschungsdesign kombiniert im Sinne einer methodischen Triangulation eine systematische Literaturrecherche, eine Dokumenten- und Prozessanalyse der BK-Unterlagen sowie die Befragung ausgewählter Fachpersonen. Dieses kombinierte Vorgehen wird im weiteren Sinn als Mixed-Methods-Ansatz verstanden. Die gewonnenen Befunde werden entlang eines in Kapitel 3 entwickelten Bezugsrahmens ausgewertet, der die Dimensionen Governance (Steuerungs- und Verantwortungsrahmen; z. B. formelle und informelle Regeln, Rollen und Zuständigkeiten), Prozesse (z. B. Abläufe und Kontrollen), Human Factor (z. B. Verhalten, Drucksituationen und Anreize der Beteiligten) sowie Awareness- und Unterstützungsinstrumente (z. B. Sensibilisierungsmassnahmen, Informationsmaterialien und praktische Hilfsmittel) unterscheidet und in ein zweistufiges Sensibilisierungskonzept überführt.

Konzeptionell gliedert sich die Arbeit damit in drei Bausteine: Erstens wird in den Kapiteln 2 und 3 ein theoretischer Bezugsrahmen zu Integrität, Governance, Informationssicherheit, Awareness-Programmen und Human Factor entwickelt. Zweitens überträgt eine kleine qualitative Studie im Sinne einer empirischen Analyse diesen Bezugsrahmen auf den Kontext der Unterschriftensammlung und prüft seine Tragfähigkeit (vgl. Kapitel 4–6). Drittens wird darauf aufbauend in Kapitel 7 ein Sensibilisierungskonzept für die BK sowie für Komitees und Sammelnde ausgearbeitet.

Der Aufbau der Arbeit ist wie folgt:

Kapitel 2 beschreibt den Kontext der Unterschriftensammlung in der Schweizer Bundespolitik. Es skizziert den rechtlichen Rahmen, den Ablauf von Volksinitiativen und fakultativen Referenden, die Rollen zentraler Beteiligter sowie typische Integritätsrisiken und bisherige Massnahmen der BK und leitet daraus die Relevanz der Sensibilisierung von Komitees und Sammelnden ab.

Kapitel 3 entwickelt den theoretischen Bezugsrahmen der Arbeit. Es verortet Integrität und Legitimität in der direkten Demokratie, führt eine informationssicherheitsorientierte Perspektive («Integrity by Design») ein, bündelt Erkenntnisse zu Awareness-Programmen und Human Factor und leitet daraus einen theoretischen Bezugsrahmen mit den Integritätshebeln «Situationen, Strukturen, Signale» für Komitees und Sammelnde ab.

Kapitel 4 konkretisiert das methodische Vorgehen. Es beschreibt den Forschungsansatz, die Literaturrecherche, die Dokumenten- und Prozessanalyse sowie die schriftlichen Kurzinterviews (per E-Mail) mit Fachpersonen und legt das Auswertungsverfahren entlang der Dimensionen des Bezugsrahmens fest.

Kapitel 5 und 6 präsentieren die Ergebnisse der Analysen auf Basis der wissenschaftlichen Literatur, der Dokumente und Prozesse der Bundeskanzlei sowie der Interviews. Kapitel 5 fasst die Befunde der Literatur- und Dokumentenanalyse entlang der Dimensionen des Bezugsrahmens zusammen und leitet erste Wirkungshebel für Sensibilisierung ab. Kapitel 6 fasst die Rückmeldungen aus der Befragung von zwei Kommunalpolitikern einer mittelgrossen aargauischen Stadt zusammen und ordnet sie entlang des gleichen Bezugsrahmens ein. Ergänzend fliessen zwei weitere schriftliche Rückmeldungen aus den Bereichen Software- und IT-Sicherheit sowie digitale Demokratie punktuell in die Interpretation und den Ausblick ein. Beide Kapitel schliessen mit Zwischenfazits, die in das Sensibilisierungskonzept überleiten.

Kapitel 7 bündelt die Befunde in einem zweistufigen Sensibilisierungskonzept (Paket A und Paket B) für die BK sowie für Komitees und Sammelnde.

Kapitel 8 diskutiert die Ergebnisse im Lichte der Forschungsfragen, ordnet sie in die einschlägige Awareness- und Human-Factor-Forschung sowie in die Verwaltungspraxis ein und reflektiert Stärken und Limitationen der Arbeit.

Kapitel 9 schliesst mit einer zusammenfassenden Schlussfolgerung, einer Reflexion des Mixed-Methods-Ansatzes und einem Ausblick auf mögliche Pilotierungen, Evaluationen und Transfers in andere Kontexte.

2 Kontext: Direkte Demokratie, Unterschriftensammlung und Integrität

Die Unterschriftensammlung ist ein Kernprozess der politischen Rechte auf Bundesebene. Ihre Integrität trägt wesentlich zur Legitimität von Volksbegehren bei. Dieses Kapitel skizziert den rechtlichen und institutionellen Kontext der Unterschriftensammlung im Rahmen der politischen Rechte auf Bundesebene. Es beschreibt die Rahmenbedingungen, unter denen Volksinitiativen und fakultative Referenden zustande kommen, und zeigt auf, in welchen Prozessphasen und Beteiligtenkonstellationen Integritätsrisiken entstehen können.

Grundlage bilden die Bundesverfassung der Schweizerischen Eidgenossenschaft (BV, 2000), das Bundesgesetz über die politischen Rechte (BPR, 1978) sowie die Verordnung über die politischen Rechte (VPR, 1978). Die von der BK veröffentlichten Leitfäden zu eidgenössischer Volksinitiative und fakultativem Referendum illustrieren den Ablauf, die formellen Anforderungen an Unterschriftenlisten und die Zuständigkeiten in verständlicher Form (Bundeskanzlei, 2025b, 2025c).

Dazu werden zunächst die verfassungs- und gesetzesrechtlichen Grundlagen der politischen Rechte (vgl. Abschnitt 2.1) sowie der Ablauf einer Volksinitiative und eines fakultativen Referendums (vgl. Abschnitt 2.2) dargestellt. Anschliessend werden die Rollen und Verantwortlichkeiten der zentralen Beteiligten – Komitees, Sammelnde, Gemeinden und BK – beschrieben (vgl. Abschnitt 2.3). Darauf aufbauend werden typische Integritätsrisiken und bisherige Massnahmen der BK zur Stärkung der Integrität in der Unterschriftensammlung aufgezeigt (vgl. Abschnitt 2.4). Ein kurzes Zwischenfazit (vgl. Abschnitt 2.5) bündelt die wichtigsten Beobachtungen und leitet zum theoretischen Bezugsrahmen in Kapitel 3 über.

2.1 Politische Rechte und rechtlicher Rahmen

Die Schweiz wird in der politischen Diskussion und Fachliteratur immer wieder als Prototyp einer direkten Demokratie bezeichnet (Ogorek, 2019). Neben den obligatorischen Volksabstimmungen bilden insbesondere die eidgenössische Volksinitiative und das fakultative Referendum zentrale Instrumente, mit denen stimmberechtigte Personen auf die Bundespolitik einwirken können. Beide Instrumente ermöglichen es, politische Vorlagen an die Urne zu bringen und damit parlamentarische Entscheidungen zu korrigieren, zu ergänzen oder zu initiieren.

Rechtsgrundlage der politischen Rechte auf Bundesebene ist in erster Linie die Bundesverfassung (BV). Die Artikel 138–139b BV regeln die eidgenössische Volksinitiative, während Artikel 141 BV das fakultative Referendum umschreibt. Auf Gesetzesstufe werden diese Bestimmungen durch das BPR und die dazugehörige VPR konkretisiert. Diese Rechtsgrundlagen definieren unter anderem die Voraussetzungen für das Zustandekommen einer Volksinitiative oder eines fakultativen

Referendums, die Anforderungen an Unterschriftenlisten, Fristen und Formvorschriften sowie Zuständigkeiten von Bund, Kantonen und Gemeinden (BPR, 1978; BV, 2000; VPR, 1978).

Unter dem Sammelbegriff «Volksbegehren» werden in dieser Arbeit sowohl Volksinitiativen als auch fakultative Referenden verstanden. Obligatorische Referenden werden nicht dazu gezählt, da für sie keine Unterschriften gesammelt werden. Damit ein Volksbegehren zustande kommt, müssen innerhalb einer festgelegten Frist eine bestimmte Anzahl gültiger, eigenhändig geleisteter Unterschriften stimmberechtigter Personen auf Unterschriftenlisten mit den gesetzlich verlangten Angaben gesammelt und von den Gemeinden bescheinigt werden. Die Integrität der Unterschriftensammlung ist damit eine zentrale Voraussetzung für die Legitimität der direktdemokratischen Entscheidprozesse. Entsprechend kommt der rechtssicheren Ausgestaltung und praxistauglichen Umsetzung der Sammel-, Prüf- und Bescheinigungsverfahren eine hohe Bedeutung zu (BPR, 1978; VPR, 1978; Bundeskanzlei, 2025b, 2025c).

2.2 Ablauf einer Volksinitiative und eines fakultativen Referendums

Obwohl Volksinitiativen und fakultative Referenden auf unterschiedlichen verfassungsrechtlichen Bestimmungen beruhen, ähneln sich die Abläufe der Unterschriftensammlung in wesentlichen Punkten. Aus Sicht der Integrität lassen sich sechs zentrale Prozessschritte unterscheiden, die auch in den von der BK veröffentlichten Unterlagen sowie in den offiziellen Leitfäden für Initiativen und Referenden abgebildet sind (BPR, 1978; BV, 2000; VPR, 1978; Bundeskanzlei, 2025b, 2025c).

1. **Lancierung und Vorbereitung des Volksbegehrens:** Bei einer Volksinitiative bildet sich ein Initiativkomitee, das den Initiativtext ausarbeitet, formell einreicht und damit die Prüfung durch die BK auslöst. Die BK prüft Titel und Wortlaut auf formale Korrektheit und publiziert den geprüften Text im Bundesblatt. Mit dieser Publikation beginnt die Sammelfrist (Vorprüfung und Publikation im Bundesblatt). Beim fakultativen Referendum entfällt dieser Schritt: Hier beginnt die Sammelfrist automatisch mit der amtlichen Veröffentlichung des fraglichen Erlasses im Bundesblatt (BPR, 1978; BV, 2000).
2. **Start der Sammelfrist:** Für Volksinitiativen beträgt die Sammelfrist 18 Monate, für fakultative Referenden 100 Tage. Innerhalb dieser Frist müssen die benötigten 100'000 (Initiative) beziehungsweise 50'000 (Referendum) gültigen Unterschriften gesammelt werden. Die amtliche Publikation im Bundesblatt markiert den Beginn dieser Fristen und schafft Transparenz für Öffentlichkeit und Behörden (BPR, 1978; BV, 2000).
3. **Unterschriftensammlung:** In der Sammelphase werden Unterschriften auf Unterschriftenlisten erfasst, die den rechtlichen Vorgaben und den Anforderungen der BK entsprechen. Sammelnde können ehrenamtlich oder gegen Entschädigung tätig sein. Sie sind dafür verantwortlich, dass die Unterschriftenlisten korrekt geführt werden, insbesondere hinsichtlich

eigenhändiger Unterschrift, Lesbarkeit und Vollständigkeit der Personendaten. In dieser Phase entstehen zahlreiche praktische Entscheidungssituationen – etwa im Umgang mit Zeitdruck, skeptischen Personen oder heiklen Sammelpraktiken –, in denen Integrität und Sensibilität gefordert sind (BPR, 1978; VPR, 1978; Bundeskanzlei, 2025b, 2025c).

4. **Stimmrechtsbescheinigung durch die Gemeinden:** Die ausgefüllten Unterschriftenbogen werden den zuständigen Gemeinden laufend zugestellt. Die Gemeinden prüfen, ob die unterzeichnenden Personen stimmberechtigt sind, und bescheinigen die Anzahl gültiger Unterschriften. Die Stimmrechtsbescheinigung bildet eine zentrale Kontrollinstanz im Verfahren: Sie verbindet die kommunale Ebene mit den direktdemokratischen Instrumenten auf Bundesebene und trägt wesentlich zur formellen Richtigkeit und Nachvollziehbarkeit der Unterschriftenlisten bei (BPR, 1978; Bundeskanzlei, 2025b, 2025c).
5. **Einreichung bei der BK:** Das Komitee reicht die bescheinigten Unterschriftenlisten innerhalb der Sammelfrist bei der BK ein. Die BK zählt die eingereichten Unterschriften, konsolidiert die von den Gemeinden bescheinigten Zahlen und stellt fest, ob die erforderliche Anzahl gültiger Unterschriften erreicht wurde. Eine Einreichung kann zu jedem Zeitpunkt der Sammelfrist erfolgen, findet in der Praxis jedoch häufig gegen deren Ende statt (BPR, 1978; Bundeskanzlei, 2025b, 2025c).
6. **Kontrollen, Publikation und Weiterleitung:** Nach Abschluss ihrer Kontrollen erstellt die BK den offiziellen Prüfbericht und veröffentlicht das Ergebnis im Bundesblatt. Bei zustande gekommenen Volksinitiativen wird der weitere politische Prozess eingeleitet (Botschaft des Bundesrates, parlamentarische Behandlung, Volksabstimmung). Beim fakultativen Referendum führt ein erfolgreiches Zustandekommen zu einer Volksabstimmung über den betreffenden Erlass. In beiden Fällen bilden Qualität und Integrität der vorangegangenen Unterschriftensammlung die Grundlage für die Legitimität des weiteren Verfahrens (BPR, 1978; BV, 2000; VPR, 1978).

Diese Prozesssicht verdeutlicht, dass Integrität nicht nur am Ende – bei der Kontrolle der Gesamtzahlen – relevant ist, sondern in jeder Etappe der Sammel-, Bescheinigungs- und Prüfprozesse (Bundeskanzlei, 2025b, 2025c).

2.3 Rollen und Verantwortlichkeiten

Die Integrität von Unterschriftensammlungen ist das Ergebnis eines Zusammenspiels verschiedener Beteiligter, die jeweils spezifische Rollen und Verantwortlichkeiten tragen (BPR, 1978; VPR, 1978; Bundeskanzlei, 2025b, 2025c).

- **Initiativ- und Referendumskomitees:** Bei Volksinitiativen bilden Komitees die formelle Trägerschaft des Volksbegehrens. Sie verantworten die Lancierung, die Ausarbeitung und

Einreichung des Initiativtexts sowie die Organisation der Unterschriftensammlung. Bei fakultativen Referenden übernehmen Komitees in der Praxis vor allem eine koordinierende Rolle: Sie entscheiden über die Ergreifung des Referendums und organisieren die Unterschriftensammlung, ohne den Inhalt des zur Abstimmung stehenden Erlasses zu verändern. In beiden Fällen gehört dazu insbesondere die sorgfältige Auswahl und Instruktion von Partnerorganisationen oder Sammelnden, die Festlegung interner Regeln zum Umgang mit Unterschriftenlisten und Personendaten sowie die Sicherstellung, dass die gesetzlichen Vorgaben eingehalten werden. Komitees sind damit zentrale Verantwortungsträger für Integrität im Sammelprozess (BPR, 1978; VPR, 1978; Bundeskanzlei, 2025b, 2025c).

- **Sammelnde (ehrenamtlich oder gegen Entschädigung):** Sammelnde stehen im direkten Kontakt mit der Bevölkerung und sind für die korrekte Erfassung der Unterschriften verantwortlich. Sie entscheiden in konkreten Situationen, wie sie auf Druck, Ablehnung oder Unklarheiten reagieren. Gerade bei entgeltlichen Sammelorganisationen können zusätzliche Anreize auftreten, etwa leistungsabhängige Entlohnung, die das Risiko unlauterer Praktiken erhöhen. Die BK betont in ihren Materialien zur Unterschriftensammlung, dass verantwortliche Stellen Unterschriftensammlungen sorgfältig organisieren, Sammelnde instruieren und Vorkehrungen zur Verhinderung von Missbräuchen treffen sollen – ein Kontext, in dem gezielte Awareness-Massnahmen besonders wichtig sein können (Bundeskanzlei, 2025b, 2025c).
- **Gemeinden:** Die Gemeinden prüfen die Stimmberechtigung der unterzeichnenden Personen und bescheinigen die Anzahl gültiger Unterschriften. Sie bilden damit eine institutionalisierte Kontrollinstanz zwischen Sammelnden und Bundesebene. Ihre Arbeit stützt sich auf klare rechtliche Vorgaben, muss aber auch im Alltag effizient und nachvollziehbar umgesetzt werden, um sowohl Rechtssicherheit als auch Praktikabilität zu gewährleisten (BPR, 1978; Bundeskanzlei, 2025b, 2025c).
- **Bundeskanzlei:** Die BK nimmt im Prozess eine doppelte Rolle ein. Einerseits agiert sie als verfahrensleitende Behörde auf Bundesebene: Sie prüft bei Volksinitiativen unter anderem Initiativtext, Titel und Form, kontrolliert bei Volksinitiativen und fakultativen Referenden die von den Gemeinden bescheinigten Unterschriftenlisten, stellt das Zustandekommen von Volksbegehren fest und publiziert die Ergebnisse. Andererseits versteht sie sich zunehmend als Gestalterin von Rahmenbedingungen zur Stärkung der Integrität, etwa durch Informationsangebote, Leitfäden und konzeptionelle Arbeiten zur Sensibilisierung von Komitees und Sammelnden (Bundeskanzlei, 2025b, 2025c). Die vorliegende Arbeit ist Teil dieser Massnahmen.

Das Zusammenspiel dieser Beteiligten zeigt, dass Integrität nicht allein durch gesetzliche Vorgaben garantiert werden kann. Entscheidend ist, wie Rollen, Verantwortlichkeiten und Informationsflüsse im Alltag gelebt – und inwiefern Komitees und Sammelnde in ihrer Verantwortung unterstützt und sensibilisiert werden (BPR, 1978; VPR, 1978; Bundeskanzlei, 2025b, 2025c).

2.4 Integritätsrisiken

In den vergangenen Jahren wurden vereinzelt Unregelmässigkeiten bei Unterschriftensammlungen bekannt, insbesondere im Zusammenhang mit Organisationen, die gegen Bezahlung Unterschriften sammeln. In einigen Fällen besteht der Verdacht, dass Unterschriften ohne Wissen der betroffenen Personen oder ohne eigenhändige Leistung erfasst wurden. Solche Vorkommnisse gefährden nicht nur die formale Gültigkeit einzelner Unterschriften, sondern untergraben auch das Vertrauen in die direkte Demokratie (Bundeskanzlei, 2025b, 2025c).

Aus Sicht der Integrität lassen sich mehrere Risikofelder unterscheiden:

- **Fälschung oder unzulässige Erfassung von Unterschriften:** Dazu gehören Konstellationen, in denen Unterschriften bewusst manipuliert oder Unterschriftenlisten entgegen den gesetzlichen Vorgaben ausgefüllt werden. Beispiele sind das Nachzeichnen oder Nachahmen von Unterschriften sowie das Eintragen von Personendaten und Unterschriften für andere Personen, ohne dass diese selbst unterschreiben. Auf den Unterschriftenlisten wird auf die Strafbarkeit unrichtiger Angaben hingewiesen (BPR, 1978; Bundeskanzlei, 2025b, 2025c).
- **Fragwürdige Sammelpraktiken und Drucksituationen:** Sammelnde können in Versuchung geraten, Personen zu bedrängen, unvollständig zu informieren oder unklare Aussagen zu machen, wenn sie beispielsweise unter starkem Zeit- oder Leistungsdruck stehen. Problematisch sind insbesondere Anreizmodelle, bei denen die Entschädigung von der Anzahl gesammelter Unterschriften abhängt (Bundeskanzlei, 2025b, 2025c).
- **Unsorgfältiger Umgang mit Personendaten und Unterlagen:** Unterschriftenlisten enthalten schützenswerte Personendaten. Risikoquellen sind etwa der unkontrollierte Transport, die Aufbewahrung in unsicheren Umgebungen oder das unbefugte Kopieren und Weiterverwenden der Listen. Solche Praktiken können datenschutzrechtliche Vorgaben verletzen, insbesondere die Grundsätze von Zweckbindung und Datensicherheit gemäss Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), und das Vertrauen der Bevölkerung schwächen (DSG, 2023; Bundeskanzlei, 2025b, 2025c).
- **Unklare Verantwortlichkeiten beim Einsatz externer Organisationen:** Wenn Komitees Sammelorganisationen beauftragen, besteht die Gefahr, dass Verantwortung faktisch ausgelagert wird. Ohne klare Vereinbarungen zu Integritätsanforderungen, Kontrollen und

Meldewegen können Lücken in der Steuerung von Risiken entstehen (BPR, 1978; Bundeskanzlei, 2025b, 2025c).

Die BK hat auf diese Risiken mit einer Kombination aus formellen Kontrollen sowie informatorischen und dialogorientierten Massnahmen reagiert. Auf der einen Seite stehen die gesetzlich verankerten Prüf- und Kontrollmechanismen – insbesondere die Stimmrechtsbescheinigung durch die Gemeinden und die abschliessende Kontrolle der eingereichten Unterschriften durch die BK. Diese Instrumente zielen primär darauf ab, die formale Gültigkeit der Unterschriften sicherzustellen und leisten einen Beitrag dazu, Unregelmässigkeiten, mögliche Fälschungen sowie unlautere Geschäftspraktiken zu erkennen (BPR, 1978; VPR, 1978; Bundeskanzlei, 2025b, 2025c). Ergänzend dazu hat die BK ein Monitoring-System (systematische Erfassung und Auswertung von Hinweisen auf Unregelmässigkeiten), einen Runden Tisch mit Vertretungen aus der politischen Praxis sowie Formate für den Austausch mit der Wissenschaft aufgebaut. Diese Massnahmen dienen dazu, Integritätsrisiken frühzeitig zu erkennen, Erfahrungen zu bündeln und Ansätze zur weiteren Stärkung der Unterschriftensammlung zu entwickeln (Bundeskanzlei, 2025a).

Auf der anderen Seite stellt die BK Informations- und Orientierungshilfen bereit, etwa in Form von Leitfäden für Initiativkomitees und Referendumsführende, Musterformularen und Hinweisen auf ihrer Website. Diese Materialien erläutern die Abläufe, die rechtlichen Anforderungen und die zentralen Verhaltensregeln in verständlicher Form und tragen dazu bei, Fehlverhalten vorzubeugen (Bundeskanzlei, 2025b, 2025c). Die Materialien richten sich primär an Komitees, unterstützen jedoch indirekt auch Sammelnde als operative Zielgruppe.

Innerhalb der BK wurden zudem erste Überlegungen dazu angestellt, wie Komitees und Sammelnde mit einfachen, praxisnahen Mitteln bei der Wahrnehmung ihrer Integritätsverantwortung unterstützt und Integritätsrisiken frühzeitig erkannt werden können. Die vorliegende Arbeit knüpft an diese Überlegungen an, entwickelt einen theoretischen Bezugsrahmen zu Integrität, Governance, Informationssicherheit, Awareness-Programmen und Human Factor und leitet daraus auf Basis empirischer Evidenz und des bestehenden Prozesswissens der BK ein evidenzbasiertes, praxisnahes Sensibilisierungskonzept für Komitees und Sammelnde ab.

Im Projektverlauf wurden diese Integritätsanforderungen entlang der drei Integritätshebel: «Situationen, Strukturen, Signale» strukturiert, auf die in den folgenden Kapiteln wiederholt Bezug genommen wird.

2.5 Zwischenfazit

Das Kontextkapitel 2 zeigte, dass die Integrität von Unterschriftensammlungen das Ergebnis eines Zusammenspiels von Rechtsgrundlagen, Prozessen und Beteiligten ist (BPR, 1978; BV, 2000; VPR,

1978; Bundeskanzlei, 2025b, 2025c). Die politischen Rechte auf Bundesebene sind rechtlich klar geregelt, und der Ablauf von Volksinitiativen und fakultativen Referenden folgt etablierten Verfahren. Gleichzeitig ist der Sammelprozess stark dezentral organisiert und in hohem Masse von der Praxis der Komitees und Sammelnden geprägt (Bundeskanzlei, 2025b, 2025c).

Für die vorliegende Arbeit lassen sich daraus drei zentrale Beobachtungen ableiten. Erstens ist die Unterschriftensammlung eine kritische Phase der direkten Demokratie, in der Integritätsverletzungen unmittelbare Auswirkungen auf die Legitimität eines Volksbegehrens haben können (BPR, 1978; BV, 2000). Zweitens nehmen Komitees eine Scharnierfunktion zwischen rechtlichen Vorgaben, externen Sammelorganisationen, ehrenamtlich oder gegen Entschädigung tätige Sammelnde und Gemeinden ein. Ihre Entscheidungen – etwa bei der Auswahl von Partnerorganisationen oder der Gestaltung interner Regeln – prägen die Qualität des Sammelprozesses wesentlich (Bundeskanzlei, 2025b, 2025c). Drittens verfügt die BK zwar über klar definierte Prüf- und Kontrollaufgaben, hat aber zugleich einen Gestaltungsspielraum bei der Sensibilisierung und Unterstützung von Komitees und Sammelnden zur Wahrung der Integrität der Unterschriftensammlungen (Bundeskanzlei, 2025b, 2025c).

Damit rücken neben den gesetzlichen Vorgaben insbesondere ein gemeinsames Rollenverständnis, alltagsnahe Verhaltensregeln und nachvollziehbare, dokumentierte Kontrollen in den Fokus (DSG, 2023; BPR, 1978; VPR, 1978).

Diese Konstellation verdeutlicht, dass Integrität im Sammelprozess nicht allein durch rechtliche Vorgaben und formale Kontrollen gewährleistet werden kann. Sie hängt auch wesentlich davon ab, wie Komitees und Sammelnde ihre Verantwortung verstehen und in konkreten Situationen handeln. Damit bildet der beschriebene Kontext die Grundlage für den in Kapitel 3 entwickelten theoretischen Bezugsrahmen, der die Themenfelder Integrität, Governance, Informationssicherheit, Awareness-Programme und Human Factor im Sammelprozess zusammenführt. Auf dieser Basis wird in Kapitel 7 ein Sensibilisierungskonzept für Komitees und Sammelnde ausgearbeitet, das darauf abzielt, Integritätsrisiken in der Unterschriftensammlung gezielt zu reduzieren.

3 Theoretischer Bezugsrahmen: Integrität, Governance, Informationssicherheit, Awareness-Programme und Human Factor

Kapitel 2 hat den rechtlichen und organisatorischen Kontext der Unterschriftensammlung in der eidgenössischen direkten Demokratie skizziert und gezeigt, in welchen Prozessphasen Integritätsrisiken entstehen können. Dieses Kapitel ordnet Integrität im Sammelprozess analytisch, verknüpft Sensibilisierung und entwickelt darauf aufbauend einen theoretischen Bezugsrahmen. Begriffe und Prozessbezüge richten sich nach dem Glossar und den Leitfäden der BK. Gesetzliche Normen werden benannt, ohne sie im Detail auszulegen (Bundeskanzlei, 2025b, 2025c).

Im Zentrum stehen drei Perspektiven: Erstens der Zusammenhang von Integrität, Legitimität und Governance in der direkten Demokratie (vgl. Abschnitt 3.1). Zweitens Konzepte der Informationssicherheit, insbesondere der Integrität von Informationen und Prozessen sowie der Ansatz «Integrity by Design» in der Gestaltung von Abläufen und Kontrollen (vgl. Abschnitt 3.2). Drittens Erkenntnisse zu Awareness-Programmen und zum Human Factor, die erklären, wie Verhalten unter Zeitdruck, bei Unsicherheit und in Anreizkonstellationen beeinflusst wird (vgl. Abschnitte 3.3 und 3.4).

Auf dieser Grundlage wird in Abschnitt 3.5 ein theoretischer Bezugsrahmen entwickelt, der zentrale Integritätsrisiken, Einflussfaktoren und Sensibilisierungsansatzpunkte für Komitees und Sammelnde systematisch ordnet. Dieser Bezugsrahmen bildet die Grundlage für die strukturierte Auswertung der Literatur, der BK-Dokumente und der vorliegenden Rückmeldungen aus der Praxis (vgl. Kapitel 5 und 6) sowie für die Ausarbeitung eines Sensibilisierungskonzepts für Komitees und Sammelnde (vgl. Kapitel 7).

3.1 Governance und Rollenverständnis

Die Integrität der Unterschriftensammlung ist nicht nur eine juristische Anforderung, sondern eine Voraussetzung für die Legitimität direktdemokratischer Entscheidungen. Legitimität bezeichnet die Anerkennung politischer Entscheidungen als gerechtfertigt – weil sie auf rechtmässigen Verfahren beruhen und grundlegende demokratische Prinzipien, wie politische Gleichheit und faire Teilhabe, respektieren (Beetham, 1991, S. 16–19, 56–57; Bühlmann et al., 2011, S. 3–4). Für Volksinitiativen und fakultative Referenden heisst dies: Stimmberechtigte Personen müssen darauf vertrauen können, dass Volksbegehren korrekt zustande kommen und Unterschriften weder manipuliert noch unter problematischen Umständen erhoben werden.

In der Demokratietheorie wird häufig zwischen drei Formen von Legitimität unterschieden (Schmidt, 2013, S. 2–3 und 8):

- **Input-Legitimität:** Beteiligung und Repräsentation – wer kann mitreden und mitentscheiden?

- **Throughput-Legitimität:** Qualität der Verfahren – wie transparent, nachvollziehbar und fair sind die Prozesse?
- **Output-Legitimität:** Ergebnisse – lösen Entscheidungen Probleme wirksam und werden sie als gerecht empfunden?

Für die vorliegende Arbeit steht vor allem die Throughput-Legitimität im Vordergrund. Die Unterschriftensammlung ist ein intermediärer Prozess: Sie liegt zeitlich vor der eigentlichen Volksabstimmung, prägt aber entscheidend, ob ein Volksbegehren überhaupt auf die Traktandenliste gelangt. Integritätsverletzungen in dieser Phase – etwa gefälschte Unterschriften, Drucksituationen oder ein sorgloser Umgang mit Personendaten – können die Legitimität des gesamten Verfahrens beeinträchtigen, selbst wenn die spätere Abstimmung formal korrekt abläuft (Schmidt, 2013, S. 5 und 8).

Aus einer Governance-Perspektive lässt sich die Unterschriftensammlung als verteiltes Steuerungsarrangement verstehen, in dem staatliche und nichtstaatliche Stellen gemeinsam Verantwortung tragen (Benz, 2004; Kooiman, 2003). Formelle Regeln werden durch die BV, das BPR und die VPR gesetzt (BPR, 1978; BV, 2000; VPR, 1978) und in dieser Arbeit als rechtlicher Rahmen benannt, ohne sie vertieft juristisch auszulegen. Ihre Wirksamkeit hängt davon ab, wie sie von Komitees, Sammelnden, Gemeinden und der BK im Alltag interpretiert und umgesetzt werden (vgl. Kapitel 2). Governance umfasst dabei nicht nur verbindliche Normen, sondern auch informelle Praktiken, Leitlinien, Schulungen und Kontrollmechanismen.

Der Begriff Integrität wird in diesem Kontext als Bündel von Eigenschaften verstanden, die zusammen die Vertrauenswürdigkeit des Sammelprozesses bestimmen und sich an gängigen Integritäts- und Governance-Konzepten orientieren (OECD, 2017, S. 11–13). Im Rahmen dieser Arbeit wird Integrität wie folgt operationalisiert:

- **Rechtskonformität:** Einhaltung der gesetzlichen Vorgaben zu Stimmberechtigung, Unterschrift, Fristen und Personendaten (z. B. Art. 60 ff. BPR; Art. 141 BV – Nennung ohne Auslegung).
- **Verfahrensfairness:** Transparente, respektvolle und nicht irreführende Ansprache von Personen im Sammelprozess.
- **Unabhängigkeit von unzulässigen Einflüssen:** Vermeidung von Drucksituationen, Täuschung oder Anreizsystemen, die Fehlverhalten begünstigen.
- **Nachvollziehbarkeit und Rechenschaftspflicht:** Klare Zuständigkeiten, dokumentierte Abläufe und wirksame Kontrollen, damit Unregelmässigkeiten erkennbar und sanktionierbar sind.

Integrität unterscheidet sich damit von eng gefassten Korruptionsbegriffen, umfasst aber Schnittstellen zu Phänomenen, wie Fälschung, Missbrauch von Personendaten oder unlauterem Verhalten im

Umgang mit Stimmberechtigten. Für Komitees und Sammelnde bedeutet dies, dass sie nicht nur «kein Gesetz brechen» dürfen, sondern aktiv dafür sorgen sollen, dass der Sammelprozess fair, transparent und verantwortungsvoll gestaltet ist.

Für die weitere Analyse sind drei analytische Dimensionen von Integrität und Governance besonders relevant:

1. **Normative und prozedurale Sicherungen:** Welche rechtlichen und organisatorischen Regeln strukturieren die Unterschriftensammlung, und wie klar sind sie für Komitees und Sammelnde zugänglich?
2. **Rollen, Verantwortung und Rechenschaftspflichten:** Wie sind Zuständigkeiten zwischen Komitees, Sammelorganisationen, Sammelnden, Gemeinden und BK verteilt, und wie werden sie im Alltag wahrgenommen (vgl. Kapitel 2)?
3. **Transparenz, Kontrolle und Umgang mit Fehlverhalten:** Welche Informationsflüsse, Kontrollmechanismen und Meldewege bestehen, um Integritätsrisiken frühzeitig zu erkennen und auf Unregelmässigkeiten zu reagieren?

Diese drei Dimensionen bilden den Brückenpfeiler zwischen demokratietheoretischen Überlegungen und der späteren Ausgestaltung eines Sensibilisierungskonzepts. Sie werden in den Abschnitten 3.2–3.4 um Konzepte aus der Informationssicherheit, der Awareness-Forschung und der Human-Factor-Perspektive ergänzt und in Abschnitt 3.5 zu einem ersten Bezugsrahmen für Komitees und Sammelnde verdichtet.

3.2 Informationssicherheit

Informationssicherheit bildet einen technischen und organisatorischen Rahmen, in dem Integrität konkret geschützt werden kann. Klassisch wird Informationssicherheit über die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit definiert und – je nach Publikation – um Aspekte, wie Authentizität und Rechenschaftspflicht, ergänzt, die in internationalen Standards häufig unter dem Begriff «Accountability» zusammengefasst werden. Entsprechende Sicherheitsmassnahmen sollen sicherstellen, dass Informationen nur von berechtigten Personen gelesen, verändert oder genutzt werden, dass Systeme zuverlässig funktionieren und dass sicherheitsrelevante Ereignisse erkennbar und rekonstruierbar sind (ENISA, 2021, S. 8; ISO/IEC, 2022, S. 12, 16; NIST, 2018, S. 29, 40, 42).

Im Kontext der Informationssicherheit bedeutet Integrität, dass Daten korrekt, vollständig und unverändert sind, solange sie nicht bewusst und autorisiert angepasst werden. Ergänzend umfasst Integrität die Widerstandsfähigkeit von Prozessen gegen unbeabsichtigte Fehler und gezielte Manipulation – etwa durch Plausibilitätsprüfungen, Zugriffskontrollen und Protokollierung. Integrität ist damit

sowohl eine Eigenschaft von Informationen als auch von Abläufen (ENISA, 2021, S. 8; ISO/IEC, 2022, S. 5; NIST, 2018, S. 32).

Übertragen auf die Unterschriftensammlung lassen sich drei Formen der Integrität unterscheiden, die für diese Arbeit zentral sind:

- **Inhaltliche Integrität:** Einträge auf Unterschriftenlisten entsprechen den tatsächlichen Angaben der unterzeichnenden Personen. Unterschriften werden nicht erfunden, nachgezeichnet oder für andere Personen geleistet, und es werden keine zusätzlichen Namen eingetragen, die nicht auf einer eigenen Willensäusserung beruhen (BPR, 1978, S. 21–29; Bundeskanzlei, 2025b, 2025c).
- **Formale Integrität:** Unterschriftenlisten erfüllen die rechtlichen und formalen Anforderungen. Dazu gehören vollständige und lesbare Angaben, die Verwendung der korrekten Liste, die Einhaltung der Sammelfrist sowie die Unterschrift durch stimmberechtigte Personen. Formale Fehler, wie unklare Datumsangaben, fehlende Wohnorte oder veraltete Formulare, können dazu führen, dass Unterschriften nicht gezählt werden. Die formalen Anforderungen werden in den Leitfäden und Musterlisten der BK grafisch erläutert und bilden den Referenzrahmen, ohne dass sie im Rahmen dieser Arbeit juristisch ausgelegt werden (Bundeskanzlei, 2025b, 2025c).
- **Prozessintegrität:** Der Weg einer Unterschriftenliste – von der Ausgabe über die Sammlung und Zwischentransporte bis hin zur Prüfung in der Gemeinde und der BK – ist nachvollziehbar, kontrolliert und möglichst manipulationsresistent gestaltet. Kritische Übergabepunkte (z. B. zwischen Komitee und Sammelorganisation oder zwischen Sammelnden und Gemeinde) sind so organisiert, dass Fehlverhalten erschwert und korrektes Handeln erleichtert wird (vgl. Kapitel 2). Die in den Leitfäden der BK enthaltenen Prozessdarstellungen und Zeitachsen dienen als Orientierung für eine nachvollziehbare und kontrollierbare Sammelkette (Bundeskanzlei, 2025b, 2025c).

Damit wird deutlich, dass Integrität als Sicherheitsziel nicht nur eine technische, sondern eine soziotechnische Dimension hat. Sie ergibt sich aus dem Zusammenspiel von Regeln, Systemen, Rollen, Kontrollen und der konkreten Praxis von Menschen, die in diesen Prozessen handeln (ENISA, 2021, S. 6, 10, 13). Genau an diesem Punkt setzt der Gedanke einer Gestaltung nach dem «by Design»-Prinzip an.

Von «Security by Design» zu «Integrity by Design»

In der Informationssicherheit hat sich der Ansatz etabliert, Sicherheitsanforderungen nicht nachträglich «aufzupfropfen», sondern von Anfang an in die Konzeption von Systemen und Prozessen zu

integrieren («Security by Design»). Im Datenschutz wird in ähnlicher Weise gefordert, dass datenschutzfreundliche Voreinstellungen und Prinzipien bereits in der Gestaltung von Anwendungen berücksichtigt werden («Privacy by Design») (Cavoukian, 2011; EDÖB, 2022, S. 3).

Für den Kontext der Unterschriftensammlung lässt sich dieses Denken als «Integrity by Design» übertragen: Integritätsanforderungen werden nicht nur in Form von Verboten und Sanktionen formuliert, sondern in die Gestaltung von Abläufen, Rollen, Hilfsmitteln und Informationsangeboten systematisch eingebaut. Zentrale Elemente einer solchen «Integrity by Design» sind:

- **Klare Rollen und Verantwortlichkeiten:** Komitees, Sammelorganisationen, Sammelnde, Gemeinden und BK wissen, wofür sie zuständig sind und wer als Ansprechperson für jedwede Aufgabe und auch für Integritätsfragen fungiert (vgl. Kapitel 2). Unklarheiten darüber, «wer eigentlich verantwortlich ist», werden reduziert.
- **Integrierte Kontrollen:** Vier-Augen-Prinzipien, Plausibilitätschecks, klare Kriterien für die Übergabe und Rücknahme von Listen sowie standardisierte Formulare sind im Prozess verankert und nicht (nur) als nachgelagerte Prüfung vorgesehen. Dadurch sinkt die Wahrscheinlichkeit, dass Fälschungen oder formale Mängel unbemerkt bleiben und werden somit reduziert.
- **Transparente Informationsflüsse:** Vorgaben und Hilfsmittel stehen Komitees und Sammelnden rechtzeitig und in verständlicher Form zur Verfügung (z. B. Leitfäden, Merkblätter, Musterlisten, FAQ). Informationsdefizite, die zu Fehlverhalten oder Fehlern beitragen können, werden reduziert.
- **Nachvollziehbarkeit und Dokumentation:** Kritische Schritte – etwa der Einsatz externer Sammelorganisationen oder der Transport von Listen – werden vorab identifiziert und so dokumentiert, dass im Nachhinein nachvollzogen werden kann, was wann durch wen erfolgt ist, ohne den Prozess unnötig zu verkomplizieren. Damit werden Fehler (aus bekannten kritischen Prozessschritten) reduziert und können gegebenenfalls nachvollzogen werden.
- **Verhältnismässigkeit:** Massnahmen werden so ausgestaltet, dass sie die Ausübung der politischen Rechte unterstützen und nicht erschweren. Integritätsschutz soll einen fairen Rahmen für alle Komitees schaffen und die Sammel- und Beteiligungsfreiheit nicht unverhältnismässig einschränken.

Verknüpfung mit Governance und Sensibilisierung

Aus Governance-Perspektive ergänzt «Integrity by Design» die in Abschnitt 3.1 diskutierten Dimensionen von Integrität und Legitimität. Integritätsanforderungen werden nicht nur normativ definiert, sondern in konkrete Prozessschritte, Zuständigkeiten und Hilfsmittel übersetzt. Dies beeinflusst

erstens die Input-Legitimität, weil es bestimmt, wie zuverlässig der Wille der Bevölkerung in Form von Unterschriften abgebildet wird, zweitens die Throughput-Legitimität, weil transparente und faire Abläufe das Vertrauen in die Durchführung der Sammelphase stärken, und drittens die Output-Legitimität, weil Entscheide auf einer belastbaren Grundlage beruhen (Scharpf, 1999; Schmidt, 2013).

Gleichzeitig genügt ein designorientierter Ansatz allein nicht: Integritätsanforderungen müssen von den beteiligten Personen verstanden, akzeptiert und im Alltag umgesetzt werden. Hier setzt der zu entwickelnde Bezugsrahmen an: Abschnitt 3.3 fokussiert auf Awareness-Programme und die Bedingungen verhaltensnaher Wirkung. Abschnitt 3.4 beleuchtet den Human Factor und typische Fehlverhaltensmuster in Druck- und Entscheidungssituationen. Abschnitt 3.5 verdichtet diese Elemente zu einem theoretischen Bezugsrahmen für Komitees und Sammelnde. Auf diese Weise verknüpft «Integrity by Design» die in Abschnitt 3.2 beschriebenen technischen Aspekte der Informationssicherheit (z. B. System- und Datenintegrität, Kontrollen) mit den organisatorischen Sicherheitsüberlegungen zu Governance, Rollen und Prozessen (vgl. Kapitel 2 und Abschnitt 3.1) und eröffnet den Übergang zur verhaltensorientierten Sensibilisierung in den Abschnitten 3.3–3.5 – eine Verbindung, die für die vorliegende Arbeit zentral ist.

3.3 Awareness-Programme und verhaltensnahe Wirksamkeit

Awareness-Programme ergänzen rechtliche Vorgaben und organisatorische Regeln um eine verhaltensorientierte Perspektive. Ihr Ziel ist nicht nur, Wissen zu vermitteln, sondern Einstellungen und Verhalten in sicherheitsrelevanten Situationen zu beeinflussen. In der Informationssicherheit gelten sie als zentrales Instrument, um das Verhalten von Mitarbeitenden und anderen Beteiligten in Richtung sicherer Handlungsweisen zu lenken und riskante Handlungen zu verringern (ENISA, 2021, S. 8, 25–26, 44; Hu et al., 2022).

Für die Integrität von Unterschriftensammlungen ist entscheidend, dass Sensibilisierung nicht bei (abstrakten) Appellen stehenbleibt, sondern das konkrete Verhalten von Komitees und Sammelnden im Sammelalltag adressiert. Dieser Abschnitt klärt zunächst Begriff und Zielsetzung von Awareness-Programmen, fasst zentrale Erkenntnisse zur Wirksamkeit zusammen und leitet daraus Kriterien für verhaltensnahe Awareness ab. Anschliessend werden Implikationen für Komitees und Sammelnde skizziert.

Begriff und Zielsetzung von Awareness-Programmen

In der Fachliteratur wird häufig zwischen Security Education (Wissensaufbau), Security Training (Fertigkeitentraining) und Security Awareness (situative Sensibilisierung) unterschieden (ENISA, 2021, S. 6–8; Hu et al., 2022; NIST, 2003, S. 2–4):

- **Education** zielt auf ein breites, eher langfristiges Verständnis von Zusammenhängen ab (z. B. Grundlagen der Informationssicherheit, rechtliche Rahmenbedingungen).
- **Training** fokussiert auf das Einüben spezifischer Fertigkeiten (z. B. Erkennen von Phishing-Mails (betrügerische Täuschungs-E-Mails), korrektes Klassifizieren von Informationen).
- **Awareness** adressiert vor allem Aufmerksamkeit, Einstellungen und Handlungsbereitschaft in konkreten Situationen. Sie soll Personen dazu bringen, Risiken wahrzunehmen, Warnsignale («Red Flags») zu erkennen und in heiklen Momenten bewusst eine sichere Option zu wählen.

In der Praxis werden diese Elemente häufig in kombinierten Sensibilisierungs- und Trainingsprogrammen umgesetzt (Security Education, Training and Awareness, SETA-Programme). Typische Ziele solcher Programme sind, Wissen über Bedrohungen und Schutzmassnahmen zu erhöhen, Einstellungen zu Sicherheit und Rechtssicherheit (Compliance) positiv zu beeinflussen und konkrete Verhaltensweisen zu verändern – etwa einen sorgfältigeren Umgang mit Daten oder die Vermeidung riskanter Handlungen (Hu et al., 2022).

Für Komitees und Sammelnde bedeutet dies: Awareness-Massnahmen sollen nicht nur verdeutlichen, dass Integrität wichtig ist, sondern sie in Situationen unterstützen, in denen sie unter Zeitdruck, mit Skepsis, Ablehnung oder problematischen Anfragen konfrontiert sind – etwa bei Sammelaktionen in engen sozialen Beziehungen, bei unklarer Stimmberechtigung oder bei heiklen Sammelpraktiken (vgl. Kapitel 2).

Evidenz zur Wirksamkeit von Awareness-Programmen

Mehrere Übersichtsarbeiten zeigen, dass Security-Awareness-Programme grundsätzlich positive Effekte haben können: Sie erhöhen typischerweise das Sicherheitswissen und verbessern Einstellungen sowie Verhaltensabsichten. Wo Verhalten tatsächlich gemessen wird, zeigt sich häufig eine zumindest kurzfristige Reduktion riskanter Handlungen (z. B. weniger Klicks auf Phishing-Links, sorgfältigerer Umgang mit Passwörtern) (Hu et al., 2022). Gleichzeitig ist die Evidenzlage heterogen und methodisch begrenzt:

- Viele Studien erfassen primär Wissen oder Selbsteinschätzungen, weniger häufig objektive Verhaltensindikatoren.
- Follow-up-Zeiträume (Nachmesszeiträume) sind oft kurz, sodass Aussagen zur Stabilität von Verhaltensänderungen begrenzt sind.
- Stichproben sind teilweise klein oder stammen aus spezifischen Kontexten (einzelne Unternehmen, Hochschulen), was die Übertragbarkeit einschränkt (Hu et al., 2022).

Neuere systematische Übersichten, die explizit verhaltensnahe Indikatoren berücksichtigen, kommen zu einem differenzierten Bild: Programme mit gut gestalteten, auf Verhalten ausgerichteten Elementen zeigen tendenziell stärkere Effekte, während rein informationsorientierte Kampagnen (z. B. Plakate, einmalige Mailings) deutlich schwächer abschneiden (ENISA, 2021, S. 23, 43, 45; Hu et al., 2022). Die in dieser Arbeit erstellte Literaturübersicht (vgl. Kapitel 4) bestätigt dieses Bild: Nur ein Teil der untersuchten Studien weist robuste, verhaltensnahe Wirkungsnachweise auf. Viele Arbeiten bleiben auf der Ebene von Wissen, Einstellungen oder Absichten.

Leitfäden von Standardisierungs- und Fachstellen betonen ähnliche Punkte: Awareness sollte als längerfristige Massnahme verstanden werden, die mit konkreten Verhaltenszielen verknüpft ist, in bestehende Prozesse eingebettet wird und durch geeignete Kontroll- und Monitoring-Mechanismen flankiert wird (ENISA, 2021, S. 6–8; NIST, 2003, S. 37–38).

Kriterien für verhaltensnahe Wirksamkeit

Für die vorliegende Arbeit steht der verhaltensnahe Effekt von Awareness im Vordergrund. Aus der Forschung lassen sich mehrere Kriterien ableiten, die darauf hinweisen, dass Awareness-Massnahmen unter bestimmten Bedingungen Verhalten beeinflussen können (ENISA, 2021, S. 21–25; Hu et al., 2022, S. 758–760):

1. **Messung von Verhalten statt nur von Wissen oder Absichten**: Studien mit hoher Aussagekraft erfassen z. B. Klickraten bei Phishing-Simulationen, die Nutzung sicherer Kommunikationskanäle oder die Häufigkeit von Meldungen. Übertragen auf die Unterschriftensammlung wären dies etwa die Meldedisziplin bei beobachtetem Fehlverhalten, die Quote formaler Fehler («Formfehlerquote») oder die durchschnittliche Klärzeit zwischen Meldung und Entscheid (ENISA, 2021, S. 21–22; Hu et al., 2022, S. 758–759).
2. **Praxisnahe Szenarien und situative Einbettung**: Awareness-Massnahmen sind wirkungsvoller, wenn sie an konkrete Arbeits- oder Alltagssituationen anknüpfen – etwa realitätsnahe Fallbeispiele, Simulationen oder Hinweise, die unmittelbar vor oder während relevanter Tätigkeiten eingesetzt werden (ENISA, 2021, S. 22–23; Hu et al., 2022, S. 758–759; NIST, 2003, S. 37–38).
3. **Wiederholung und Verstärkung über die Zeit**: Einmalige Schulungen können kurzfristige Effekte erzielen, diese nehmen jedoch häufig wieder ab. Programme mit regelmässigen Wiederholungen (z. B. periodische Kampagnen, Erinnerungen (Reminder), kurze Lerneinheiten (Micro-Learnings) erreichen stabilere Verhaltensänderungen (ENISA, 2021, S. 23–24; Hu et al., 2022, S. 759; NIST, 2003, S. 37–38).
4. **Klarheit der Verhaltensanforderungen**: Botschaften wirken stärker, wenn die adressierten Personen genau wissen, was von ihnen erwartet wird (z. B. «Unterschriftenlisten nie

unbeaufsichtigt liegen lassen», «bei Unsicherheit Sammeln abbrechen und Rücksprache halten»). Allgemeine Appelle («Integrität ist wichtig») genügen nicht (ENISA, 2021, S. 24; Hu et al., 2022, S. 758–760).

5. **Unterstützendes Umfeld und Vorbildfunktion**: Awareness entfaltet sich besser, wenn Schlüsselpersonen das gewünschte Verhalten vorleben und organisatorische Rahmenbedingungen konsistent sind (realistische Zielvorgaben, faire Meldewege, keine einseitigen Fehlanreize). Awareness kann Integritätsprobleme in Strukturen und Anreizsystemen nicht kompensieren, sondern sie nur sichtbar machen und adressieren (ENISA, 2021, S. 24–25; OECD, 2017, S. 63–65).

Diese Kriterien bilden den Massstab für die Bewertung der Wirksamkeit von Sensibilisierungselementen in dieser Arbeit. Sie werden bei der Auswertung der Literatur (vgl. Kapitel 4) und bei der Gestaltung des Sensibilisierungskonzepts (vgl. Kapitel 7) genutzt, um Massnahmen möglichst verhaltensnah auszurichten.

Implikationen für Komitees und Sammelnde

Übertragen auf die Integrität von Unterschriftensammlungen bedeutet der skizzierte Forschungsstand:

- **Kurze, situationsnahe Hilfsmittel**: Für Komitees und Sammelnde sind kurze, konkrete und alltagsnahe Hilfsmittel besonders relevant – etwa kompakte Verhaltensregeln, Checklisten oder «Dos und Don'ts», die direkt im Sammelalltag eingesetzt werden können.
- **Klar formulierte Verhaltensregeln**: Verhaltensregeln sollten klar, positiv formuliert und mit Beispielen verknüpft sein, die typische heikle Situationen adressieren (z. B. Sammeln im privaten Umfeld, Umgang mit unsicheren Angaben, Transport und Aufbewahrung von Unterschriftenlisten; vgl. Kapitel 2).
- **Wiederholung und Auffrischung**: Die Wirksamkeit lässt sich erhöhen, wenn Sensibilisierung nicht nur am Anfang der Sammelphase stattfindet, sondern über die Zeit aufgefrischt wird – etwa durch kurze Erinnerungen an kritische Zeitpunkte (Start der Sammelfrist, intensive Sammelphasen, Einbindung externer Sammelorganisationen).
- **Verhaltensnahe Sensibilisierung durch die BK**: Für die BK eröffnet dies die Möglichkeit, Sensibilisierung so zu gestalten, dass sie verhaltensnah wirkt: durch zielgruppengerechte Materialien, klare Verhaltensbotschaften und Formate, die sich leicht in den Sammelalltag integrieren lassen. Dabei ist es wichtig, Terminologie und Rollenbezeichnungen konsistent mit dem Glossar und den Leitfäden der BK zu verwenden (Bundeskanzlei, 2025b, 2025c).

Damit bildet dieses Kapitel zu Awareness-Programmen die Brücke zwischen den in den Abschnitten 3.1 und 3.2 beschriebenen Überlegungen zu Integrität, Governance und Informationssicherheit sowie dem Human Factor. Abschnitt 3.4 knüpft daran an, indem er den Human Factor und typische Fehlverhaltensmuster in Druck- und Entscheidungssituationen näher beleuchtet.

3.4 Human Factor

In der vorliegenden Arbeit bezeichnet der Begriff «Drucksituationen» Situationen, in denen Sammelnde unter sozialem, zeitlichem oder leistungsbezogenem Druck stehen – einschliesslich besonders kritischer Druck- und Entscheidungssituationen im Kontext der Unterschriftensammlung.

Integritätsrisiken entstehen im Zusammenspiel von Regeln, Strukturen und menschlichem Verhalten. Der Human Factor bezeichnet die Gesamtheit der menschlichen Eigenschaften, die das Funktionieren von Prozessen positiv oder negativ beeinflussen können – von Aufmerksamkeit, Urteilsfähigkeit und Routine bis hin zu Emotionen, sozialen Dynamiken und Anreizstrukturen (Reason, 1990, 1997). Für die Unterschriftensammlung bedeutet dies: Selbst bei klaren gesetzlichen Vorgaben und formal korrekten Prozessen können Fehlverhalten und Integritätsverletzungen auftreten, wenn Personen unter Druck geraten, Situationen falsch einschätzen oder problematische Anreize bestehen.

Dieser Abschnitt skizziert zentrale Formen unbeabsichtigten und intendierten Fehlverhaltens, die Rolle von Druck- und Entscheidungssituationen sowie typische soziale Dynamiken im Sammelalltag. Darauf aufbauend werden Ansatzpunkte für Sensibilisierung aus einer Human-Factor-Perspektive abgeleitet.

Unbeabsichtigte Fehler und begrenzte Aufmerksamkeit

In der Sicherheits- und Human-Factor-Literatur wird zwischen unbeabsichtigten Fehlern (z. B. Versprechen, Versehen) und bewussten Regelverletzungen unterschieden (Reason, 1990). Unbeabsichtigte Fehler entstehen häufig, wenn Personen abgelenkt sind, mehrere Dinge gleichzeitig tun, müde sind oder Routinetätigkeiten unaufmerksam ausführen. Typische Muster sind:

- **Slips**: Die Absicht ist korrekt, die Ausführung misslingt (z. B. falsches Feld ausfüllen, Zahl vertauschen).
- **Lapses**: Relevante Informationen werden vergessen oder übersehen (z. B. Datum nicht eintragen, Wohnort nicht ergänzen).
- **Missverständnisse**: Vorgaben werden falsch interpretiert, weil sie unklar oder zu komplex formuliert sind.

Bei der Unterschriftensammlung können solche Fehler dazu führen, dass formale Anforderungen nicht erfüllt werden – etwa durch unvollständige oder unleserliche Angaben, die Verwendung

falscher Listen oder Fehleinschätzungen der Stimmberechtigung (z. B. Unterschriften von Personen, die auf Bundesebene nicht stimmberechtigt sind). Diese Fehler sind in der Regel nicht Ausdruck bewusster Manipulation, können aber die Integrität des Sammelprozesses beeinträchtigen, wenn sie systematisch auftreten oder bestimmte Gruppen überproportional betreffen.

Druck-, Anreiz- und Entscheidungssituationen

Neben unbeabsichtigten Fehlern spielt die Art und Weise eine Rolle, wie Personen in heiklen Situationen Entscheidungen treffen. Typische Druck- und Anreizsituationen im Sammelalltag sind:

- Zeitdruck, etwa kurz vor Ablauf der Sammelfrist oder bei ambitionierten Sammelzielen.
- Soziale Erwartungen, z. B. wenn die Sammelaktion stark emotional aufgeladen ist oder im engen Freundes- und Familienkreis stattfindet.
- Materielle oder symbolische Anreize, etwa Entschädigungen für Sammelnde, Wettbewerbscharakter zwischen Teams oder die Hoffnung auf Anerkennung und Erfolg bei knapper Unterschriftenlage.

In solchen Situationen steigt das Risiko, dass Personen Regeln situativ relativieren («dieses eine Mal», «es ist ja für eine gute Sache») oder problematische Praktiken tolerieren – etwa das Ausfüllen von Angaben für andere Personen, das Sammeln in Kontexten, in denen sich Menschen schwer frei äussern können, oder das bewusste Ausblenden von Zweifeln an der Stimmberechtigung. Auch das Unterlassen von Meldungen bei beobachtetem Fehlverhalten kann eine Folge von Drucksituationen sein, wenn Personen befürchten, als illoyal wahrgenommen zu werden oder Konflikte auszulösen.

Soziale Dynamiken im Sammelalltag

Der Human Factor umfasst neben individuellen Aspekten auch soziale Dynamiken. Wahrgenommenes «Normverhalten» im unmittelbaren Umfeld beeinflusst stark, was als akzeptabel gilt. Wenn in einem Sammelteam der Eindruck entsteht, dass «alle das so machen», sinkt die Hemmschwelle für grenzüberschreitende Praktiken. Umgekehrt können klare Vorbilder und eine Teamkultur, die Integrität betont, positiven Einfluss entfalten (Cialdini & Goldstein, 2004).

Relevante Dynamiken sind unter anderem:

- **Gruppendruck und Loyalität**: Sammelnde wollen das Komitee oder Team nicht enttäuschen und scheuen sich, auf Probleme hinzuweisen.
- **Informelle Regeln**: Neben offiziellen Vorgaben bilden sich unausgesprochene Praktiken heraus, die den Alltag prägen («so machen wir das hier»).
- **Rationalisierung**: Personen rechtfertigen problematisches Verhalten nachträglich vor sich selbst, etwa durch Verweis auf den politischen Zweck oder auf das Verhalten anderer.

Solche Dynamiken sind nicht spezifisch für die Unterschriftensammlung, gewinnen hier aber besondere Relevanz, weil der Prozess stark auf Vertrauen und Selbstorganisation beruht und die direkte staatliche Kontrolle in der Sammelphase begrenzt ist.

Ansatzpunkte für Sensibilisierung aus Human-Factor-Sicht

Eine humanfaktororientierte Sensibilisierung setzt dort an, wo Fehler und Fehlverhalten typischerweise entstehen: in konkreten Situationen unter konkreten Rahmenbedingungen (Reason, 1990, 1997). Daraus ergeben sich mehrere Ansatzpunkte für ein Sensibilisierungskonzept:

- **Typische Fehlersituationen sichtbar machen**: Komitees und Sammelnde sollten auf klassische «Fehlerfallen» aufmerksam gemacht werden – etwa häufige formale Fehler, stressbedingte Nachlässigkeiten oder Situationen, in denen Stimmberechtigung schwer zu beurteilen ist.
- **Drucksituationen antizipieren**: Sensibilisierung kann dazu beitragen, Druckmomente früh zu erkennen (z. B. Sammeln kurz vor Fristende) und Strategien zu entwickeln, um Integrität auch unter Zeitdruck zu wahren (z. B. Sammelziele realistisch planen, Qualität vor Quantität betonen).
- **Konkrete Entscheidungsregeln formulieren**: Klare Verhaltensregeln für heikle Situationen («Wenn …, dann …») reduzieren Interpretationsspielräume und geben Sammelnden Sicherheit, wie sie sich korrekt verhalten sollen – etwa beim Umgang mit unsicheren Angaben oder bei Sammelanfragen in abhängigen oder besonders verletzlichen Beziehungen.
- **Positive Vorbilder und Teamkultur stärken**: Komitees können eine Kultur fördern, in der das Ansprechen von Bedenken ausdrücklich erwünscht ist und als Beitrag zur Integrität verstanden wird. Das reduziert die Hemmschwelle, auf Probleme hinzuweisen, und stärkt die gemeinsame Verantwortung.
- **Niederschwellige Meldewege schaffen**: Wenn Sammelnde wissen, an wen sie sich bei Unsicherheiten oder Beobachtungen wenden können – und dass sie dabei unterstützt statt sanktioniert werden –, steigt die Wahrscheinlichkeit, dass Integritätsrisiken frühzeitig adressiert werden.

Für die BK bedeutet dies, dass Sensibilisierungsmassnahmen nicht nur Informationen zu rechtlichen Vorgaben vermitteln sollten, sondern Sammelnde in genau jenen Situationen unterstützen, in denen menschliche Faktoren Integrität gefährden können. Dies umfasst sowohl die Gestaltung der Materialien (z. B. adressatengerechte Sprache, Szenarien, Entscheidungsregeln) als auch die Art und Weise, wie Komitees als Multiplikatoren eingebunden werden.

Abschnitt 3.5 greift diese Überlegungen auf und fasst die in den Abschnitten 3.1 bis 3.4 entwickelten Elemente – Integrität und Governance, Informationssicherheit und «Integrity by Design», Awareness-Programme und Human Factor – zu einem theoretischen Bezugsrahmen zusammen, der als Arbeitsgrundlage für die empirische Analyse in Kapitel 4–6 und für das Sensibilisierungskonzept in Kapitel 7 dient.

3.5 Zusammenfassung

Die bisherigen Ausführungen zu Integrität, Governance, Informationssicherheit, Awareness-Programmen und Human Factor (vgl. Kapitel 2 sowie Abschnitte 3.1–3.4) bleiben zunächst auf einer allgemeinen und theoretischen Ebene. Damit sie für die konkrete Fragestellung dieser Arbeit nutzbar werden, braucht es einen klar strukturierten Bezugsrahmen, der die theoretischen Bausteine auf die Situation von Komitees und Sammelnden in der Unterschriftensammlung überträgt. Dieses Kapitel fasst die zentralen Dimensionen zusammen und definiert, wie sie weiterverwendet werden.

Ziel und Funktion des Bezugsrahmens

Der theoretische Bezugsrahmen erfüllt drei Funktionen:

1. **Strukturierung der empirischen Erhebung:** Er leitet ab, welche Themen in schriftlichen Kurzinterviews (per E-Mail) und Dokumentenanalysen gezielt angesprochen werden (z. B. Rollenverständnis, Umgang mit Drucksituationen, interne Regeln und Schulungen), damit sowohl formelle Vorgaben als auch gelebte Praxis und situative Herausforderungen sichtbar werden.
2. **Orientierung bei der Auswertung:** Er bietet Kategorien, entlang derer beobachtete Praktiken und Aussagen systematisch eingeordnet werden können (z. B. Governance, Prozesse, Verhalten, Unterstützungsinstrumente), um Muster, Lücken und Spannungsfelder zu identifizieren.
3. **Brücke zum Sensibilisierungskonzept:** Er sorgt dafür, dass das in Kapitel 7 zu entwickelnde Sensibilisierungskonzept direkt an identifizierten Einflussfaktoren und Situationen ansetzt – etwa bei unklaren Rollen, wiederkehrenden Drucksituationen oder fehlenden Unterstützungsinstrumenten – und nicht «neben» der empirischen Evidenz steht.

Der theoretische Bezugsrahmen ist somit kein zusätzliches Theoriegebäude, sondern eine Verdichtung der in den Kapiteln 2 und 3 beschriebenen Elemente auf jene Aspekte, die für Komitees und Sammelnde in der Praxis von Relevanz sind.

Zentrale Dimensionen: Governance, Prozesse, Verhalten, Unterstützung

Auf Basis der vorangegangenen Kapitel lassen sich vier zentrale Dimensionen unterscheiden, die für die Integrität der Unterschriftensammlung besonders relevant sind.

1. **Governance und Rollenverständnis (vgl. Abschnitt 3.1):** Diese Dimension umfasst die formellen und informellen Regeln, Verantwortlichkeiten und Wertvorstellungen innerhalb von Komitees sowie in Organisationen, die Sammelnde einsetzen (z. B. externe Sammelorganisationen). Relevant sind insbesondere: Klarheit der Zuständigkeiten (z. B. wer ist für Integritätsfragen zuständig?), interne Vorgaben zum Umgang mit Unterschriftenlisten und Personendaten sowie der «Tone from the Top» in Bezug auf Integrität und Transparenz. Hier fliessen die Überlegungen zu Integrität, Legitimität und Governance aus Abschnitt 3.1 ein.
2. **Informationssicherheit (vgl. Abschnitt 3.2):** Diese Dimension knüpft direkt an den Kontext der Unterschriftensammlung an (vgl. Kapitel 2). Im Fokus stehen kritische Prozessschritte (z. B. Sammlung, Transport, Stimmrechtsbescheinigung), typische Risikofelder (z. B. Fälschungen, Drucksituationen, Umgang mit Personendaten) und vorhandene oder fehlende Kontrollmechanismen. Zentral ist die Frage, an welchen Stellen im Prozess aus Sicht der Praxis besonders heikle Situationen entstehen und wie sie aktuell adressiert werden. Hier schliesst die Perspektive von Informationssicherheit und «Integrity by Design» an (vgl. Abschnitt 3.2).
3. **Awareness-Programme und verhaltensnahe Wirksamkeit (vgl. Abschnitt 3.3):** Diese Dimension verbindet die Erkenntnisse zu Awareness-Programmen mit den spezifischen Bedürfnissen von Komitees und Sammelnden. Betrachtet werden insbesondere vorhandene Informations- und Schulungsangebote (z. B. Leitfäden, Merkblätter, Briefings), deren Reichweite, Verständlichkeit und Praxisnähe sowie Potenziale für zusätzliche, leicht umsetzbare Instrumente (z. B. Kurzchecklisten, standardisierte Briefings, Hinweise auf Unterschriftenlisten). Beispiele sind klar strukturierte Unterschriftenlisten mit gut sichtbaren Kurzhinweisen, wie «nur eigenhändige Unterschrift» oder «kein Eintrag ohne Zustimmung», kurze Briefings für Sammelnde oder niedrigschwellige Meldewege, damit bei Unklarheiten Unterstützung gesucht werden kann, statt «im Zweifel selbst zu entscheiden». Diese Dimension bildet die direkte Grundlage für die spätere Ausgestaltung des Sensibilisierungskonzepts (vgl. Kapitel 7).
4. **Human Factor (vgl. Abschnitt 3.4):** Diese Dimension macht die in Abschnitt 3.3 und 3.4 diskutierten verhaltensbezogenen Aspekte greifbar. Sie fokussiert auf typische Druck- und Entscheidungssituationen (z. B. Fristende, Zielvorgaben, leistungsabhängige Entschädigungen), unbeabsichtigte Fehler und begrenzte Aufmerksamkeit sowie soziale Normen und Gruppendynamiken bei Komitees sowie unter Sammelnden (einschliesslich Teams externer Sammelorganisationen). Ziel ist es, jene «Mikro-Situationen» zu identifizieren, in denen

Integritätsverletzungen besonders wahrscheinlich sind – und damit Ansatzpunkte für gezielte Sensibilisierung zu schaffen.

Anwendung des theoretischen Bezugsrahmens

Für die spätere Bewertung von Sensibilisierungsmassnahmen (vgl. Kapitel 7) sind insbesondere verhaltensnahe Indikatoren relevant. Geeignete Grössen sind zum Beispiel die Formfehlerquote, der Anteil ungültiger Unterstützungsbekundungen gemäss Stimmrechtsbescheinigung, die Meldedisziplin (Anzahl Meldungen pro Anzahl Unterschriften) oder die durchschnittliche Klärzeit zwischen Meldung und Entscheid. Sie ermöglichen es, Entwicklungen im Zeitverlauf oder Unterschiede zwischen verschiedenen Vorgehensweisen zu beobachten, ohne bereits eine konkrete Evaluationsstudie vorwegzunehmen.

In der weiteren Arbeit dient der theoretische Bezugsrahmen als «Brille», durch die empirischen Befunde betrachtet und interpretiert werden:

- Bei der Planung der empirischen Erhebung werden Interviewfragen und Auswertungsraster so gestaltet, dass sie die vier Dimensionen gezielt abdecken.
- In der Analyse der Ergebnisse werden Beobachtungen und Aussagen den Dimensionen zugeordnet, um systematisch Lücken, Spannungsfelder und gute Praktiken zu identifizieren, die für die Sensibilisierung relevant sind.
- Bei der Entwicklung des Sensibilisierungskonzepts in Kapitel 7 werden Massnahmen dort angesetzt, wo der Bezugsrahmen Schwachstellen oder Hebelpunkte aufzeigt – etwa bei unklaren Rollen, wiederkehrenden Drucksituationen oder fehlenden Unterstützungsinstrumenten.

Der theoretische Bezugsrahmen aus Kapitel 3 bildet damit die Grundlage für einen strukturierten, praxisnahen Analyse- und Gestaltungsprozess. Der hier definierte Bezugsrahmen macht diesen Zusammenhang explizit und sorgt dafür, dass die späteren Empfehlungen für die BK sowie für Komitees und Sammelnde nachvollziehbar aus den vorangegangenen Überlegungen abgeleitet werden können. Das folgende Kapitel 4 beschreibt das methodische Vorgehen, mit dem dieser Bezugsrahmen in der Literaturrecherche, der Dokumenten- und Prozessanalyse sowie in den schriftlichen Rückmeldungen aus der Praxis angewendet wird und die theoretischen Dimensionen für die empirische Analyse operationalisiert.

Zusammengefasst verbindet der theoretische Bezugsrahmen vier Perspektiven: Governance (Rollen und Zuständigkeiten), Prozesse (Abläufe und Kontrollen), Human Factor (kritische Situationen und soziale Dynamiken) sowie Awareness- und Unterstützungsinstrumente (Materialien, Briefings, Checklisten; vgl. Abbildung 1). In der empirischen Analyse (vgl. Kapitel 5 und 6) dienen diese

Dimensionen als «Brille», durch die Befunde geordnet werden. In Kapitel 7 werden darauf aufbauend Sensibilisierungselemente entwickelt, die an klar identifizierten Hebelpunkten ansetzen.

Abbildung 1: Theoretischer Bezugsrahmen zur Integrität in der Unterschriftensammlung (eigene Darstellung).

4 Methodik und Forschungsdesign

Dieses Kapitel konkretisiert auf Basis des in Kapitel 3 entwickelten Bezugsrahmens das methodische Vorgehen der Arbeit. Es beschreibt den Forschungsansatz, die systematische Literaturrecherche, die Dokumenten- und Prozessanalyse sowie die Befragung von Fachpersonen und legt das Auswertungsverfahren fest.

4.1 Forschungsansatz

Diese Arbeit ist als qualitativ ausgerichtete explorative Fallstudie mit Fokus auf die BK und den Prozess der Unterschriftensammlung auf Bundesebene konzipiert (Creswell & Plano Clark, 2018, S. 2–3; Yin, 2018, S. 38–39, 45–46). In einem erweiterten Verständnis von Mixed Methods kombiniert das Forschungsdesign unterschiedliche Datenquellen und methodische Zugänge: eine systematische Literaturrecherche, eine Dokumenten- und Prozessanalyse der BK-Unterlagen sowie schriftliche Rückmeldungen von Fachpersonen. Ausgangspunkt bilden das in Abschnitt 1.3 beschriebene Ziel, die BK, Initiativ- und Referendumskomitees sowie Sammelnde wirksamer für Integritätsrisiken zu sensibilisieren (Bundeskanzlei, 2025b, 2025c), der in Kapitel 2 dargestellte Kontext sowie der in Kapitel 3 entwickelte theoretische Bezugsrahmen zu Integrität, Governance, Informationssicherheit, Awareness-Programmen und Human Factor (DSG, 2023; BPR, 1978; BV, 2000; VPR, 1978). Die Methodik ist darauf ausgerichtet, diese konzeptionellen Überlegungen mit empirischen Beobachtungen aus Praxis und Forschung zu verbinden und daraus ein praxistaugliches Sensibilisierungskonzept abzuleiten.

Die Unterschriftensammlung wird als konkreter Anwendungsfall betrachtet, in dem Governance-Strukturen, operative Prozesse, menschliches Verhalten und Awareness-Massnahmen zusammenwirken (vgl. Abschnitt 3.5). Der Forschungsansatz zielt darauf ab, diese Zusammenhänge systematisch entlang dieser vier Dimensionen zu erfassen: Wo entstehen Integritätsrisiken, wie sind sie im bestehenden Regelwerk abgebildet, wie erleben die am Sammelprozess Beteiligten kritische Situationen, und welche Unterstützung erhalten sie heute?

Vor diesem Hintergrund strukturieren die in Abschnitt 1.3 formulierten Forschungsfragen (F1–F3) den weiteren Aufbau der Arbeit und das methodische Vorgehen in Kapitel 4.

Zur Beantwortung dieser Forschungsfragen werden mehrere komplementäre Datenquellen kombiniert. Erstens wird eine systematische Literaturrecherche zu Awareness-Programmen und Human-Factor-Massnahmen im Bereich Informationssicherheit und verwandten Feldern durchgeführt, mit Fokus auf verhaltensnahe Wirksamkeit und Übertragbarkeit (vgl. Abschnitt 4.2) (ENISA, 2021, S. 6–8, 23; Hu et al., 2022). Zweitens werden zentrale Dokumente und Prozessbeschreibungen der BK zur Unterschriftensammlung entlang des in Kapitel 3 entwickelten Bezugsrahmens analysiert, um

Integritätsanforderungen, bestehende Massnahmen und mögliche Lücken zu identifizieren (vgl. Abschnitt 4.3) (Bundeskanzlei, 2025b, 2025c). Drittens werden ausgewählte Fachpersonen per E-Mail zu einer schriftlichen, leitfadengestützten Kurzbefragung eingeladen, um praxisnahe Sichtweisen, Erfahrungen und Grenzen der Umsetzung zu erfassen (vgl. Abschnitt 4.4) (Yin, 2018, S. 161–164).

Die Auswertung folgt einem integrierenden Vorgehen (vgl. Abschnitt 4.5): Die Befunde aus Literatur, Dokumenten und Interviews werden jeweils entlang der Dimensionen: Governance, Prozesse, Human Factor sowie Awareness und Unterstützung strukturiert und anschliessend zusammengeführt (Kuckartz, 2018, S. 97–115). Dadurch entsteht ein konsistentes Bild darüber, wo im Sammelprozess besonders sensible Situationen auftreten, welche Governance-, Prozess- und Human-Factor-Aspekte dabei eine Rolle spielen und mit welchen Sensibilisierungsmassnahmen diese Hebelpunkte adressiert werden können.

Der Mixed-Methods-Ansatz ist damit nicht Selbstzweck, sondern dient der Triangulation von Perspektiven und der konzeptionell-gestaltenden Zielsetzung der Arbeit (Flick, 2014, S. 182–186). Normative und rechtliche Anforderungen in Kapitel 2 werden mit wissenschaftlicher Evidenz in Kapitel 3 und 5 sowie praktischen Erfahrungen aus der BK und dem Umfeld der Unterschriftensammlung verknüpft (DSG, 2023; BPR, 1978; BV, 2000; VPR, 1978; Bundeskanzlei, 2025b, 2025c). So soll sichergestellt werden, dass das in Kapitel 7 entwickelte Sensibilisierungskonzept für Komitees und Sammelnde sowohl wissenschaftlich fundiert als auch im behördlichen Alltag der BK anschlussfähig und umsetzbar ist.

In dieser Arbeit werden Rechtsgrundlagen benannt, nicht ausgelegt. Für den Kontext der Unterschriftensammlung sind insbesondere die Bestimmungen zu Volksbegehren in der Bundesverfassung, im BPR und in der VPR sowie die allgemeinen Datenschutzgrundsätze des DSG relevant (z. B. DSG Art. 5 f.; BPR Art. 58–75; BV Art. 138–141; VPR Art. 23). Die empirische Analyse konzentriert sich darauf, wie diese Rahmenbedingungen in Prozessen, Rollen und Sensibilisierungsmassnahmen der BK sichtbar werden.

4.2 Literaturrecherche

Die Literaturrecherche bildet die empirische Grundlage für den theoretischen Bezugsrahmen in Kapitel 3 und die späteren Gestaltungsempfehlungen in Kapitel 7. Ziel ist es, systematisch zu erfassen, welche Arten von Awareness- und Human-Factor-Massnahmen in der aktuellen Forschung beschrieben werden und welche Evidenz zur verhaltensnahen Wirksamkeit vorliegt (ENISA, 2021, S. 6–8, 21; Hu et al., 2022, S. 752–753). Im Vordergrund stehen Ansätze, die sich auf sicherheitsrelevantes Verhalten beziehen und sich grundsätzlich auf den Kontext von Komitees und Sammelnden bei eidgenössischen Volksbegehren übertragen lassen.

4.2.1 Geltungsbereich

Die Literaturrecherche umfasst den Zeitraum 2020–2025 und berücksichtigt deutsch- und englischsprachige Quellen. Für den evidenzbasierten Teil der Awareness- und Human-Factor-Literatur (insbesondere in den Abschnitten 3.3, 3.4 und 5) wird dieser Zeitraum systematisch abgedeckt. Ergänzend werden ausgewählte, etablierte Grundlagenwerke ausserhalb dieses Zeitfensters einbezogen, etwa die klassischen Beiträge von Reason (1990, 1997) und Beetham (1991), soweit sie für die theoretische Fundierung zentral sind. Im Vordergrund stehen Studien und Berichte mit Bezug zur Schweiz, zur Europäischen Union sowie international relevante Arbeiten, sofern sie methodisch und kontextuell übertragbar sind. Dazu zählen insbesondere der Bericht der European Union Agency for Cybersecurity (ENISA) aus dem Jahr 2021 zu Cybersecurity-Awareness, die Empfehlung der Organisation for Economic Co-operation and Development (OECD) aus dem Jahr 2017 zur Public Integrity (öffentliche Integrität) sowie das Cybersecurity Framework (Rahmenwerk zur Cybersicherheit) des National Institute of Standards and Technology (NIST) aus dem Jahr 2018. Im Zentrum stehen Zielgruppen, wie Mitarbeitende in Organisationen, Verwaltungspersonal, Lernende sowie die breite Öffentlichkeit. Ergänzend fliessen Arbeiten ein, die explizit politische Partizipation oder demokratische Prozesse adressieren.

4.2.2 Datenbasis und Suchstrategie

Die Datengrundlage bilden peer-reviewte Fachartikel, Konferenzbeiträge, Berichte von Behörden und Fachorganisationen, wie ENISA, NIST und OECD, sowie ausgewählte Abschlussarbeiten, sofern sie eine transparente Methodik aufweisen. Die Quellen wurden über fachliche Literaturdatenbanken, Suchmaschinen und Referenzketten (Schneeballverfahren) identifiziert. Die Suchbegriffe kombinierten Schlagworte aus den Bereichen Informationssicherheit, Cybersecurity, Awareness, Training, Verhalten, Compliance und Kampagnen (z. B. security awareness, phishing training, security behavior, compliance), orientiert an etablierten Vorgehensweisen für systematische Literaturrecherchen (vom Brocke et al., 2009; Webster & Watson, 2002). Eingeschlossen wurden Beiträge, die konkrete Awareness- oder Trainingsmassnahmen beschreiben oder die Gestaltung, Messung bzw. Rahmenbedingungen solcher Massnahmen systematisch analysieren.

4.2.3 Kategorien

Zur Strukturierung der Literatur wurde ein Kategorienschema mit vier Hauptkategorien verwendet, das an bestehende Übersichten und Rahmenwerke angelehnt und für den Kontext dieser Arbeit präzisiert wurde (ENISA, 2021, S. 25–26, 37–38, 43, 47; Hu et al., 2022, S. 753–755):

- **Trainings (E-Learning / Workshops):** Kursmodule, Micro-Learnings, Gamification-Ansätze (spielerische Elemente), Präsenztrainings und regelmässige Auffrischungen (Refreshers).
- **Simulationen:** Eingebettete Simulationen, insbesondere Phishing-Simulationen mit Feedback-Loops (Rückmeldeschleifen) und Auswertung über Verhaltenskennzahlen.
- **Kampagnen / Initiativen:** Breiten-Sensibilisierung (z. B. nationale Kampagnen, Programme für Schulen oder Verwaltungen, Online-Portale).
- **Messmodelle, Rahmenwerke und Reviews:** Systematische Übersichten, Rahmenwerke und Sets von Key Performance Indicators (KPI) zur Planung, Messung und Bewertung von Awareness- und Trainingsprogrammen.

Jede identifizierte Quelle wurde einer oder mehreren dieser Kategorien zugeordnet, um Interventionstyp, Kontext und Zielgrössen vergleichbar zu machen. Die Zuordnung ermöglicht es, die in Kapitel 3 eingeführten Dimensionen: Governance, Prozesse, Human Factor und Awareness/Unterstützung mit konkreten Interventionsformen zu verknüpfen.

4.2.4 Einschluss- und Ausschlusskriterien

Eingeschlossen wurden Beiträge mit nachvollziehbarer empirischer oder konzeptioneller Basis, insbesondere: peer-reviewte Studien, Feld- oder Vorher-Nachher-Untersuchungen, Evaluationsberichte von Behörden sowie systematische Reviews und Rahmenwerke (ENISA, 2021, S. 6–8; Hu et al., 2022, S. 753). Ausgeschlossen wurden dagegen rein marketingorientierte Inhalte (z. B. Produktbroschüren, Blogbeiträge ohne Methodik), Public-Relations-Texte ohne transparente Datenbasis sowie Arbeiten, deren Kontext sich nicht sinnvoll auf die Schweizer Verwaltung oder vergleichbare Organisationen übertragen lässt.

4.2.5 Evidenzlogik

Um die Aussagekraft der gefundenen Studien hinsichtlich verhaltensnaher Wirksamkeit einzuordnen, wurde ein dreistufiges, für diese Arbeit entwickeltes Bewertungsraster verwendet. Jede Quelle wurde danach beurteilt, ob und wie sie die Wirkung von Awareness-Massnahmen beschreibt, in Anlehnung an evidenzbasierte Klassifikationen in bestehenden Reviews (ENISA, 2021, S. 23, 30; Hu et al., 2022):

- **«super ja» (hohe Evidenz):** robuste Studien mit klar nachgewiesener Verhaltenswirkung (z. B. signifikante Reduktion von Klick- oder Fehlerraten, Zunahme von Meldungen), häufig mit Vorher-Nachher-Designs oder kontrollierten Vergleichen.
- **«ja» (mittlere Evidenz):** Studien, die Wirkung auf Verhalten, Verhaltensabsichten, Wissen oder Einstellungen empirisch untersuchen, deren Design oder Messgrössen jedoch

Einschränkungen aufweisen (z. B. kurze Follow-up-Zeiträume, kleine Stichproben, selbstberichtete Daten).

- **«nein» (keine direkte Evidenz):** konzeptionelle Beiträge, Rahmenwerke oder Erfahrungsberichte ohne belastbare Outcome-Daten (messbare Wirkungs- oder Verhaltensdaten) oder mit lediglich allgemeinen Aussagen zur Wirkung.

Insgesamt wurden 128 Quellen in einer Evidenztabelle erfasst, davon 69 Beiträge mit verhaltensnaher Evidenz (15 mit hoher, 54 mit mittlerer Evidenz) und 59 ohne direkte Wirkungsmessung. Die vollständige Übersicht mit Kontext, Interventionstyp, Messgrössen und Zuordnung zur Evidenzkategorie ist in der Evidenztabelle in Anhang A dokumentiert.

4.2.6 Analyseschritte und Verknüpfung mit dem theoretischen Bezugsrahmen

Die Ergebnisse der Literaturrecherche fliessen in zweifacher Hinsicht in die weitere Arbeit ein. Erstens bilden sie die Grundlage für die in Kapitel 3 dargestellten theoretischen Überlegungen zu Awareness-Programmen, verhaltensnaher Wirksamkeit und Human Factor. Zweitens dienen sie in Kapitel 5 als Ausgangspunkt, um zentrale Wirkungshebel (z. B. Wiederholung, soziale Einbettung, radikale Einfachheit) systematisch zu beschreiben und mit den Integritätsanforderungen der BK zu verknüpfen (ENISA, 2021, S. 6–7; NIST, 2003, S. 35, 45, 2018, S. 38; OECD, 2017, S. 3, 7–8). Damit stellt die Literaturrecherche sicher, dass das in dieser Arbeit entwickelte Sensibilisierungskonzept für Komitees und Sammelnde nicht auf Einzelmeinungen oder Einzelfällen beruht, sondern auf einer breiten und kritisch bewerteten Evidenzbasis zur Gestaltung und Wirksamkeit von Awareness-Massnahmen in sicherheitsrelevanten Kontexten.

4.3 Dokumenten- und Prozessanalyse

Die Dokumenten- und Prozessanalyse verknüpft den in Kapitel 2 beschriebenen Kontext der politischen Rechte mit dem theoretischen Bezugsrahmen aus Kapitel 3 und den spezifischen Fragestellungen dieser Arbeit. Sie dient dazu, die bestehenden Regelungen, Leitfäden und Abläufe der BK systematisch daraufhin zu untersuchen, an welchen Stellen Integritätsrisiken sichtbar werden und wo sich realistische Ansatzpunkte für Sensibilisierungsmassnahmen ergeben (BPR, 1978; BV, 2000; VPR, 1978; Bundeskanzlei, 2025b, 2025c).

4.3.1 Ziel und Funktion der Analyse

Ziel der Dokumenten- und Prozessanalyse ist es, die BK-spezifische Ausgangslage entlang der vier Dimensionen des Bezugsrahmens – Governance, Prozesse, Human Factor sowie Awareness- und

Unterstützungsinstrumente – zu strukturieren (vgl. Abschnitt 3.5). Konkret erfüllt die Analyse drei Funktionen:

1. **Abbildung des normativen und prozessualen Rahmens** der Unterschriftensammlung aus Sicht der BK, basierend auf den einschlägigen Rechtsgrundlagen und den von der BK bereitgestellten Prozessdarstellungen (DSG, 2023; BPR, 1978; BV, 2000; VPR, 1978; Bundeskanzlei, 2025b, 2025c).
2. **Identifikation von Integritätsrisiken und kritischen Situationen** im bestehenden Prozess – insbesondere in den Phasen Vorbereitung, Sammlung, Stimmrechtsbescheinigung und Einreichung, wie sie bereits im Zwischenbericht skizziert wurden.
3. **Ableitung von Hebelpunkten für Sensibilisierung**, an denen Awareness-Massnahmen der BK mit vertretbarem Aufwand ansetzen können (z. B. Gestaltung von Leitfäden, Unterschriftenbogen, standardisierten Schreiben).

Damit bildet die Dokumenten- und Prozessanalyse eine Brücke zwischen den allgemeinen Mustern der Awareness-Literatur (vgl. Abschnitt 3.3) und der konkreten Prozessrealität von Komitees und Sammelnden im Umfeld der BK (ENISA, 2021, S. 6–7, 29–30; Hu et al., 2022, S. 752–754, 756–757).

4.3.2 Datenbasis: Leitfäden, Prozessbeschreibungen und Konzeptentwürfe der BK

Die Analyse stützt sich auf drei Gruppen von Dokumenten, die in Abstimmung mit der BK ausgewählt wurden:

1. **Öffentlich zugängliche Leitfäden und Informationsangebote der BK:** Dazu gehören insbesondere die von der BK veröffentlichten Informationen und Leitfäden zu Volksinitiativen und fakultativen Referenden, inklusive Musterformularen und Layoutvorgaben für Unterschriftenbogen (Bundeskanzlei, 2025b, 2025c). Diese Materialien fassen die rechtlichen Anforderungen und Prozessschritte in verständlicher Form zusammen und sind zentrale Orientierungspunkte für Komitees und Sammelnde.
2. **Prozessbeschreibungen und Ablaufschemata:** Wo verfügbar – werden Prozessdarstellungen zur Stimmrechtsbescheinigung in den Gemeinden sowie zur nachgelagerten Prüfung der Unterschriften durch die BK einbezogen. Diese Dokumente konkretisieren, wie die im BPR und in der VPR festgelegten Aufgaben praktisch umgesetzt werden (BPR, 1978; VPR, 1978).
3. Interne Konzeptentwürfe zu künftigen Sensibilisierungsmassnahmen (Entwurfsstand): Ergänzend werden von der BK zur Verfügung gestellte Entwürfe in abstrahierter Form berücksichtigt, in denen erste Ideen für Sensibilisierung von Komitees und Sammelnden skizziert

sind. Diese Unterlagen werden nicht wörtlich zitiert und nicht im Literaturverzeichnis aufgeführt. In der Arbeit werden nur verallgemeinerte Inhalte dargestellt.

Die Auswahl folgt einem gezielten Sampling: Berücksichtigt werden nur Unterlagen, die den Sammelprozess und die Rolle der BK unmittelbar regeln oder die ausdrücklich darauf ausgerichtet sind, Komitees und Sammelnde zu informieren und zu unterstützen. Damit ist sichergestellt, dass die Analyse jene Stellen abdeckt, an denen Sensibilisierung realistisch ansetzen kann – etwa im Kontakt zwischen BK und Komitees oder in der Kommunikation mit Gemeinden.

4.3.3 Analyseschritte und Verknüpfung mit dem theoretischen Bezugsrahmen

Die Auswertung der Dokumente erfolgt als strukturierende qualitative Inhaltsanalyse: Relevante Textpassagen werden entlang eines deduktiv entwickelten Kategorienschemas codiert, das direkt aus dem Bezugsrahmen abgeleitet ist (Governance, Prozesse, Human Factor, Awareness/Unterstützung; vgl. Abschnitt 3.5). Das Vorgehen orientiert sich an etablierten Verfahren der qualitativen Inhaltsanalyse (Kuckartz, 2018, S. 97–105; Mayring, 2015, S. 67–90):

- **Governance:** Aussagen zu Rollen, Verantwortlichkeiten, Aufsicht und Rechenschaftspflichten (z. B. Aufgaben von Komitees, Sammelnden, Gemeinden und Bundeskanzlei).
- **Prozesse:** Beschreibungen von Abläufen, Kontrollen und Schnittstellen – insbesondere zu den Phasen Vorbereitung, Sammlung, Stimmrechtsbescheinigung und Einreichung.
- **Human Factor:** Hinweise auf typische Drucksituationen, Fehlanreize, Graubereiche oder interpretierbare Regelungen, die das Verhalten von Komitees und Sammelnden beeinflussen können.
- **Awareness- und Unterstützungsinstrumente:** Konkrete Materialien, Hinweise, Beispiele oder Checklisten, mit denen die BK korrektes Verhalten fördern will (z. B. Formulierungen in Leitfäden, Erklärkästen auf Unterschriftenbogen, FAQ).

Die detaillierte Beschreibung der Auswertungsschritte und der Verknüpfung mit den übrigen Datenquellen (Literatur und Interviews) erfolgt in Abschnitt 4.5.

4.3.4 Prozessorientierte Verdichtung: Situationen, Strukturen, Signale

Auf Basis der codierten Dokumente wird in einem zweiten Schritt eine prozessorientierte Verdichtung vorgenommen. Für jede zentrale Prozessphase im Sammelprozess werden drei Elemente herausgearbeitet:

- **Situationen:** typische Entscheidungsmomente und Konstellationen, in denen Integrität gefährdet sein kann (z. B. der Einsatz externer Sammelorganisationen, Sammeln kurz vor Fristende, Umgang mit unklarer Stimmberechtigung).

- **Strukturen:** bestehende Regeln, Kontrollen und Meldewege, die diese Situationen absichern sollen (z. B. Vorgaben zu Unterschriftenlisten, Stimmrechtsbescheinigung, interne Kontrollmechanismen).
- **Signale:** explizite und implizite Botschaften der BK, die faires Sammeln als Norm sichtbar machen (z. B. Formulierungen in Leitfäden, Hinweise auf korrekte Sammelpraktiken, Ansprechstellen bei Fragen).

Diese Verdichtung knüpft an die im Projektverlauf entwickelte Integritätslogik der drei Integritätshebel: «Situationen, Strukturen, Signale» an (vgl. Abschnitt 2.4). Sie macht sichtbar, an welchen Punkten bereits starke Signale bestehen und wo Lücken oder Unschärfen auftreten, ohne an dieser Stelle bereits Ergebnisse im Detail vorwegzunehmen.

4.3.5 Beitrag zur Beantwortung der Forschungsfragen

Die Ergebnisse der Dokumenten- und Prozessanalyse fliessen auf zwei Ebenen in die weitere Arbeit ein und leisten einen direkten Beitrag zur Beantwortung der Forschungsfragen (vgl. Abschnitt 1.3):

- **Beitrag zu F1 (Integritätsrisiken und kritische Situationen):** Die Analyse zeigt, welche Integritätsanforderungen im bestehenden Regelwerk verankert sind, an welchen Stellen der Prozess besonders anfällig für Fehlverhalten oder Missverständnisse ist und wo aus Sicht der BK bereits Vorkehrungen getroffen wurden. Sie liefert damit eine systematische Grundlage, um typische Integritätsrisiken und kritische Situationen im Sammelprozess zu beschreiben.
- **Beitrag zu F3 (Sensibilisierungskonzept für die BK sowie für Komitees und Sammelnde):** Gleichzeitig markiert die prozessorientierte Verdichtung jene Punkte, an denen Sensibilisierungsmassnahmen der BK mit vertretbarem Aufwand ansetzen können – etwa bei der Ausgestaltung von Leitfäden, Unterschriftenbogen oder Unterstützungsangeboten für Komitees und Sammelnde. Diese Einsichten bilden die prozessuale Landkarte, auf der das in Kapitel 7 entwickelte Sensibilisierungskonzept verortet wird.

In Kombination mit der Literaturrecherche (vgl. Abschnitt 4.2) und den Interviews mit Fachpersonen (vgl. Abschnitt 4.4) trägt die Dokumenten- und Prozessanalyse damit dazu bei, die Forschungsfragen dieser Arbeit nicht abstrakt, sondern konkret entlang der realen BK-Prozesse zu beantworten und die später vorgeschlagenen Massnahmen nachvollziehbar im bestehenden System zu verankern.

4.4 Interviews mit Fachpersonen

Die in den Abschnitten 4.2 und 4.3 beschriebenen Auswertungsschritte stützen sich primär auf wissenschaftliche Literatur sowie auf gesetzliche Grundlagen, Leitfäden und Prozessdokumente der BK. Um diese eher normativen und dokumentenbasierten Perspektiven zu ergänzen, wurde im Rahmen der vorliegenden Arbeit zusätzlich eine schriftliche, leitfadengestützte Kurzbefragung per E-Mail mit Fachpersonen durchgeführt. Dadurch fliessen Erfahrungen aus Politik, Verwaltung, IT-Sicherheit und digitaler Demokratie in die Analyse ein und der in Kapitel 3 entwickelte Bezugsrahmen kann mit konkreten Einschätzungen aus der Praxis gespiegelt werden.

4.4.1 Zielsetzung und Einbettung

Ergänzend zur Literaturrecherche sowie zur Dokumenten- und Prozessanalyse wurden gezielt Einschätzungen von Fachpersonen eingeholt. Ziel dieser Kurzbefragungen ist es, den in Kapitel 3 entwickelten Bezugsrahmen zur Integrität der Unterschriftensammlung mit praktischen Erfahrungen aus Politik, Verwaltung und IT-Sicherheit zu spiegeln und blinde Flecken zu identifizieren (vgl. Abschnitt 3.5).

Im Vordergrund stehen drei Fragen:

1. In welchen Situationen rund um Unterschriftensammlungen und politische Kampagnen werden Integritätsrisiken konkret sichtbar?
2. Wo verläuft aus Sicht erfahrener Fachpersonen aus der Praxis die Grenze zwischen «hart, aber noch legitim» und klar problematischen Sammelpraktiken?
3. Welche realistischen Handlungshebel sieht die Praxis für Sensibilisierungsmassnahmen der BK, ohne die politische Neutralität zu gefährden und ohne die Eigenverantwortung der Komitees zu verletzen – und wie lassen sich Sammelnde dabei wirksam unterstützen?

Die Einschätzungen der Fachpersonen dienen damit als qualitative Ergänzung zur Evidenz aus der Awareness-Literatur und zur Analyse der BK-Leitfäden. Sie helfen, die im Bezugsrahmen beschriebenen Dimensionen: Governance, Prozesse, Human Factor sowie Awareness- und Unterstützungsinstrumente mit konkreten Beispielen und Einschätzungen aus der Praxis zu unterlegen (vgl. Abschnitt 3.5).

4.4.2 Auswahl der Fachpersonen

Die Auswahl der angefragten Personen erfolgte gezielt (purposive sampling) entlang der Fragestellung und der vier Dimensionen des Bezugsrahmens. Angestrebt wurde eine Mischung aus politischen, behördlichen und sicherheitsbezogenen Perspektiven mit direktem Praxisbezug. Interviews

mit Fachpersonen eignen sich insbesondere, wenn spezifisches Kontext- und Erfahrungswissen zu komplexen Prozessen rekonstruiert werden soll (Gläser & Laudel, 2009, S. 11–13).

Konkret wurden folgende Profile angefragt:

- eine Gemeinderätin einer aargauischen Gemeinde mit Ressortverantwortung, u. a. für Finanzen, Sicherheit und Umwelt sowie Einsitz in Feuerwehr- und Bevölkerungsschutzgremien
- zwei Kommunalpolitiker einer mittelgrossen aargauischen Stadt, davon einer mit langjähriger Erfahrung als Chef einer kantonalen Kriminalpolizei
- ein Absolvent einer Schweizer Hochschule, der in einer Abschlussarbeit Fragen der digitalen Demokratie und der digitalen Unterschriftensammlung (E-Collecting) untersucht hat und heute unternehmerisch in diesem Feld tätig ist
- ein Unternehmer im Bereich Software- und IT-Sicherheit, der u. a. für Lernplattformen und sicherheitsrelevante IT-Infrastrukturen Verantwortung trägt
- ein Politikberater und Lehrbeauftragter an einer Schweizer Universität mit Erfahrung in staatspolitischen und sicherheitspolitischen Fragestellungen

Die Personen werden in der Arbeit in der Regel über ihre Funktion beschrieben (z. B. «Gemeinderätin Sicherheit/Finanzen», «Politikberater») und nicht mit vollem Namen, um den Fokus auf die inhaltlichen Beiträge zu legen.

Die Auswahl folgt damit dem Charakter von Interviews mit Fachpersonen, bei denen nicht Repräsentativität im statistischen Sinn angestrebt wird, sondern die Tiefe und Relevanz der fachlichen Perspektive (Gläser & Laudel, 2009, S. 96–98). Je nach Rücklauf der Anfragen werden in Kapitel 6 jene Interviews ausgewertet, zu denen substanzielle inhaltliche Rückmeldungen eingegangen sind. Die Zahl der eingegangenen Rückmeldungen und Absagen wird in Kapitel 6 transparent ausgewiesen.

Im Rahmen der empirischen Erhebung konnten insgesamt vier substanzielle schriftliche Rückmeldungen gewonnen werden. Zwei Rückmeldungen stammen von Kommunalpolitikern einer mittelgrossen aargauischen Stadt, davon eine von einem ehemaligen Chef einer kantonalen Kriminalpolizei. Eine Rückmeldung stammt von einem Unternehmer im Bereich Software- und IT-Sicherheit, der u. a. für Lernplattformen und sicherheitsrelevante IT-Infrastrukturen Verantwortung trägt. Eine weitere Rückmeldung stammt von einem Absolventen einer Schweizer Hochschule, der sich in einer Abschlussarbeit mit Fragen der digitalen Demokratie und des E-Collecting befasst hat und heute unternehmerisch in diesem Feld tätig ist. Von insgesamt sechs angefragten Fachpersonen gingen damit vier Rückmeldungen ein. Zwei Fachpersonen lehnten die Teilnahme ab, darunter eine aus Zeitgründen (vgl. Kapitel 6 und Anhang B3).

4.4.3 Erhebungsdesign und Durchführung

Aufgrund des vorgegebenen zeitlichen Rahmens und der starken inhaltlichen Fokussierung wurde ein schriftliches Kurzinterview-Design gewählt. Die angefragten Fachpersonen erhielten per E-Mail einen kurzen Kontext zur Arbeit (Thema, Auftraggeberin BK, Forschungsziel) sowie drei offene Leitfragen.

Die Fragen sind so gestaltet, dass sie an konkrete Situationen und Erfahrungen der Befragten anknüpfen (etwa Integritätsrisiken, Drucksituationen oder den Umgang mit vulnerablen Gruppen), gleichzeitig die persönliche Einschätzung zur Grenze zwischen legitimen und problematischen Praktiken abfragen und Einschätzungen zu realistischen Handlungsmöglichkeiten der BK und deren Grenzen ermöglichen.

Die Interviews sind damit als leitfadengestützte, teilstandardisierte Befragungen von Fachpersonen konzipiert: Bei allen Befragten orientieren sich die Fragen an denselben drei inhaltlichen Kernbereichen, die konkrete Formulierung wurde je nach Funktion leicht angepasst (z. B. Bezug auf Gemeindeexekutive, Stadtpolitik oder Politikberatung). Dieses Vorgehen erlaubt einen Vergleich der Einschätzungen entlang der Forschungsfragen und des Bezugsrahmens, ohne die Offenheit für unerwartete Hinweise zu verlieren (Gläser & Laudel, 2009, S. 39–42).

Die Antworten werden von den Befragten schriftlich per E-Mail übermittelt. Die Einleitung zur Befragung informiert darüber, dass eine Beantwortung in Stichworten oder kurzen Sätzen genügt und dass die Aussagen in der Arbeit ausschliesslich in funktionsbezogener Form ausgewertet werden (z. B. «Gemeinderätin Sicherheit/Finanzen», «Politikberater»). Personendaten, wie Namen, Kontaktdaten oder Parteizugehörigkeiten, werden in der Arbeit nicht dokumentiert. Es gelten Datensparsamkeit und Zweckbindung.

Für die weitere Auswertung in Abschnitt 4.5 werden die Texte in ein einheitliches Format überführt und entlang der Dimensionen des Bezugsrahmens (Governance, Prozesse, Human Factor, Awareness- und Unterstützungsinstrumente) kategorisiert. Grundlage bildet eine inhaltlich strukturierende qualitative Inhaltsanalyse, wie sie in der Methodenliteratur für die systematische Auswertung von Interview- und Dokumententexten beschrieben wird (Kuckartz, 2018, S. 97–105; Mayring, 2015, S. 67–90). Die Interviews bilden damit – im Zusammenspiel mit Literatur- und Dokumentenanalyse – eine zusätzliche Grundlage für die Ableitung der Sensibilisierungselemente in Kapitel 7.

4.4.4 Datenschutz und Vertraulichkeit

Die Interviews mit Fachpersonen werden ausschliesslich zum in dieser Arbeit beschriebenen Forschungszweck verwendet. Die Antworten werden anonymisiert in funktionsbezogener Form dargestellt. Rohdaten (E-Mails) bleiben im Projektkontext und werden nicht an Dritte weitergegeben.

4.5 Auswertungsverfahren

Die Auswertung der erhobenen Daten folgt einer inhaltlich strukturierenden qualitativen Inhaltsanalyse mit Triangulation. Literatur, Dokumente der BK und Interviews mit Fachpersonen werden entlang des in Abschnitt 3.5 entwickelten Bezugsrahmens (Governance, Prozesse, Human Factor sowie Awareness- und Unterstützungsinstrumente) analysiert und zu Integritätshebeln verdichtet. Die Auswertung erfolgt in drei Schritten: Zunächst werden die Literatur- und Dokumentenbasis entlang des Kategorienschemas codiert und verdichtet. Anschliessend werden die Interviews mit Fachpersonen im gleichen Kategoriensystem ausgewertet. Im dritten Schritt werden die Ergebnisse aus Literatur-, Dokumenten- und Interviewanalyse trianguliert, indem sie den Integritätshebeln «Situationen», «Strukturen» und «Signale» zugeordnet und auf Konsistenzen und Spannungsfelder geprüft werden (Kuckartz, 2018, S. 97–105; Mayring, 2015, S. 67–90).

4.5.1 Auswertungslogik und analytischer Bezugsrahmen

Als übergreifender analytischer Bezugsrahmen dient der theoretische Bezugsrahmen aus Abschnitt 3.5. Die vier Dimensionen: Governance, Prozesse, Human Factor sowie Awareness- und Unterstützungsinstrumente bilden die Hauptkategorien, entlang derer alle Datenquellen ausgewertet werden. Ergänzend werden die Integritätshebel «Situationen», «Strukturen» und «Signale» verwendet, um verhaltensnahe Ansatzpunkte für Sensibilisierung zu identifizieren.

Die Auswertungslogik folgt einer inhaltlich strukturierenden qualitativen Inhaltsanalyse. Zunächst werden deduktiv Kategorien aus dem Bezugsrahmen und den Forschungsfragen (vgl. Abschnitte 1.3 und 3.5) abgeleitet, zum Beispiel «Rollen- und Verantwortlichkeitsklarheit», «Kontrollen im Sammelprozess», «Drucksituationen und Fehlanreize» oder «Awareness-Materialien und Unterstützungsinstrumente». Diese Kategorien werden im Zuge der Codierung induktiv um Unterkategorien ergänzt, wenn die Daten wiederkehrende Themen sichtbar machen, die im Bezugsrahmen noch nicht abgebildet sind (z. B. spezifische Drucksituationen bei bezahlten Sammelorganisationen oder typische Formfehler bei Unterschriftenlisten). Ein solches kombiniertes deduktiv-induktives Vorgehen entspricht der in der Methodenliteratur beschriebenen inhaltlich strukturierenden qualitativen Inhaltsanalyse (Kuckartz, 2018, S. 97–105; Mayring, 2015, S. 67–90).

Die codierten Textstellen werden in einer Auswertungstabelle entlang dieser Kategorien erfasst. Dadurch entsteht eine Matrix, in der sich für jede Datenquelle (Awareness-Literatur, BK-Leitfäden und Prozessdokumente, Einschätzungen der Fachpersonen) nachvollziehen lässt, welche Aspekte der vier Dimensionen abgedeckt sind und wo Lücken bestehen. Die konkrete inhaltliche Darstellung der Ergebnisse erfolgt in den Kapiteln 5 und 6.

4.5.2 Auswertung der Literatur- und Dokumentenbasis

Für die Literatur- und Dokumentenbasis wird die bereits im Zwischenbericht aufgebaute Evidenztabelle weitergeführt und für die vorliegende Arbeit systematisch ausgewertet. Die Awareness-Literatur wird zunächst entlang der Evidenzlogik «super ja / ja / nein» im Hinblick auf verhaltensnahe Wirksamkeit klassifiziert. Pro Quelle werden Zielsetzung, Studiendesign, Zielgruppe, Messgrössen und zentrale Befunde in einer Tabelle erfasst (Hu et al., 2022, S. 752–753).

In einem zweiten Schritt werden die Textzusammenfassungen dieser Quellen mit der in Unterabschnitt 4.5.1 beschriebenen Kategorienstruktur codiert. Wichtige Ausschnitte – zum Beispiel zu wirksamen Formaten (Micro-Learnings, wiederkehrende Reminder, Peer-Effekte (Einfluss von Teamnormen und Vorbildern)), zur Einbettung in Governance- und Managementstrukturen oder zu Nebenwirkungen von Massnahmen – werden den Dimensionen: Governance, Prozesse, Human Factor sowie Awareness- und Unterstützungsinstrumente zugeordnet (Kuckartz, 2018, S. 97–105).

Parallel dazu werden die Leitfäden, Merkblätter und Prozessbeschreibungen der BK als eigener Dokumentenkorpus behandelt und entlang derselben Kategorien analysiert (Bundeskanzlei, 2025b, 2025c). Dabei wird insbesondere geprüft, welche Integritätsanforderungen, Rollenbilder, Kontrollen und Hinweise bereits explizit formuliert sind und wo aus Sicht des Bezugsrahmens Lücken bestehen. Zur Einordnung dieser Governance- und Awareness-Aspekte werden ergänzend ausgewählte internationale Referenzrahmen herangezogen, insbesondere die OECD-Empfehlung zur öffentlichen Integrität («Recommendation on Public Integrity») aus dem Jahr 2017, das NIST Cybersecurity Framework aus dem Jahr 2018 sowie die Norm ISO/IEC 27001 in der Fassung von 2022 der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC).

Die Auswertung der Literatur- und Dokumentenbasis ist darauf ausgerichtet, drei Ziele zu erreichen:

1. **Identifikation verhaltensnaher Wirkungshebel:** Es wird herausgearbeitet, welche Formate, Prinzipien und Rahmenbedingungen in der Literatur mit beobachtbarem Verhalten verknüpft sind (z. B. iterative Kampagnen, zielgruppenspezifische Materialien, Kombination von Awareness-Massnahmen mit prozessintegrierten Kontrollen) und wie erfolgreiche Awareness-Programme international gestaltet werden, etwa in Kampagnen des Bundesamts für Cybersicherheit (BACS) in der Schweiz oder von ENISA (BACS, 2024; ENISA, 2024).
2. **Analyse der bestehenden BK-Materialien:** Es wird analysiert, welche Integritätsanforderungen, Rollenbilder, Kontrollen und Hinweise sich bereits in Leitfäden und Prozessbeschreibungen der BK finden und wo aus Sicht der vier Dimensionen des Bezugsrahmens zusätzliche Präzisierungen oder Unterstützungsangebote angezeigt sein könnten.
3. **Verdichtung zu Integritätshebeln:** Die codierten Befunde werden zu den Integritätshebeln «Situationen», «Strukturen» und «Signale» verdichtet. So sollen typische Risikosituationen,

Rahmenbedingungen in Strukturen und mögliche Warnsignale, beziehungsweise Ansatzpunkte für Sensibilisierung systematisch herausgearbeitet werden.

Die Ergebnisse dieser Verdichtung bilden die Grundlage für Kapitel 5, in dem die wesentlichen Wirkungshebel der Awareness-Literatur, ihre prozessuale Verortung in den BK-Materialien sowie ihre Übertragbarkeit auf die BK und die Unterschriftensammlung dargestellt werden.

4.5.3 Auswertung der Interviews mit Fachpersonen und Triangulation

Die schriftlichen Interviews mit Fachpersonen werden nach einem vergleichbaren Schema ausgewertet. Die Antworten werden in ein einheitliches Format überführt (eine Zeile pro Person, eine Spalte pro Frage) und anschliessend mittels inhaltlich strukturierender Inhaltsanalyse codiert (Gläser & Laudel, 2009, S. 199–204, 212–214; Kuckartz, 2018, S. 180–184).

Für jede Antwort werden drei Schritte durchgeführt:

1. **Zuordnung zu Dimensionen und Hebeln:** Aussagen werden den vier Dimensionen des Bezugsrahmens sowie den Integritätshebeln «Situationen», «Strukturen» und «Signale» zugeordnet. Beispiele sind konkrete Drucksituationen beim Sammeln, Einschätzungen zu Anreizmodellen, Hinweise auf Schwachstellen in Strukturen und Abläufen oder Vorschläge für pragmatische Sensibilisierungsmassnahmen.
2. **Verdichtung auf Kernaussagen:** Pro Interview werden wenige, in funktionsbezogener Form formulierte Kernaussagen herausgearbeitet (z. B. «Gemeinderätin Sicherheit/Finanzen», «Politikberater», «Unternehmer im Bereich Software- und IT-Sicherheit»). Dabei steht der inhaltliche Beitrag im Vordergrund. Die Personen werden nicht namentlich, sondern über ihre Funktion beschrieben.
3. **Vergleich mit Literatur und Dokumenten (Triangulation):** In einem Triangulationsschritt werden die Einschätzungen der Fachpersonen mit den Ergebnissen aus Literatur- und Dokumentenanalyse verglichen (Flick, 2018, Kapitel 2). Übereinstimmungen stützen bestehende Befunde, Unterschiede oder neue Hinweise weisen auf zusätzliche Integritätsrisiken oder Handlungsspielräume hin, die im Literaturkorpus noch nicht abgebildet sind.

Die Ergebnisse dieser Auswertung fliessen in Kapitel 6 ein, in dem die empirischen Befunde aus den Interviews mit Fachpersonen dargestellt werden. In Kapitel 7 werden sie gemeinsam mit den Ergebnissen aus Kapitel 5 verwendet, um das Sensibilisierungskonzept und die konkreten Bausteine für die BK sowie für Komitees und Sammelnde zu entwickeln.

Auf diese Weise entsteht ein konsistenter Auswertungsprozess, in dem sich theoretischer Bezugsrahmen, Literatur- und Dokumentenbasis sowie Einschätzungen der Fachpersonen gegenseitig

ergänzen und in einem integrierten Bild von Integritätsrisiken und Sensibilisierungsmöglichkeiten zusammengeführt werden.

4.6 Gütekriterien und Limitationen

Das in Kapitel 4 beschriebene Forschungsdesign folgt einer qualitativ ausgerichteten Fallstudienlogik mit Mixed-Methods-Elementen. Entsprechend orientiert sich die Beurteilung der Qualität weniger an statistischer Repräsentativität, sondern an Gütekriterien qualitativer Sozialforschung, wie Glaubwürdigkeit, Nachvollziehbarkeit, Übertragbarkeit und Reflexivität (Flick, 2018, S. 10–13, 15–16; Kuckartz, 2018, S. 15–21; Mayring, 2015, S. 124–126). Gleichzeitig sind die zentralen Limitationen des Vorgehens transparent offenzulegen, um die Reichweite der Schlussfolgerungen realistisch einzuordnen.

4.6.1 Gütekriterien des Forschungsdesigns

Die Glaubwürdigkeit der Ergebnisse wird insbesondere durch Triangulation gestützt. Die Arbeit verknüpft unterschiedliche Datentypen – wissenschaftliche Literatur, offizielle Dokumente der BK sowie Einschätzungen der Fachpersonen – und analysiert sie entlang eines konsistenten Bezugsrahmens (vgl. Abschnitt 3.5 und 4.5). Übereinstimmungen zwischen diesen Quellen stärken die Plausibilität der Befunde. Abweichungen werden bewusst als Hinweise auf Spannungsfelder oder blinde Flecken behandelt und in den Ergebnis- und Diskussionskapiteln aufgegriffen (Flick, 2018, S. 22–23).

Die Nachvollziehbarkeit wird durch eine möglichst transparente Dokumentation des Vorgehens sichergestellt. Kapitel 4 legt die einzelnen Schritte von der Datenauswahl über die Kategorienbildung bis zur Auswertung offen. Wo sinnvoll, werden diese Schritte durch Tabellen und Abbildungen ergänzt (z. B. Evidenztabelle, Auswertungsschemata, Übersicht der Kategorien). Dadurch soll die Analyse für Dritte prüfbar sein und – zumindest in wesentlichen Teilen – repliziert oder auf andere Kontexte übertragen werden können (Kuckartz, 2018; Mayring, 2015).

Die Übertragbarkeit der Ergebnisse wird nicht im Sinn statistischer Verallgemeinerung angestrebt, sondern im Sinn analytischer Verallgemeinerung. Das heisst, die aus der Fallstudie «Bundeskanzlei und Unterschriftensammlung» abgeleiteten Integritätshebel und Sensibilisierungskonzepte sollen vor allem als analytische Linse dienen, die sich auf ähnliche Konstellationen anwenden lässt (z. B. andere staatliche Stellen mit Governance-Verantwortung im demokratischen Prozess). Die im Bezugsrahmen beschriebenen Dimensionen und Integritätshebel bilden dafür den zentralen Referenzpunkt (Yin, 2018, S. 73–75).

Die Verlässlichkeit des Vorgehens wird dadurch unterstützt, dass für alle Datentypen (Literatur, Dokumente, Interviews) eine einheitliche Auswertungslogik verwendet wird (vgl. Unterabschnitt 4.5.1).

Die Kombination aus deduktiven Kategorien (aus Bezugsrahmen und Forschungsfragen) und induktiven Unterkategorien folgt etablierten Vorgehensweisen der inhaltlich strukturierenden qualitativen Inhaltsanalyse (Kuckartz, 2018; Mayring, 2015). Zudem werden Zitate und Beispiele in den Ergebniskapiteln so ausgewählt, dass sie typische Muster illustrieren und nicht Einzelfälle überbetonen.

Schliesslich wird durch eine reflexive Einordnung der eigenen Rolle und der Rahmenbedingungen versucht, Interpretationsspielräume sichtbar zu machen. Dazu gehört die explizite Trennung von Beschreibung und Bewertung in den Ergebniskapiteln sowie eine sprachliche Zurückhaltung bei der Formulierung von Aussagen («kann als Hinweis verstanden werden», «deutet darauf hin», «im Rahmen dieser Fallstudie»), wie sie in der qualitativen Forschung empfohlen wird (Flick, 2018).

4.6.2 Limitationen des Forschungsdesigns

Trotz dieser Vorkehrungen weist das Forschungsdesign mehrere Limitationen auf, die für die Interpretation der Ergebnisse berücksichtigt werden müssen.

Erstens handelt es sich um eine Einzelfallstudie zur Schweizerischen BK im Kontext eidgenössischer Volksbegehren. Die rechtlichen, institutionellen und kulturellen Rahmenbedingungen der direkten Demokratie in der Schweiz sind spezifisch. Die Ergebnisse lassen sich daher nicht direkt auf andere Staaten oder demokratische Systeme übertragen. Auch innerhalb der Schweiz steht die BK in einer besonderen Rolle, die sich von anderen Bundesbehörden oder kantonalen Stellen unterscheidet (Yin, 2018, S. 84–86).

Zweitens ist der empirische Teil auf eine begrenzte Anzahl von Fachpersonen beschränkt, die gezielt (purposive sampling) entlang der Fragestellung ausgewählt wurden (vgl. Unterabschnitt 4.4.2) (Gläser & Laudel, 2009, S. 117–118). Dieses Vorgehen ist für Interviews mit Fachpersonen üblich, führt aber dazu, dass die Perspektiven nicht repräsentativ für alle potenziell relevanten Beteiligtengruppen sind. Zudem besteht immer die Möglichkeit eines Non-Response-Bias (systematische Verzerrung durch ausbleibende oder selektive Rückmeldungen), falls angefragte Personen nicht reagieren, eine Teilnahme ablehnen oder nur knapp antworten. Die Arbeit begegnet dieser Limitation, indem sie die Zahl der befragten Profile transparent macht und die Ergebnisse als illustrative Einsichten statt als umfassendes Stimmungsbild interpretiert.

Drittens basieren sowohl Literatur- und Dokumentenanalyse als auch Interviews mit Fachpersonen auf Textmaterial, das jeweils in einem bestimmten Kontext entstanden ist. Offizielle Dokumente der BK sind normativ und rechtlich geprägt und spiegeln in erster Linie eine institutionelle Perspektive. Interviews mit Fachpersonen liefern subjektive Einschätzungen, die ihrerseits von individuellen Erfahrungen, Rollen und Interessen beeinflusst sind. Direkte Beobachtungen von Sammelsituationen oder experimentelle Designs zur Messung von Verhaltensänderungen sind im Rahmen dieser Arbeit

nicht vorgesehen, was die Möglichkeit kausal orientierter Aussagen bewusst einschränkt (Flick, 2018, S. 11–12).

Viertens ist die Arbeit durch einen engen zeitlichen Rahmen begrenzt. Dies wirkt sich insbesondere auf den Umfang der empirischen Erhebung (Anzahl Interviews, Iterationen in der Auswertung) und auf die Tiefe aus, mit der bestimmte Aspekte – etwa spezifische Sammelkontexte oder kantonale Besonderheiten – vertieft werden können. Literatur und Dokumente wurden sorgfältig, aber nicht im Sinn einer systematischen Vollerhebung ausgewählt. Auch hier ist von einem wohlbegründeten, aber nicht vollständigen Bild auszugehen (Kuckartz, 2018, S. 100).

4.6.3 Umgang mit Limitationen

Mit diesen Limitationen wird in der Arbeit bewusst und transparent umgegangen. Die wichtigsten Einschränkungen werden in den Ergebnis- und Diskussionskapiteln jeweils dort benannt, wo sie für die Einordnung einzelner Befunde relevant sind (z. B. bei der Interpretation von Fachpersonenzitaten oder bei der Übertragung von Awareness-Studien auf die spezifische Rolle der BK).

Die Kombination aus unterschiedlichen Datenquellen und Perspektiven (Triangulation) dient dazu, die Auswirkungen einzelner Limitationen zu verringern: Wo Literatur, BK-Dokumente und Einschätzungen der Fachpersonen in dieselbe Richtung weisen, kann von robusteren Hinweisen gesprochen werden, als wenn eine Aussage nur in einer einzelnen Quelle auftaucht (Flick, 2018, S. 21–23). Gleichzeitig werden aus der Fallstudie bewusst keine generalisierenden Aussagen über «alle Komitees», «alle Sammelnden» oder «die Schweizer Bevölkerung» abgeleitet, sondern es werden Integritätshebel und Sensibilisierungsansätze formuliert, die im Kontext der BK und eidgenössischer Volksbegehren plausibel und begründbar erscheinen.

Insgesamt soll Abschnitt 4.6 dazu beitragen, die Ergebnisse der Arbeit in Kapitel 5 bis 7 als das einzuordnen, was sie sind: gut begründete, empirisch und theoretisch abgestützte, aber notwendigerweise kontext- und zeitgebundene Einsichten in die Frage, wie Integrität und Manipulationsprävention bei Unterschriftensammlungen unterstützt werden können.

Wo sinnvoll, werden die Ergebnisse jeweils im Licht der einschlägigen Rechtsgrundlagen (z. B. DSG Art. 5, 6; BPR Art. 58–75; BV Art. 138–141; VPR Art. 23) sowie der öffentlichen Leitfäden und Prozessdarstellungen der BK gelesen, ohne diese im Rahmen dieser Arbeit eigenständig auszulegen.

Das folgende Kapitel 5 bündelt vor diesem Hintergrund die Ergebnisse der Literatur- und Dokumentenanalyse und identifiziert jene Wirkungshebel, die für die weitere Konzeptentwicklung besonders relevant sind.

5 Ergebnisse der Literatur- und Dokumentenanalyse

Kapitel 3 hat einen theoretischen Bezugsrahmen zu Integrität, Governance, Informationssicherheit, Awareness-Programmen und Human Factor entwickelt und die fünf Themenfelder entlang der vier Dimensionen: Governance, Prozesse, Human Factor sowie Awareness- und Unterstützungsinstrumente systematisch verknüpft. Kapitel 4 hat darauf aufbauend beschrieben, wie dieser Rahmen in der Literaturrecherche, der Dokumenten- und Prozessanalyse sowie in der schriftlichen Befragung von Fachpersonen operationalisiert wird.

Dieses Kapitel bündelt die Ergebnisse der Literatur- und Dokumentenanalyse. Im Zentrum steht die Frage, welche Erkenntnisse die aktuelle Forschung zu Awareness und Human Factor zur verhaltensnahen Wirksamkeit von Sensibilisierungsmassnahmen liefert und wie gut die bestehenden Materialien und Prozesse der BK diese Wirkungshebel bereits abdecken. Damit bildet das Kapitel die Brücke zwischen dem theoretischen Bezugsrahmen und der späteren empirischen Auswertung der Fachpersoneninterviews sowie der Entwicklung des Sensibilisierungskonzepts.

Die Darstellung erfolgt im Sinne eines Zwischenstands der Gesamtauswertung, da die Einschätzungen der Fachpersonen in Kapitel 6 noch hinzukommen und in Kapitel 7 gemeinsam mit den hier identifizierten Wirkungshebeln trianguliert werden.

Abschnitt 5.1 gibt zunächst einen Überblick über die Evidenzbasis der ausgewerteten Awareness-Literatur im Zeitraum 2020–2025 und verweist auf die vollständige Evidenztabelle in Anhang A. Abschnitt 5.2 beschreibt zentrale Wirkungshebel, die sich in der Literatur wiederkehrend als wirksam erweisen, insbesondere Wiederholung, soziale Einbettung und radikale Einfachheit. Abschnitt 5.3 ordnet diese Befunde in die übergeordnete Governance-Schicht von Rahmenwerken und Kulturmodellen ein und zeigt bestehende Messlücken auf. Abschnitt 5.4 überträgt die identifizierten Wirkungshebel auf den Kontext der BK, von Komitees und Sammelnden. Ein kurzes Zwischenfazit in Abschnitt 5.5 leitet zu den empirischen Ergebnissen in Kapitel 6 und zur Konzeptentwicklung in Kapitel 7 über.

5.1 Evidenzübersicht 2020–2025

Die Literaturrecherche hat 128 Quellen zur Gestaltung und Wirksamkeit von Awareness- und Human-Factor-Massnahmen identifiziert, die den in Kapitel 4 beschriebenen Suchkriterien entsprechen. Im Fokus stehen Beiträge, die sich auf sicherheitsrelevantes Verhalten beziehen und grundsätzlich auf den Kontext von Komitees und Sammelnden bei eidgenössischen Volksbegehren übertragbar sind. Die vollständige Evidenztabelle mit Angaben zu Intervention und Kontext, Studiendesign und Messgrössen, zentralen Befunden und zugeordneter Evidenzkategorie ist in Anhang A dokumentiert.

Im Hinblick auf verhaltensnahe Wirksamkeit wird die Literatur entlang einer dreistufigen Evidenzlogik eingeordnet, die in Unterabschnitt 4.2.5 beschrieben wurde: Studien mit hoher Evidenz (z. B. randomisierte Experimente mit beobachtetem Verhalten) werden als «super ja», solche mit mittlerer Evidenz (z. B. Vorher-Nachher-Designs, Verhaltensabsichten, quasi-experimentelle Designs) als «ja» und Beiträge ohne direkte Wirkungsmessung als «nein» klassifiziert. Von den 128 Quellen weisen 15 eine hohe und 54 eine mittlere Evidenzstufe auf. 59 Beiträge beschreiben Konzepte, Programme oder Rahmenwerke, ohne verhaltensnahe Effekte systematisch zu messen. Dies entspricht rund 12 % der Quellen mit hoher, 42 % mit mittlerer und 46 % ohne direkte verhaltensnahe Evidenz und verdeutlicht die breite, zugleich heterogene Evidenzbasis (ENISA, 2021, S. 23, 29–30; Hu et al., 2022).

Inhaltlich deckt der Korpus ein breites Spektrum an Massnahmen ab: klassische Awareness-Trainings, Phishing-Simulationen, wiederkehrende Micro-Learnings, kampagnenartige Kommunikationsformate, Gamification-Ansätze sowie Governance-orientierte Rahmenwerke und Leitfäden (z. B. ENISA-Empfehlungen, NIST-Programme, OECD-Integritätsrichtlinien) (ENISA, 2021, S. 25–26, 30–31; NIST, 2018, S. 31; OECD, 2017, S. 3–4, 7–8). Während ein Teil der Studien eher auf Wissenszuwachs, Einstellungsänderungen oder Verhaltensabsichten fokussiert, liegt bei den höher eingestuften Evidenzquellen der Schwerpunkt auf beobachtbarem Verhalten – etwa auf der Klickrate bei Phishing-Simulationen, der Meldebereitschaft bei sicherheitsrelevanten Vorfällen oder der Nutzung von bereitgestellten Unterstützungsinstrumenten.

Über alle Quellen hinweg zeigt sich ein konsistentes Muster: Awareness-Massnahmen entfalten dann vergleichsweise robuste Verhaltenseffekte, wenn sie klar auf konkrete Entscheidungssituationen ausgerichtet sind, wiederholt eingesetzt werden und in bestehende Strukturen und Rollenbilder eingebettet sind. Breite, einmalige Kampagnen ohne Bezug zu spezifischen Situationen oder ohne Anschluss an organisatorische Prozesse weisen demgegenüber schwächere oder schwerer nachweisbare Effekte auf. Diese Beobachtung bildet den Ausgangspunkt für die Identifikation der in Abschnitt 5.2 beschriebenen Wirkungshebel.

5.2 Zentrale Wirkungshebel der Awareness-Literatur

Die systematische Auswertung der Evidenztabelle zeigt drei Wirkungshebel, die über die in Kapitel 3 beschriebenen allgemeinen Kriterien hinaus als besonders tragfähig erscheinen: Wiederholung, soziale Einbettung und radikale Einfachheit. Sie ergänzen sich gegenseitig und lassen sich gut mit den vier Dimensionen des in Kapitel 3 entwickelten Bezugsrahmens verbinden.

Wiederholung bezieht sich auf die regelmässige, dosierte Wiederaufnahme zentraler Inhalte in Form von Micro-Learnings, kurzen Refreshers oder situativen Erinnerungen. Studien zu Phishing-

Simulationen und wiederkehrenden Lernimpulsen zeigen, dass sich Verhaltensindikatoren – etwa die Klickrate auf schädliche Links oder die Bereitschaft, verdächtige Vorfälle zu melden – insbesondere dann verbessern, wenn Mitarbeitende mehrfach und in unterschiedlichen Situationen mit ähnlichen Entscheidungsmustern konfrontiert werden (Hu et al., 2022). Anstelle einmaliger, umfangreicher Schulungen erweisen sich kurze, wiederkehrende Lernanlässe als wirksamer, um Routinen zu verändern und gewünschtes Verhalten einzuüben. Im Bezugsrahmen stärkt Wiederholung vor allem die Dimensionen Prozesse (Einbettung in wiederkehrende Abläufe) und Awareness- und Unterstützungsinstrumente (serielle Lernformate statt Einzelmassnahmen).

Soziale Einbettung verweist darauf, dass Verhalten nicht isoliert, sondern in sozialen Konstellationen stattfindet. Die Literatur zeigt, dass Vorbilder, Peer-Effekte, Teamnormen und klare Rollenbilder massgeblich beeinflussen, ob Awareness-Botschaften im Alltag tatsächlich umgesetzt werden. Programme sind erfolgreicher, wenn Führungskräfte oder zentrale Rollen sichtbar mit gutem Beispiel vorangehen, Erwartungen an sicheres Verhalten explizit formuliert und im Teamalltag eingefordert werden sowie Austausch über Erfahrungen und Fehler möglich ist. Soziale Einbettung verknüpft damit die Dimensionen: Governance (Rollen- und Verantwortlichkeitsklarheit), Human Factor (Teamdynamiken, Anreize) und Awareness- und Unterstützungsinstrumente (Formate, die Austausch und Vorbildwirkung ermöglichen).

Radikale Einfachheit beschreibt den Befund, dass Inhalte und Formate dann besonders wirksam sind, wenn sie sprachlich klar, inhaltlich fokussiert und in der Länge stark begrenzt sind. Viele Studien berichten, dass Zielgruppen kurze, konkret formulierte Hinweise («Was tue ich, wenn …?») und wenige, klar priorisierte Verhaltensregeln besser aufnehmen und erinnern als umfangreiche Broschüren oder abstrakte Leitsätze. Einfachheit betrifft nicht nur Sprache und Gestaltung, sondern auch die Reduktion auf wenige Kernbotschaften pro Massnahme. Im Bezugsrahmen stärkt dieser Wirkungshebel insbesondere die Dimension Awareness- und Unterstützungsinstrumente, wirkt aber auch auf Prozesse, wenn Formulare, Checklisten oder Standardbriefe so gestaltet sind, dass sie gewünschtes Verhalten «mitdenken».

Gemeinsam ist den drei Wirkungshebeln, dass sie konkrete Entscheidungssituationen ins Zentrum stellen und an realen Handlungskontexten ansetzen, anstatt nur abstrakte Prinzipien zu vermitteln. Sie sind damit anschlussfähig an die in Kapitel 3 beschriebenen Integritätshebel: «Situationen, Strukturen, Signale»: Wiederholung macht typische Situationen sichtbar und übt sie ein, soziale Einbettung verankert Strukturen und Rollen, radikale Einfachheit sorgt für klare Signale im Sammelalltag. Kurz gefasst: Awareness-Massnahmen wirken dort am stärksten, wo sie wiederholt, gemeinsam und einfach sind.

Die zahlreichen Governance-orientierten Rahmenwerke, Leitfäden und Kulturmodelle, die in der Literatur ebenfalls vertreten sind, werden in Abschnitt 5.3 vertieft betrachtet. Dort wird aufgezeigt, wie sie die drei genannten Wirkungshebel rahmen, zugleich aber eine Messlücke hinsichtlich verhaltensnaher Wirksamkeit offenlassen – und damit den Gestaltungsraum für die BK und das in dieser Arbeit entwickelte Sensibilisierungskonzept definieren.

5.3 Governance-Schicht und Messlücke

Neben verhaltensnahen Studien umfasst der Literaturkorpus zahlreiche Rahmenwerke, Leitfäden und Programme, die primär auf der Governance-Ebene ansetzen. Sie formulieren Prinzipien guter Informationssicherheits- und Integritätssteuerung, definieren Rollen und Verantwortlichkeiten, schlagen Kennzahlen vor und betonen die Bedeutung einer unterstützenden Kultur. Typische Elemente sind klare Zuständigkeiten für Sicherheit und Integrität, regelmässige Risikoanalysen, definierte Eskalationswege, Awareness-Strategien sowie Berichts- und Monitoring-Pflichten (ENISA, 2021, S. 9, 14; ISO/IEC, 2022, S. 3–4, 8–9; NIST, 2018, S. 23–24, 26, 39; OECD, 2017, S. 6–7).

Im Lichte des in Kapitel 3 entwickelten Bezugsrahmens adressieren diese Beiträge insbesondere die Dimension Governance: Sie legen fest, wer wofür verantwortlich ist, wie Programme formal verankert werden und welche Prozesse zur Steuerung und Überwachung vorgesehen sind. Teilweise beschreiben sie auch, wie Awareness-Massnahmen in bestehende Prozesse eingebettet werden können und welche Erwartungen an das Verhalten von Mitarbeitenden oder Freiwilligen gerichtet werden. Konkrete Aussagen zu typischen Drucksituationen, alltagsnahen Entscheidungsschwellen oder individuell erlebten Zielkonflikten bleiben jedoch meist abstrakt oder werden nur exemplarisch illustriert.

Gerade im Bereich der Messung zeigt sich eine deutliche Messlücke: Viele Rahmenwerke schlagen Kennzahlen, wie Anzahl durchgeführter Schulungen, Teilnahmequoten, Anzahl verschickter Kommunikationsmassnahmen oder die Existenz formaler Richtlinien, vor. Weniger verbreitet sind hingegen Indikatoren, die tatsächliche Verhaltensänderungen oder den Umgang mit kritischen Situationen systematisch erfassen. Nur ein kleiner Teil der Literatur verknüpft Governance-Elemente explizit mit beobachtbarem Verhalten, etwa indem Meldequoten, Reaktionszeiten oder Fehlerhäufigkeiten entlang definierter Prozesse ausgewertet werden (vgl. Abschnitt 5.2 sowie Anhang A).

Diese Messlücke ist für den Kontext der BK besonders relevant. Komitees und Sammelnde sind keine klassischen Organisationen mit stabilen Strukturen und langjährigen Mitarbeitenden, sondern zeitlich begrenzte Zusammenschlüsse mit hoher Fluktuation und oft begrenzten Ressourcen. Viele Governance-Empfehlungen aus der allgemeinen Literatur lassen sich nur eingeschränkt auf diese Realität übertragen. Gleichzeitig eröffnet die Lücke zwischen abstrakter Governance-Schicht und

konkreten Verhaltensindikatoren einen Gestaltungsspielraum: Es besteht Bedarf an schlanken, kontextsensitiven Messgrössen, die sowohl der besonderen Stellung der BK als zentrale Stelle als auch den Arbeitsbedingungen von Komitees und Sammelnden gerecht werden.

Für diese Arbeit bedeutet dies: Die Governance-orientierten Beiträge bilden einen wichtigen Orientierungsrahmen, liefern aber nur begrenzt Antworten auf die Frage, wie Sensibilisierungsmassnahmen im Sammelalltag wirken und wie sich ihre Wirkung pragmatisch messen lässt. Genau an dieser Schnittstelle setzt die weitere Analyse an, indem sie die identifizierten Wirkungshebel mit den spezifischen Strukturen, Prozessen und Drucksituationen im Kontext der Unterschriftensammlung verknüpft.

5.4 Übertragung auf Bundeskanzlei, Komitees und Sammelnde

Die drei in Abschnitt 5.2 beschriebenen Wirkungshebel – Wiederholung, soziale Einbettung und radikale Einfachheit – entfalten ihre Wirkung nur, wenn sie an die institutionellen Rollen der BK und die Arbeitsrealität von Komitees und Sammelnden angepasst werden. Die Literatur legt nahe, dass Awareness-Massnahmen dort am wirksamsten sind, wo sie sich eng an konkrete Situationen, bestehende Strukturen und erkennbare Signale anlehnen. Dies korrespondiert mit den in Kapitel 3 beschriebenen Integritätshebeln: «Situationen, Strukturen, Signale».

Für die BK bedeutet dies vor allem eine Rolle als Rahmensetzerin und Unterstützerin:

- **Wiederholung** kann dort verankert werden, wo die BK ohnehin mit Komitees in Kontakt steht – etwa bei der Anmeldung einer Volksinitiative, beim Versand von Sammelunterlagen oder bei der Kommunikation von Fristen und formalen Anforderungen (Bundeskanzlei, 2025b, 2025c). Kurze, wiederkehrende Hinweise auf typische Integritätsrisiken und erwartetes Verhalten können an diese Kontaktpunkte geknüpft werden, ohne zusätzlichen bürokratischen Aufwand zu erzeugen.
- **Soziale Einbettung** kann gestärkt werden, indem Rollen und Erwartungen klar benannt werden: Komitees übernehmen Verantwortung für den fairen und gesetzeskonformen Verlauf der Sammlung, Sammelnde vertreten diese Haltung gegenüber der Bevölkerung. Die BK kann diese Rollen durch Formulierungen in Leitfäden, in der Korrespondenz und in Beispielmaterialien sichtbar machen, ohne selbst in die Binnenorganisation der Komitees einzugreifen.
- **Radikale Einfachheit** ist bei allen Materialien zentral, die Komitees und Sammelnde von der BK erhalten. Anstatt umfangreicher, schwer zugänglicher Dokumente sind kurze, klar strukturierte Unterlagen gefragt, die wenige zentrale Botschaften enthalten: Was ist erlaubt, was ist heikel, was ist zu tun, wenn Unsicherheit entsteht?

Für Komitees stellen die Wirkungshebel vor allem eine Chance dar, mit begrenzten Ressourcen ein Mindestmass an Integritätskultur aufzubauen:

- **Wiederholung** kann in einfachen Formen erfolgen, etwa durch kurze Briefings zu Beginn von Sammelaktionen, durch wiederkehrende Erinnerungen in internen Chats oder durch das regelmässige Ansprechen typischer heikler Situationen (z. B. Druck, «noch schnell ein paar Unterschriften zu holen»).
- **Soziale Einbettung** zeigt sich darin, dass einzelne Personen im Komitee eine Vorbildrolle übernehmen, klare Signale setzen und bei Verstössen oder Grenzfällen ansprechbar sind. Kleine, informelle Teams können hier besonders wirksam sein, wenn Normen explizit gemacht werden.
- **Radikale Einfachheit** bedeutet für Komitees, dass sie Sammelnden klare, knappe Leitlinien an die Hand geben: wenige Regeln, konkrete Beispiele, klare Ansprechpersonen. Umfangreiche interne Regelwerke sind für Freiwillige und temporär Engagierte meist weder realistisch noch wirksam.

Für Sammelnde werden die Wirkungshebel im unmittelbaren Kontakt mit der Bevölkerung konkret:

- **Wiederholung** wirkt in Form von eingeübten Reaktionen auf typische Situationen: Wie reagiere ich, wenn eine Person mich zu aggressiverem Vorgehen drängt? Wie gehe ich mit Unterschriften um, bei denen ich Zweifel habe? Solche Reaktionen können durch einfache Rollenspiele, Merkfragen oder kurze Beispiele vorbereitet werden.
- **Soziale Einbettung** zeigt sich im Bewusstsein, Teil eines Komitees zu sein, das bestimmte Standards vertritt. Sammelnde handeln nicht nur als Individuen, sondern als sichtbare Repräsentierende eines Volksbegehrens. Das kann in einfachen Kernbotschaften («Wir sammeln sauber, oder wir sammeln nicht») sichtbar gemacht werden.
- **Radikale Einfachheit** ist für Sammelnde besonders wichtig: In der Praxis bleibt oft wenig Zeit, um nachzulesen oder nachzufragen. Hilfreich sind daher Materialien, die mit wenigen Blicken verständlich sind – etwa eine einseitige Übersicht mit «Dos und Don’ts», eine kurze Checkliste für kritische Situationen oder klar formulierte Antworten auf häufige Fragen.

Insgesamt zeigt die Übertragung, dass die in der Literatur identifizierten Wirkungshebel gut mit der Rollenverteilung im Schweizer System der direkten Demokratie vereinbar sind. Die BK kann Rahmen, Prozesse und einfache Unterstützungsinstrumente bereitstellen, Komitees können diese in ihre Strukturen und Abläufe übersetzen, Sammelnde können sie in konkreten Situationen anwenden. Entscheidend ist dabei, dass die Massnahmen verhaltensnah, ressourcenschonend und anschlussfähig an die bestehenden Prozesse der Unterschriftensammlung bleiben.

5.5 Zwischenfazit und Implikationen für die Konzeptphase

Die Ergebnisse der Literatur- und Dokumentenanalyse lassen sich in drei Kernpunkten zusammenfassen:

Erstens zeigt die Evidenzbasis, dass Awareness-Massnahmen dann vergleichsweise robuste Verhaltenseffekte entfalten, wenn sie sich an konkreten Entscheidungssituationen orientieren und mit Wiederholung, sozialer Einbettung und radikaler Einfachheit arbeiten. Breite, einmalige Kampagnen ohne klaren Bezug zum Alltag bleiben demgegenüber häufig wirkungsarm oder schwer messbar.

Zweitens verdeutlichen die Governance-orientierten Rahmenwerke, dass klare Rollen, Prozesse und Steuerungsmechanismen eine wichtige Grundlage für Integrität und Informationssicherheit bilden. Gleichzeitig bleibt die Messung verhaltensnaher Wirkung oft vage. Die Lücke zwischen abstrakter Governance-Schicht und konkreten Verhaltensindikatoren ist in vielen Beiträgen sichtbar und eröffnet Gestaltungsspielräume für kontextspezifische, pragmatische Lösungen.

Drittens wird deutlich, dass der Kontext der Unterschriftensammlung für eidgenössische Volksbegehren besondere Anforderungen stellt: Komitees und Sammelnde agieren unter Zeitdruck, mit heterogenen Hintergründen und begrenzten Ressourcen. Sensibilisierungskonzepte müssen daher schlank, fokussiert und anschlussfähig an bestehende Prozessschritte der BK sein, statt ein umfassendes, schwer umsetzbares Programm zu beinhalten.

Für die weitere Konzeptphase bedeutet dies, dass das Sensibilisierungskonzept auf zwei Ebenen ansetzen sollte: auf der Ebene der BK als Rahmensetzerin und Prozessverantwortliche sowie auf der Ebene von Komitees und Sammelnden, die integritätsfördernde Verhaltensweisen im Sammelalltag konkret leben. Die in diesem Kapitel identifizierten Wirkungshebel werden dafür entlang der Integritätshebel: «Situationen, Strukturen, Signale» gebündelt und bilden die inhaltliche Grundlage für ein schlankes, auf wenige Bausteine fokussiertes «Minimal Viable Awareness-Paket» (minimal umsetzbare Sensibilisierungslösung) für Komitees und Sammelnde sowie für die BK-seitigen Rahmenelemente.

Kapitel 6 ergänzt diese Befunde punktuell aus Sicht der Praxis. Im Zentrum stehen die schriftlichen Rückmeldungen von zwei Kommunalpolitikern, die entlang des Bezugsrahmens eingeordnet werden. Ergänzend fliessen die Einschätzungen eines Unternehmers im Bereich Software- und IT-Sicherheit sowie eines im Feld digitaler Demokratie und E-Collecting tätigen Unternehmers ein (vgl. Kapitel 6 und Anhang B3). Kapitel 6 zeigt, wie die beschriebenen Wirkungshebel und Messlücken im konkreten Arbeitsalltag wahrgenommen werden und welche zusätzlichen Anforderungen oder Einschränkungen sich daraus ergeben. Darauf aufbauend entwickelt Kapitel 7 ein Sensibilisierungskonzept, das die evidenzbasierten Wirkungshebel mit den institutionellen Rahmenbedingungen und den Bedürfnissen von Komitees und Sammelnden verbindet.

6 Ergebnisse der empirischen Erhebung

Dieses Kapitel wertet die schriftlichen Rückmeldungen von zwei Kommunalpolitikern aus, die im Rahmen der empirischen Erhebung zur Integrität von Unterschriftensammlungen befragt wurden (vgl. Abschnitt 4.4 sowie Anhang B3.1 und B3.2). Ergänzend wurden zwei weitere schriftliche Rückmeldungen eines Unternehmers im Bereich Software- und IT-Sicherheit sowie eines im Feld digitaler Demokratie und E-Collecting tätigen Unternehmers eingeholt (vgl. Anhang B3.3 und B3.4). Sie fliessen punktuell in die Interpretation und den Ausblick ein, stehen jedoch nicht im Zentrum der fallbezogenen Auswertung dieses Kapitels. Die Auswertung folgt der in Abschnitt 4.5 beschriebenen Logik der inhaltlich strukturierenden qualitativen Inhaltsanalyse und ordnet die Aussagen entlang des in Kapitel 3 entwickelten Bezugsrahmens ein.

Im Zentrum stehen drei Fragen:

- Wie wird die Integrität von Unterschriftensammlungen im Schweizer Kontext wahrgenommen?
- Wo verläuft aus Sicht der befragten Personen die Grenze zwischen legitimer politischer Überzeugung und manipulativen Praktiken?
- Welche Rolle und welche Grenzen werden einer behördlichen Sensibilisierung – insbesondere durch die BK – eingeräumt?

Die Ergebnisse sind aufgrund der schmalen empirischen Basis – im Zentrum stehen zwei schriftliche Rückmeldungen aus der kommunalen Praxis – nicht repräsentativ, sondern als illustrative Einsichten zu verstehen, die mit der Literatur- und Dokumentenanalyse aus Kapitel 5 gespiegelt werden.

6.1 Datengrundlage und Einordnung

Die fallbezogene Auswertung in diesem Kapitel stützt sich primär auf zwei schriftliche Rückmeldungen von Kommunalpolitikern, die im Rahmen der in Abschnitt 4.4 beschriebenen Kurzbefragung gewonnen wurden. Die Rückmeldungen stammen von zwei Mitgliedern einer mittelgrossen aargauischen Stadt, von denen einer zugleich langjährige Erfahrung als Chef einer kantonalen Kriminalpolizei mitbringt (vgl. Anhang B3.1 und B3.2).

Insgesamt liegen zum Zeitpunkt der Ausarbeitung dieser Arbeit vier substanzielle schriftliche Rückmeldungen vor: Neben den beiden kommunalpolitischen Antworten wurde eine Rückmeldung eines Unternehmers im Bereich Software- und IT-Sicherheit sowie eine weitere Rückmeldung eines im Bereich digitaler Demokratie und E-Collecting tätigen Unternehmers eingeholt (vgl. Anhang B3.3 und B3.4). Von insgesamt sechs angefragten Fachpersonen gingen damit vier Rückmeldungen ein. Zwei Fachpersonen lehnten die Teilnahme ab, darunter eine aus Zeitgründen.

Für die Auswertung der kommunalpolitischen Perspektiven werden die beiden Antworten als gemeinsamer Textkorpus behandelt und entlang der Kategorien ausgewertet, die in Unterabschnitt 4.5.1 beschrieben wurden: Wahrnehmung von Integritätsrisiken, Grenzziehung zwischen legitimer Überzeugung und Manipulation, Rolle des Staates und Ansatzpunkte für Sensibilisierung. Einzelne Formulierungen werden in diesem Kapitel sinngemäss zusammengefasst. Die vollständigen Wortlaute sind in Anhang B3.1 und B3.2 dokumentiert.

Vor dem Hintergrund der in Abschnitt 4.6 diskutierten Limitationen werden die Rückmeldungen der Kommunalpolitiker als kleine Fallstudien interpretiert: Sie können Hinweise auf verbreitete Haltungen und Erwartungshaltungen liefern, erheben aber keinen Anspruch auf ein umfassendes Stimmungsbild. Entsprechend werden die Ergebnisse vorsichtig formuliert und mit den theoretischen und dokumentenbasierten Befunden aus Kapitel 2 bis 5 verschränkt. Die zusätzlichen Perspektiven aus IT-Sicherheit und digitaler Demokratie ergänzen diese Fallstudien punktuell, insbesondere im Hinblick auf künftige Fragestellungen rund um E-Collecting.

6.2 Wahrnehmung der Integrität im Schweizer Kontext

Beide Kommunalpolitiker beschreiben die Integrität von Unterschriftensammlungen in der Schweiz insgesamt als eher wenig problematisch. Im Unterschied zu vielen anderen Staaten wird das System der direkten Demokratie als grundsätzlich vertrauenswürdig wahrgenommen. Offensichtliche Fälschungen oder organisierte Manipulationen gelten als seltene Ausnahmefälle.

Gleichzeitig verweist insbesondere der ehemalige Chef der kantonalen Kriminalpolizei darauf, sich in beruflicher wie politischer Tätigkeit nicht vertieft mit konkreten Fällen von Integritätsverletzungen befasst zu haben. Dies deutet darauf hin, dass Integritätsfragen im Umfeld von Unterschriftensammlungen in der breiten politischen Praxis eher am Rand wahrgenommen werden und entsprechende Problemlagen möglicherweise nur bei offensichtlichen Verstössen (z. B. Fälschung von Unterschriften) sichtbar werden.

Der zweite Kommunalpolitiker ergänzt diese Perspektive, indem er auf künftige Integritätsrisiken im Kontext von E-Collecting verweist. In seiner Darstellung stehen weniger einzelne Sammelsituationen im Vordergrund als vielmehr Fragen nach Systemlandschaft, Datenstandorten, Zugriffsrechten, Aufbewahrungsfristen und Sanktionen bei Missbrauch. Integrität wird damit nicht nur als Eigenschaft des Verhaltens von Komitees und Sammelnden, sondern ebenso als Eigenschaft der dahinterliegenden digitalen Infrastrukturen verstanden.

In der Gesamtbetrachtung stützt die Kombination aus grundsätzlich positiver Gesamteinschätzung und begrenzter eigener Fallkenntnis die in Kapitel 2 beschriebene Beobachtung, dass viele Integritätsrisiken latent bleiben und im Normalbetrieb nicht zwingend als Problem artikuliert werden.

Integrität erscheint damit weniger als akutes Krisenfeld, sondern als grundsätzlich vorhandenes, gleichwohl verletzbares Gut – insbesondere in Graubereichen des Alltagsverhaltens und bei der künftigen Ausgestaltung digitaler Sammelkanäle.

6.3 Grenze zwischen legitimer Überzeugungsarbeit und Manipulation

Besonders deutlich äussern sich die Befragten zur Frage, wo aus ihrer Sicht die Grenze zwischen legitimer politischer Überzeugungsarbeit und problematischer Manipulation verläuft.

Als legitime Elemente hebt der ehemalige Chef der kantonalen Kriminalpolizei das klare, auch «plakative» In-den-Vordergrund-Stellen der eigenen Argumente hervor, ebenso das Weglassen «gegnerischer» Argumente in der Kampagnenkommunikation. Auch Werbung «in eigener Sache» – etwa durch Medienberichte, Standaktionen oder Hausbesuche – sowie «motivierende Überzeugungsarbeit» im Verwandten- und Bekanntenkreis betrachtet er als zulässigen Bestandteil politischer Willensbildung. Damit bestätigt die Rückmeldung, dass ein breiter Spielraum für engagierte, auch zugespitzte politische Kommunikation als zulässig und demokratiekonform betrachtet wird.

Zugleich zieht der Kommunalpolitiker mehrere klare rote Linien: «Eigentliche Lügen» sollen unter keinen Umständen in Kampagnen einfliessen, auch «Halbwahrheiten» sind nach seiner Einschätzung zu vermeiden. Die Fälschung von Unterschriften wird ausdrücklich als verboten und strafbar bezeichnet, und die Sammlung von Unterschriften bei Personen, die «nicht oder nur bedingt in der Lage sind, die Thematik der Kampagne zu erfassen», wird als grenzwertig und nicht zulässig beurteilt.

Besonders sichtbar wird diese Grenzziehung an einer in der Praxis häufig diskutierten Grauzone: dem Ausfüllen von Unterschriftenbogen für andere Personen. Hier vertritt der Befragte die Haltung, dies sei zulässig, sofern die betroffenen Personen transparent informiert sind und genau wissen, unter welche Kampagne sie schlussendlich ihre Unterschrift setzen. Entscheidend ist aus seiner Sicht, dass die unterschreibende Person eine eigenständige, informierte Entscheidung trifft – unabhängig davon, wer das Formular physisch ausfüllt.

Der zweite Kommunalpolitiker betont demgegenüber vor allem, dass Stimmberechtigte eine informierte Risikoabwägung vornehmen können sollen. Aus seiner Sicht ist es für legitime politische Überzeugungsarbeit zentral, dass die Vor- und Nachteile eines Begehrens für das Land klar dargestellt werden und dass das Parlament die Vorlage vorberät und eine Empfehlung abgibt. Manipulativ wird Kommunikation dort, wo zentrale Informationen weggelassen oder Sachverhalte verzerrt dargestellt werden, sodass Stimmberechtigte die Tragweite ihres Entscheids nicht mehr einschätzen können.

Die Rückmeldungen zeigen damit, dass die Grenze zwischen legitimer Überzeugung und Manipulation nicht an einzelnen Sammeltechniken allein festgemacht wird, sondern an einer Kombination aus Transparenz, Freiwilligkeit und inhaltlicher Redlichkeit. Graubereiche entstehen dort, wo formal zulässige Praktiken (z. B. Ausfüllen von Bögen für Dritte) in der Praxis unterschiedlich streng interpretiert und je nach Kontext unterschiedlich bewertet werden.

6.4 Einordnung entlang des Bezugsrahmens

Die Aussagen der beiden Kommunalpolitiker lassen sich mit den in Abschnitt 3.5 beschriebenen Dimensionen des Bezugsrahmens verknüpfen: Governance, Prozesse, Human Factor sowie Awareness- und Unterstützungsinstrumente.

Aus Governance-Sicht bestätigen die Rückmeldungen die Bedeutung klarer normativer Leitplanken. Das strikte Verbot von Fälschungen und Lügen sowie die Zurückweisung manipulativer Praktiken gegenüber Personen mit eingeschränkter Urteilsfähigkeit spiegeln die in Kapitel 2 skizzierten Anforderungen an faire und transparente Verfahren. Gleichzeitig wird deutlich, dass die Integrität «in aller Regel» gewährleistet sei und die direkte Demokratie als etabliertes, vertrauenswürdiges System wahrgenommen wird.

Auf Prozessebene werden vor allem jene Situationen sichtbar, in denen sich Integritätsrisiken verdichten: Hausbesuche, Sammelaktionen im Bekanntenkreis, Sammeln bei vulnerablen Personen oder das Ausfüllen von Bögen für Dritte. Diese Konstellationen entsprechen typischen «Situationen» im Sinn der in Kapitel 3 beschriebenen Integritätshebel, in denen Komitees und Sammelnde unter Zeitdruck Entscheidungen treffen müssen. Im Kontext von E-Collecting kommen prozessuale Fragen der Qualitätssicherung, des Systembetriebs, der Zugriffssteuerung und der Reaktion auf Datenpannen hinzu.

Bezogen auf den Human Factor wird deutlich, dass Integrität nicht nur von Regeln abhängt, sondern von situativen Einschätzungen und persönlichen Haltungen: Was als «motivierende Überzeugungsarbeit» verstanden wird, kann aus Sicht Betroffener bereits als Druck erlebt werden. Ebenso kann die Einschätzung, eine Person sei «nicht oder nur bedingt in der Lage, die Thematik zu erfassen», in der Praxis schwierig sein. Diese Ambivalenzen korrespondieren mit den in Abschnitt 3.4 beschriebenen Druck- und Entscheidungssituationen.

Schliesslich liefern die Aussagen Hinweise für Awareness- und Unterstützungsinstrumente. Die klare Benennung weniger, leicht verständlicher Grundsätze («keine Lügen», «keine Fälschungen», besondere Zurückhaltung bei vulnerablen Personen) passt zu den in Kapitel 5 identifizierten Wirkungshebeln: Wiederholung, soziale Einbettung und radikale Einfachheit. Die Hinweise zum Umgang mit E-Collecting – Fragen nach Datenstandorten, Zugriffsrechten, Aufbewahrungsfristen und

Missbrauchssanktionen – verdeutlichen zudem, dass Sensibilisierung sich nicht nur auf Sammelnde «an der Front», sondern auch auf die Gestaltung und Kommunikation der zugrundeliegenden Systeme und Prozesse beziehen sollte.

6.5 Zwischenfazit und Implikationen für das Sensibilisierungskonzept

Die Auswertung der Rückmeldungen der beiden Kommunalpolitiker sowie ergänzender schriftlicher Rückmeldungen aus den Bereichen Software- und IT-Sicherheit sowie digitale Demokratie bietet eine punktuelle, aber instruktive Ergänzung zur Literatur- und Dokumentenanalyse:

- Sie bestätigt, dass grundlegende Integritätsprinzipien – keine Fälschungen, keine Lügen, besondere Zurückhaltung gegenüber vulnerablen Personen – im politischen Alltag unbestritten sind. Einzelne Befragte nennen darüber hinaus normative Kriterien, die sie für redliche politische Kampagnenarbeit relevant erachten (z. B. Gesetzmässigkeit, Verhältnismässigkeit, wirtschaftliche Umsetzbarkeit, Mehrwert für die Bevölkerung). Diese Kriterien sind als individuelle Einordnung zu verstehen und werden nicht als behördliche Prüfmassstäbe übernommen.
- Sie zeigt, dass einzelne Sammelpraktiken, die aus Governance-Perspektive als heikel gelten können (z. B. Ausfüllen von Bögen für Dritte), von politischen Beteiligten teilweise als vertretbar eingeordnet werden, solange Transparenz gewährleistet ist und Stimmberechtigte eine eigenständige, informierte Entscheidung treffen können.
- Sie verdeutlicht, dass Integritätsfragen in der Wahrnehmung einzelner Fachpersonen aus der Praxis eher als Randthema erscheinen und Sensibilisierung daher niederschwellig, konkret und ressourcenschonend ausgestaltet werden sollte.
- Sie macht sichtbar, dass Integrität zunehmend auch als Frage der Gestaltung digitaler Infrastrukturen verstanden wird: Fragen zu Datenstandorten, Zugriffsrechten, Aufbewahrungsfristen, Missbrauchssanktionen und zur rechtlichen Grundlage von E-Collecting stehen im Zentrum der geäusserten Besorgnisse.

Insbesondere im Rahmen dieser Fallstudie können die beiden kommunalpolitischen Rückmeldungen als Hinweise darauf verstanden werden, dass ein Sensibilisierungskonzept der BK zwei Ziele gleichzeitig verfolgen muss: Es soll rote Linien klar und verständlich markieren und zugleich den legitimen Handlungsspielraum politischer Kampagnen respektieren. Sensibilisierungsmaterialien sollten daher an realistische Alltagsrisiken in der Unterschriftensammlung anknüpfen, typische Risikosituationen – etwa Sammeln im nahen sozialen Umfeld, Stellvertretung beim Unterschreiben, Umgang mit vulnerablen Personen oder Fragen zu E-Collecting – konkret adressieren und Komitees und Sammelnde in ihrer Eigenverantwortung stärken, statt Kampagneninhalte zu steuern. Auf dieser

Grundlage entwickelt Kapitel 7 ein Sensibilisierungskonzept, das die evidenzbasierten Wirkungshebel aus Kapitel 5 mit den hier skizzierten Praxiswahrnehmungen und den institutionellen Rahmenbedingungen der BK verbindet. Ergänzend machen die schriftlichen Rückmeldungen aus den Bereichen Software- und IT-Sicherheit sowie digitale Demokratie deutlich, dass Integrität zunehmend auch als Gestaltungsaufgabe digitaler Infrastrukturen verstanden wird. Sie stützen insbesondere jene Sensibilisierungselemente, die auf Transparenz von Datenflüssen, klare Verantwortlichkeiten und robuste technische Rahmenbedingungen im Umfeld von E-Collecting abzielen (vgl. Anhang B3.3 und B3.4).

7 Entwicklung des Sensibilisierungskonzepts

Dieses Kapitel bündelt die bisherigen Ergebnisse der Arbeit zu einem zweistufigen Sensibilisierungskonzept für Komitees und Sammelnde. Ausgangspunkt sind der in Kapitel 3 entwickelte Bezugsrahmen mit den Integritätshebeln: «Situationen, Strukturen, Signale», die Ergebnisse der Literatur- und Dokumentenanalyse (vgl. Kapitel 5) sowie die praxisnahen schriftlichen Rückmeldungen von vier Fachpersonen, darunter zwei Kommunalpolitiker (vgl. Kapitel 6 und Anhang B3). Gemeinsam zeigen diese Befunde, dass Integritätsrisiken zwar real sind, aber primär dort entstehen, wo Zeitdruck, unklare Zuständigkeiten oder überhöhte Erwartungen aufeinandertreffen – und dass wirksame Sensibilisierung kurz, fokussiert und gut in den Sammelalltag integrierbar sein muss.

Darauf aufbauend folgt die Entwicklung eines Sensibilisierungskonzepts, das nicht auf umfassende Programme oder zusätzliche Kontrollstufen setzt, sondern auf gezielte Impulse entlang des bestehenden Prozesses der Unterschriftensammlung. Im Zentrum steht die Stärkung der Eigenverantwortung von Komitees und Sammelnden, unterstützt durch klare Signale und einfache Hilfsmittel. Das Konzept besteht aus zwei ineinandergreifenden Paketen:

- **Paket A**: ein BK-seitiger Rahmen, der Integrität an ausgewählten Kontaktpunkten in die bestehenden Abläufe der BK integriert.
- **Paket B**: ein Minimal Viable Awareness-Paket mit praxistauglichen, freiwillig nutzbaren Hilfsmitteln für Komitees und Sammelnde.

Paket A definiert, wie die BK ihre Rolle als Rahmensetzerin und Unterstützerin wahrnehmen kann, ohne die politische Freiheit der Komitees einzuschränken. Paket B adressiert die operative Ebene der Unterschriftensammlung und stellt Komitees und Sammelnden kompakte Werkzeuge zur Verfügung, mit denen sie ihre Integritätskultur eigenständig stärken können. Beide Pakete folgen gemeinsamen Designprinzipien, die im nächsten Abschnitt erläutert werden.

7.1 Designprinzipien

Bei der Ausarbeitung des Sensibilisierungskonzepts wurden fünf Designprinzipien zugrunde gelegt. Sie verbinden die theoretischen und empirischen Befunde der vorherigen Kapitel mit den praktischen Rahmenbedingungen der BK sowie der Arbeitsweise von Komitees und Sammelnden.

Erstens: Evidenzbasiert und pragmatisch

Das Konzept stützt sich auf jene Wirkungshebel der Awareness-Literatur, für die eine verhaltensnahe Wirksamkeit belegt ist – insbesondere Wiederholung, soziale Einbettung und radikale Einfachheit. Zugleich wird der Befund ernst genommen, dass gross angelegte Programme im politischen

Alltag oft schwer umsetzbar sind. Das Sensibilisierungskonzept setzt daher auf wenige, klar umsetzbare Elemente mit hoher Anschlussfähigkeit an den Sammelalltag, statt auf eine Vielzahl ambitionierter, aber kaum realisierbarer Massnahmen.

Zweitens: Prozessorientiert und situationsbezogen

Anstatt Integrität abstrakt zu adressieren, knüpft das Konzept an konkrete Situationen im Prozess der Unterschriftensammlung an. Die Verdichtung auf: «Situationen, Strukturen, Signale» dient als Raster: In welchen Situationen entstehen typische Integritätsrisiken? Welche bestehenden Strukturen (Regeln, Abläufe, Meldewege) können diese Risiken abfedern? Und welche Signale der BK und der Komitees machen deutlich, welches Verhalten erwartet wird? Paket A und B sind so gestaltet, dass sie entlang dieser drei Elemente greifen.

Drittens: Rollen- und freiheitskompatibel

Die BK agiert in ihrer Rolle als neutrale Rahmensetzerin. Das Konzept respektiert die politische Handlungsfreiheit der Komitees und die Vielfalt der Sammelstrategien. Paket A konzentriert sich auf Rahmenelemente, die aus der Perspektive der Verwaltung legitim sind (z. B. Hinweise in Leitfäden, standardisierte Textbausteine, interne Checklisten). Paket B stellt den Komitees und Sammelnden Hilfsmittel zur Verfügung, deren Nutzung freiwillig ist und die von den Komitees inhaltlich und sprachlich an ihre kampagnenspezifischen Bedürfnisse angepasst werden können.

Viertens: Radikal einfach und ressourcenschonend

Komitees sind häufig temporär organisierte Projektstrukturen mit begrenzten personellen und finanziellen Ressourcen. Sammelnde sind oft ehrenamtlich oder Teilzeit engagiert. Entsprechend setzt das Konzept auf Formate, die mit minimalem Aufwand genutzt werden können: ein Integritäts-Check auf einer Seite, ein Einseiter «Faires Sammeln» für Sammelnde, eine kurze Checkliste für heikle Situationen. Für die BK bedeutet dies, dass Paket A primär über bestehende Kommunikationskanäle und Dokumente umgesetzt wird, ohne neue, aufwendige Programme aufzubauen.

Fünftens: Anschlussfähig und beobachtbar

Vor dem Hintergrund der in Kapitel 5 identifizierten Messlücke im Bereich der Awareness-Programme wurde das Konzept so angelegt, dass erste Wirkungen im Rahmen des Machbaren beobachtet werden können. Statt ambitionierte Kennzahlensysteme vorzuschlagen, fokussiert es auf wenige Indikatoren, die im Alltag der BK erhoben werden können (z. B. dokumentierte Nutzung von Merkblättern, Rückmeldungen von Komitees, qualitative Hinweise aus der Praxis). Damit bleibt die

Umsetzung realistisch, ermöglicht aber dennoch eine schrittweise Überprüfung und Weiterentwicklung der Massnahmen.

Diese fünf Designprinzipien bilden den verbindenden Rahmen für Paket A und Paket B. Sie stellen sicher, dass das Sensibilisierungskonzept sowohl theoretisch verankert als auch praktikabel ist und die verschiedenen Rollen im System der Unterschriftensammlung respektiert.

7.2 Paket A – BK-seitiger Rahmen

Paket A beschreibt, wie die BK Integrität in ihre bestehenden Abläufe und Kommunikationskanäle zur Unterschriftensammlung einbetten kann, ohne neue formelle Verpflichtungen für Komitees zu schaffen. Im Zentrum steht die Frage, an welchen Prozesspunkten die BK relativ niederschwellig ansetzen kann, um «Situationen, Strukturen, Signale» sichtbar zu machen und dadurch die Eigenverantwortung der Komitees zu stärken.

Verankerung an bestehenden Kontaktpunkten

Ausgehend vom in Kapitel 2 beschriebenen Ablauf einer Volksinitiative und eines fakultativen Referendums lassen sich mehrere Kontaktpunkte identifizieren, an denen die BK direkt oder indirekt mit Komitees interagiert: erste Informationsanfragen, die formelle Anmeldung eines Volksbegehrens, die Behandlung des Unterschriftenbogens (inkl. Übersetzung), sowie – je nach Konstellation – der Austausch zu Fristen, formellen Anforderungen und Rückfragen. Paket A sieht vor, an ausgewählten dieser Kontaktpunkte kurze Integritätselemente zu verankern. Beispiele sind:

- Ein kurzer Hinweis auf Integrität und Verantwortung bereits in der schriftlichen Bestätigung der Anmeldung eines Komitees.
- Der Verweis auf ein Integritäts-Merkblatt im Leitfaden für Komitees.
- Ein Standardhinweis auf die Möglichkeit, Unklarheiten und heikle Situationen frühzeitig mit der BK zu besprechen.

Damit werden Integritätsfragen dort angesprochen, wo Komitees ohnehin mit der BK in Kontakt stehen – ohne zusätzliche Formulare oder eigenständige Programme einzuführen.

Prozessvorgaben und interne Checklisten

Neben extern sichtbaren Signalen umfasst Paket A interne Elemente für die Mitarbeitenden der BK. Eine kurze Checkliste kann sicherstellen, dass Integrität in den relevanten Prozessschritten systematisch angesprochen wird, etwa mit Fragen wie: Wurde das Integritäts-Merkblatt dem Komitee zugestellt? Wurde auf die Meldewege bei Verdachtsfällen hingewiesen? Wurden heikle Sammelkonstellationen (z. B. Einsatz von Drittorganisationen) thematisiert, sofern sie im Gespräch zur

Sprache kamen? Solche Checklisten dienen nicht der zusätzlichen Kontrolle der Komitees, sondern der Qualitätssicherung innerhalb der BK und tragen zu konsistenten Signalen über verschiedene Dossiers hinweg bei.

Signale in schriftlichen Unterlagen

Ein weiterer Baustein von Paket A sind kurze, klar formulierte Integritätspassagen in bestehenden Dokumenten der BK – etwa im Leitfaden für Volksbegehren oder in standardisierten Schreiben. Diese Passagen können zentrale Botschaften aufnehmen, die sich aus Literatur und Praxis ergeben: keine Unterschriften ohne Wissen und Wollen der unterzeichnenden Person, besondere Sorgfalt bei Personen mit eingeschränkter Urteilsfähigkeit, Transparenz beim Ausfüllen von Formularen für Dritte – sowie der Hinweis, dass Integrität auch im Interesse des Komitees selbst liegt. Wichtig ist eine neutrale, unterstützende Sprache, die auf gemeinsame Verantwortung statt auf Drohkulisse setzt.

Paket A ist somit bewusst schlank ausgestaltet. Es baut auf bestehenden Abläufen und Dokumenten auf und stärkt die Rolle der BK als Rahmensetzerin und Ansprechstelle bei Integritätsfragen. Zugleich schafft es die Grundlage dafür, dass Paket B in der Praxis überhaupt bei den Komitees ankommt: Hinweise in Leitfäden und Schreiben verweisen gezielt auf die Hilfsmittel, die den Komitees und Sammelnden zur Verfügung gestellt werden.

7.3 Paket B – Minimal Viable Awareness-Paket für Komitees und Sammelnde

Paket B richtet sich direkt an Komitees und Sammelnde. Es übersetzt die in Kapitel 5 herausgearbeiteten Wirkungshebel und die in Kapitel 6 sichtbar gewordenen Praxisperspektiven in konkrete, leicht nutzbare Hilfsmittel. Ziel ist ein Minimal Viable Awareness-Paket, das mit begrenzten Ressourcen eingesetzt werden kann und dennoch eine spürbare Wirkung auf die Integritätskultur der Komitees entfaltet.

Das Paket umfasst drei zentrale Bausteine, die in Anhang C dieser Arbeit prototypisch illustriert werden.

Baustein 1: Integritäts-Check für Komitees (A4)

Der Integritäts-Check ist als einseitige Selbstreflexionshilfe für Komitees gedacht, idealerweise zu Beginn der Kampagne oder beim Eintritt neuer Schlüsselpersonen. Er besteht aus 5–7 Aussagen und Fragen, die entlang der Integritätshebel: «Situationen, Strukturen, Signale» strukturiert sind. Beispiele sind:

- Haben wir innerhalb des Komitees klar festgelegt, wer Sammelnde instruiert und bei Fragen zu Integrität ansprechbar ist?
- Wie gehen wir mit Angeboten externer Sammelorganisationen um, insbesondere wenn Konditionen oder Praktiken schwer überprüfbar sind?
- Haben wir im Komitee darüber gesprochen, welche Sammelpraktiken wir bewusst nicht einsetzen wollen, selbst wenn sie formal zulässig wären?

Die Komitees können den Check gemeinsam ausfüllen, offene Punkte sammeln und daraus konkrete Vereinbarungen ableiten. Die BK stellt den Check in einer neutralen Grundversion zur Verfügung. Komitees können ihn inhaltlich und sprachlich an ihre Kampagne anpassen.

Ein prototypischer Textvorschlag findet sich in Anhang C.2.

Baustein 2: Einseiter «Faires Sammeln» für Sammelnde

Der Einseiter richtet sich an alle Personen, die im Auftrag eines Komitees Unterschriften sammeln – unabhängig davon, ob sie ehrenamtlich oder entgeltlich tätig sind. Er vermittelt auf einer Seite die wichtigsten Grundsätze für faires Sammeln in einfacher, verständlicher Sprache. Typische Elemente sind eine kurze Einleitung («Warum Integrität beim Sammeln wichtig ist»), 5–7 knappe Leitlinien (z. B. keine Unterschriften ohne Einverständnis, keine irreführenden Aussagen zum Inhalt der Vorlage, besondere Vorsicht bei vulnerablen Personen), ein kurzer Hinweis darauf, wie Sammelnde vorgehen sollen, wenn sie unsichere oder heikle Situationen erleben (z. B. Rückfragen an das Komitee statt improvisierte Lösungen) sowie der Verweis auf eine Ansprechperson im Komitee. Zudem ist er in einer bewusst einfachen Du-Form gehalten, damit er im Sammelalltag direkt verwendet werden kann.

Der Einseiter kann Komitees als Basis dienen, um eigene Instruktionen oder Schulungen für Sammelnde aufzubauen. Die BK liefert mit Paket B einen prototypischen Textvorschlag. Layout und Feinschliff können von den Komitees an ihre Kampagne und ihr Corporate Design angepasst werden. Ein entsprechender Einseiter ist in Anhang C.3 prototypisch ausgearbeitet.

Baustein 3: Kurz-Checkliste «Heikle Situationen und rote Linien»

Die Kurz-Checkliste fokussiert auf 3–5 typische Situationen, in denen Integritätsrisiken empirisch besonders häufig auftreten können, etwa Sammeln im Freundeskreis, Sammeln bei Personen mit eingeschränkter Urteilsfähigkeit, Haustürbesuche, Sammeln an Orten mit hohem sozialen Druck oder das Ausfüllen des Formulars für Dritte. Für jede Situation werden zwei Fragen beantwortet:

- Woran erkenne ich, dass die Situation heikel werden könnte?

- Was ist ein fairer Umgang mit dieser Situation im Sinne der Integrität der Unterschriftensammlung?

Die Checkliste kann den Einseiter «Faires Sammeln» ergänzen oder als eigenständiges Hilfsmittel eingesetzt werden. Sie eignet sich insbesondere für kurze Briefings zu Beginn einer Sammelaktion oder zur Nachbesprechung konkreter Erfahrungen von Sammelnden.

Paket B ist bewusst so konzipiert, dass seine Elemente modular einsetzbar sind. Komitees können alle Bausteine übernehmen oder einzelne Elemente auswählen, die zu ihrer Arbeitsweise passen. Die Hilfsmittel sind als Vorschläge gedacht. Die Verantwortung für Inhalt, Einsatz und allfällige Anpassungen liegt bei den Komitees. Die BK schafft mit der Bereitstellung lediglich einen gemeinsamen Ausgangspunkt, der auf evidenzbasierten Wirkungshebeln und klaren Integritätsprinzipien beruht.

Eine mögliche Ausgestaltung dieser Checkliste ist in Anhang C.4 dargestellt.

7.4 Wirkungslogik und Indikatoren

Die Wirkungslogik des vorgeschlagenen Sensibilisierungskonzepts lässt sich als mehrstufige Kette beschreiben, die auf den in Kapitel 3 eingeführten Dimensionen und den in Kapitel 5 identifizierten Wirkungshebeln aufbaut.

Auf der Governance- und Prozessebene setzt Paket A an: Die BK verankert Integrität an ausgewählten Kontaktpunkten mit den Komitees, ergänzt interne Checklisten und stärkt damit konsistente Signale («Integrität ist Teil unserer gemeinsamen Verantwortung»). Gleichzeitig verweist sie explizit auf die Hilfsmittel aus Paket B. Dadurch steigt die Wahrscheinlichkeit, dass Integritätsfragen in der frühen Phase eines Volksbegehrens überhaupt thematisiert werden und nicht nur reaktiv bei Vorkommnissen.

Auf der Ebene des Human Factor setzt Paket B an: Komitees erhalten konkrete Werkzeuge, um das Thema Integrität in ihren eigenen Strukturen zu verankern – durch den Integritäts-Check, durch klare, einfache Leitlinien für Sammelnde und durch eine Checkliste für heikle Situationen. Diese Hilfsmittel unterstützen Komitees und Sammelnde dabei, typische Druck- und Grauzonensituationen zu erkennen und im Sinne der Integrität zu bewältigen. Wiederholung (z. B. durch regelmässige Nutzung der Materialien), soziale Einbettung (gemeinsame Besprechung im Komitee oder in Sammelgruppen) und radikale Einfachheit (einseitige, leicht verständliche Formate) wirken hier zusammen.

Vor dem Hintergrund der in Kapitel 5 beschriebenen Messlücke ist das Konzept so gestaltet, dass erste Wirkungen pragmatisch beobachtet werden können, ohne ein komplexes Monitoring-System einzuführen. Mögliche Indikatoren im Sinne von «beobachtbaren Hinweisen» sind:

- **Prozessnahe Indikatoren**: Wird dokumentiert, dass Integritäts-Merkblätter und Hilfsmittel an Komitees versandt oder bei der Anmeldung aktiv angeboten wurden, beispielsweise über einfache Vermerke im Dossier oder eine Checkbox im Fachsystem? Gibt es interne Rückmeldungen von Mitarbeitenden, dass Integrität konsequent in den relevanten Prozessschritten angesprochen wurde?
- **Rückmeldungen aus der Praxis**: Gehen bei der BK oder bei Komitees Rückmeldungen ein, die auf eine aktive Auseinandersetzung mit den Materialien hindeuten (z. B. Verständnisfragen, Hinweise auf Anpassungswünsche, Beispiele guter Praxis)?
- **Hinweise aus Verdachts- und Meldesituationen:** Verändert sich die Qualität der Meldungen zu Unregelmässigkeiten (z. B. frühere Meldungen, differenziertere Schilderung von Situationen), ohne dass dies als unmittelbare Erfolgskennzahl interpretiert würde?

Diese Indikatoren verstehen sich nicht als umfassendes Evaluationsdesign, sondern als erste Grundlage, um die Umsetzung des Sensibilisierungskonzepts zu begleiten und bei Bedarf anzupassen. Sie knüpfen an bereits bestehende Steuerungs- und Dokumentationspraktiken der BK an und lassen sich schrittweise ausbauen, falls sich dies als sinnvoll erweist.

7.5 Abgrenzung zu weiteren Massnahmen

Das vorgestellte Sensibilisierungskonzept versteht sich als spezifischer Beitrag zur Stärkung der Integrität von Unterschriftensammlungen im bestehenden institutionellen Rahmen. Es ersetzt weder strafrechtliche Bestimmungen noch formelle Prüf- und Kontrollmechanismen auf Ebene der BK, der Kantone oder der Gemeinden. Ebenso wenig greift es in die politische Willensbildung der Stimmberechtigten oder in die inhaltliche Gestaltung von Kampagnen ein.

Paket A und Paket B ergänzen vielmehr diese bestehenden Elemente, indem sie Bewusstsein schaffen, Verantwortlichkeiten klären und einfache Hilfsmittel zur Verfügung stellen. Dort, wo rechtliche oder organisatorische Reformen diskutiert werden (etwa im Bereich der Zulassung von Sammelorganisationen oder der Ausgestaltung von Strafnormen), kann das Sensibilisierungskonzept unterstützend wirken, ersetzt aber keine politischen Entscheide.

Auch im Bereich der wissenschaftlichen Evaluierung sind weitere Schritte denkbar, die über den Rahmen dieser Arbeit hinausgehen. So könnten beispielsweise vertiefte Studien zur Wirksamkeit einzelner Materialien, standardisierte Befragungen von Komitees und Sammelnden oder vergleichende Analysen mit anderen Demokratien aufzeigen, in welchem Ausmass die hier

vorgeschlagenen Massnahmen tatsächlich zu einer Stärkung der Integrität beitragen. Das vorliegende Konzept legt dafür eine erste, kontextbezogene Grundlage: Es zeigt, wo die BK mit verhältnismässigen Mitteln ansetzen kann, um Komitees und Sammelnde in ihrer Integritätsverantwortung zu unterstützen und Verdachtsfällen bei Unterschriftensammlungen präventiv zu begegnen.

8 Diskussion

Dieses Kapitel ordnet die Ergebnisse der Arbeit ein, führt die Befunde aus Literatur-, Dokumenten- und Prozessanalyse sowie der empirischen Erhebung zusammen und beantwortet die in Abschnitt 1.3 formulierten Forschungsfragen. Auf dieser Basis werden die Resultate in den Kontext bestehender Awareness- und Human-Factor-Forschung sowie der Verwaltungspraxis der BK und verwandter Stellen eingeordnet. Abschliessend werden Implikationen für die BK und andere Behörden diskutiert sowie Stärken, Limitationen und weiterer Forschungsbedarf aufgezeigt.

8.1 Beantwortung der Forschungsfragen

Die drei Forschungsfragen strukturieren die gesamte Arbeit (vgl. Abschnitt 4.1). In der Gesamtbetrachtung der Kapitel 5–7 ergibt sich folgendes Bild:

F1 – Integritätsrisiken und kritische Situationen

Die Analyse der rechtlichen Grundlagen, Prozessbeschreibungen und Leitfäden der BK zeigt, dass Integrität bei Unterschriftensammlungen an mehreren Stellen explizit adressiert wird, insbesondere bei der Ausgestaltung der Unterschriftenbogen, der Stimmrechtsbescheinigung und der Rolle der Gemeinden im Bescheinigungsprozess (vgl. Kapitel 2 und Abschnitt 4.3). Gleichzeitig treten entlang des Sammelprozesses typische kritische Situationen zutage: der Einsatz externer Sammelorganisationen, Sammeln unter Zeitdruck kurz vor Fristende, der Umgang mit vulnerablen Personen sowie Graubereiche bei der Darstellung von Vorlageinhalt und Konsequenzen. Die Literatur- und Dokumentenanalyse sowie die Rückmeldung aus der Praxis deuten darauf hin, dass Integritätsrisiken weniger aus einem einzelnen «Skandalpunkt» entstehen, sondern aus der Kombination von Situationen, unklaren Strukturen und widersprüchlichen Signalen (vgl. Kapitel 5 und 6). Die in Abschnitt 2.4 eingeführten Integritätshebel: «Situationen, Strukturen, Signale» erweisen sich damit als tragfähige Linse, um diese Risiken systematisch zu beschreiben.

F2 – Wirksame Awareness-Ansätze

Die Evidenztabelle zur Awareness- und Human-Factor-Literatur (vgl. Anhang A) und deren Auswertung in Kapitel 5 zeigen, dass klassische, rein wissensorientierte Schulungsformate in vielen Kontexten nur begrenzte verhaltensnahe Wirkung entfalten. Stattdessen weisen die Studien auf mehrere wiederkehrende Erfolgsfaktoren hin: kürzere, kontextspezifische Lernimpulse, die Verknüpfung von Wissen mit konkreten Handlungsoptionen in typischen Situationen, die Einbettung in bestehende Prozesse und Rollen sowie eine gewisse Wiederholung über die Zeit hinweg, ohne Überforderung zu erzeugen. Übertragen auf Komitees und Sammelnde bei eidgenössischen Volksbegehren

bedeutet dies, dass aufwendige Trainingsprogramme mit hohem Zeit- und Ressourcenbedarf wenig realistisch sind. Wirksamer erscheint ein Ansatz, der Integritätsbotschaften direkt an entscheidungsnahen Punkten im Sammelprozess platziert, verständliche Beispiele bietet und Komitees wie auch Sammelnde mit einfachen, rasch nutzbaren Hilfsmitteln unterstützt (vgl. Abschnitt 5.2 und 5.4).

F3 – Sensibilisierungskonzept für die BK sowie für Komitees und Sammelnde

Kapitel 7 zeigt, wie sich die Befunde aus F1 und F2 in ein zweistufiges Sensibilisierungskonzept überführen lassen, das sowohl zur Rolle als auch zum Handlungsspielraum der BK passt (vgl. Abschnitt 7.1–7.3). Paket A verankert Integrität und Manipulationsprävention in den bestehenden Governance- und Prozessstrukturen der BK, unter anderem durch eine klarere Verortung des Themas in Leitfäden, Prozessdarstellungen und internen Zuständigkeiten. Paket B bietet mit dem Integritäts-Check für Komitees, dem Einseiter «Faires Sammeln» für Sammelnde und der Kurz-Checkliste für heikle Situationen drei leichtgewichtige, praxistaugliche Bausteine, die direkt an den identifizierten Integritätshebeln ansetzen. Das Sensibilisierungskonzept beantwortet F3 damit in dem Sinn, dass es konkrete, umsetzbare Instrumente formuliert, die sich in den bestehenden Rahmen einfügen und zugleich auf verhaltensnahe Wirksamkeit abzielen, ohne rechtliche oder organisatorische Reformen vorwegzunehmen.

Insgesamt lässt sich festhalten, dass die Arbeit die Forschungsfragen nicht in Form abschliessender, generalisierbarer Aussagen beantwortet, sondern als kontextbezogene, empirisch und theoretisch abgestützte Vorschläge für die BK und die Praxis der Unterschriftensammlung.

8.2 Einordnung in Forschung (Awareness/Human Factor) und Verwaltungspraxis

Die Ergebnisse der Arbeit fügen sich in mehrere bestehende Diskussionsstränge ein.

Aus Sicht der Awareness- und Human-Factor-Forschung bestätigt die Arbeit zunächst zentrale Erkenntnisse aktueller Studien: Sicherheit und Integrität lassen sich nicht allein durch technische oder rechtliche Massnahmen gewährleisten, sondern hängen in hohem Mass von Alltagsentscheidungen einzelner Personen ab. Wirksame Awareness-Programme adressieren diese Entscheidungen kontextspezifisch, nutzen Alltagssituationen als Anker und kombinieren Information mit konkreten Handlungsoptionen. Das hier entwickelte Sensibilisierungskonzept überträgt diese Logik in einen demokratischen Kernprozess: Statt generischer Schulungen wird auf kurze, situationsnahe Impulse gesetzt, die direkt im Sammelprozess ansetzen – etwa beim Planen einer Sammelkampagne, beim Anleiten neuer Sammelnder oder beim Umgang mit Verdachtsmomenten.

Zugleich schliesst die Arbeit an Governance- und Integritätsdiskussionen im öffentlichen Sektor an. Internationale Rahmenwerke zu Public Integrity und Good Governance betonen seit Längerem, dass

formelle Regeln durch gelebte Normen und klare Signale ergänzt werden müssen, damit sie wirksam werden. Die Integritätshebel: «Situationen, Strukturen, Signale» greifen diese Einsicht auf und übersetzen sie in den spezifischen Kontext der Unterschriftensammlung: Die BK agiert hier nicht als «Kontrollinstanz im Hintergrund», sondern als zentrale Stelle, die mit Leitfäden, Formularen und Kommunikationswegen wesentlich mitprägt, wie Komitees und Sammelnde Integrität verstehen und umsetzen.

In der Verwaltungspraxis der BK und verwandter Stellen, wie dem BACS oder europäischen Einrichtungen (z. B. ENISA), zeigt sich ein ähnlicher Trend: Sicherheit und Integrität werden zunehmend als Querschnittsaufgaben verstanden, bei denen technische Schutzmassnahmen, organisatorische Regeln und Sensibilisierung zusammenspielen. Die vorliegende Arbeit trägt dazu bei, diese Logik auf den Bereich der politischen Rechte und insbesondere auf die Unterschriftensammlung zu übertragen. Sie macht sichtbar, dass sich Ansätze aus der Informationssicherheit – etwa risikobasierte Awareness, Fokus auf menschliches Verhalten in Drucksituationen oder indikatorenbasierte Erfolgskontrolle – mit dem demokratietheoretischen Anspruch der BK verbinden lassen, ohne inhaltlich in politische Debatten einzugreifen (BACS, 2024; ENISA, 2024).

8.3 Implikationen für BK und andere Behörden

Für die BK ergeben sich aus den Ergebnissen mehrere praktische Implikationen.

Erstens unterstreicht die Arbeit, dass Sensibilisierung als Prozess zu verstehen ist, nicht als einmalige Kampagne. Die vorgeschlagenen Bausteine von Paket A und B lassen sich schrittweise in bestehende Produkte und Abläufe integrieren – etwa beim Überarbeiten von Leitfäden, beim Aktualisieren von Online-Informationen oder bei der Kommunikation mit Komitees und Sammelnden. Dadurch kann die BK Integritätsbotschaften verstetigen, ohne neue, ressourcenintensive Programme aufbauen zu müssen.

Zweitens zeigen die Befunde, dass Schnittstellen im Sammelprozess zentrale Hebelpunkte sind. Dazu gehören insbesondere die Anmeldung und Begleitung von Volksinitiativen und fakultative Referenden, die Bereitstellung und Prüfung von Unterschriftenbogen, der Kontakt mit Komitees bei Rückfragen sowie die Kommunikation zu Verdachts- und Meldesituationen. Das Sensibilisierungskonzept legt nahe, an diesen Schnittstellen gezielt klare Signale zu setzen, Zuständigkeiten sichtbar zu machen und Komitees sowie Sammelnde mit niedrigschwelligen Hilfsmitteln zu unterstützen. Dies stärkt nicht nur die Integrität des Sammelprozesses, sondern auch die Transparenz der Rolle der BK.

Drittens sprechen die Ergebnisse dafür, Monitoring- und Reflexionsschleifen aufzubauen, die über das reine Erfassen von Verdachtsfällen hinausgehen (vgl. Abschnitt 7.4). Rückmeldungen aus

Komitees, Sammelnden und Gemeinden, Beobachtungen zu typischen Missverständnissen sowie Hinweise aus Meldesituationen können systematisch genutzt werden, um Materialien und Prozesse weiterzuentwickeln. Die in Abschnitt 7.4 skizzierten Indikatoren bieten dafür einen Ausgangspunkt.

Für andere Behörden und weitere Beteiligte ergeben sich ebenfalls Anknüpfungspunkte. Kantone und Gemeinden, die im Bescheinigungsprozess eine wichtige Rolle spielen, könnten Teile des Sensibilisierungskonzepts – insbesondere die Logik der Integritätshebel – übernehmen, um die eigenen Informations- und Unterstützungsangebote zu schärfen. Auf Bundesebene können Stellen mit Schnittstellen zu politischen Prozessen oder Kampagnenkommunikation prüfen, inwiefern sich der hier skizzierte Ansatz auf verwandte Kontexte (z. B. Umgang mit digitalen Kampagnen, Social Media oder E-Collecting) übertragen lässt. Die Arbeit zeigt damit exemplarisch, wie ein sicherheits- und verhaltensorientierter Blick auf Integrität in der direkten Demokratie konkret ausgestaltet werden kann.

8.4 Stärken, Limitationen, Forschungsbedarf

Die Arbeit weist mehrere Stärken auf, die zur Tragfähigkeit der Ergebnisse beitragen. Der theoretische Bezugsrahmen verknüpft Integrität, Governance, Informationssicherheit, Awareness-Programme und Human Factor in einem konsistenten Raster (vgl. Kapitel 3). Darauf aufbauend kombiniert das Forschungsdesign unterschiedliche Datenquellen – wissenschaftliche Literatur, Dokumente und Prozessbeschreibungen der BK sowie Einschätzungen aus der Praxis – und wertet sie entlang einer einheitlichen Kategorienlogik aus (vgl. Kapitel 4 und 5–7). Die Integrationsleistung besteht darin, diese Befunde in ein konkretes, prozessorientiertes Sensibilisierungskonzept zu überführen, das sich am realen Sammelprozess und am Handlungsspielraum der BK orientiert.

Gleichzeitig sind die Limitationen der Arbeit zu berücksichtigen. Wie in Abschnitt 4.6 ausgeführt, handelt es sich um eine kontextgebundene Einzelfallstudie zur BK im Rahmen der Schweizer direkten Demokratie. Die rechtlichen und institutionellen Besonderheiten dieses Settings begrenzen die Übertragbarkeit auf andere Staaten oder demokratische Systeme. Auch innerhalb der Schweiz ist die Perspektive auf die BK fokussiert. Kantonale und kommunale Sichtweisen fliessen nur punktuell ein. Hinzu kommt, dass der empirische Teil – trotz gezielter Auswahl relevanter Fachpersonen – aufgrund von Rücklauf und zeitlichen Rahmenbedingungen auf vier schriftliche Rückmeldungen beschränkt ist (zwei Kommunalpolitiker, ein Unternehmer im Bereich Software- und IT-Sicherheit, ein im Feld digitaler Demokratie und E-Collecting tätiger Unternehmer; vgl. Kapitel 6 und Anhang B3). Die kommunalpolitischen Rückmeldungen werden im Sinne explorativer Fallstudien vertieft ausgewertet, die weiteren Perspektiven fliessen punktuell in Interpretation und Ausblick ein. Die Ergebnisse zeigen Haltungen und Spannungsfelder auf, erheben aber keinen Anspruch darauf, die Vielfalt der Perspektiven von Komitees, Sammelnden oder Behörden vollständig abzubilden.

Eine weitere Limitation betrifft die Übertragung der Awareness-Evidenz auf den spezifischen Kontext von Komitees und Sammelnden. Ein grosser Teil der ausgewerteten Studien stammt aus Unternehmens- oder Verwaltungsumgebungen mit stabilen Strukturen und Ressourcen. Die Arbeit nimmt hier eine analytische Übertragung vor und begründet, weshalb bestimmte Designprinzipien (z. B. kurze Lernimpulse, Situationsnähe, Kombination von Wissen und Handlungsoptionen) auch für oft ehrenamtlich organisierte Komitees relevant sind. Gleichwohl bleibt offen, in welchem Ausmass die vorgeschlagenen Materialien in der Praxis tatsächlich genutzt und als hilfreich erlebt werden.

Daraus ergibt sich ein klarer Forschungsbedarf. Künftige Arbeiten könnten das Sensibilisierungskonzept in Form von Pilotprojekten erproben, etwa mit ausgewählten Komitees und Sammelnden, und dessen Wirkung mit geeigneten qualitativen und quantitativen Methoden evaluieren. Denkbar sind standardisierte Befragungen zu Wahrnehmung und Nutzung der Materialien, vertiefte Interviews mit Komitees, Gemeinden und BK-Mitarbeitenden oder vergleichende Analysen mit anderen Demokratien, die ähnliche Instrumente einsetzen. Ebenso könnten spezifische Aspekte – etwa der Umgang mit bezahlten Sammelorganisationen, digitale Sammelformen oder die Rolle der Gemeinden – in eigenen Studien vertieft werden.

Insgesamt ist das vorgestellte Sensibilisierungskonzept als fundierten, praxistauglichen Ausgangspunkt zu verstehen, auf dem die BK und weitere Beteiligte weiter aufbauen können. Es bietet einen strukturierten, evidenzbasierten Ansatz, um Integrität und Manipulationsprävention bei Unterschriftensammlungen stärker in den Blick zu rücken, und macht zugleich transparent, wo die Grenzen des aktuellen Wissens liegen und welche Fragen weiterer Klärung bedürfen.

9 Schlussfolgerung

Dieses Kapitel bündelt die zentralen Ergebnisse der Arbeit, reflektiert den gewählten Mixed-Methods-Ansatz und skizziert einen Ausblick für Praxis und weitere Forschung. Im Fokus steht die Frage, welchen Beitrag die Arbeit zur Sensibilisierung von Komitees und Sammelnden für Integrität und Manipulationsprävention in der Unterschriftensammlung leistet – und wie dieser Beitrag von der BK und weiteren Beteiligten weiterentwickelt werden kann.

9.1 Zusammenfassung der zentralen Ergebnisse

Ausgehend von der Ausgangsfrage, wie Komitees und Sammelnde wirksam für Integrität in der Unterschriftensammlung sensibilisiert werden können, lassen sich die drei Forschungsfragen (F1–F3; vgl. Abschnitt 1.3) in der Gesamtbetrachtung der Kapitel 2–8 wie folgt beantworten.

Zur ersten Forschungsfrage (F1) zeigt die Analyse des rechtlichen und organisatorischen Kontextes, dass Integrität in der Unterschriftensammlung ein eigenständiges Sicherheitsziel ist, das über formale Rechtmässigkeit hinausgeht. Entlang des Sammelprozesses treten typische Integritätsrisiken zutage – etwa beim Einsatz externer Sammelorganisationen, in Drucksituationen gegen Fristende oder im Umgang mit vulnerablen Personen. Diese Risiken entstehen weniger an einem einzelnen «kritischen Punkt», sondern aus dem Zusammenspiel von Situationen, unklaren Strukturen und widersprüchlichen Signalen. Die Integritätshebel: «Situationen, Strukturen, Signale» bieten eine tragfähige Linse, um diese Konstellationen systematisch zu erfassen und gezielt anzusprechen.

Zur zweiten Forschungsfrage (F2) macht die Auswertung der Awareness- und Human-Factor-Literatur deutlich, dass klassische, stark wissensorientierte Schulungen im Kontext knapper Ressourcen und hoher Fluktuation nur begrenzt verhaltensnahe Wirkung entfalten. Wirksamer erscheinen kürzere, kontextspezifische Lernimpulse, die mit konkreten Handlungsoptionen in typischen Situationen verknüpft sind und in bestehende Prozesse und Rollen eingebettet werden. Übertragen auf Komitees und Sammelnde bedeutet dies: Sensibilisierung sollte nicht als separates Trainingsprogramm verstanden werden, sondern als Folge von klaren Hinweisen, Materialien und Unterstützungsangeboten an entscheidungsnahen Stellen des Sammelprozesses.

Zur dritten Forschungsfrage (F3) zeigt die Entwicklung des Sensibilisierungskonzepts, dass sich diese Erkenntnisse in ein zweistufiges, prozessorientiertes Design überführen lassen. Paket A stärkt die BK-seitige Verankerung von Integrität – etwa durch eine klarere Verortung in Leitfäden, Prozessdarstellungen und Zuständigkeiten. Paket B übersetzt die Integritätshebel in drei konkrete, leichtgewichtige Instrumente: einen Integritäts-Check für Komitees, einen Einseiter «Faires Sammeln» für Sammelnde und eine Kurz-Checkliste für heikle Situationen. Zusammen bilden Bezugsrahmen und

Sensibilisierungskonzept einen konsistenten Ansatz, der zur Rolle der BK passt und Komitees sowie Sammelnde dort abholt, wo Integritätsentscheidungen tatsächlich getroffen werden.

Insgesamt liefert die Arbeit damit keine allgemeingültigen Aussagen über alle Formen politischer Beteiligung, sondern kontextbezogene, empirisch und theoretisch abgestützte Vorschläge für den Umgang mit Integritätsrisiken in der Unterschriftensammlung und die Rolle der BK in diesem Prozess.

9.2 Reflexion des Mixed-Methods-Ansatzes

Der in Kapitel 4 beschriebene Mixed-Methods-Ansatz erweist sich im Rückblick als geeignet, die komplexe Fragestellung dieser Arbeit zu bearbeiten. Die Kombination aus Literatur- und Dokumentenanalyse, der Auswertung einer evidenzbasierten Awareness-Literaturbasis, der Einbeziehung von Einschätzungen aus der Praxis sowie der konzeptionellen Ausarbeitung eines Sensibilisierungskonzepts ermöglicht eine Annäherung an das Thema aus mehreren Perspektiven.

In dieser Arbeit wird der Begriff Mixed Methods im Sinne eines erweiterten, qualitativ geprägten Kombinationsansatzes verwendet, bei dem unterschiedliche Datenquellen (Literatur, Dokumente, schriftliche Rückmeldungen) trianguliert werden. Eine klassische Kombination grosser quantitativer und qualitativer Datensätze war aufgrund des Rahmens nicht Ziel der Studie.

Eine Stärke des Vorgehens liegt in der engen Verknüpfung von Theorie, Kontext und Gestaltung. Der Bezugsrahmen zu Governance, Prozessen, Human Factor sowie Awareness- und Unterstützungsinstrumenten schafft eine strukturierte Grundlage, auf der die verschiedenen Datenquellen systematisch eingeordnet werden können. Die Evidenztabelle zur Awareness-Literatur, die Analyse der Materialien der BK und die praxisbezogenen Rückmeldungen werden entlang derselben Kategorien ausgewertet und in Kapitel 5–7 zusammengeführt. Dadurch entsteht ein konsistenter Argumentationsstrang, der direkt in die Entwicklung der Sensibilisierungsbausteine einfliesst.

Gleichzeitig werden im Forschungsdesign bewusst Grenzen gesetzt, die der Mixed-Methods-Ansatz nicht aufheben kann. Der empirische Teil bleibt aufgrund des Rücklaufs auf wenige, ausgewählte Rückmeldungen beschränkt und ist bewusst als Ergänzung zur Literatur- und Dokumentenanalyse konzipiert, nicht als eigenständige, repräsentative Erhebung. Die Arbeit verzichtet zudem auf experimentelle oder quantitative Evaluationsdesigns, die eine direkte Messung der Wirksamkeit der vorgeschlagenen Materialien erlauben würden. Der Mehrwert des Mixed-Methods-Ansatzes liegt damit primär in der Triangulation von Perspektiven, der Schärfung der Fragestellungen und der Ableitung eines praxistauglichen Konzepts – weniger in statistischer Verallgemeinerbarkeit.

Vor diesem Hintergrund ist der Mixed-Methods-Ansatz als angemessener Kompromiss zu verstehen: Er erlaubt es, die komplexe Rolle der BK und die praktische Realität von Komitees und

Sammelnden abzubilden, ohne den Rahmen dieser Arbeit zu sprengen. Die bewusste Transparenz über Stärken und Grenzen des Vorgehens bildet einen integralen Bestandteil der Schlussfolgerungen.

9.3 Ausblick: Pilotierung, Evaluation und Transfer

Die Ergebnisse der Arbeit eröffnen mehrere Ansatzpunkte für die Weiterentwicklung in Praxis und Forschung.

Für die BK liegt ein naheliegender nächster Schritt darin, das Sensibilisierungskonzept schrittweise in bestehenden Strukturen zu erproben. Denkbar sind zunächst kleinere Pilotierungen, etwa im Rahmen einzelner Volksinitiativen oder Referenden, bei denen Komitees gezielt eingeladen werden, den Integritäts-Check zu nutzen und den Einseiter «Faires Sammeln» sowie die Kurz-Checkliste in der Sammelpraxis zu testen. Rückmeldungen aus solchen Pilotprojekten können genutzt werden, um Inhalte, Sprache und Form der Materialien zu verfeinern und deren Verankerung in Leitfäden, Webseiten und Kommunikationsabläufen der BK gezielt weiterzuentwickeln.

Mittelfristig bietet sich an, die in Abschnitt 7.4 skizzierten Indikatoren und Reflexionsschleifen aufzubauen. Dazu gehören etwa strukturierte Rückmeldemöglichkeiten für Komitees und Sammelnde, systematische Auswertungen von Verdachtsfällen oder Anfragen sowie interne Lernschlaufen innerhalb der BK. Auf dieser Basis könnte sich die Sensibilisierung von Komitees und Sammelnden zu einem wiederkehrenden Bestandteil der Pflege der politischen Rechte entwickeln – vergleichbar mit bestehenden Aktivitäten im Bereich Informationssicherheit oder Datenschutz.

Darüber hinaus eröffnet die Arbeit Perspektiven für weitere Forschung. Künftige Studien könnten die Nutzung und Wirkung der vorgeschlagenen Materialien empirisch evaluieren, etwa durch standardisierte Befragungen, vertiefte Interviews oder begleitende Fallstudien mit Komitees, Gemeinden und Mitarbeitenden der BK. Ein naheliegendes Feld für solche Anschlussarbeiten ist der von der BK lancierte partizipative Prozess zu E-Collecting mit Hackathon (ko-kreatives Entwicklungsformat), Online-Veranstaltungen und schriftlichem Dialog, in dem unterschiedliche Umsetzungsvarianten diskutiert und weiterentwickelt werden (Bundeskanzlei, 2024). Dort werden zentrale Fragen zur digitalen Unterschriftensammlung – etwa zur Vermeidung von Mehrfachunterschriften im hybriden Betrieb, zur Wahrung des Stimmgeheimnisses, zur Barrierefreiheit sowie zu Vertrauen und Transparenz (z. B. durch Open-Source-Lösungen (öffentlich einsehbarer Quellcode)) – vertieft behandelt. Die hier entwickelten Integritätshebel und Sensibilisierungsbausteine könnten in diesem Kontext adaptiert und getestet werden. Weitere Fragestellungen betreffen den Umgang mit neuen Sammelformen (z. B. digitale Kampagnen oder E-Collecting im Regelbetrieb), die Rolle von bezahlten Sammelorganisationen oder die Übertragbarkeit des Integritätskonzepts auf andere demokratische

Prozesse. Künftige Arbeiten könnten zudem Perspektiven aus Professionen mit stark ausgeprägten Verantwortungskodizes gegenüber vulnerablen Personen (z. B. Medizin, Pflege, Sozialarbeit) einbeziehen, um Integritätsfragen in Sammelsituationen mit Abhängigkeitsverhältnissen weiter zu präzisieren. In diesem Sinn versteht sich die Arbeit als Ausgangspunkt, auf dem Verwaltungspraxis und Wissenschaft gemeinsam weiterarbeiten können, um Integrität und Manipulationsprävention in der direkten Demokratie langfristig zu stärken.

Literaturverzeichnis

BACS. (2024). *Einsatz von KI bei Cyberangriffen – Fokusthema des BACS im «European Cyber Security Month»*. https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/ecsm-2024-start.html

Beetham, D. (1991). *The Legitimation of Power*. Macmillan Education Ltd. https://doi.org/10.1007/978-1-349-21599-7

Benz, A. (Hrsg.). (2004). *Governance—Regieren in komplexen Regelsystemen: Eine Einführung*. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-90171-8

Bühlmann, M., Merkel, W., Müller, L., & Wessels, B. (2011). The Democracy Barometer: A new instrument to measure the quality of democracy. *European Political Science*, *11*(4), 519–536. https://doi.org/10.1057/eps.2011.46

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1) (2023). https://www.fedlex.admin.ch/eli/cc/2022/491/de

Bundesgesetz über die politischen Rechte (BPR; SR 161.1) (1978). https://www.fedlex.admin.ch/eli/cc/1978/688_688_688/de

Bundeskanzlei. (2024). *E-Collecting*. https://www.bk.admin.ch/bk/de/home/politische-rechte/e-collecting.html

Bundeskanzlei. (2025a). *Integrität von Unterschriftensammlungen*. https://www.bk.admin.ch/bk/de/home/politische-rechte/volksinitiativen/integritaet.html

Bundeskanzlei. (2025b). *Referenden – Informationen und Leitfäden der Bundeskanzlei*. https://www.bk.admin.ch/bk/de/home/politische-rechte/referenden.html

Bundeskanzlei. (2025c). *Volksinitiativen – Informationen und Leitfäden der Bundeskanzlei*. https://www.bk.admin.ch/bk/de/home/politische-rechte/volksinitiativen.html

Bundesverfassung der Schweizerischen Eidgenossenschaft (BV; SR 101) (2000). https://www.fedlex.admin.ch/eli/cc/1999/404/de

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices*. Information and Privacy Commissioner of Ontario. https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf

Cialdini, R. B., & Goldstein, N. J. (2004). Social Influence: Compliance and Conformity. *Annual Review of Psychology*, *55*(1), 591–621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and Conducting Mixed Methods Research* (Third edition). SAGE. https://collegepublishing.sagepub.com/products/designing-and-conducting-mixed-methods-research-3-241842

EDÖB. (2022). *Das neue Datenschutzgesetz aus Sicht des EDÖB*. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). https://www.edoeb.admin.ch/de/das-neue-datenschutzgesetz-aus-sicht-des-edob

ENISA. (2021). *Raising awareness of cybersecurity: A key element of national cybersecurity strategies*. European Union Agency for Cybersecurity (ENISA). https://data.europa.eu/doi/10.2824/363629

ENISA. (2024). *Promoting security in the digital world during the European Cybersecurity Month*. https://www.enisa.europa.eu/news/promoting-security-in-the-digital-world-during-the-european-cybersecurity-month

Flick, U. (2014). *An Introduction to Qualitative Research* (Edition 5). SAGE. https://uk.sagepub.com/en-gb/eur/an-introduction-to-qualitative-research/book278983

Flick, U. (2018). *Doing Triangulation and Mixed Methods* (2nd edition). SAGE. https://methods.sagepub.com/book/mono/doing-triangulation-and-mixed-methods/toc

Gläser, J., & Laudel, G. (2009). *Experteninterviews und qualitative Inhaltsanalyse: Als Instrumente rekonstruierender Untersuchungen* (3., überarbeitete Auflage). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91538-8

Hu, S., Hsu, C., & Zhou, Z. (2022). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

ISO/IEC. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (No. ISO/IEC 27001:2022). International Organization for Standardization (ISO). https://www.iso.org/standard/27001

Kooiman, J. (2003). *Governing as Governance*. SAGE. https://uk.sagepub.com/en-gb/eur/governing-as-governance/book225057

Kuckartz, U. (2018). *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung* (4. Auflage). Beltz Juventa. https://www.fachportal-paedagogik.de/literatur/vollanzeige.html?FId=3313781

Mayring, P. (2015). *Qualitative Inhaltsanalyse: Grundlagen und Techniken* (12., überarbeitete Auflage). Beltz. https://www.untertor.ch/detail/ISBN-9783407257307/Mayring-Philipp/Qualitative-Inhaltsanalyse

NIST. (2003). *Building an Information Technology Security Awareness and Training Program* (No. NIST Special Publication 800-50). National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (No. NIST CSWP 04162018). National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

OECD. (2017). *Recommendation of the Council on Public Integrity* (No. OECD/LEGAL/0435). Organisation for Economic Co-operation and Development (OECD). https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0435

Ogorek, R. (2019). *Stellungnahme zum Gesetzesentwurf der Fraktion DIE LINKE «zur Stärkung der direkten Demokratie im Grundgesetz»* (No. 19(4)241 C; Ausschussdrucksache, S. 1–6). Deutscher Bundestag, Ausschuss für Inneres und Heimat. https://www.bundestag.de/resource/blob/628978/66cb59d87f55f7a7d2f95fa9dcaa8561/A-Drs-19-4-241-C.pdf

Reason, J. (1990). *Human error* (20th printing). Cambridge University Press. https://www.lehmanns.ch/shop/geisteswissenschaften/487776-9780521314190-human-error

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Routledge, Taylor & Francis Group. https://www.taylorfrancis.com/books/mono/10.4324/9781315543543/managing-risks-organizational-accidents-james-reason

Scharpf, F. W. (1999). *Governing in Europe: Effective and Democratic?* Oxford University Press. https://academic.oup.com/book/11939

Schmidt, V. A. (2013). Democracy and legitimacy in the European Union revisited: Input, output and 'throughput'. *Political Studies*, *61*(1), 2–22. https://doi.org/10.1111/j.1467-9248.2012.00962.x

Verordnung über die politischen Rechte (VPR; SR 161.11) (1978). https://www.fedlex.admin.ch/eli/cc/1978/712_712_712/de

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. *ECIS 2009 Proceedings*, 2206–2217. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=ecis2009

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), 13–23. https://doi.org/10.2307/4132319

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (Sixth edition). SAGE. https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150

Hilfsmittelverzeichnis

Hilfsmittel	Verwendung	Betroffene Stellen
Privates Lektorat durch Drittperson	Durchsicht der gesamten Arbeit hinsichtlich Rechtschreibung, Grammatik, Zeichensetzung, Satzbau und Lesefluss; keine inhaltliche Überarbeitung.	Gesamte Arbeit
Zotero (Literaturverwaltungssoftware)	Verwaltung der Literaturangaben, Organisation der Quellen sowie Unterstützung beim Erstellen des Literaturverzeichnisses.	Literaturverzeichnis sowie die entsprechenden Quellenangaben im Fliesstext.
Akademische Suchmaschinen (Google Scholar, Semantic Scholar, Scinapse)	Systematische Recherche nach wissenschaftlicher Literatur zu Integrität von Unterschriftensammlungen, Informationssicherheit, Awareness und Human Factor. Nutzung für Vorwärts- und Rückwärtszitationen, zum Auffinden von Volltexten sowie zur Prüfung bibliografischer Angaben (z. B. Autorenschaft, Publikationsjahr, DOI).	Kapitel 2–5 (insbesondere vgl. Abschnitt 4.2 zur Literaturrecherche) sowie die Evidenztabelle in Anhang A.
Visualisierungs- und Mapping-Tools (Open Knowledge Maps, Connected Papers, Litmaps)	Unterstützung bei der thematischen Strukturierung des Literaturkorpus durch Visualisierung von Themenclustern und Zitierbeziehungen. Identifikation von Kernpublikationen, angrenzenden Themenfeldern und Forschungslücken im Bereich Awareness, Human Factor und Integrität von Unterschriftensammlungen.	Kapitel 3 und 5 sowie die Gruppierung und Einordnung der Quellen in Anhang A.
Canva (Online-Gestaltungswerkzeug)	Gestaltung einer Abbildung zur Visualisierung des theoretischen Bezugsrahmens (Layout und einfache grafische Elemente).	Abbildung in Abschnitt 3.5.
Microsoft Office (Word)	Textverarbeitung, Layout und Formatierung der Bachelorarbeit (Strukturierung der Kapitel, Formatierung von Tabellen, Abbildungen, Verzeichnissen und Seitenlayout) sowie Nutzung der integrierten Rechtschreib- und Grammatikprüfung.	Gesamte Arbeit
ChatGPT (OpenAI, webbasiertes KI-Assistenzsystem; Custom-GPT «BK-Thesis-Coach, Legal Mode»)	Unterstützung bei der Strukturierung von Textpassagen, der sprachlichen Überarbeitung (Formulierungsvarianten und Präzisierung) sowie bei Konsistenzprüfungen von Begrifflichkeiten und Kapitelübergängen auf Basis eines eigenen Prompts mit klar definierten rechtlichen und stilistischen Leitplanken (keine Rechtsauslegung, politisch neutral).	Gesamte Arbeit

Abbildungsverzeichnis

Abbildung 1: Theoretischer Bezugsrahmen zur Integrität in der Unterschriftensammlung (eigene Darstellung). 28

Tabellenverzeichnis

Tabelle 1: Evidenztabelle – Quellen mit hoher verhaltensnaher Evidenz («super ja») (eigene Darstellung, basierend auf Literaturrecherche 2020–2025). 91

Tabelle 2: Evidenztabelle – Quellen mit mittlerer verhaltensnaher Evidenz («ja») (eigene Darstellung, basierend auf Literaturrecherche 2020–2025). 114

Tabelle 3: Evidenztabelle – Quellen ohne direkte verhaltensnahe Evidenz («nein») (eigene Darstellung, basierend auf Literaturrecherche 2020–2025). 137

Abkürzungsverzeichnis

Abkürzung	Beschreibung
BACS	Bundesamt für Cybersicherheit
BK	Schweizerische Bundeskanzlei
BPR	Bundesgesetz über die politischen Rechte
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
DSG	Bundesgesetz über den Datenschutz (Datenschutzgesetz)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
ENISA	European Union Agency for Cybersecurity
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Informationstechnologie
KI	Künstliche Intelligenz
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
VPR	Verordnung über die politischen Rechte

Anhang A – Evidenztabelle Awareness- und Human-Factor-Literatur (2020–2025)

A1 – Ziel und Einordnung

Die Evidenztabelle dokumentiert die 128 ausgewerteten Beiträge zur Gestaltung und Wirksamkeit von Awareness- und Human-Factor-Massnahmen im Zeitraum 2020–2025. Sie macht die in Kapitel 4 beschriebenen Such- und Auswertungsschritte transparent und ergänzt die Verdichtung in Kapitel 5 um eine detaillierte Übersicht. Im Fokus stehen Beiträge mit Bezug zu sicherheitsrelevantem Verhalten, die grundsätzlich auf den Kontext von Komitees und Sammelnden bei eidgenössischen Volksbegehren übertragbar sind.

Die Quellen sind nach Evidenzstufen gruppiert: Zuerst werden Studien mit hoher verhaltensnaher Evidenz («super ja»), anschliessend Beiträge mit mittlerer Evidenz («ja») und danach Beiträge ohne direkte verhaltensnahe Wirkungsmessung («nein») aufgeführt. Innerhalb der drei Blöcke erfolgt die Sortierung alphabetisch nach der Kurzzitierform (Autor, Jahr).

A2 – Evidenzlogik

Die Einteilung in die Evidenzstufen «super ja», «ja» und «nein» folgt der in Unterabschnitt 4.2.5 beschriebenen Evidenzlogik. Berücksichtigt werden insbesondere Studiendesign, Art der Messgrössen (z. B. beobachtetes Verhalten, Verhaltensabsichten) sowie die Nähe zum Sammelkontext von Komitees und Sammelnden.

A3 – Aufbau der Tabelle

Die Tabelle ist einheitlich strukturiert. Jede Zeile entspricht einer Quelle und enthält insbesondere folgende Angaben:

- **Nr.** – Laufende Nummer über alle 128 Quellen.
- **Quelle/Zitation (Autor, Jahr)** – Kurzangabe der Studie bzw. Publikation.
- **Intervention und Kontext** – Kurzbeschreibung der Massnahme bzw. des Settings (z. B. Phishing-Simulation, Micro-Learning, Governance-Framework).
- **Studiendesign und Messgrössen** – Zentrale Merkmale des Designs (z. B. randomisiertes Experiment, Vorher-Nachher-Design) und verwendete Messgrössen (z. B. Klickrate, Meldequoten, Verhaltensabsichten).
- **Wirkung (Evidenzstufe)** – Zuordnung zur Evidenzstufe («super ja», «ja», «nein»).
- **Relevanz und Kontext** – Kurzvermerk zur Einordnung (z. B. Sektor, Region, besondere Hinweise zur Übertragbarkeit).

Die in Unterabschnitt 4.2.3 beschriebenen Kategorien (Trainings, Simulationen, Kampagnen, Messmodelle, Rahmenwerke) werden in den Kurzbeschreibungen unter «Intervention und Kontext» berücksichtigt, aber nicht als eigene Spalte ausgewiesen.

A4 – Quellen mit hoher verhaltensnaher Evidenz («super ja»)

Nr.	Quelle/Zitation (Autor, Jahr)	Intervention und Kontext	Studiendesign und Messgrössen	Wirkung (Evidenzstufe)	Relevanz und Kontext
1	Ascic (2023): Cybersecurity-Awareness-Training in irischem KMU	Zwei simulierte Phishing-Kampagnen und ein einmaliger Cybersecurity-Awareness-Workshop zu E-Mail-Risiken in einem irischen KMU mit 42 Mitarbeitenden; 25 Mitarbeitende nehmen am Präsenztraining teil.	Feldexperiment mit Vorher-Nachher-Design (erste vs. zweite Phishing-Kampagne) und beobachteten Öffnungs-, Klick- und Melderaten als Hauptmessgrössen.	super ja – Klickrate sinkt von 65 % auf 12 %, Meldungen an die IT steigen von 2 auf 15; keine Workshop-Teilnehmenden klicken in der zweiten Kampagne, ein aggregierter Human-Factor-Risikowert wird um 52 % reduziert.	Irischer KMU-Kontext mit klar verhaltensnahen Kennzahlen; gut auf Awareness-Massnahmen zu E-Mail-Risiken in KMU und Verwaltung (inkl. Komitees und Sammelnde) übertragbar.
2	Berens et al. (2024): Video + Phishing-Warn-Tool	Online-Experiment mit Between-Subjects-Design mit 409 Teilnehmenden: verglichen werden ein NoPhish-Phishing-Awareness-Video, das link-zentrische Warn-Tool TORPEDO (Browser-Extension) sowie die Kombination aus beidem gegenüber zwei Status-quo-Bedingungen ohne zusätzliche Unterstützung. Teilnehmende beurteilen E-Mails mit verschiedenen URL-Manipulationen (ähnliche Domains, IP-Adressen, manipulierte Subdomains).	Between-Subjects-Onlineexperiment mit fünf Bedingungen und zufälliger Zuteilung; gemessen werden Erkennungsleistung für Phishing- und legitime E-Mails, Sensitivität (d′) und Entscheidungskriterium (C).	super ja – TORPEDO verbessert die Erkennung von Phishing-Links signifikant gegenüber den Status-quo-Bedingungen, und die Kombination aus NoPhish-Video und TORPEDO erreicht über viele URL-Tricks hinweg nahezu optimale Erkennungsraten.	Internationaler Online-Kontext; zeigt die kombinierte Wirkung von Awareness-Video und technischer Unterstützung und ist methodisch gut auf E-Mail-Umgebungen in Verwaltung, Organisationen sowie Komitees und Sammelnde übertragbar.
3	Berens, Mossano & Volkamer (2024): Fünfminütiges Anti-Phishing-Video	Fünfminütiges Anti-Phishing-Awareness-Video, in zwei Studienphasen mit insgesamt rund 280 Teilnehmenden evaluiert; Teilnehmende beurteilen in	Zweiphasiges Vorher-Nachher-Design mit Laboraufgaben; Erhebung der Erkennungsleistung vor und nach dem Video sowie nach fünf Monaten,	super ja – Die Erkennungsleistung für Phishing- vs. legitime E-Mails steigt direkt nach dem Video und bleibt über fünf Monate erhöht; Erkennungsstrategien und	Deutschland – Laborstudie; zeigt nachhaltige Effekte eines sehr kurzen Awareness-Videos und ist methodisch gut auf Schulungsformate in Organisationen, Verwaltung

		Laboraufgaben E-Mails als legitim oder Phishing.	zusätzlich Messung von Erkennungsstrategien und Selbstvertrauen beim Erkennen.	Selbstvertrauen verbessern sich, verhaltensnahe KPIs wie Klick- oder Melderaten werden jedoch nicht erfasst.	sowie Komitees und Sammelnde übertragbar.
4	Chen et al. (2024): Gruppen- und Rollenspieltraining zu Phishing	Prä-registriertes Anti-Phishing-Training mit 105 Mitarbeitenden einer europäischen Universität; zwei interaktive Formate (Gruppendiskussion vs. Rollenspiel) werden mit einer Kontrollgruppe ohne Training verglichen, Fokus auf Umgang mit verdächtigen E-Mails.	Mixed-Design-Experiment mit Randomisierung in drei Gruppen, drei Messzeitpunkten (vor dem Training, direkt danach, Follow-up) und drei in-situ-Phishingtests; gemessen werden Selbstwirksamkeit, Support-Seeking-Intentionen und tatsächliches Meldeverhalten gegenüber Phishing-E-Mails.	super ja – Beide Trainings erhöhen Selbstwirksamkeit und Support-Seeking-Intention deutlich; insbesondere das Rollenspiel führt zu signifikant höherem Support-Seeking, und Teilnehmende der Trainings melden mehr in-situ-Phishing-E-Mails als die Kontrollgruppe.	EU-Universitätskontext; zeigt, dass interaktive Workshops (Diskussion und Rollenspiel) verhaltensnahe Kennzahlen wie Meldeverhalten verbessern und ist gut auf Schulungssettings in Organisationen, Verwaltung sowie für Komitees und Sammelnde adaptierbar.
5	Ho et al. (2025): Wirksamkeit von Phishing-Trainings in der Praxis	Achtmonatige Feldstudie in einem grossen US-Universitätsklinikum (UCSD Health) mit 19’789 Vollzeit-Mitarbeitenden; in zehn realistischen Phishing-Simulationskampagnen werden jährliches Awareness-Online-Training (KnowBe4) und embedded Phishing Training (Proofpoint) mit verschiedenen Trainingsseiten nach Fehlklick gegenüber einer neutralen 404-Kontrollbedingung untersucht.	Randomisierte Langzeit-Feldstudie mit mehrfachen Phishing-Simulationen; gemessen werden Klick- bzw. Fail-Raten über Kampagnen hinweg, Verweildauer auf Trainingsseiten, Abschlussquoten der Trainingsmodule sowie der Zusammenhang zwischen Trainingsabschluss und Fail-Rate.	super ja – Es zeigt sich kein Zusammenhang zwischen dem Abschluss des jährlichen Awareness-Trainings und der Fail-Wahrscheinlichkeit in Phishing-Simulationen; embedded Phishing Training reduziert die Fail-Rate statistisch signifikant, im Schnitt jedoch nur um rund 1,7 Prozentpunkte gegenüber der Kontrollgruppe, mehrere Kampagnen weisen weiterhin Fail-Raten von über 10 % und sehr kurze Trainingszeiten auf.	US-Gesundheitsverbund mit sehr grosser Stichprobe; methodisch starke, verhaltensnahe Evidenz, die die Grenzen klassischer Standard-Trainingsprogramme aufzeigt und konzeptionell gut auf grosse Organisationen und Verwaltungen (inkl. Schweiz) übertragbar ist, auch für Komitees und Sammelnde als Warnsignal gegen reines Pflicht-Training.
6	Jayakrishnan, Banahatti & Lodha (2022):	PickMail als webbasiertes E-Mail-Phishing-Trainingsspiel für 478 Mitarbeitende eines IT-Unternehmens; Spielende absolvieren einen kurzen Pre-	Vorher-Nachher-Design mit integrierter Spieltelemetrie; gemessen werden Korrektheit bei der Einstufung von E-Mails als legitim oder	super ja – Die Korrektheit steigt von 76,83 % auf 92,62 %, während False-Positive-Rate (0,25 → 0,08) und False-Negative-Rate (0,17 →	Internationaler Unternehmenskontext; zeigt klare verhaltensnahe Verbesserungen durch ein Serious Game und ist gut auf E-Mail-

	PickMail-Serious-Game	Test, durchlaufen drei Trainingslevel in einer realitätsnahen Webmail-Oberfläche mit verschiedenen Phishing-Merkmalen (Domänen, URLs, Anhänge, Formulare) und schliessen mit einem Post-Test ab.	Phishing sowie False-Positive- und False-Negative-Raten im Pre- und Post-Test.	0,07) deutlich sinken, mit besonders starken Zugewinnen bei Mitarbeitenden ohne IT-Hintergrund.	Trainings in Organisationen, Verwaltung sowie für Komitees und Sammelnde adaptierbar.
7	Koning & Bullee (2024): Cybersecurity-Escape-Room im Gesundheitswesen	Beweglicher Cybersecurity-Escape-Room, der vor Ort in 26 Gesundheitsorganisationen eingesetzt wird; 96 Mitarbeitende aus dem Gesundheitswesen durchlaufen in Teams Rätsel zu E-Mail-Nutzung, Passwörtern, Ransomware, Social Engineering, Incident Reporting und Software-Updates auf Basis realitätsnaher Szenarien.	Prä-Post-Design mit Kontrollgruppe (n = 29) und Follow-up nach rund einem Monat; gemessen werden HAIS-Q-Gesamt- und Subskalenwerte (Wissen, Einstellungen, Verhalten) zu sechs Cybersecurity-Themen.	super ja – Der Gesamt-HAIS-Q-Score verbessert sich unmittelbar nach dem Escape-Room signifikant ($t(95) = -6{,}259$, $p < 0{,}001$) und bleibt nach einem Monat erhöht ($t(25) = -2{,}946$, $p = 0{,}006$); insbesondere steigen Werte zu E-Mail-Nutzung, Passwörtern, Social Engineering und Software-Updates, wobei Dropout und unklare Zuordnung der Effekte zu einzelnen Spielelementen als Limitationen genannt werden.	NL-Gesundheitssektor (EU-Kontext); zeigt, dass ein gamifizierter Escape-Room Wissen, Einstellungen und selbstberichtetes Verhalten verbessert und ist besonders für Spitäler und Gesundheitsorganisationen, aber auch für andere sicherheitskritische Organisationen in der Schweiz relevant.
8	Lain et al. (2024): Embedded Phishing-Training – Content, Nudges und Incentives	Gross angelegte Embedded Phishing-Studie in einem grossen Schweizer Unternehmen mit 4’554 zufällig ausgewählten Mitarbeitenden; über sechs Wochen erhalten sie drei simulierte Phishing-E-Mails im normalen Arbeitsalltag, nach gefährlichen Aktionen greifen unterschiedliche Varianten von Training, Nudges (Reminder-Mails) und Belohnungen.	Mixed-Methods-Feldstudie mit randomisierter Zuteilung zu mehreren Experimentalbedingungen; quantitativ werden gefährliche Aktionen (Klicks und Eingaben), Wiederholungsfehler, Melderaten und Nutzung der Trainingsinhalte gemessen, qualitativ werden 25 Mitarbeitende zu Wahrnehmung, Akzeptanz und Verständnis von Embedded	super ja – Embedded Phishing-Training wirkt primär über den Nudging- bzw. Reminder-Effekt: deterrentartige Reminder reduzieren die Wahrscheinlichkeit späterer gefährlicher Aktionen signifikant gegenüber der Kontrollgruppe, während der eigentliche Trainingscontent kaum genutzt wird; verzögertes Training ist mindestens so wirksam wie sofortiges Training, Belohnungs-Incentives	Schweiz – Studie in einem grossen Schweizer Unternehmen mit hoher ökologischer Validität; liefert direkt übertragbare Evidenz für die Gestaltung von Embedded Phishing-Training in Schweizer Verwaltung und Organisationen und unterstreicht, dass Phishing vor allem ein Aufmerksamkeits- und Zeitdruckproblem ist, nicht primär ein Wissensproblem.

			Phishing-Training interviewt.	verbessern sicheres Verhalten und Melderaten nicht.	
9	Lain, Kostiainen & Čapkun (2022): Langfristige Phishing-Simulationen in Organisationen	15-monatige Feldstudie in einer Grossorganisation mit über 14’000 Mitarbeitenden; im normalen Arbeitsalltag werden wiederholt simulierte Phishing-E-Mails versendet, ergänzt um kontextuelle Warnhinweise in E-Mails, embedded Training nach Fehlverhalten und einen Reporting-Button zum Melden verdächtiger E-Mails.	Langfristige Feldstudie mit zahlreichen Phishing-Kampagnen; gemessen werden Klickraten, gefährliche Aktionen (z. B. Eingabe von Zugangsdaten, Aktivieren von Makros) und Meldungen über den Reporting-Button, differenziert nach Massnahmen (Warnhinweise, embedded Training, Reporting).	super ja – Kontextuelle Warnhinweise reduzieren die Anfälligkeit deutlich und verbessern die Erkennung von Phishing-E-Mails; embedded Training im Phishing-Flow führt zu keinem nachhaltigen Resilienzgewinn und kann die Suszeptibilität teilweise erhöhen; der Reporting-Button erweist sich als besonders wirksam, da Crowdsourcing eine schnelle Erkennung neuer Kampagnen bei vertretbarem Aufwand ermöglicht.	Schweiz – Studie im Umfeld einer grossen Schweizer Organisation; liefert differenzierte, verhaltensnahe Evidenz zu Warnhinweisen, embedded Training und Reporting und ist mit hoher Übertragbarkeit für Schweizer Verwaltung und andere Grossorganisationen sowie für die Ausgestaltung von Meldekanälen für Komitees und Sammelnde relevant.
10	Rahartomo, Ghaleb & Ghafari (2025): Game-based Phishing-Awareness	3D-Serious-Game zur Sensibilisierung für Clone-, SMS- und Spear-Phishing mit dynamisch generierten Dialogen und Fragen auf Basis eines Large Language Models; Experimentalgruppe spielt das Spiel über zwei Wochen, Kontrollgruppe erhält kein Spiel.	Randomisiertes Gruppenexperiment mit 28 Teilnehmenden (Experimental- vs. Kontrollgruppe); gemessen werden Leistung in einem standardisierten Google-Phishing-Quiz sowie Awareness und Selbstvertrauen via Fragebogen nach der Intervention.	super ja – Die Experimentalgruppe erzielt im Phishing-Quiz im Mittel rund 86 % gegenüber rund 62 % in der Kontrollgruppe (Differenz ca. 24 Prozentpunkte, $p \approx 0{,}00014$); über 90 % der Spielenden erreichen mindestens 75 % richtige Antworten (vs. rund 29 % in der Kontrollgruppe), zudem steigt das selbsteingeschätzte Vertrauen in die Erkennung von Phishing-Versuchen deutlich.	Deutschland – Forschung mit einem prototypischen, LLM-basierten Serious Game; zeigt das Potenzial spielbasierter Awareness-Trainings und ist methodisch gut auf gamifizierte Formate in Organisationen, Verwaltung sowie für Komitees und Sammelnde übertragbar, auch wenn reale Klick- oder Meldekennzahlen fehlen.
11	Schöni et al. (2024): Personalisiertes	Online-Phishing-Training mit 96 Teilnehmenden aus einem Online-Panel; auf Basis eines Phishing-Kompetenzscores werden sie in drei	Vorher-Nachher-Design mit beobachteter Phishing-Suszeptibilität als Hauptmessgrösse; gemessen werden Klick- und	super ja – Phishing-Suszeptibilität sinkt im Schnitt um rund 24 %, und anfängliche Unterschiede zwischen den	CH-Forschung mit klar verhaltensnahen Kennzahlen; zeigt die Wirksamkeit personalisierter Trainings und ist gut auf Awareness-

	Phishing-Training	Kompetenzstufen eingeteilt und erhalten je ein personalisiertes Paket aus kurzem Erklärvideo, Erkennungsübung und Remindern zur Stärkung der Erkennungsfähigkeit.	Erkennungsleistungen vor und nach dem Training, aufgeschlüsselt nach Kompetenzstufen.	drei Kompetenzgruppen gleichen sich weitgehend an.	Massnahmen in Verwaltung sowie für Komitees und Sammelnde adaptierbar.
12	Strating (2024): Meta-Analyse zu Awareness-Training im Gesundheitswesen	Systematische Auswertung von Interventionsstudien im Gesundheitssektor, in denen Informationssicherheits- und Awareness-Trainings zur Prävention von Social-Engineering-Angriffen (z. B. Phishing, Pretexting) eingesetzt werden.	Systematische Literaturrecherche kombiniert mit quantitativer Meta-Analyse; zusammengeführt werden Effektgrössen aus mehreren Studien zu Awareness-Trainings, ergänzt um eine Analyse zentraler Gestaltungsbausteine (dynamischer Inhalt, Warnmechanismen, Trainingsintensität).	super ja – Die Meta-Analyse zeigt insgesamt eine moderate, statistisch abgesicherte Effektstärke zugunsten von Awareness-Trainings bei der Verhinderung erfolgreicher Social-Engineering-Angriffe; besonders wirksam sind Trainings mit dynamischem Inhalt, klaren Warnhinweisen und hoher Intensität.	Internationaler Gesundheitssektor; liefert eine verdichtete Evidenzbasis zur Wirksamkeit von Awareness-Trainings und ist besonders relevant für Schweizer Spitäler und Gesundheitsorganisationen sowie für die Ableitung wirksamer Gestaltungsprinzipien in verwaltungsnahen Kontexten.
13	Tóth et al. (2025): Kontinuierliches Phishing-Training & emotionale Trigger	12-monatiges kontinuierliches Phishing-Awareness-Programm in 20 Organisationen mit über 1’300 Mitarbeitenden; mehr als 13’000 simulierte Phishing-E-Mails mit unterschiedlichen emotionalen und kontextuellen Merkmalen (z. B. Dringlichkeit, Autorität, Personalisierung). Nach jedem erfolgreichen Phishing-Versuch wird ein verpflichtendes, eingebettetes Awareness-Training über das HR-System zugewiesen.	Longitudinale Feldstudie mit fortlaufender Erfassung von Verhaltensdaten; ausgewertet werden erfolgreiche Kompromittierungen, unsichere Aktionen und deren Entwicklung über 12 Monate, ergänzt durch nicht-parametrische Korrelations- und Regressionsmodelle zu emotionalen und kontextuellen Triggern.	super ja – Kontinuierliche Phishing-Simulationen kombiniert mit verpflichtendem Training halbieren erfolgreiche Kompromittierungen innerhalb von rund sechs Monaten und senken die Phishing-Suszeptibilität über 12 Monate deutlich; emotionale Trigger wie Dringlichkeit und Autorität erhöhen die Erfolgswahrscheinlichkeit von Angriffen, Personalfluktuation führt zu messbaren Schwankungen im Awareness-Niveau.	International (20 Unternehmen, Realwelt-Verhaltensdaten); bietet seltene Langzeit-Evidenz zur Wirksamkeit kontinuierlicher Phishing- und Awareness-Programme und ist konzeptionell gut auf Schweizer Verwaltung und Unternehmen übertragbar, auch wenn die Ergebnisse bislang nur als arXiv-Preprint ohne Peer-Review vorliegen.
14	Williams, Zafar & Gupta (2024): SETA-	Action-Research-Projekt in einem grossen US-Gesundheitsunternehmen mit 307	Action-Research-Studie mit experimenteller Vorher-Nachher-Auswertung;	super ja – Klickraten auf simulierte Phishing-E-Mails sinken nach Einführung des	US-Gesundheitssektor mit hohem Schutzbedarf; zeigt, dass theoriegeleitete SETA-

	Programm im Gesundheitswesen	medizinischen und administrativen Mitarbeitenden; auf Basis der Selbstregulationstheorie wird ein neues SETA-Programm entwickelt, das klassische Schulungselemente mit konkreten Verhaltenszielen, Reflexionsaufgaben und angepassten Phishing-Szenarien kombiniert.	anhand von simulierten Phishing-E-Mails werden Klickraten vor und nach Einführung des neuen SETA-Programms getrennt nach medizinischem und administrativem Personal mittels Chi-Quadrat-Tests verglichen.	neuen SETA-Programms signifikant gegenüber dem bisherigen Training (für medizinisches und administratives Personal), was eine messbare Verhaltensverbesserung im realen Gesundheitskontext zeigt.	Programme Phishing-Verhalten im Feld verbessern können und ist methodisch gut auf Spitäler, Gesundheitsorganisationen und andere sicherheitskritische Organisationen in der Schweiz übertragbar.
15	Yin et al. (2025): Post-Simulation-Feedback vs. Embedded Training	Drei gross angelegte Feldexperimente auf einer produktiven Phishing-Simulationsplattform: In realen Kampagnen erhalten mehrere tausend Mitarbeitende realistisch gestaltete Phishing-E-Mails; verglichen werden embedded «just-in-time»-Feedbackseiten nur für Klickende mit non-embedded Post-Simulation Feedback per Sammel-Mail an alle.	Randomisierte Feldexperimente mit mehreren Phishing-Kampagnen; gemessen werden Fail- bzw. Klickraten über Wochen und Monate nach den Interventionen, differenziert nach Trainingsbedingung (embedded vs. non-embedded Feedback).	super ja – Non-embedded Post-Simulation Feedback an alle Mitarbeitenden verbessert Erkennung und Wachsamkeit gegenüber Phishing-E-Mails über längere Zeit deutlich; klassisches embedded «just-in-time»-Training zeigt geringere und weniger nachhaltige Effekte und kann defensives Verhalten bzw. Reaktanz auslösen.	International – methodisch sehr starke Feldstudien mit hoher externer Validität; Ergebnisse sind direkt auf Organisationen und Verwaltungen (inkl. Schweiz) übertragbar und liefern einen wichtigen Impuls, reine embedded-only-Ansätze zugunsten inklusiver, nicht-stigmatisierender Feedback-Formate zu überdenken – auch für Komitees und Sammelnde relevant.

Tabelle 1: Evidenztabelle – Quellen mit hoher verhaltensnaher Evidenz («super ja») (eigene Darstellung, basierend auf Literaturrecherche 2020–2025).

A5 – Quellen mit mittlerer verhaltensnaher Evidenz («ja»)

Nr.	Quelle/Zitation (Autor, Jahr)	Intervention und Kontext	Studiendesign und Messgrössen	Wirkung (Evidenzstufe)	Relevanz und Kontext
16	Action Fraud / UK NCSC (2024/25): Suspicious Email Reporting Service (SERS)	Nationaler Meldekanal für Phishing in Grossbritannien: Verdächtige E-Mails werden an report@phishing.gov.uk weitergeleitet, SMS/Spam an die Kurznummer 7726; der Dienst wird gemeinsam von Action Fraud (City of London Police) und dem National Cyber Security Centre betrieben und in nationalen Awareness-Kampagnen beworben.	Operativer Reporting- und Takedown-Service; ausgewiesen werden Volumen gemeldeter E-Mails und SMS sowie Anzahl identifizierter und entfernter Scam-Kampagnen bzw. Scam-Webseiten seit dem Start im April 2020.	ja – Bis April 2025 wurden über 41 Millionen verdächtige E-Mails gemeldet, woraus rund 217’000 Betrugskampagnen und knapp 400’000 Scam-Webseiten entfernt wurden; die Kennzahlen belegen Reichweite und Takedown-Wirkung, enthalten aber keine verhaltensnahen Messgrössen zu Suszeptibilität oder individueller Verhaltensänderung.	Internationales Beispiel eines zentralen nationalen Reporting- und Takedown-Services mit transparenten Output-KPIs; konzeptionell relevant für Diskussionen zu Meldekanälen und Meldeservices in der Schweiz, jedoch ohne direkte Evidenz zu Awareness- oder Trainingswirkungen auf das Verhalten der Bevölkerung.
17	Alluqmani et al. (2025): Review zu Security-Awareness-Training	Narrative Literaturübersicht zu Security-Awareness-Training (SAT) gegen Phishing, mit Fokus auf empirische Studien aus den Jahren 2021–2024 zu Simulationen, personalisierten Trainingsinhalten, kultur- und kontextsensitiven Modulen sowie psychologischen und demografischen Einflussfaktoren.	Qualitative Literaturübersicht auf Basis von über 30 peer-reviewten Arbeiten; ausgewertet werden berichtete Effektgrössen, Trainingsdesigns (z. B. simulationbasiert, adaptiv, verhaltensnah) und Einflussfaktoren auf Phishing-Suszeptibilität.	ja – Die Übersicht kommt zum Schluss, dass SAT im Durchschnitt die Anfälligkeit für Phishing reduziert, insbesondere wenn Trainings simulationsbasiert, adaptiv, verhaltensnah und regelmässig wiederholt sind; gleichzeitig werden heterogene Effektgrössen, fehlende Standardisierung von Erfolgskennzahlen sowie offene Fragen zur Langzeitwirkung und zu Trainingsermüdung hervorgehoben.	Internationaler, organisationsübergreifender Überblick; bietet eine verdichtete Synthese aktueller Evidenz und Best Practices zu SAT und ist inhaltlich gut für Schweizer Verwaltung und Unternehmen nutzbar, auch wenn keine eigenständigen verhaltensnahen Messungen durchgeführt werden.
18	BACS (2025): Jahresbericht 2024	Tätigkeits- und Lagebericht über das erste Jahr des BACS mit eigenem KPI-Set zu	Deskriptiver Berichts- und KPI-Ansatz ohne Kontrollgruppe; ausgewiesen	ja – Der Bericht macht Reichweite, Resonanz und institutionelle Verankerung der	Schweiz – zentrale Referenz für nationale Awareness- und Austauschaktivitäten

		Awareness-, Austausch- und Meldeformaten; u. a. Nationale Cybersicherheitskonferenz (rund 280 Teilnehmende, NPS 59) und wöchentlicher Cybersecurity Switzerland Hub (CSH) mit rund 350 Teilnehmenden pro Woche und stark wachsender Community.	werden Teilnehmendenzahlen, Community-Wachstum, Zufriedenheitswerte (z. B. NPS), sowie Meldestatistiken zu Cybervorfällen (z. B. Phishing, Betrug, Schwachstellen, Bug-Bounty).	Awareness- und Austauschformate durch konkrete Output- und Engagement-KPIs sichtbar, berichtet aber keine verhaltensbezogenen Outcome-Kennzahlen (z. B. Veränderungen von Klick-/Meldequoten oder sicherheitsrelevantem Verhalten) und enthält keine systematische Wirksamkeitsevaluation von Trainings- oder Kampagnenmassnahmen.	sowie deren KPI-Set; liefert wichtigen Kontext für Schweizer Sensibilisierungsstrategien und Meldekanäle, aber keine verhaltensbasierten Wirksamkeitsnachweise, die direkt in die Evidenz zu Awareness- und Human-Factor-Massnahmen eingehen.
19	Berens, Aldag & Volkamer (2021): Interaktive NoPhish-Präsenzschulung	Interaktive Präsenzschulung auf Basis der NoPhish-Materialien mit 19 Mitarbeitenden einer deutschen Polizeibehörde; kombiniert Folien, Beispiele zu typischen Phishing-Tricks (z. B. URLs, Anhänge) und aktive Abstimmungen bzw. Quizfragen zur Erkennung verdächtiger E-Mails.	Vorher-Nachher-Retentionsdesign mit E-Mail-Quiz vor der Schulung, unmittelbar danach und nach vier Monaten; gemessen wird die Erkennungsleistung für legitime vs. Phishing-E-Mails auf Item-Ebene.	ja – Kurzfristig verbessern sich die Erkennungsleistungen bei vielen Beispielen, der längerfristige Effekt nach vier Monaten lässt sich statistisch jedoch nicht robust absichern; die berichtete Effektstärke ist hoch, wird aber durch die sehr kleine Stichprobe (19 Personen) und die daraus resultierende geringe Teststärke relativiert.	DE-Polizeibehörde im sicherheitskritischen Umfeld; inhaltlich gut auf Schweizer Polizei, Verwaltung und andere sicherheitsrelevante Organisationen übertragbar, aber aufgrund der kleinen Stichprobe nur als vorsichtige Evidenz zu werten.
20	Berens et al. (2022): Reminder-Timing bei Phishing-Awareness	12-Kapitel-E-Learning zu Phishing-Awareness (adaptiert aus Reinheimer et al.) in die universitäre Lernplattform integriert; Studierende bearbeiten die Kapitel mit kurzen Übungen, die jeweils bestanden werden müssen, und beurteilen E-Mail-Screenshots als legitim oder Phishing.	Within-Subjects-Retentionsstudie mit drei Messzeitpunkten (vor dem Training, direkt danach, nach fünf Monaten); gemessen werden Erkennungsleistung für legitime vs. Phishing-E-Mails sowie Signal-Detection-Kennzahlen (Sensitivität d′, Entscheidungskriterium c).	ja – Sensitivität und Erkennungsleistung bleiben auch nach fünf Monaten signifikant besser als vor dem Training, ohne signifikante Abnahme gegenüber direkt nach dem Training; die Aussagekraft wird jedoch durch die kleine Follow-up-Stichprobe (16 vollständige Datensätze) und den Studierendenkontext eingeschränkt.	EU-/DE-Hochschulkontext; liefert einen empirischen Referenzpunkt für Reminder-Timings in Awareness-Programmen (eher Richtung sechs Monate) und ist methodisch gut auf E-Learning-gestützte Schulungen in Organisationen und Verwaltung übertragbar, auch wenn verhaltensnahe Real-welt-KPIs fehlen.

21	Brehmer, Steinherr & Stöckl (2024): Neue Impulse für Awareness-Programme	Zwei erprobte SETA-Ansätze für Studierende an einer deutschen Universität: (1) interaktives Lernvideo mit choice-based storytelling und realen Campus-Szenen zu «bad USB» und Incident-Meldung; (2) semesterbegleitendes Business Game, in dem Studierende in Rollen (u. a. IT-Beratung, Studierende, Universitätsmitarbeitende) in vier 90-minütigen Sessions Bedrohungsanalyse, Phishing, Umgang mit sensiblen Daten und Incident Response bearbeiten.	Pre-Post-Test (n = 60) zur Informationssicherheits-Awareness rund um Incident Response beim interaktiven Video sowie standardisierte Befragung nach dem Business Game (35 Rückmeldungen) zu Motivation, Interesse und selbsteingeschätztem Wissenszuwachs.	ja – Das interaktive Video führt zu einer signifikanten und starken Verbesserung der Awareness zu Incident Response; das Business Game wird von der Mehrheit als (sehr) angenehm und interessant bewertet und geht mit einem messbaren Wissenszuwachs einher, verhaltensnahe Kennzahlen wie reale Fehler- oder Klickraten fehlen jedoch.	EU-/DE-Hochschulkontext; konzeptionell gut auf Schweizer Hochschulen und weiterbildende Programme für Verwaltung und Organisationen übertragbar, liefert aber primär wissens- und einstellungsbezogene, nicht direkt verhaltensnahe Evidenz.
22	DeCusatis et al. (2022): Cybersecurity-Awareness-Escape-Room	Virtueller 3D-Escape-Room «ARI 3D» auf Basis der Unity-Engine: Spielende steuern einen Roboter-Avatar durch mehrere Levels mit Mini-Games zu grundlegenden Cybersecurity-Themen (u. a. Passwörter, Phishing, Internetbetrug, Netzwerksicherheit, Ethik); getestet mit 120 Teilnehmenden (90 vor dem Studium, 30 Studierende).	Vorher-Nachher-Design mit standardisierten Awareness-Tests vor und nach dem Spiel; zusätzlich Bewertung der Anwendung anhand des Octalysis-Gamification- Rahmenwerks mit acht Motivationsmetriken.	ja – Die Vorher-/Nachher-Tests zeigen eine Zunahme der Cybersecurity-Awareness; fünf von acht Octalysis-Metriken erreichen Werte von mindestens 7,9 von 10, konkrete Effektgrössen oder verhaltensnahe Kennzahlen (z. B. reale Fehler- oder Klickraten) werden jedoch nicht berichtet.	Internationaler Hochschul- und Nachwuchskontext (USA); konzeptionell gut auf Schweizer Schulen, Hochschulen und Nachwuchsprogramme übertragbar, liefert aber nur begrenzte verhaltensnahe Evidenz für den Einsatz von Escape-Room-Formaten.
23	Delso-Vicente et al. (2025): Review zu Policy-Compliance & Cybersecurity	Systematische Literaturübersicht zu Compliance mit Informationssicherheitsrichtlinien, basierend auf 1’059 identifizierten und nach PRISMA gefilterten Artikeln (Publikationen 2001–2023) aus mehreren Fachdatenbanken; im Fokus stehen verhaltens- und	PRISMA-konforme systematische Literaturreview; analysiert werden Studien zu Informationssicherheits-Policy-Compliance entlang etablierter theoretischer Modelle (u. a. Theory of Planned Behavior, Protection Motivation Theory) und	ja – Die Review zeigt konsistent, dass höhere Informationssicherheits-Awareness, wahrgenommene Wirksamkeit von Sicherheitsmassnahmen, unterstützende Sicherheitskultur und aktive Managementbeteiligung mit besserer Policy-Compliance	Internationaler, branchenübergreifender Überblick über private und öffentliche Organisationen; inhaltlich sehr relevant für Schweizer Verwaltung und Unternehmen, um Awareness-Programme im Zusammenspiel mit Kultur, Führung und

		technologiebezogene Faktoren, die Mitarbeitendenverhalten in Bezug auf Informationssicherheit prägen.	Clustern wie Einstellungen, subjektive Normen, wahrgenommene Kontrolle, Informationssicherheits-Awareness (ISA), organisatorische Kultur, Managementunterstützung und technologische Rahmenbedingungen.	zusammenhängen; gleichzeitig betont sie, dass Awareness allein nicht ausreicht und wirksame Strategien zielgruppenspezifische Awareness-Programme mit Managementengagement, sozialen Kontrollen sowie Anreiz- und Sanktionsmechanismen kombinieren müssen, während robuste Langzeit-Verhaltensdaten weiterhin begrenzt sind.	technologischen Faktoren zu verorten und Policy-Compliance nicht isoliert als reines Schulungsthema zu behandeln.
24	Drury et al. (2022): Anti-Phishing-Lernspiele mit URL-Fokus	Vergleichsstudie mit 133 Teilnehmenden zu drei Anti-Phishing-Learning-Games: Entscheidungs-Spiel (binäre Klassifikation), Analyse-Spiel (URLs in Teile zerlegen und Kategorien zuordnen) und Erstellungs-Spiel (bösartige URLs erzeugen); alle Spiele vermitteln ein strukturiertes Vorgehen zur Analyse von URLs.	Drei-Gruppen-Vorher-Nachher-Design mit URL-Klassifikationsaufgaben (benigne vs. bösartige URLs) und zusätzlicher Erfassung des Entscheidungsvertrauens; Vergleich der Lernzuwächse zwischen den drei Spielmechaniken.	ja – Alle drei Spiele führen zu signifikant besseren Klassifikationsleistungen im Nachtest, das strukturierte URL-Parsen verbessert die Erkennungsleistung insgesamt; zwischen den unterschiedlichen Spielmechaniken zeigen sich keine klaren verhaltensbezogenen Vorteile, und es werden nur kurzfristige Laborleistungen ohne reale Angriffe oder Langzeitwirkung erfasst.	DE-Forschung im Laborumfeld; gut als Baustein für spielbasiertes Awareness-Training in Schweizer Organisationen nutzbar, liefert aber nur begrenzte verhaltensnahe Evidenz zur Wirkung auf reale Phishing-Situationen.
25	ENISA (2024): ECSM 2023 – Campaign report «Be Smarter than a Hacker»	EU-weite Awareness-Kampagne «Be Smarter than a Hacker» mit Social-Engineering-Fokus; zentrale Landing-Page mit Musikvideos, Kurzvideos zu «Red Flags», Cybercriminal-Profil-Video, Infografiken, interaktivem Quiz, Tipps, Postern und über 200 Social-Media-Posts, ausgerollt als	Kampagnen- und KPI-Reporting ohne Kontrollgruppe; ausgewertet werden Reichweite, Impressions, Interaktionen, Follower-Zuwächse und Performance einzelner Formate und Kanäle (z. B. Kampagnensong, länderspezifische	ja – Der Bericht weist hohe Reichweiten- und Engagement-Kennzahlen aus (Millionen Impressions und Interaktionen sowie stark performende Inhalte wie der Kampagnensong und «Red Flag»-Videos), berichtet jedoch keine systematischen Vorher-Nachher-Messungen	EU-weite Behördenkampagne mit Beteiligung einzelner nicht-EU-Länder (u. a. Schweizer Adaption des Kampagnensongs); dient als Referenz für nationale und behördliche Sensibilisierungskampagnen in der Schweiz, liefert aber nur Output- und Engagement-

		jahrübergreifende Kommunikationsstrategie in allen EU-Mitgliedstaaten.	Adaptionen, thematische Aktionstage).	von Wissens- oder Verhaltensänderungen (z. B. Vorher-Nachher-Vergleiche, Klick- oder Meldequoten).	KPIs und keine direkte Evidenz zu Awareness- oder Verhaltenswirkungen.
26	Gamisch & Pöhn (2023): Awareness-Kampagnen in einem KMU	Fallstudie in einem KMU mit zwei simulierten Phishing-Übungen (vor und nach Awareness-Massnahmen); Mitarbeitende werden drei Kampagnenvarianten zugeordnet (zirkulare Kampagne mit E-Mails und Materialien, Quiz-Kampagne, Online-Seminar), alle erhalten zusätzlich ein Handout.	Prä-Post-Design mit zwei Phishing-Simulationen; gemessen werden Klickrate, Fehlerrate, Melderate und ein zusammengesetzter Resilienzfaktor, ergänzt durch eine Befragung zur Wahrnehmung und Akzeptanz der unterschiedlichen Kampagnenformate.	ja – Alle Kampagnen verbessern die Erkennung von Phishing-Mails; besonders als «angenehm» wahrgenommene Kampagnen erreichen die besten Werte in der zweiten Phishing-Übung, Resilienzfaktoren steigen und Fehlerraten sinken, ein Teil der Mitarbeitenden bleibt jedoch anfällig, und die Ergebnisse sind auf einen einzelnen KMU-Kontext begrenzt.	DE-KMU-Fallstudie; konzeptionell gut auf Awareness-Kampagnen in Schweizer KMU und Verwaltung übertragbar, mit verhaltensnahen Kennzahlen, aber eingeschränkter Generalisierbarkeit aufgrund des Single-Case-Designs.
27	Gasiba, Lechner & Pinto-Albuquerque (2020): Sifu Secure-Coding-Plattform	Online-Plattform «Sifu» für Cybersecurity-Challenges im Bereich Secure Coding: Spielende bearbeiten C/C++-Code-Challenges, deren Lösungen automatisch gegen Secure-Coding-Guidelines geprüft werden; ein «intelligenter Coach» gibt schrittweise Hinweise. Die Plattform wurde in vier realen CSC-Events mit insgesamt 71 Spielenden (mehrheitlich Softwareentwickelnde aus der Industrie) eingesetzt.	Feldanwendung mit begleitenden Umfragen; während der vier Events werden standardisierte Fragebögen eingesetzt, die u. a. wahrgenommene Qualität der Challenges, Nützlichkeit für das Erkennen von Schwachstellen und Beitrag zum Verständnis sicherer Softwareentwicklung auf Likert-Skalen erfassen.	ja – Die Teilnehmenden stimmen mehrheitlich (meist über 4 von 5 Punkten) zu, dass die Challenges qualitativ gut sind, bei der Erkennung von Schwachstellen helfen und das Verständnis von Secure-Coding-Guidelines stärken; es fehlen jedoch objektive Vorher-Nachher-Kennzahlen zu Codequalität oder tatsächlichem Secure-Coding-Verhalten.	Internationaler Industrie- und Workshopkontext; konzeptionell gut auf Secure-Coding-Awareness für Schweizer Softwareentwickelnde und Organisationen übertragbar, liefert aber primär selbstauskunftsbasierte und keine verhaltensnahen Wirksamkeitsdaten.
28	Grill et al. (2025): Training for Improved	Verhaltensorientiertes Programm «Training for Improved Information Security Culture» (TIISC) mit zwei	16-monatiges, longitudinales randomisiertes Kontrollgruppendesign; wiederholte Befragungen zu	ja – Das Programm verbessert informationssicherheitsbezogenes Führungsverhalten und das	Schwedische Langzeitstudie mit hohem methodischem Anspruch; gut auf Schweizer Verwaltung und grössere

	Information Security Culture	Komponenten: informationssicherheitsbezogenes Training für Mitarbeitende und CBT-basiertes Führungskräftetraining für Vorgesetzte, umgesetzt in mehreren Arbeitsgruppen eines Unternehmens.	Sicherheitsverhalten, Sicherheitsklima und informationssicherheitsbezogener Führung sowie kontinuierliche Messung der Phishing-Suszeptibilität.	sicherheitsbezogene Lernen von Mitarbeitenden signifikant; Effekte auf weitere Verhaltensindikatoren und Sicherheitsklima bleiben jedoch begrenzt, und nicht alle gewünschten Verhaltensänderungen werden erreicht.	Organisationen übertragbar, die kombinierte Mitarbeitenden- und Führungskräftetrainings zur Stärkung der Informationssicherheitskultur einsetzen wollen.
29	Gwenhure & Rahayu (2024): Gamification für Cybersecurity-Awareness bei Non-IT-Fachpersonen	Systematische Literaturübersicht zur Gamification von Cybersecurity-Awareness für nicht-IT-Fachpersonen; aus mehreren hundert Treffern werden fünf empirische Studien ausgewählt, in denen spielerische Elemente wie Storytelling, Team-Leaderboards und interaktive Szenarien in Awareness-Settings für non-IT-Mitarbeitende und Lernende eingesetzt werden.	PRISMA-orientierte systematische Literaturreview; analysiert werden Studiendesigns, eingesetzte Spielelemente und deren Zuordnung zu konkreten Lernzielen sowie berichtete Effekte auf Wissen, Interesse, Engagement und Verhalten der Teilnehmenden.	ja – Die betrachteten Studien zeigen konsistent kurzfristige Zuwächse bei Wissen, Interesse, Engagement und teilweise auch gewünschtem Verhalten; gleichzeitig ist die Evidenzbasis klein, einzelne Spielelemente werden selten isoliert evaluiert, und es fehlen nahezu vollständig belastbare Daten zur Langzeitwirksamkeit und zu möglichen Gewöhnungs- bzw. Habituationseffekten.	Internationaler, auf nicht-technische Mitarbeitende fokussierter Überblick; inhaltlich gut nutzbar für Schweizer Verwaltung und Unternehmen zur Einordnung von Chancen und Grenzen gamifizierter Awareness-Ansätze, insbesondere im Hinblick auf Zielgruppenpassung und offene Fragen zur nachhaltigen Verhaltenswirkung.
30	Hart et al. (2020): Riskio Serious Game	Tabletop-Serious-Game «Riskio» für Teams von 3–5 Personen unter Leitung einer fachkundigen Spielleitung; Spielende übernehmen abwechselnd die Rolle von Angreifenden und Verteidigenden in einer fiktiven Universitätsstelle, identifizieren Angriffe über ein Attack-Kartendeck, wählen passende Sicherheitskontrollen aus einem Defence-Deck und diskutieren Risiken sowie Gegenmassnahmen.	Experimente mit Studierenden und Mitarbeitenden, ausgewertet auf Basis des Technology-Acceptance-Models; erhoben werden u. a. wahrgenommene Nützlichkeit, Benutzerfreundlichkeit und intendierte Nutzung des Spiels sowie Einschätzungen zur Verbesserung der Cybersecurity-Awareness.	ja – Die Befragungen zeigen hohe Akzeptanz und wahrgenommene Wirksamkeit des Spiels für die Erhöhung der Cybersecurity-Awareness, insbesondere bei Mitarbeitenden; es werden jedoch keine objektiven Vorher-Nachher-Kennzahlen zu Wissen, Fehlerquoten oder realem Sicherheitsverhalten erhoben.	UK-Forschung mit Fokus auf nicht-technische Mitarbeitende; konzeptionell gut auf Schweizer Organisationen mit gemischten Teams aus Fachpersonen und nicht-IT-Mitarbeitenden übertragbar, liefert aber primär subjektive Akzeptanz- und Wirksamkeitsindikatoren statt verhaltensnaher Evidenz.

31	Hijji et al. (2022): CAT-Framework für Remote-Mitarbeitende	Dreistufiges Cybersecurity-Awareness- und -Training-Framework (CAT) für Remote-Work-Mitarbeitende mit 25 Kernpraktiken: Level «Awareness» (Sensibilisierung), «Training» (Wissensaufbau) und «Practical & Assessment» (praktische Übungen mit Wissensmessung), inklusive KI-gestützter Komponenten zur adaptiven Wissensbewertung.	Fallstudienbasierte Evaluation in mehreren Organisationen; erfasst werden Fähigkeitsstufen von Mitarbeitenden, wahrgenommene Nützlichkeit des Rahmenwerks und die Eignung zur Ableitung passender Awareness- und Trainingsmassnahmen, primär über strukturierte Befragungen und Einstufungen.	ja – Das Framework wird in den Fallstudien als hilfreich wahrgenommen, unterstützt die Einteilung von Mitarbeitenden in Fähigkeitsniveaus und hilft Organisationen bei der Priorisierung von Awareness- und Trainingsmassnahmen; es fehlen jedoch systematische Vorher-Nachher-Messungen konkreter Verhaltenskennzahlen wie Phishing-Klicks oder Incident-Meldungen.	Internationaler Remote-Work-Kontext; konzeptionell gut auf Schweizer Verwaltung und Unternehmen mit Homeoffice-Anteil übertragbar, insbesondere zur strukturierten Planung und Segmentierung von Awareness- und Trainingsmassnahmen, trotz begrenzter verhaltensnaher Wirksamkeitsdaten.
32	Hillman, Harel & Toch (2023): Phishing-Training im Grossunternehmen	Kontrolliertes Feldexperiment in einer israelischen Finanzinstitution mit rund 5’000 Mitarbeitenden; über drei Kampagnen werden simulierte Phishing-E-Mails mit unterschiedlicher Formulierung (generisch vs. personalisiert) im Rahmen eines bestehenden Awareness-Programms versendet.	Feldexperiment mit wiederholten Phishing-Simulationen; gemessen werden Click-Through-Raten (CTR) pro Kampagne, Unterschiede zwischen generischen und personalisierten E-Mails sowie zwischen Geschäftsbereichen, ergänzt um den zeitlichen Bezug zu vorangehenden Awareness-Trainings.	ja – Simulierte Phishing-E-Mails führen zu hohen Klickraten, insbesondere personalisierte Mails erzeugen signifikant höhere CTRs; die CTR unterscheidet sich deutlich zwischen Geschäftsbereichen, während Zeitpunkt und Inhalt der vorangehenden Awareness-Trainings keinen signifikanten Einfluss auf das Klickverhalten zeigen und damit auf eine begrenzte Wirksamkeit der eingesetzten Trainingsformate hinweisen.	Internationaler Finanzsektorkontext mit grosser Belegschaft; liefert verhaltensnahe Evidenz zu Grenzen klassischer Phishing-Trainings und ist direkt anschlussfähig für grosse Schweizer Organisationen und Verwaltungen, die datengetriebene Awareness-Programme aufbauen oder nachschärfen wollen.
33	Hodhod et al. (2023); Drevin et al. (2023); Damenu et al. (2025): Serious Games für	Serious Games und gamifizierte Lernanwendungen für Kinder und Jugendliche von der Vorschule bis zur Sekundarstufe; typischerweise mobile Spiele, 3D-Umgebungen oder Unterrichtsprojekte zu	Überwiegend Vorher-Nachher-Designs mit Wissenstests, Einstellungs- und Motivationsskalen; ergänzt durch eine systematische Literaturübersicht zu 90+ Cybersecurity-Lernspielen	ja – Studien zeigen vor allem kurzfristige Zuwächse bei Wissen, Aufmerksamkeit und Einstellungen sowie hohe Spielmotivation; verhaltensnahe Kennzahlen (z. B. reales Online-Verhalten, Klick-	Internationaler Schul- und Jugendkontext; inhaltlich interessant als Inspiration für spielbasierte Cybersecurity-Bildung, aber nur eingeschränkt direkt auf Schweizer Verwaltung,

	Kinder und Jugendliche	Passwörtern, sicherer E-Mail-Nutzung, Betrug im Netz und Datenschutz (z. B. CyberHero, Safety Snail).	für Kinder und Jugendliche, die Studienqualität und methodische Lücken (z. B. Kontrollgruppen, Langzeitmessung) analysiert.	oder Melderaten) und robuste Langzeitdaten sind selten, und methodische Qualität variiert.	Organisationen sowie Komitees und Sammelnde übertragbar, da verhaltensnahe Evidenz und Erwachsenensettings weitgehend fehlen.
34	Hu, Hsu & Zhou (2022): Review zu SETA-Programmen	Systematische Literaturübersicht zu Security-Education-, Training- und Awareness-Programmen (SETA) mit 80 Artikeln aus den Jahren 1998–2020; ordnet Programme nach Zielen, Inhalten, verwendeten Theorien und Zielgrössen (Wissen, Einstellungen, Verhaltensabsichten, Verhalten) und betrachtet unterschiedliche Organisationskontexte.	Systematische Literaturreview mit strukturierter Suche und Auswahl; analysiert werden berichtete Effekte auf Wissen, Einstellungen, Verhaltensabsichten und Verhalten sowie Kontextfaktoren wie Managementunterstützung, Sicherheitskultur und Programmgestaltung.	ja – Viele SETA-Studien berichten positive Effekte auf Sicherheitswissen, Einstellungen und Verhaltensabsichten, die Evidenz zu stabilen Verhaltensänderungen ist jedoch heterogen und methodisch begrenzt (u. a. wenige Langzeitstudien); klare Zieldefinition, organisatorische Einbettung und starke Managementunterstützung werden als zentrale Erfolgsfaktoren hervorgehoben.	Internationaler, branchenübergreifender Überblick; dient als theoretische und empirische Grundlage für die Gestaltung und Bewertung von Awareness-Programmen in Schweizer Organisationen und Verwaltungen, insbesondere zur Einordnung von Wissens- vs. Verhaltenswirkungen und Kontextfaktoren.
35	Jaffray, Finn & Nurse (2021): SherLOCKED Serious Game	2D-Top-down-Serious-Game SherLOCKED, eingesetzt in einer Einführungsveranstaltung zur Cybersicherheit für 112 Studierende an einer britischen Universität; die Spielenden steuern eine Detektivin durch drei Level und beantworten Multiple-Choice-Fragen zu Grundbegriffen der Cybersicherheit (u. a. CIA-Triade, Angriffe, Risikomanagement), um Vorlesungsinhalte zu wiederholen und zu vertiefen.	Anonyme Online-Befragung mit Vorher-Nachher-Selbsteinschätzung des Verständnisses und der Konfidenz auf einer 5-Punkte-Skala unmittelbar vor und nach dem Einsatz des Spiels.	ja – 87,5 % der Studierenden geben an, dass das Spiel ihr Verständnis der Vorlesungsinhalte verbessert, die durchschnittliche Konfidenz in das eigene Verständnis steigt und 65,2 % möchten SherLOCKED zur Prüfungsvorbereitung erneut nutzen; es werden jedoch keine objektiven Wissens- oder Verhaltenskennzahlen erhoben.	Internationaler Hochschulkontext; konzeptionell gut auf Schweizer Hochschulen und tertiäre Weiterbildung übertragbar, liefert aber primär subjektive Wirksamkeits- und Motivationsindikatoren statt verhaltensnaher Evidenz.
36	Katsantonis et al. (2025):	Kollaboratives Tabletop-Serious-Game «Yellow Training» auf Basis des tCOFELET-Rahmenwerk: Lernende	Qualitative Pilotstudie mit zwei Spielsitzungen und insgesamt 11 Postgraduate-Studierenden;	ja – Die Pilotstudie zeigt hohe Beteiligung, intensive Diskussionen zu Risiken (z. B. unsichere URLs,	Universitärer Kontext in Griechenland; konzeptionell gut für Awareness-Workshops in Schweizer

	«Yellow Training» Tabletop-Game	übernehmen Rollen von Mitarbeitenden in einem fiktiven Unternehmen und treffen gemeinsam Entscheidungen zu Alltagsaufgaben, Schutzmassnahmen und der Abwehr von Angriffen (u. a. Brute-Force-, Pretexting- und Phishing-Szenarien); umgesetzt hybrid mit Tabletop-Simulator sowie physischen Karten und Boards.	strukturierte Beobachtung durch Lehrperson und Forschende, ergänzt um qualitative Auswertung von Teamdynamik, Kommunikation und Entscheidungsfindung.	verdächtige E-Mails) und wiederholte Hinweise auf gegenseitiges Lernen im Team; es werden jedoch keine quantitativen Sicherheitskennzahlen erhoben (kein Vorher-Nachher-Vergleich, keine Klickraten, keine Aussagen zur Langzeitwirkung).	Verwaltung und Organisationen adaptierbar (v. a. für Team- und Entscheidungsworkshops), liefert bisher aber nur qualitative Hinweise auf Sensibilisierung und Zusammenarbeit ohne harte, verhaltensnahe KPIs.
37	Kävrestad et al. (2022): Kontextuelles vs. Game-based Phishing-Training	Simuliertes Anti-Phishing-Training mit 41 Universitätsangehörigen, randomisiert auf drei Bedingungen: Game-based Training (Google-Jigsaw-Phishing-Quiz), Context-Based Micro-Training (kurze, kontextsensitive Hinweise direkt in der Mailumgebung) und Kontrollgruppe ohne Training; alle klassifizieren E-Mails in einem realistisch gestalteten Postfach.	Randomisiertes Drei-Gruppen-Experiment mit Eye-Tracking; gemessen werden Klassifikationsscores für legitime vs. Phishing-E-Mails, Nutzung von Phishing-Indikatoren (Blickmuster) und Unterschiede zwischen Game-based und kontextbasierter Mikro-Schulung.	ja – Beide Trainingsformen verbessern das Verhalten gegenüber der Kontrollgruppe; CBMT führt zu signifikant höheren Klassifikationsscores und stärkerer Nutzung von Phishing-Indikatoren als das Game-based Training, allerdings erkennen weniger als 10 % der Teilnehmenden alle E-Mails korrekt, und viele bleiben trotz Training anfällig.	Schwedisch-britische Forschung im Hochschulkontext; gut auf europäische und Schweizer Organisationen übertragbar und ein wichtiger Hinweis darauf, dass kontextnahe Mikro-Trainings in der Arbeitsumgebung wirksamer sein können als reine Spiele, wobei Training allein die Anfälligkeit aber nicht vollständig beseitigt.
38	Kassner & Schönbohm (2022): Serious Game «Sir Firewall»	Online-Serious-Game «Sir Firewall» zur Phishing-Sensibilisierung, getestet in einer Studie mit 61 Mitarbeitenden aus verschiedenen Unternehmen; die Spielenden durchlaufen drei Level («erkennen», «bewerten», «handeln») in einer Rittergeschichte und setzen sich dabei mit typischen Merkmalen von Phishing-E-Mails auseinander.	Mixed-Methods-Ansatz mit standardisiertem Fragebogen und Leitfadeninterviews; erfasst werden Motivation, wahrgenommene Wissenszunahme, Vergleich mit klassischen Schulungen und Einstellungen zum Einsatz des Spiels, primär über Likert-Skalen und qualitative Rückmeldungen.	ja – Rund 90 % der Teilnehmenden geben an, durch das Spiel mehr über Phishing gelernt zu haben und sich besser in der Lage zu fühlen, Phishing-E-Mails zu erkennen; die selbsteingeschätzte Wissensstufe steigt von etwa 3,2 auf 4,2 (Skala 1–5). Es fehlen jedoch Kontrollgruppe, objektive Verhaltenskennzahlen und Langzeitmessungen, sodass die	Internationales DE-Serious-Game mit Fokus auf Unternehmensmitarbeitende; konzeptionell gut in Awareness-Programme von Organisationen in der Schweiz integrierbar, liefert aber vor allem subjektive Wirksamkeitsindikatoren und keine belastbaren Langfrist- oder Verhaltensdaten.

				verhaltensnahe Wirksamkeit nur eingeschränkt belegbar ist.	
39	Khando, Rusu & González (2021): Review zu Informationssicherheits-Awareness	Systematische Literaturübersicht mit 51 empirischen Studien zu Informationssicherheits-Awareness in privaten und öffentlichen Organisationen; analysiert werden Branchen- und Organisationstypen, eingesetzte Instrumente (u. a. Trainings, Kampagnen, Policies, technische Kontrollen) und Zielgrössen wie Wissen, Einstellungen und Verhalten.	PRISMA-orientierte systematische Literaturreview; Studien werden entlang eines Rahmenmodells mit vier Einflussbereichen (individuell, organisatorisch, technisch, regulatorisch) und nach eingesetzten Awareness-Massnahmen und berichteten Outcome-Variablen strukturiert.	ja – Viele Studien berichten positive Effekte von Awareness-Massnahmen, insbesondere auf Wissen und Einstellungen; die Evidenzlage zu stabilen Verhaltensänderungen und die Qualität der Messgrössen bleibt jedoch heterogen. Kombinierte Ansätze mit Managementunterstützung, wiederkehrenden Trainings und klaren Richtlinien erweisen sich tendenziell als wirksamer als isolierte Einzelmassnahmen.	Internationaler Überblick über private und öffentliche Organisationen; inhaltlich sehr relevant für Schweizer Verwaltung und Unternehmen, um Awareness-Massnahmen im Zusammenspiel mit organisatorischen, technischen und regulatorischen Faktoren einzuordnen und nicht als reine Schulungsmassnahmen zu betrachten.
40	Köhler et al. (2022): Podcasts vs. Videos im Cybersecurity-MOOC	Sechswöchiger Cybersecurity-MOOC (openHPI) mit >900 Lernenden; ein optionaler Deep-Dive-Inhalt wird in drei Formaten angeboten: Interviewvideo (zwei Personen mit Bild), Interview-Podcast (gleiche Audio-Spur ohne Video) und traditioneller Ein-Personen-Podcast. Lernende werden im Round-Robin-Verfahren einem Format zugeordnet, nach jedem Deep Dive folgen Quiz und kurze Befragung.	Vergleichsstudie in einem MOOC mit quasi-experimenteller Zuteilung; gemessen werden Quiz-Ergebnisse und Kursperformance als Lernleistungsindikatoren sowie Umfragen zu Verständlichkeit, Akzeptanz und wahrgenommenem Lernerfolg in den drei Formaten.	ja – Lernleistung und Quiz-Ergebnisse unterscheiden sich zwischen Video- und Podcast-Gruppen praktisch nicht; audio-basierte Formate werden von vielen Lernenden als gut verständlich und leicht zu verfolgen bewertet, der Interview-Podcast schneidet bei Verständlichkeit und subjektiver Bewertung am besten ab, während der traditionelle Ein-Personen-Podcast am wenigsten geschätzt wird.	DE-MOOC-Kontext; konzeptionell gut auf Awareness-Kurse und Weiterbildungsangebote für Schweizer Öffentlichkeit und Verwaltung übertragbar und ein Hinweis darauf, dass (gut gestaltete) Audioformate eine gleichwertige Alternative zu Video für vertiefende Cybersecurity-Inhalte sein können.
41	Köhler, Pünter & Meinel (2023): Videoformate im	Randomized Controlled Trial mit über 1’500 Teilnehmenden in einem kostenlosen Cybersecurity-MOOC; nach einem	Randomisiertes Gruppenexperiment mit Wissensfragen, Transferaufgaben (u. a. Klassifikation von E-	ja – Folienslide-Videos führen zu den besten Ergebnissen bei Wissensabfragen, Animationsvideos zu den	DE-MOOC-Kontext; hoch relevant für die Gestaltung von Awareness-Videos in Schweizer Verwaltung und

	Cybersecurity-MOOC	Vortest werden Lernende zufällig einem von drei Videoformaten zugeteilt (Folienslides mit Voice-over, Interviewformat, Animationsvideo) und absolvieren den Kurs mit dem jeweils zugewiesenen Format.	Mails als Phishing/nicht Phishing) sowie einem mehrmonatigen Phishing-Test als Verhaltensmass; Auswertung der Unterschiede zwischen den Videoformaten.	besten Ergebnissen bei Transferaufgaben; im realen Phishing-Test schneiden Lernende mit Animationsvideo tendenziell am besten ab, die Unterschiede im Verhalten sind jedoch statistisch nur schwach bzw. nicht signifikant.	Organisationen, da die Studie zeigt, dass unterschiedliche Videoformate unterschiedliche Stärken hinsichtlich Wissen, Transfer und (begrenzter) Verhaltenswirkung haben.
42	Le-Nye, Yaacoub & Possik (2024): Vergleich von education-based und game-based Phishing-Training	Quantitative Studie mit 115 Teilnehmenden zur Wirksamkeit verschiedener Phishing-Awareness-Strategien: klassische Kursformate (education-based) und interaktive Lernspiele (game-based); für alle Teilnehmenden wird eine Kennzahl zur Phishing-Vulnerabilität erhoben, ergänzt um demografische Angaben (u. a. Alter, Tätigkeitsbereich).	Quasi-experimentelles Design mit Erfassung der Phishing-Vulnerabilität vor bzw. nach den jeweiligen Trainingsformaten sowie anschliessender Modellierung mit Machine-Learning-Ansätzen (Logistic Regression, Random Forest), um Prädiktoren der Anfälligkeit zu identifizieren.	ja – Sowohl klassische Kurse als auch game-based Ansätze senken die gemessene Phishing-Vulnerabilität, die Unterschiede zwischen den Formaten bleiben jedoch begrenzt; Alter und Tätigkeitsbereich erweisen sich als stärkere Prädiktoren für Anfälligkeit als das konkrete Lernformat, was auf Grenzen bestehender Strategien und die Notwendigkeit laufender Anpassung hinweist.	Internationale Studie mit heterogener Stichprobe; besonders relevant für die zielgruppengerechte Gestaltung von Trainings in Schweizer Organisationen und Verwaltung, da sie zeigt, dass demografische Faktoren und Tätigkeitskontexte bei der Auslegung von Awareness-Strategien stärker berücksichtigt werden müssen als das reine Format (Kurs vs. Spiel).
43	Marshall, Sturman & Auton (2024): Scoping Review zu E-Mail-Phishing-Trainings	Scoping Review zu E-Mail-Phishing-Trainings (2003–2023) mit Fokus auf Trainingsmodalitäten wie eingebettete vs. eigenständige Trainings, passive vs. interaktive / E-Learning- / instructor-led-Formate sowie gamifizierte Ansätze; kartiert werden zudem die eingesetzten Outcome-Kennzahlen zur Phishing-Suszeptibilität (z. B. Klick-/Fail-Raten, Wissensscores).	PRISMA-orientierte Scoping Review mit systematischer Suche in PsycINFO, PubMed und Web of Science; 42 Studien werden eingeschlossen und entlang von Trainingsart, Designmerkmalen und berichteten Outcome-Variablen (Wissen, Erkennung, Klick-/Fail-Raten, Verhalten über die Zeit) strukturiert.	ja – Die eingeschlossenen Studien zeigen insgesamt deutliche kurzfristige Verbesserungen (z. B. im Mittel rund 20 Prozentpunkte bessere Erkennung von Phishing-Mails oder -URLs), gleichzeitig bleibt ein relevanter Anteil der Nutzenden auch nach Training anfällig (etwa ein Viertel wird weiterhin getäuscht). Die Evidenz zu nachhaltigen Verhaltensänderungen ist begrenzt und	Internationaler, breit angelegter Überblick über E-Mail-Phishing-Trainings und deren Grenzen; inhaltlich gut auf Schweizer Organisationen und Verwaltung übertragbar, insbesondere zur realistischen Einordnung von kurz- vs. langfristigen Effekten und zur Ableitung von Designprinzipien für wirksamere Awareness-Programme.

				heterogen; intensivere, aktivierende Formate mit detailliertem Feedback und einer Kombination aus aufmerksamkeits- und cue-basierten Ansätzen schneiden besser ab als einmalige, rein passive Massnahmen, ein Restrisiko bleibt jedoch bestehen.	
44	Morić et al. (2025): Education & Phishing-Simulation an einer Universität	Studie an einer kroatischen Universität mit drei kontrollierten Phishing-Simulationen über mehrere Organisationsbereiche hinweg sowie einem organisierten Online-Training (zielgerichtetes Instruktionsmodul); in allen Wellen werden Klicks auf Phishing-Links, Eingabe von Zugangsdaten und Meldungen verdächtiger E-Mails erfasst, eine Kampagne findet unmittelbar vor einem Feiertag statt.	Mehrwellige Feldstudie mit wiederholten Phishing-Simulationen und Vergleich von Schulungs- vs. Nicht-Schulungsgruppen; ausgewertet werden Compromise-Raten (Klick + Dateneingabe), Melderaten und Zusammenhänge mit demografischen Merkmalen (Alter, Bereich, Bildungsniveau) sowie Effekte des zeitlichen Kontexts (z. B. vor Feiertagen).	ja – Die organisierte Online-Schulung reduziert die Zahl kompromittierter Personen nur marginal; es zeigen sich keine statistisch bedeutsamen Unterschiede zwischen Schulungs- und Nicht-Schulungsgruppen. Deutlich stärker wirken Kontext- und Timingeffekte: Die vor-Feiertags-Kampagne weist signifikant höhere Kompromittierungsraten auf. Die Autorenschaft schliesst, dass einzelne Awareness-Massnahmen allein nicht ausreichen und kontinuierliche, kontextsensitive Ansätze nötig sind.	EU-/Universitätskontext mit hoher Übertragbarkeit auf Hochschulen und öffentliche Verwaltungen in der Schweiz; liefert verhaltensnahe Evidenz zu begrenzter Wirkung einzelner Online-Trainings und zur Bedeutung von Kontext- und Timingfaktoren bei der Gestaltung von Awareness- und Phishing-Simulationsprogrammen.
45	Mouncey & Ciobotaru (2025): Social-Media-Phishing & Awareness-Bildung	Online-Befragung von 73 Instagram-Nutzenden zu Erfahrungen mit Social-Media-Phishing, bereits absolvierter Anti-Phishing-Bildung (z. B. Trainings, Kampagnen), wahrgenommener digitaler Kompetenz und Einstellungen zu Awareness-Angeboten.	Querschnittsstudie mit standardisiertem Online-Fragebogen; ausgewertet werden Zusammenhänge zwischen absolvierter Awareness-Bildung, wahrgenommener digitaler Kompetenz und Einschätzungen zur Nützlichkeit von Trainings mittels deskriptiver	ja – Absolvierte Phishing-Bildung geht mit höher eingeschätzter digitaler Kompetenz und wahrgenommenen Sicherheitsgewinnen auf Instagram einher; Teilnehmende, die Trainings besucht haben, beurteilen diese als hilfreich, gleichzeitig nennen viele zeitliche Hürden	International (UK-Studie zu Social-Media-Phishing); inhaltlich relevant für die Ausgestaltung und Kommunikation von Awareness-Angeboten für die breite Öffentlichkeit in der Schweiz, liefert aber keine direkten Verhaltensdaten.

			Statistik, linearer Regression und Inhaltsanalyse der offenen Antworten.	und die Erwartung, dass Trainings langweilig oder wenig relevant seien; verhaltensbezogene Kennzahlen (z. B. reale Klick- oder Melderaten) werden nicht erhoben.	
46	NCSC/BACS (2025): Umsetzung der Nationalen Cyberstrategie 2024	Erster jährlicher Umsetzungsbericht zur Nationalen Cyberstrategie (NCS) 2023–2027; für das Jahr 2024 werden Status und Fortschritt sämtlicher NCS-Massnahmen dokumentiert, darunter Aktivitäten zu Awareness, Cyberhygiene, Kampagnen, Aus- und Weiterbildung, Lagekommunikation sowie Meldekanälen und Reporting-Plattformen wie antiphishing.ch und report.ncsc.admin.ch.	Strategischer Umsetzungs- und Tätigkeitsbericht mit programmatischen Kennzahlen (z. B. Anzahl Meldungen zu Cybervorfällen, identifizierte Phishing-Webseiten, Anzahl und Typ von Kampagnen und Austauschformaten); keine kontrollierten Wirksamkeitsstudien, sondern Monitoring von Output- und Programm-KPIs.	ja – Der Bericht weist konkrete Programm- und Output-KPIs aus (z. B. 62’954 Meldungen zu Cybervorfällen im Jahr 2024 und 20’872 identifizierte Phishing-Webseiten) und ermöglicht damit eine Einordnung von Umfang, Reichweite und Ausbau nationaler Awareness-, Melde- und Kampagnenmassnahmen; eine systematische Outcome-Evaluation im engeren Sinn (z. B. Vorher-Nachher-Analysen von Klick-/Meldequoten oder verhaltensbezogenen Kennzahlen) erfolgt jedoch nicht.	Schweiz – zentrale Referenz für die nationale Cyberstrategie und deren Umsetzung; zeigt, welche Awareness-, Kampagnen- und Reporting-Massnahmen auf strategischer Ebene eingesetzt und wie sie über Kennzahlen gesteuert werden, liefert aber keine direkten Nachweise zur verhaltensnahen Wirksamkeit einzelner Trainings- oder Sensibilisierungsmassnahmen.
47	NCSC (2025): Annual Review 2024	Jahresbericht über das achte Jahr des National Cyber Security Centre (NCSC, UK), der die Aktivitäten vom 1. September 2023 bis 31. August 2024 zusammenfasst; Schwerpunkt auf den Active-Cyber-Defence-Diensten (u. a. Web Check, Mail Check, Early Warning, «Check Your Cyber Security») und dem Suspicious Email Reporting Service	Strategischer Jahres- und Tätigkeitsbericht mit Service- und Takedown-KPIs; ausgewiesen werden u. a. Anzahl eingegangener SERS-Reports (im Berichtszeitraum >10.5 Mio., kumuliert seit 2020 >34 Mio.), Zahl entfernter Scam-URLs sowie weitere Kennzahlen zu geprüften Domains, IP-	ja – Der Bericht liefert konkrete Output-Kennzahlen zu SERS und anderen ACD-Diensten (Reports, entfernte Scam-URLs, eingebundene Domains und Organisationen) und zeigt damit Reichweite sowie technische Wirkung der Services; eine systematische Evaluation von Verhaltensänderungen bei Bevölkerung oder	Internationaler Referenzpunkt für nationale Reporting- und Active-Cyber-Defence-Ansätze; gut als Vergleichsfolie zu Schweizer BACS-/NCSC-Kennzahlen nutzbar und relevant für Diskussionen über nationale Meldekanäle und Takedown-Mechanismen, liefert aber keine direkte Evidenz zur verhaltensnahen

		(SERS), über den die Bevölkerung verdächtige E-Mails melden kann.	Schwachstellen und entfernten «commodity campaigns».	Organisationen (z. B. Vorher-Nachher-Analysen von Klick- oder Meldequoten, kontrollierte Studien zu Awareness- oder Trainingsmassnahmen) erfolgt jedoch nicht.	Wirksamkeit von Awareness- oder Trainingsprogrammen.
48	Piki et al. (2024): Digital Game-Based Learning für Cybersecurity	Konzept- und Übersichtsarbeit zu digitalem Game-Based Learning (DGBL) im Bereich Cybersecurity; analysiert werden theoretische und pädagogische Grundlagen, bestehende Forschungs- und Entwicklungsarbeiten sowie eine Auswahl vorhandener Cybersecurity-Spiele, ergänzt um eine eigene Pilotentwicklung, um Designanforderungen und Lernpotenziale zu erproben.	Narrative Review mit strukturierter Analyse der Literatur und existierender Spiele sowie einer Pilotentwicklung, für die vor allem Lernziele, didaktische Einbettung und wahrgenommene Wirksamkeit beschrieben werden; es werden keine standardisierten Vorher-Nachher-Verhaltenskennzahlen erhoben.	ja – Die Arbeit fasst Studien zusammen, die zeigen, dass DGBL-Interesse, Motivation und das Verständnis grundlegender Cybersecurity-Konzepte fördern kann; gleichzeitig wird hervorgehoben, dass viele Spiele nur in kleinen, kurzzeitigen Studien ohne standardisierte verhaltensnahe Kennzahlen evaluiert sind und dass Ressourcen, didaktische Qualität und Curriculums-Einbettung die breite Nutzung begrenzen.	Internationales Hochschul- und Bildungsumfeld; inhaltlich gut nutzbar für Schweizer Schulen, Hochschulen und Organisationen, die spielbasierte Awareness-Formate prüfen oder einführen möchten, liefert aber primär konzeptionelle Leitplanken und nur begrenzt harte Verhaltens-Evidenz.
49	Pirta-Dreimane et al. (2025): CAPE-Hybrid-Escape-Room	Technologiegestützter, hybrider Cybersecurity-Escape-Room («CAPE») für Studierende: Teams übernehmen als CSIRT ein Incident-Response-Team in einem fiktiven Energieunternehmen und bearbeiten in einem kombinierten physischen und virtuellen Labor Szenarien über den gesamten Incident-Management-Lebenszyklus; das Training integriert vorbereitende Lernvideos (Flipped Classroom), gamifizierte Aufgaben mit Punktesystem sowie beobachtete	Mixed-Methods-Pilotstudie mit Escape-Room-Sessions in Teams; erfasst werden gelöste Aufgabenanteile, selbsteingeschätzte Kompetenzen in zentralen Bereichen des Incident Management (vor/nach dem Training) sowie Rückmeldungen zu Interesse, Motivation und wahrgenommenem Wissenszuwachs.	ja – Teams lösen im Schnitt rund 60 % der Aufgaben (bis ca. 80 % im Bestfall), selbsteingeschätzte Kompetenzen in mehreren Bereichen des Incident Management steigen signifikant, und der grosse Teil der Teilnehmenden berichtet erhöhtes Interesse und Wissenszuwachs; die Evidenz basiert jedoch auf kleiner Stichprobe und überwiegend auf Selbstauskünften ohne reale Verhaltenskennzahlen oder Langzeitmessung.	Hochschulumgebung in Lettland/Norwegen; konzeptionell gut auf Schweizer Hochschulen und spezialisierte Incident-Response-Trainings übertragbar, liefert vor allem Hinweise zu Kompetenz- und Motivationszuwachs, aber keine verhaltensnahen Langfristeffekte.

		Teamarbeit und anschliessende Reflexion.			
50	Prümmer, van Steen & van den Berg (2025): Meta-Analyse zu Endnutzer-Trainings	Meta-Analyse zu Cybersecurity-Trainings für Endnutzende auf Basis eines systematischen Reviews und einer ergänzenden Literatursuche; insgesamt werden 69 Studien mit unterschiedlichen Trainingsformaten und -settings (z. B. E-Learning, Workshops, Spiele, Simulationen) berücksichtigt.	Quantitative Meta-Analyse mit getrennten Effektgrössen für (1) Verhaltens-Prädiktoren wie Wissen, Einstellungen und Intentionen und (2) tatsächliches Verhalten (z. B. Klick-/Fail-Raten, Policy-Compliance), ergänzt um Moderatoranalysen zu Trainingsmethode, Mehrmethoden-Ansätzen, Plattform (online/offline) und sozialem Setting.	ja – Insgesamt zeigt sich ein klar positiver Gesamteffekt von Trainings auf Endnutzende im mittleren Bereich, besonders ausgeprägt bei Wissen, Einstellungen und Intentionen; für tatsächliche Verhaltensänderungen ergeben sich hingegen nur kleine, teilweise nicht signifikante Effekte, was auf eine Lücke zwischen Awareness und gelebtem Verhalten hinweist.	EU / international – hochwertige Gesamtbilanz zur Wirksamkeit von Endnutzer-Trainings, direkt auf Schweizer Organisationen und Verwaltung übertragbar; besonders relevant für die BK zur realistischen Einordnung von Awareness-Massnahmen, da sie deutliche Effekte auf Wissen und Einstellungen, aber nur begrenzte Verhaltensänderungen belegt.
51	Prümmer, van Steen & van den Berg (2024): Systematisches Review zu Cybersecurity-Trainings	Systematisches Review zu aktuellen Cybersecurity-Trainingsmethoden und deren Einfluss auf organisatorisches Verhalten; erfasst werden verschiedenste Formate (z. B. game- und simulationsbasierte Ansätze, klassische E-Learnings, Workshops) sowie unterschiedliche Zielgruppen in Organisationen.	PRISMA-basiertes systematisches Review mit Suche in fünf Datenbanken (Web of Science, ACM Digital Library, ProQuest, PubMed, PsycINFO); von 16’771 Treffern werden 142 Studien eingeschlossen und nach Trainingsformat, Zielgruppe und Evaluationsdesign (häufig Pre-/Post-Designs mit eher kleinen Stichproben, teils Studierende oder Allgemeinbevölkerung) strukturiert ausgewertet.	ja – Die Mehrheit der eingeschlossenen Studien berichtet positive Effekte von Trainings auf sicherheitsrelevantes Verhalten (z. B. weniger riskante Klicks, bessere Policy-Compliance, gesteigertes Sicherheitsbewusstsein), die Evidenz ist jedoch heterogen und methodisch begrenzt (kurze Nachbeobachtungszeiträume, nicht-experimentelle Designs, kleine und teils nicht-repräsentative Stichproben); das Review empfiehlt robustere Designs, längere Follow-ups und stärkeren Fokus auf Verhaltensmessung.	EU / internationaler Überblick; inhaltlich gut auf Schweizer Organisationen und Verwaltung übertragbar, da das Review sowohl Wirksamkeit als auch methodische Lücken aktueller Trainingsstudien sichtbar macht und damit eine Meta-Sicht für die Planung und Bewertung eigener Awareness-Programme liefert.
52	Quinkert, Degeling & Holz	Langzeit-Feldstudie mit rund 429’000 simulierten Phishing-E-Mails über etwa 1,5 Jahre in	Beobachtende Longitudinalanalyse ohne Randomisierung; ausgewertet	ja – Mit fortschreitender Teilnahme an den Awareness-Programmen sinken die	EU / international – kommerzieller Awareness-Anbieter mit überwiegend

	(2021): Spotlight on Phishing	77 Unternehmen, die Awareness-Programme eines Beratungsanbieters nutzen; analysiert werden Klickverhalten, Zeit bis zum Klick sowie Unterschiede zwischen technischen und psychologischen Vektoren (z. B. Autorität, Neugier, Zeitdruck).	werden die Entwicklung der Klickraten über wiederholte Kampagnen hinweg sowie Unterschiede nach Angriffsvektor, Unternehmen und Zeit bis zum Klick.	durchschnittlichen Klickraten über alle Unternehmen hinweg von etwa 19 % auf rund 10 %, was auf einen mittelfristigen Trainingseffekt hinweist; bestimmte psychologische Vektoren (insbesondere Autorität und Neugier) bleiben jedoch über den gesamten Zeitraum besonders effektiv, und alternative Einflussfaktoren können mangels kontrolliertem Design nicht ausgeschlossen werden.	europäischen Unternehmen; hohe konzeptionelle Übertragbarkeit auf Firmen und Organisationen in der Schweiz, insbesondere hinsichtlich typischer Verläufe von Phishing-Kampagnen und der Bedeutung psychologischer Trigger für anhaltende Restanfälligkeit.
53	Reinheimer et al. (2020): Phishing-Awareness & Reminder-Timing	Phishing-Awareness-Programm in einer deutschen Behörde mit 409 Mitarbeitenden: obligatorische, vor Ort durchgeführte Tutorials im «Train-the-Trainer»-Ansatz, die grundlegende Phishing-Merkmale und sicheres Verhalten beim Umgang mit E-Mails vermitteln. Die Phishing-Erkennungsleistung für legitime vs. betrügerische E-Mails wird mehrfach über den Programmverlauf hinweg gemessen, anschliessend werden verschiedene Reminder-Formate (u. a. Video, interaktive Beispiele, Text) getestet.	Longitudinale Feldstudie mit wiederholten Messungen der Erkennungsleistung (vor dem Programm, direkt danach, nach vier und nach sechs Monaten) sowie einem Vergleich mehrerer Reminder-Massnahmen; Hauptmessgrössen sind Treffer- und Fehlerraten bei der Klassifikation von E-Mail-Beispielen (Phishing vs. legitim).	ja – Direkt nach dem Programm und nach vier Monaten erkennen Mitarbeitende Phishing- und legitime E-Mails signifikant besser als vor dem Training; nach sechs Monaten ist dieser Effekt nicht mehr nachweisbar. Reminder auf Basis von Videos und interaktiven Beispielen erzielen die beste Auffrischungswirkung und halten den Leistungsvorteil mindestens weitere sechs Monate, sodass Erinnerungen im Abstand von rund sechs Monaten empfohlen werden.	EU (deutsche öffentliche Verwaltung) – inhaltlich direkt anschlussfähig für Schweizer Behörden und Verwaltungseinheiten, insbesondere für die Planung von Phishing-Awareness-Programmen mit geeigneten Erinnerungsintervallen und wirksamen Reminder-Formaten.
54	Rizzoni et al. (2022): Phishing-Simulation im Spital	Phishing-Simulation in einem grossen italienischen Spital mit über 6’000 Mitarbeitenden; drei Kampagnen im Abstand	Mehrwellige Feldstudie mit drei Phishing-Kampagnen; gemessen werden Öffnungs- und Klickraten für	ja – Personalisierte Phishing-E-Mails werden deutlich häufiger geöffnet und angeklickt als generische Nachrichten;	Internationaler europäischer Spitalfall; fachlich direkt anschlussfähig für Phishing-Simulationen in Schweizer

		von jeweils rund vier Monaten vergleichen generische mit personalisierten Phishing-E-Mails im Rahmen des jährlichen Trainings- und Risiko-Assessments, ausgewertet werden Öffnungs- und Klickraten sowie organisatorische Reaktionen.	generische vs. personalisierte E-Mails sowie qualitative Rückmeldungen und organisatorische Reaktionen (z. B. Beschwerden, Anpassung oder Abbruch von Kampagnen).	die Studie zeigt damit die besondere Wirksamkeit gezielter, kontextnaher Phishing-Versuche, verweist aber auch auf organisatorische Spannungen, ethische Fragen und Grenzen von Simulationen im Klinikbetrieb.	Spitälern und anderen grossen Organisationen, insbesondere hinsichtlich Risiko-Nutzen-Abwägung und Gestaltung ethisch vertretbarer Kampagnen.
55	Scherb et al. (2023): «The Get In» Cyberattack-Simulation	Serious Game «The Get In» als Cyberattack-Simulation: Spielende schlüpfen in die Rolle einer angreifenden Person und führen u. a. Social-Engineering-/Phishing-Angriffe, SQL-Injections, Metasploit-Exploits und Bad-USB-Szenarien durch; eingesetzt im Lehrkontext zur Vermittlung von Cyberangriffen und Verteidigungsmassnahmen.	Kurzfristige Vorher-Nachher-Befragung mit zwei unverbundenen Stichproben (32 Fragebögen vor, 15 nach dem Spiel); erfasst werden vor allem selbsteingeschätztes Verständnis von Phishing-Angriffen, Angriffswegen und Cybersecurity-Konzepten.	ja – Die selbsteingeschätzte Verständnisskala zu Phishing-Angriffen und Angriffswegen verbessert sich nach dem Spiel, und die meisten Teilnehmenden berichten, durch das Spiel mehr über Cyberangriffe gelernt zu haben; es liegen jedoch nur subjektive Kurzfrist-Effekte ohne objektive Verhaltenskennzahlen oder Langzeitmessung vor.	Schweiz (FHNW-Entwicklung); gut als ergänzender, spielbasierter Awareness-Baustein in Ausbildung und Weiterbildung einsetzbar, liefert aber nur begrenzte Evidenz zur verhaltensnahen und langfristigen Wirksamkeit.
56	Schneider & Zanwar (2020): CySecEscape – Escape Room für KMU	Tragbarer Escape-Room-Prototyp, der direkt in Büroräumen von KMU aufgebaut wird: Kleingruppen von 2–4 Mitarbeitenden spielen ein 40-minütiges Szenario zu finanziellem Betrug und einem abgetauchten Mitarbeitenden und lösen Rätsel zu Passwörtern, Social Engineering, Geräteschutz und Umgang mit Daten, eingerahmt durch kurzes Briefing und Debriefing.	Design-Science-Prototyp mit mehreren Spielrunden in KMU; erfasst werden vor allem qualitative Rückmeldungen der Teilnehmenden zu Realitätsnähe, Identifikation mit der Arbeitssituation, wahrgenommenem Lerngewinn und Motivation, ohne standardisierte Vorher-Nachher-Tests oder Verhaltenskennzahlen.	ja – Die Studie berichtet hohe Akzeptanz, starke Identifikation mit der eigenen Arbeitssituation und eine gesteigerte Wahrnehmung von Cyberrisiken; die Evidenz beruht jedoch überwiegend auf qualitativen Rückmeldungen ohne objektive, verhaltensnahe Kennzahlen (z. B. Klick- oder Melderaten) oder Langzeitmessung.	Schweiz / EU – FHNW-nahe KMU-Studie; der portable Escape-Room-Ansatz ist gut auf Schweizer KMU, Verwaltungseinheiten und kleinere Organisationen übertragbar, liefert aber primär Hinweise zu Wahrnehmung und Motivation statt zu messbaren Verhaltensänderungen.
57	Schöps et al. (2024):	Simulierte Phishing-Kampagne in einem Grossunternehmen;	Querschnittsbefragung mit 408 Mitarbeitenden	ja – Mitarbeitende, die auf eine simulierte Phishing-E-	EU / international – Fallstudie in einem europäischen

	Simulated Stress bei Phishing-Kampagnen	direkt nach Klicken auf bzw. Melden einer simulierten Phishing-E-Mail werden Mitarbeitende zu Wahrnehmung der Kampagne, erlebtem Stress und Phishing-Selbstwirksamkeit befragt, ergänzt durch halbstrukturierte Interviews zu Erfahrungen und Einstellungen gegenüber Simulated Phishing Campaigns (SPCs).	unmittelbar nach dem Ereignis plus 21 qualitative Interviews; Erhebung von Stress, negativen Emotionen, Phishing-Selbstwirksamkeit sowie Wahrnehmung und Akzeptanz von SPCs.	Mail geklickt haben, berichten signifikant höheren Stress und niedrigere Phishing-Selbstwirksamkeit als Mitarbeitende, die die E-Mail gemeldet haben; SPCs werden mehrheitlich als grundsätzlich positiv und potenziell effektiv wahrgenommen, gleichzeitig weist die Studie auf relevante Nebenwirkungen hin und enthält keine Verhaltensmessung mit Vorher-Nachher-Vergleich.	Grossunternehmen; liefert wichtige Hinweise zu Stress, Verunsicherung und Selbstwirksamkeit im Zusammenhang mit Phishing-Simulationen und ist gut auf Organisationen und Verwaltungen (inklusive Schweiz) übertragbar, insbesondere als Ergänzung zu rein klickratenorientierten Awareness-Programmen.
58	Schweizer Armee (2024): Phishing-Sensibilisierung 2024	Phishing-Sensibilisierungskampagne «Keine Chance dem Phishing» für rund 3’200 Milizangehörige mit dienstlicher @mil.admin.ch-Adresse: Während des Truppendienstes erhalten sie realistisch gestaltete, unterschiedlich schwierige simulierte Phishing-E-Mails («Credential Theft», «Website Infection», «Bad Attachment») und sollen Verdachtsfälle über ein Outlook-Spam-Plug-in melden, um Crowd-Reporting aufzubauen.	Zwischenbilanz einer mehrwelligen Phishing-Simulation ohne Kontrollgruppe oder Vorher-Nachher-Design; gemessen werden gefahrlose vs. riskante Aktionen (z. B. Öffnen von Anhängen, Dateneingabe) sowie die Melderate über das Spam-Plug-in.	ja – Zum Stichtag 26. August 2024 zeigen 86 % der getesteten Personen gesamthaft ein gefahrloses Verhalten, bei 14 % wird riskantes Verhalten beobachtet; 18 % der Empfangenden melden die simulierten Phishing-E-Mails über das Plug-in. Die Armee bewertet dies als positive Zwischenbilanz, betont aber weiteres Verbesserungspotenzial bei der Nutzung des Melde-Buttons und beim Abbau reflexartiger Klicks; eine systematische Wirksamkeitsevaluation mit Vorher-Nachher-Vergleich fehlt.	Schweiz – direkt auf den Schweizer Militärkontext zugeschnitten; fachlich gut auf andere sicherheitskritische staatliche Organisationen mit vergleichbarer E-Mail-Infrastruktur übertragbar und als Referenz für verhaltensnahe Kennzahlen in nationalen Sensibilisierungskampagnen nutzbar.
59	Shillair et al. (2022): Cybersecurity	Nationalvergleich von 80 Staaten auf Basis des Cybersecurity Capacity Maturity Model (CMM) des Global	Beobachtungsstudie mit länderübergreifender Sekundärdatenanalyse: CEAT-Scores werden mit	ja – Höhere CEAT-Scores stehen in einem positiven und statistisch signifikanten Zusammenhang mit der	International (80 Staaten); strategisch relevant für die Schweiz, da die Studie zeigt, wie nationale

	Education, Awareness & Training	Cybersecurity Capacity Centre; im Fokus steht die Dimension «Cybersecurity Education, Awareness Raising and Training (CEAT)» mit Indikatoren zu Bildungsprogrammen, Awareness-Initiativen und Trainings auf nationaler Ebene.	einem Index zur Vitalität von Internetnutzung und -diensten in Beziehung gesetzt, kontrolliert u. a. für Wohlstandsniveau und Verbreitung der Internetnutzung; für Länder mit tiefen CEAT-Scores werden ergänzend qualitative Hemmnisse und Herausforderungen beschrieben.	Vitalität von Internetnutzung und -diensten, was darauf hinweist, dass Staaten mit stärker ausgebauten Bildungs-, Awareness- und Trainingsinitiativen tendenziell besser entwickelte Internetdienste haben; aufgrund des beobachtenden Designs und fehlender verhaltensnaher Kennzahlen zu konkreten Programmen lassen sich jedoch keine kausalen Aussagen zur Wirksamkeit einzelner Awareness-Massnahmen ziehen.	Bildungs-, Awareness- und Trainingsinitiativen in Kapazitätsmodelle eingebettet und mit Indikatoren zur digitalen Entwicklung verknüpft werden können, ohne jedoch verhaltensbezogene Outcome-Daten zu einzelnen Programmen zu liefern.
60	Spithoven & Drenth (2024): Embedded Phishing-Experiment in Gemeinde	Eingebettetes Phishing-Experiment in einer der 15 grössten niederländischen Gemeinden: Zwei realistische Phishing-Wellen werden an alle Mitarbeitenden versendet (T1: 26.10.2021, T2: 17.03.2022). Zwischen T1 und T2 wird einer zufällig ausgewählten Gruppe ein freiwilliges Online-Microlearning zu Phishing angeboten, während die übrigen Mitarbeitenden als Vergleichsgruppe dienen; parallel werden organisationsspezifische Risikoprofile nach Rolle und Funktion gebildet.	Feldexperiment mit zwei Phishing-Kampagnen und randomisiert zugewiesener Microlearning-Gruppe; gemessen werden Klicks auf Phishing-Links, Eingabe von Zugangsdaten, Melderaten verdächtiger E-Mails sowie Zugehörigkeit zu Risikoprofilen («never clickers», «occasional clickers», «repeat clickers») nach Alter, Funktion und Rolle.	ja – Das freiwillige Online-Microlearning zeigt keinen messbaren Effekt auf Klick-, Credential- oder Melderaten zwischen T1 und T2; besonders exponierte Gruppen nehmen das Angebot überdurchschnittlich selten wahr und das Experiment zeigt damit die Grenzen freiwilliger Online-Microlearnings auf. Die Studie empfiehlt für diese Risikogruppen verbindlichere, massgeschneiderte Offline-Trainings und nutzt die Risikoprofile als Grundlage für gezieltere Awareness-Massnahmen.	EU – Studie in einer grossen niederländischen Gemeinde; kontextnah und sehr gut auf Schweizer Städte, Gemeinden und Verwaltungen übertragbar, insbesondere hinsichtlich der Grenzen freiwilliger Microlearnings und des Nutzens organisationsspezifischer Risikoprofile für zielgruppengerechte Sensibilisierung.
61	Subramanian (2023): Nudge-	Experimenteller Vergleich von nudge-basierten Informations-sicherheits-Postern (inkl.	Online-Focus-Group mit Fragebogen; Poster werden entlang mehrerer	ja – Nudge-basierte Poster erzielen einen rund 11 % höheren Gesamt-Score als	International – generischer Ansatz zum Design von Awareness-Postern;

	Theorie für Awareness-Poster	Poster mit «discouraging nudge») mit klassischen Awareness-Postern ohne Nudge; 51 berufstätige Personen aus unterschiedlichen Branchen bewerten die Poster in einer webbasierten Fokusgruppen-/Survey-Studie.	Kriterien (u. a. Verständlichkeit, Relevanz, Einfluss auf Sicherheitsverhalten) bewertet und in einem Weighted-Sum-Modell hinsichtlich ihrer wahrgenommenen Wirksamkeit verglichen.	klassische Poster ohne Nudge, insbesondere das Poster mit «discouraging nudge»; dies deutet auf positivere Verhaltensintentionen und eine bessere Compliance-Wahrnehmung hin, basiert aber auf einer kleinen Stichprobe ohne formale Signifikanztests und ohne reale Verhaltensdaten.	konzeptionell gut auf Sicherheitskampagnen in Schweizer Organisationen und Verwaltung übertragbar, liefert jedoch primär Hinweise zu wahrgenommener, nicht zu verhaltensnah gemessener Wirksamkeit.
62	Srivastava et al. (2024): Awareness-Programme im Schulbereich	Systematische Übersicht zu Cybersecurity-Awareness-Programmen in der Schulbildung (K–12) weltweit, basierend auf Studien von 2011–2023 zu Cyber-Safety, Cyber-Hygiene und Awareness-Initiativen; betrachtet werden Curricula, Kampagnen, Modelle und Selbstbewertungs-Tools sowie typische Umsetzungsherausforderungen (Ressourcen, Lehrkompetenzen, Aktualität der Inhalte).	Systematisches Review nach Kitchenham & Charters und PRISMA; analysiert Evaluationsansätze wie Fragebogen, Wissens- und Einstellungstests sowie Modelle wie das Kirkpatrick-Modell, mit Fokus auf berichtete Effekte und methodische Qualität der Wirksamkeitsmessung.	ja – Die Review zeigt, dass einzelne schulische Awareness-Programme positive Effekte auf Wissen, Einstellungen und teilweise Verhalten von Lernenden berichten, gleichzeitig aber grosse Unterschiede in Qualität und Tiefe der Evaluation bestehen; robuste Langzeitdaten zu Verhaltensänderungen und standardisierte KPIs sind selten, und es besteht ein deutlicher Bedarf an systematischer, modellgestützter Wirksamkeitsmessung.	International (Schulbildung K–12); fachlich gut nutzbar für Schweizer Schulen und zuständige Behörden, um bestehende Cybersecurity-Awareness-Programme einzuordnen, typische Evaluations- und Wirksamkeitslücken zu erkennen und nationale Initiativen gezielt weiterzuentwickeln.
63	Sulaiman et al. (2022): Cybersecurity-Verhalten und PMT in Regierungsorganisationen	Querschnittsstudie mit 446 Mitarbeitenden in malaysischen Regierungsorganisationen auf Basis der Protection-Motivation-Theorie; ein standardisierter Fragebogen erfasst Bedrohungseinschätzung (Schweregrad, Verwundbarkeit), Bewältigungseinschätzung (Response-Efficacy, Self-	Querschnittsdesign mit PLS-SEM; analysiert werden Zusammenhänge zwischen Bedrohungs- und Bewältigungseinschätzungen, Verantwortung und selbstberichteten Cybersecurity-Verhaltensweisen.	ja – Höhere wahrgenommene Schwere, Verwundbarkeit, Response-Efficacy, Self-Efficacy und Verantwortung hängen signifikant positiv mit selbstberichteten Cybersecurity-Verhaltensweisen zusammen; es handelt sich jedoch um eine Momentaufnahme ohne Vorher-	International (Regierungssektor in Malaysia); inhaltlich sehr relevant für Schweizer Verwaltung zur Einordnung, wie Bedrohungswahrnehmung, Wirksamkeitseinschätzung und Verantwortungsnorm mit Sicherheitsverhalten zusammenhängen, liefert aber keine

		Efficacy), Verantwortungsgefühl und selbstberichtetes Cybersecurity-Verhalten.		Nachher-Messung oder Evaluation konkreter Awareness-Trainings, sodass keine direkte Wirksamkeit einzelner Massnahmen ausgewiesen wird.	verhaltensnahe Interventions-Evaluation.
64	Surdjono et al. (2025): Mobile-Learning-Cyber-Hygiene-Training	Mobile-Learning-basiertes Cybersecurity-Awareness-Programm für 68 Studierende aus Accounting und Finance, entwickelt nach dem 4D-Modell (Define, Design, Develop, Disseminate); das Programm kombiniert kurze Lerneinheiten mit interaktiven Elementen und fokussiert auf grundlegende Cyber-Hygiene-Praktiken.	Pre-Post-Evaluation ohne Kontrollgruppe mit Validitätsfragebogen, Cybersecurity-Awareness-Tests und Fragebogen zu Cyber-Hygiene-Praktiken; ausgewertet werden Wissenszuwachs und selbstberichtete Veränderungen im Cyber-Hygiene-Verhalten.	ja – Die Studie berichtet eine deutliche Zunahme des Wissens und der berichteten Cyber-Hygiene-Praktiken nach Programmteilnahme, u. a. einen hohen Gain-Score von 0,72 für das Verständnis von Cybersecurity-Konzepten und Effektivitätswerte im Bereich «effektiv» bis «sehr effektiv» für mehrere Cyber-Hygiene-Aspekte; die Evidenz beruht jedoch auf Kurzfristmessungen, Tests und Selbstauskünften ohne Kontrollgruppe.	Internationales Hochschulumfeld (Indonesien); konzeptionell gut auf Schweizer Berufs- und Hochschulbildung mit nicht-technischen Lernenden übertragbar, liefert vor allem Hinweise zu Wissens- und Einstellungszuwachs, weniger zu langfristigen, verhaltensnahen Effekten.
65	Tempestini et al. (2023): Cybersecurity Awareness Inventory (CAIN)	Entwicklung und erste Validierung des «Cybersecurity Awareness Inventory» (CAIN), eines standardisierten Wissenstests mit 46 Items auf Basis von ISO/IEC 27032; eingesetzt bei Studierenden, um Cybersecurity-Wissen in Bezug auf praxisrelevante Vorfälle zu erfassen.	Querschnittsstudie mit 277 Studierenden; CAIN-Scores werden mit durch die IT-Abteilung dokumentierten Sicherheitsvorfällen und Risikomeldungen verknüpft und zwischen drei Risikogruppen (kein, niedriges, mittleres Risiko) statistisch verglichen.	ja – Niedrigere CAIN-Scores sind mit einer höheren Zahl gemeldeter Sicherheitsvorfälle verbunden, und die Scores unterscheiden sich signifikant zwischen risikofreier und mittlerer Risikogruppe; CAIN wird als geeignetes Instrument zur Identifikation von Wissenslücken und zur Evaluation von Awareness-Massnahmen vorgeschlagen, ohne dass bereits konkrete Trainings- oder	International (Messinstrument; gut nutzbar für Schweizer Organisationen zur standardisierten Erfassung von Cybersecurity-Wissen und zur Ableitung gezielter Awareness- und Trainingsbedarfe, auch wenn es noch keine Langzeit-Verhaltensdaten gibt).

				Zeitverläufe verhaltensnah untersucht werden.	
66	Volz (2025): Design and Evaluation of a Security Awareness Escape Room	Konzeption und prototypische Umsetzung eines Security-Awareness-Escape-Rooms mit mehreren Rätseln zu Passwortsicherheit, Social Engineering und sicherem Umgang mit IT-Systemen; erprobt mit Teilnehmenden aus einer Hochschul- bzw. Büroumgebung.	Formative Evaluationsstudie mit standardisierten Fragebögen zu subjektiven Eindrücken, wahrgenommenem Lerngewinn, Motivation, Involvement und Nutzungsakzeptanz nach dem Escape-Room-Einsatz.	ja – Der Escape-Room wird als motivierend, realitätsnah und hilfreich für das Verständnis grundlegender Security-Themen bewertet; die Evidenz stützt sich vor allem auf Akzeptanz- und Selbstberichte, ohne objektive Vorher-Nachher-Kennzahlen zu Wissen oder Verhalten.	International (Hochschul-/Bürokontext; konzeptionell gut auf Präsenztrainings in Schweizer Verwaltung und Organisationen übertragbar, aber ohne verhaltensbasierte Wirksamkeitsmessung).
67	Yeoh, Thai & Zhang (2022): Simulated phishing attack and embedded training campaign	Wiederholte simulierte Phishing-Kampagnen in einem Unternehmen: Mitarbeitende erhalten realistisch gestaltete Phishing-E-Mails; bei Klick auf den Link werden sie auf eine Trainingsseite mit Erkennungsmerkmalen und Handlungsempfehlungen weitergeleitet, sodass Simulation und Mikro-Lerneinheit direkt im Arbeitsalltag kombiniert werden.	Feldstudie mit mehreren Phishing-Wellen über mehrere Monate, Auswertung von Klick- und Melderaten nach jeder Kampagne sowie Vergleich der Entwicklung über Abteilungen und Zeit.	ja – Die Klickraten sinken über den Kampagnenverlauf und die Melderaten steigen, was auf eine messbare, aber begrenzte Verhaltensverbesserung hindeutet; ein Teil der Mitarbeitenden bleibt trotz wiederholter Simulationen anfällig, und längerfristige Effekte über den Untersuchungszeitraum hinaus bleiben unklar.	International (Unternehmenskontext; konzeptionell gut übertragbar auf wiederholte Phishing-Simulationen mit eingebettetem Training in Schweizer Organisationen und Verwaltung, insbesondere zur realistischen Einschätzung von Nutzen und Grenzen solcher Kampagnen).
68	Zahid, Hussein & Mahdi (2024): Measuring Individuals Cybersecurity Awareness Based on Demographic Features	Keine Intervention, sondern Messmodell: Erhebung eines Cybersecurity-Awareness-Scores in der Allgemeinbevölkerung mit Fokus auf demografische Unterschiede (Geschlecht, Bildungsniveau, Alter) und drei Awareness-Dimensionen (Passwortsicherheit, technisches Verhalten, sozialer Einfluss).	Quantitative Querschnittsstudie mit 415 Teilnehmenden; 17-Item-Fragebogen zu Passwortsicherheit, technischem Verhalten und sozialem Einfluss. Aggregation der Antworten zu einem Cybersecurity-Awareness-Score; Auswertung mittels Hypothesentests und multipler Regression zur Bestimmung des	ja – Frauen weisen im Mittel signifikant höhere Awareness-Scores auf, während Bildungsniveau und Alter keinen signifikanten Einfluss zeigen. Passwortsicherheit trägt am stärksten zum Gesamt-Awareness-Score bei. Die Studie liefert damit wichtige Zusammenhänge zwischen Awareness und demografischen Merkmalen,	International (Hochschul- und Organisationskontext); zeigt, wie demografische Merkmale bei der Segmentierung berücksichtigt werden können, und ist gut nutzbar für Schweizer Organisationen zur zielgruppenspezifischen Ausrichtung von Awareness-Programmen.

			Einflusses von Geschlecht, Bildungsniveau und Alter auf den Score.	jedoch keinen Wirksamkeitsnachweis für konkrete Trainingsmassnahmen.	
69	Zheng & Becker (2023): Phishing to improve detection	Adversariales Mindset-Training: Teilnehmende sehen ein Video aus Sicht eines fiktiven Angreifers und verfassen anschliessend drei Spear-Phishing-E-Mails. Verglichen wird dieses Training mit einem konventionellen Awareness-Video sowie mit keiner Schulung, um zu prüfen, ob die «Angreiferperspektive» die Erkennungsfähigkeit stärkt.	Zwei Experimente mit insgesamt 183 Teilnehmenden: Messung der Erkennungsleistung in einer Mock-Inbox-Aufgabe (Phishing vs. legitime Mails) sowie in einer späteren simulierten Phishing-Kampagne in einer öffentlichen Organisation; Kennzahl u. a. Kompromittierungsrate in der Simulation.	ja – Das adversariale Mindset-Training führt zu besserer Erkennungsleistung als keine Schulung und zu geringerer Anfälligkeit in der simulierten Phishing-Kampagne (ca. 5 % vs. 14,4 % Kompromittierungsrate im Vergleich zum konventionellen Training). Die Effekte werden aber nur als statistische Tendenz ausgewiesen (begrenzte Stichprobe, geringe Power), und es liegen keine Langzeitdaten über mehr als zwei Wochen vor.	International (Uni- und Organisationskontext); das adversarial Mindset-Training ist konzeptionell gut auf Schweizer Organisationen und Verwaltung übertragbar – insbesondere als innovativer Baustein zusätzlich zu klassischen Awareness-Videos.

Tabelle 2: Evidenztabelle – Quellen mit mittlerer verhaltensnaher Evidenz («ja») (eigene Darstellung, basierend auf Literaturrecherche 2020–2025).

A6 – Quellen ohne direkte verhaltensnahe Evidenz («nein»)

Nr.	Quelle/Zitation (Autor, Jahr)	Intervention und Kontext	Studiendesign und Messgrössen	Wirkung (Evidenzstufe)	Relevanz und Kontext
70	Ajayi et al. (2025): Using AI and Machine Learning to Predict and Mitigate Cybersecurity Risks in Critical Infrastructure	PRISMA-basierte Literaturübersicht zu Ansätzen der künstlichen Intelligenz (KI) und des Machine Learning für die Cybersecurity in kritischen Infrastrukturen (z. B. Energie, Transport, Gesundheit), mit Fokus auf überwachte und unüberwachte Lernverfahren, Anomalieerkennung und erklärbare KI (XAI) für Intrusion Detection, Schwachstellenbewertung und Echtzeit-Risikomitigation.	Systematische Literaturstudie gemäss PRISMA-Prozess; Auswertung und Kategorisierung vorhandener Fallstudien und technischer Ansätze zu KI-/ML-basierten Sicherheitskontrollen in Industrial-Control- und anderen kritischen Systemen, ohne eigene empirische Primärdatenerhebung zu menschlichem Verhalten.	nein – Zeigt das Potenzial KI-/ML-gestützter Sicherheitskontrollen zur Risikoreduktion in kritischen Infrastrukturen, liefert jedoch keinen Wirksamkeitsnachweis für Awareness- oder Trainingsmassnahmen und keine verhaltensbezogenen Kennzahlen zu Mitarbeitenden.	International; technisch fokussierter Überblick für Betreiber kritischer Infrastrukturen, nur indirekt für Awareness-Programme in Schweizer Organisationen nutzbar, da der Fokus auf technischen Kontrollen liegt und nicht auf der verhaltensnahen Wirksamkeit von Awareness- oder Human-Factor-Massnahmen.
71	Argyridou et al. (2023): Cyber Hygiene Methodology	Explorative Cyber-Hygiene-Methodik im Gesundheitswesen auf Basis einer einmaligen Online-Befragung von 356 Mitarbeitenden in vier Rollen über drei europäische Gesundheitsorganisationen; ein 28-Fragen-Fragebogen zu sieben Cybersecurity- und Datenschutz-Risikokategorien wird in Risiko-Scores und passende humanzentrierte Kontrollen übersetzt.	Querschnittliche Online-Befragung mit 356 Mitarbeitenden in vier Rollen in drei europäischen Gesundheitsorganisationen; Auswertung eines 28-Fragen-Fragebogens zu sieben Risikokategorien in Form von Risiko-Scores (1–5), Risikostrategien und abgeleiteten human-zentrierten Kontrollen.	nein – Leitet aus einer einmaligen Befragung Risiko-Scores und passende Awareness- und Trainingskontrollen ab, evaluiert jedoch nicht die Wirksamkeit implementierter Massnahmen (keine Vorher-Nachher- oder verhaltensbezogenen Kennzahlen, keine Evaluation real durchgeführter Trainings oder Kampagnen).	EU / international; drei europäische Gesundheitsorganisationen, besonders relevant für Schweizer Spitäler und Gesundheitsorganisationen als Grundlage zur Planung zielgerichteter Awareness-Programme, ohne direkten Wirksamkeitsnachweis der vorgeschlagenen Kontrollen.
72	BACS (2025): Anti-Phishing Bericht 2024	Nationaler Fachbericht des BACS über Phishing-Meldungen an die Plattform antiphishing.ch und weitere Kanäle; beschreibt Meldewege,	Deskriptiver Monitoring-Bericht ohne Interventions- oder Vergleichsgruppe; Auswertung operativer Meldedaten (u. a. 975’309	nein – Liefert Lage- und Output-Kennzahlen (Meldungen, bestätigte Phishing-URLs, Markenmissbrauch etc.), aber keine verhaltensnahe	Schweiz; zentrale Referenz für Umfang, Muster und betroffene Marken bei Phishing, als Hintergrund- und KPI-Basis zur

		Triage, Analyse und Takedown von Phishing-Webseiten in der Schweiz im Jahr 2024.	Meldungen und 20’872 bestätigte Phishing-Webseiten) mit Kennzahlen zu Volumen, Markenmissbrauch und Hosting.	Wirkungsmessung konkreter Awareness- oder Trainingsmassnahmen.	Einbettung der Wirksamkeitsdiskussion von Awareness- und Integritätsmassnahmen geeignet, ohne selbst Kampagnen- oder Trainingswirkungen zu evaluieren.
73	BACS (2025): Cyber Security Month 2025 – Gemeinsam gegen Phishing	Nationale Sensibilisierungskampagne des BACS im Rahmen des Cyber Security Month (1.–31. Oktober 2025) mit Fokus auf Online-Daten und Phishing; umfasst ein interaktives Phishing-Quiz (entwickelt mit Netpathie und Jugendlichen), Online-Informationen und Materialien sowie einen öffentlichen Online-Brownbag-Lunch mit Kampagnenbotschafter Ivano Somaini.	Keine formale Wirkungsstudie; Medienmitteilung und Kampagnenseiten beschreiben Inhalt, Zielgruppen und Aktivitäten der Kampagne, ohne systematisches Design zur Messung von Verhaltensänderungen (keine Vorher-Nachher-Erhebung, keine Auswertung von Klick- oder Meldeverhalten).	nein – Stellt Ziele, Botschaften und Massnahmen der Kampagne dar, berichtet jedoch keine verhaltensnahen Outcome-Kennzahlen oder Evaluationsdaten zur Wirksamkeit der Sensibilisierung.	Schweiz; zentrale nationale Awareness-Kampagne mit direktem Bezug zu Bevölkerung, Berufstätigen und Verwaltung, gut als Referenz für staatliche Sensibilisierungsinitiativen nutzbar, jedoch ohne veröffentlichte Wirksamkeitsdaten.
74	BACS (2025): Halbjahresbericht 2025/1 – Informationssicherung	Halbjahresbericht des BACS zur Cyberbedrohungslage in der Schweiz und international im 1. Halbjahr 2025; umfasst Meldestatistiken zu Cybervorfällen (u. a. Betrug, Phishing, Ransomware) sowie eine Phänomen- und Trendanalyse.	Deskriptiver Lage- und Monitoring-Bericht ohne Interventions- oder Vergleichsgruppe; Auswertung operativer Meldedaten (35’727 Meldungen) mit KPIs zu Meldetypen, betroffenen Zielgruppen, genutzten Angriffskanälen und missbrauchten Marken/Domains.	nein – Stellt Lage- und Meldestatistiken dar, liefert aber keine verhaltensnahe Wirkungsmessung konkreter Awareness-Trainings, Kampagnen oder anderer Sensibilisierungsmassnahmen.	Schweiz; offizieller Lagebericht des BACS, zentrale Grundlage für das Verständnis der nationalen Bedrohungslage und als Baseline-/Kontextbasis für die Einordnung von Awareness- und Integritätsmassnahmen geeignet, ohne selbst deren Wirksamkeit zu evaluieren.
75	BACS (2025): «Keine Ausreden – machen!» (S-U-P-E-R.ch) – nationale	Nationale Sensibilisierungskampagne S-U-P-E-R.ch 2025 unter dem Motto «Keine Ausreden – machen!» (ca. 24. April bis 31. Mai 2025) mit einer breiten Partnerallianz aus	Keine formale Wirkungsstudie; Medienmitteilungen und Kampagnenseiten beschreiben Ziele, Inhalte, Laufzeit und Partner der Kampagne, ohne	nein – Vermittelt Botschaften, Beispiele und Handlungsempfehlungen zur Cybersicherheit, berichtet jedoch keine verhaltensnahen Wirkungskennzahlen oder	Schweiz; staatlich koordinierte nationale Awareness-Kampagne mit direkter Relevanz für Bevölkerung, KMU und Behörden und als wichtiger Referenzpunkt für

	Sensibilisierungskampagne für Cybersicherheit 2025	BACS, Schweizerischer Kriminalprävention, kantonalen und städtischen Polizeikorps, SBB, Post, Schweizerischem Versicherungsverband und weiteren Partnern; Start an der Berner Publikumsmesse BEA mit Infostand, Aktionen und Wettbewerb, anschliessend Online-Kampagne über S-U-P-E-R.ch mit praxisnahen Tipps, Stories, Videos und dem Kartenspiel «Cards against Cybersecurity».	systematisches Evaluationsdesign oder verhaltensbezogene Outcome-Messgrössen (keine Vorher-Nachher-Erhebungen, keine Auswertung von Klick- oder Meldeverhalten).	differenzierten Evaluationsdaten zur tatsächlichen Verhaltensänderung der Zielgruppen.	staatliche Sensibilisierungsinitiativen nutzbar, jedoch ohne veröffentlichte Wirksamkeitsdaten.
76	BACS / NCSC (2024): Halbjahresbericht 2024/1 – Informationssicherung	Halbjährlicher Lagebericht zur Cyberbedrohungslage in der Schweiz und international, basierend auf der Meldestatistik der nationalen Melde- und Analysestelle; im ersten Halbjahr 2024 werden 34’789 Meldungen zu Cybervorfällen erfasst und nach Phänomenen (u. a. Betrug, Phishing, Spam) sowie Zielgruppen (Privatpersonen, Unternehmen) ausgewertet.	Deskriptiver Lage- und Monitoring-Bericht ohne Interventionsdesign; systematische Aufbereitung der Meldestatistik mit Zeitreihen und Verteilungen nach Phänomenen, Zielgruppen und ausgewählten Fallbeispielen, ohne Zuordnung zu spezifischen Awareness-Massnahmen.	nein – Liefert eine systematische Lage- und Meldestatistik (z. B. Anzahl Meldungen, Phänomenverteilung, Entwicklung gegenüber Vorperioden), untersucht aber nicht die Wirksamkeit einzelner Awareness-Massnahmen (keine Vorher-Nachher-Vergleiche oder Evaluation konkreter Kampagnen oder Trainings).	Schweiz; offizieller Lagebericht des BACS, zentrale Referenz für die nationale Bedrohungslage und als Kontext- und KPI-Grundlage für die Planung und Einordnung von Awareness- und Präventionsprogrammen.
77	BACS / NCSC (2025): Halbjahresbericht 2024/2 – Informationssicherung	Halbjährlicher Lagebericht zur Cyberbedrohungslage in der Schweiz und international auf Basis der Meldestatistik und ausgewählter Fallanalysen; im zweiten Halbjahr 2024 erhält das BACS 28’165 Meldungen zu Cybervorfällen, insgesamt 62’954 Meldungen im ganzen Jahr, aufgeschlüsselt nach	Deskriptiver Lage- und Monitoring-Bericht ohne Interventionsdesign; systematische Auswertung der Meldestatistik mit Zeitreihen, Phänomenverteilungen, Zielgruppenanalysen und Fallbeispielen, ohne Zuordnung zu spezifischen Awareness-Massnahmen oder	nein – Liefert eine umfangreiche statistische Grundlage zu Häufigkeit, Verteilung und Entwicklung von Cybervorfällen, evaluiert jedoch nicht systematisch die Wirksamkeit einzelner Awareness-Massnahmen oder Kampagnen (keine Vorher-Nachher-Vergleiche, keine	Schweiz; offizieller Halbjahresbericht des BACS, zentrale Datengrundlage zur Einbettung und Bewertung von Schweizer Awareness- und Präventionsprogrammen im Kontext der nationalen Bedrohungslage, ohne direkte Wirkungsmessung dieser Massnahmen.

		Phänomenen (u. a. Betrug, Phishing, Spam) und Zielgruppen (rund 90 % Privatpersonen, 10 % Unternehmen/Behörden).	programmspezifischen KPIs.	Zurechnung von Änderungen in der Meldestatistik auf spezifische Trainings oder Kampagnen).	
78	BACS / NCSC (2024): Sensibilisierung der Öffentlichkeit	Zentrale Übersichts- und Koordinationsseite des BACS zur Sensibilisierung der Öffentlichkeit; bündelt seit 2020 laufende und abgeschlossene Schweizer Awareness-Projekte und Kampagnen (z. B. ECSM, S-U-P-E-R.ch, themenspezifische Aktionen) mit dem Ziel, die heterogene Öffentlichkeit über Cyberrisiken zu informieren, Synergien zu nutzen und neue Projekte zu unterstützen.	Kein formales Evaluationsdesign; Überblicks- und Informationsseite, welche Auftrag, Ziele und Beispiele unterstützter Projekte beschreibt, ohne standardisierte Vorher-Nachher-Messung oder systematische Erhebung verhaltensbezogener Outcome-Kennzahlen.	nein – Erläutert Auftrag, Zielsetzung und Beispiele staatlich unterstützter Sensibilisierungsprojekte (inkl. Verweis auf Kampagnen wie ECSM und S-U-P-E-R.ch), liefert jedoch keine publizierten Kennzahlen zur Verhaltenswirkung (z. B. Veränderungen im Sicherheitsverhalten, Klick- oder Meldequoten, differenzierte Reichweitenanalysen).	Schweiz; zentrale Referenz für staatlich koordinierte Sensibilisierung der Öffentlichkeit im Bereich Cybersicherheit und Nachweis der Umsetzung der NCS-Massnahme «Sensibilisierung der Öffentlichkeit», wichtig für den BK-Kontext, aber ohne direkte Wirksamkeitskennzahlen.
79	Barrientos, Jacobs & Dawkins (2021): Advancing the NIST Phish Scale	Weiterentwicklung der NIST Phish Scale als Methode zur Einstufung der menschlichen Erkennungsschwierigkeit von Phishing-E-Mails; erneute Bewertung der ursprünglichen Phishing-Beispiele und Anwendung der Skala auf zusätzliche Mails aus realen Trainingsübungen.	Methodenorientierte Validierungsstudie ohne Interventions- oder Vorher-Nachher-Design; Analyse von Ratings (Cues, Premise Alignment, Difficulty) im Vergleich zu beobachteten Klickraten und Vorbereitung einer Usability-Studie mit Fachpersonen aus der Praxis.	nein – Fokussiert auf die Validierung und Verfeinerung der Messmethode, nutzt Klickraten lediglich zur Einordnung der Skala und berichtet keine verhaltensnahe Evaluation konkreter Awareness-Trainings.	International; relevantes Methodenpapier für Organisationen (inkl. Schweizer Behörden), die Phishing-Simulationen durchführen und Klickraten systematisch kontextualisieren wollen, liefert jedoch keinen direkten Wirksamkeitsnachweis für Awareness-Programme.
80	Bouma et al. (2024): Cyber Security in Hospitals	Entwicklung eines mehrstufigen, adaptiven Netzwerkmodells, das Lern- und Entscheidungsprozesse von Mitarbeitenden in Spitälern während Phishing-Trainingssimulationen abbildet; Modellierung	Konzeptionelle Modellierungsstudie ohne empirische Datenerhebung; Simulation von Verhaltensverläufen in Phishing-Szenarien mit Parametern zu Lernraten, Feedback und	nein – Zeigt in Simulationen plausibel, dass Feedbacklernen die modellierte Anfälligkeit auf Phishing reduziert, liefert aber keinen empirischen Wirksamkeitsnachweis, da reale Klick- oder	International (Spitalfokus); fachlich anschlussfähig für die Gestaltung und Simulation von Phishing-Trainings in Schweizer Spitälern und grossen Organisationen, dient jedoch primär als

		wiederholter Simulationen und Feedbackschleifen auf Basis des COM-B- Rahmenwerks (Capability, Opportunity, Motivation).	Kontextfaktoren, um Veränderungen der simulierten Phishing-Suszeptibilität über die Zeit zu analysieren.	Meldekennzahlen aus Spitälern fehlen.	konzeptionelles Modell ohne direkte verhaltensnahe Wirksamkeitsmessung realer Trainings.
81	Brunken et al. (2023): Hidden Costs of Simulated Phishing Campaigns	Fallstudie zur Einführung eines kombinierten Security-Awareness-Programms (SAC) und von Phishing-Simulationen (PSC) in einer grossen EU-Organisation mit über 30’000 Mitarbeitenden; Analyse des gesamten Beschaffungs- und Einführungsprozesses inkl. technischer Integration und Governance.	Qualitative Fallstudie auf Basis von Dokumenten, teilnehmender Beobachtung und halbstrukturierten Interviews; Erfassung von Prozessschritten, Stakeholderbeteiligung, Integrationsaufwänden sowie Schätzung des Ressourcenverbrauchs (Personenstunden und Kosten) für Proof-of-Concept und Einführung.	nein – Fokussiert auf Ressourcen-, Zeit- und Akzeptanzkosten der Einführung von PSC/SAC und zeigt erhebliche «Hidden Costs», liefert jedoch keine verhaltensnahe Outcome-Evaluation (z. B. Veränderung von Klick- oder Meldequoten durch das Programm).	EU / international; besonders relevant für Schweizer Behörden und grosse Organisationen, die Phishing-Simulationen ausschreiben oder einführen wollen, da der Beitrag eine empirische Grundlage für realistische Kosten-Nutzen-Abwägungen und die Einbettung von PSC in einen umfassenden Sicherheits- und Awarenessansatz bietet.
82	BSI (2024): Die Lage der IT-Sicherheit in Deutschland 2024	Nationaler Lage- und Trendbericht des Bundesamts für Sicherheit in der Informationstechnik zur IT-Sicherheit in Deutschland; beschreibt jährlich Bedrohungslage, Angriffsflächen, Gefährdungen und Resilienz von Staat, Wirtschaft und Gesellschaft, inkl. Phishing, Social Engineering, Ransomware und Schwachstellen.	Deskriptiver Monitoring- und Lagebericht ohne Interventions- oder Vergleichsgruppen; Auswertung von Vorfalldaten, technischen Indikatoren und Meldestatistiken mit Kennzahlen zu Bedrohungen (z. B. Phishing/Social Engineering, Malware-Varianten, Vorfälle gegen kritische Infrastrukturen) und qualitativen Fallbeispielen.	nein – Liefert Kennzahlen und qualitative Analysen zur Bedrohungs- und Vorfalllage, evaluiert jedoch nicht systematisch die Wirksamkeit spezifischer Awareness- oder Trainingsmassnahmen (keine Vorher-Nachher-Designs, keine verhaltensnahe Outcome-Messung von Kampagnen).	EU (Deutschland); nationaler Lage- und Trendbericht mit hoher Relevanz als Referenz-Lagebild und Vergleichsfolie für die Schweizer Situation (BACS), insbesondere zur Einordnung von Phishing- und Social-Engineering-Trends und zur Begründung des Bedarfs an Awareness-Massnahmen, ohne deren Wirksamkeit direkt zu messen.
83	Burita, Klaban & Racil (2022): Education and Training Against	Konzept für ein universitäres Trainingssystem mit simulierten Phishing-E-Mails: Registrierte Nutzende erhalten regelmässig generierte Phishing-Nachrichten, deren Reaktionen	Konzeptionelle Systembeschreibung ohne empirische Vorher-Nachher-Studie; Darstellung der technischen Architektur, der E-Mail-Template-Engine und	nein – Beschreibt Design und Funktionsweise eines simulierten Phishing-Trainingssystems, berichtet aber keine verhaltensnahe Wirksamkeitsmessung (z. B.	International (CZ-Hochschule); konzeptionell gut auf Schweizer Hochschulen und Verwaltung übertragbar als Vorlage für ein adaptives Phishing-Trainingssystem,

	Threat of Phishing Emails	aufgezeichnet und mit unmittelbaren Feedback-E-Mails (Fehleranalyse, Erkennungsmerkmale, mögliche Konsequenzen) beantwortet werden; Schwierigkeitsgrad und Frequenz werden adaptiv an die individuelle Resilienz angepasst.	des geplanten adaptiven Trainings- und Feedbackprozesses, jedoch ohne Auswertung realer Klick- oder Meldekennzahlen.	Veränderung der Fail-Rate vor/nach Einsatz).	jedoch ohne empirischen Nachweis der Wirksamkeit.
84	Canham, Dawkins & Jacobs (2024): Differential Phishing Susceptibility	Empirische Human-Centered-Security-Studie mit Studierenden und Mitarbeitenden einer Universität; über vier Wochen erhalten die Teilnehmenden acht E-Mails (vier Phishing, vier legitime Kontrollen), parallel Erhebung individueller Merkmale (Persönlichkeit, Wissen, Nutzung).	Quasi-experimentelles Feldsetting mit wiederholten Phishing- und Kontroll-E-Mails; Messung von Phishing-Suszeptibilität (Klickverhalten) sowie Erhebung von Persönlichkeitsmerkmalen (Big Five, Locus of Control), Sicherheits- und Phishingwissen sowie Technologie- und E-Mail-Nutzung zur Bildung von Risikoprofilen und Validierung der NIST Phish Scale.	nein – Untersucht Unterschiede in der Phishing-Anfälligkeit und die Validität der Phish Scale (u. a. «Repeat Clickers») und zeigt eine gute Passung zwischen Schwierigkeitsgrad und Klickraten, evaluiert jedoch keine spezifischen Awareness- oder Trainingsprogramme.	International (Universitätsumfeld in den USA); konzeptionell wichtig für Organisationen (inkl. Schweizer Verwaltung), die Phishing-Simulationen einsetzen, Risikogruppen identifizieren und die Schwierigkeit von Phishing-Mails einordnen wollen, liefert aber keinen direkten Wirksamkeitsnachweis von Awareness-Trainings.
85	Canham et al. (2021): Phishing for Long Tails	Längsschnittanalyse des Verhaltens von über 6’000 Mitarbeitenden einer US-Universität über 20 simulierte Phishing-Kampagnen in 19 Monaten; erfasst werden Fehlklicks (inkl. Dateneingabe) und Meldungen verdächtiger E-Mails, auf deren Basis Gruppen wie «never clickers», «occasional clickers», «repeat clickers» und «protective stewards» gebildet werden.	Longitudinales Beobachtungsdesign mit 20 Mock-Phishing-Kampagnen; Auswertung von Klick- und Meldeverhalten über 19 Monate, Clusterbildung in Verhaltensgruppen und Berechnung von Anteilen an Gesamtfehlern und Meldungen.	nein – Liefert detaillierte Verhaltenskennzahlen (z. B. geringer Anteil «repeat clickers» mit hohem Anteil an Fehlklicks, hoher Beitrag von «protective stewards» zu Meldungen), evaluiert jedoch keine spezifische Awareness- oder Trainingsintervention und berichtet keine Vorher-Nachher-Wirksamkeit eines Programms.	International (Universitätskontext in den USA); inhaltlich sehr relevant für die Segmentierung von Mitarbeitenden und die Ausrichtung von Phishing-Simulationen und Awareness-Programmen in Schweizer Organisationen, ohne direkten Wirksamkeitsnachweis einer konkreten Massnahme.

86	Charalambous & Stavrou (2025): Harnessing the Right Talent for SETA Programs	Konzept- und Mapping-Studie, die zentrale Wissensgebiete und übertragbare Kompetenzen von Fachpersonen identifiziert, die für die Entwicklung wirksamer Security-Education-, Training- und Awareness-(SETA-)Programme verantwortlich sind.	Konzeptionelle Analyse und Rollen-Mapping ohne empirische Vorher-Nachher- oder Verhaltensmessung; Zuordnung von Wissens- und Kompetenzanforderungen zu Cybersecurity-Rollen im ENISA European Cybersecurity Skills Framework und Ableitung geeigneter Rollenprofilkombinationen für SETA-Teams.	nein – Bietet einen kompetenzbasierten Rahmen zur Zusammensetzung interdisziplinärer SETA-Entwicklungsteams und leitet Annahmen für wirksamere Programme ab, berichtet jedoch keine empirische Evaluation spezifischer Awareness- oder Trainingsmassnahmen.	EU / international; strategisch relevant für Schweizer Organisationen zur Besetzung und Ausrichtung von SETA-Teams und zur Stärkung der Sicherheitskultur, jedoch ohne direkten verhaltensnahen Wirksamkeitsnachweis von Awareness-Programmen.
87	Chourasia (2025): AI-Enhanced Cybersecurity Training	Konzeptioneller Rahmen für KI-unterstützte Cybersecurity-Trainings in Cyber-Ranges und Cyber-Exercises; vorgeschlagen wird ein Modell der Mensch–KI-Interaktion, das Trainingsübungen, Cyber-Ranges, Learning-Analytics-Werkzeuge, multimodale Analytik und pädagogische Strategien integriert.	Konzeptionelle Überblicks- und Rahmenarbeit ohne empirische Primärdatenerhebung; diskutiert Einsatzszenarien von KI und Learning Analytics in Trainingsumgebungen, jedoch ohne konkrete Vorher-Nachher-Messung oder verhaltensbezogene Kennzahlen.	nein – Skizziert Potenziale und Herausforderungen von KI und Learning Analytics für Cybersecurity-Trainings, beschreibt aber kein implementiertes Programm mit empirischer Evaluation oder verhaltensnahen Outcome-Daten.	International; konzeptioneller Rahmen, strategisch relevant für Schweizer Organisationen, die Cyberübungen perspektivisch mit KI und Learning Analytics erweitern wollen, liefert jedoch keinen direkten Wirksamkeitsnachweis für Awareness- oder Trainingsmassnahmen.
88	Dawkins & Jacobs (2023): NIST Phish Scale User Guide	Anwenderleitfaden zur NIST Phish Scale, einem Rahmenwerk zur Bewertung der menschlichen Erkennungsschwierigkeit von Phishing-E-Mails; kombiniert Message Cues (sichtbare Hinweise im E-Mail) und Premise/Workplace Alignment (Passung der Story zum Arbeitskontext), inklusive Worksheets und Beispielen zur Einstufung der Detection Difficulty.	Konzeptioneller Leitfaden ohne eigene empirische Studie; beschreibt Vorgehen zur Bewertung von Phishing-E-Mails entlang der beiden Dimensionen und zur Ableitung von Schwierigkeitskategorien, die zur Interpretation von Klick- und Report-Raten in Phishing-Simulationen genutzt werden können.	nein – Erläutert Methode und Anwendung der Phish Scale in Trainings- und Simulationsprogrammen, verweist auf frühere Validierungsarbeiten, enthält jedoch keine eigenen verhaltensnahen Outcome-Daten zur Wirksamkeit von Awareness- oder Trainingsmassnahmen.	International; standardisierbares Bewertungsmodell, das sich direkt in Phishing-Simulations- und Awareness-Programme (auch in Schweizer Organisationen) integrieren lässt, um Klick- und Meldequoten nach Schwierigkeit der Lures zu interpretieren, ohne selbst Evaluationsdaten zur Verhaltenswirkung zu liefern.

89	DsiN (2024): DsiN-Sicherheitsindex 2024 – KI-Sicherheit im Alltag	Jährlicher Bevölkerungsindex (0–100) zur digitalen Sicherheitslage von Privatpersonen in Deutschland; kombiniert Sicherheitswissen, Sicherheitsverhalten, erlebte Sicherheitsvorfälle und wahrgenommene Bedrohungslage, mit Schwerpunkt 2024 auf «KI-Sicherheit im Alltag» (u. a. Phishing, E-Mail-Anhänge, Online-Banking, Smart Home, KI-Dienste).	Wiederkehrende repräsentative Bevölkerungsbefragung mit Indexbildung aus vier Faktoren (Wissen, Verhalten, Vorfälle, Verunsicherung); Auswertung nach soziodemografischen Merkmalen und Themenfeldern, inkl. Trendanalyse über mehrere Erhebungsjahre.	nein – Dient als Monitoring-Instrument für Wissen, Verhalten, Vorfälle und Verunsicherung und zeigt Trends (z. B. Tiefststand von 55.7 Punkten), evaluiert aber keine spezifischen Awareness- oder Trainingsmassnahmen mit Vorher-Nachher-Design oder verhaltensnahen Outcome-Kennzahlen.	EU (Deutschland); nationaler Bevölkerungsindex mit hoher Relevanz als Beispiel für die Messung von Sicherheitswissen, -verhalten und Bedrohungswahrnehmung in der Bevölkerung und als mögliche Referenz für vergleichbare Indizes oder Kampagnen-Evaluationen im Schweizer Kontext, ohne direkte Evaluation einzelner Awareness-Interventionen.
90	EU Academy / ENISA (2024–2025): AR-in-a-Box Game	Online-Cyber-Awareness-Game im Rahmen des ENISA-Toolkits «Awareness Raising in a Box (AR-in-a-Box)», bereitgestellt über die EU Academy; dient als gamifizierter Baustein von Awareness-Programmen und ermöglicht es Organisationen, grundlegendes Cyberwissen spielerisch zu testen und zu vertiefen.	Kein formales Studiendesign; das Game wird als Bestandteil des AR-in-a-Box-Toolkits und der EU Academy beschrieben, mit verschiedenen Versionen und Stilen sowie Hinweisen zur Einbettung in Awareness-Programme, jedoch ohne systematische Erhebung von Verhaltenskennzahlen.	nein – Wird als Ressource zur Sensibilisierung und Gamification eingesetzt, es liegen aber keine publizierten Evaluationsstudien oder verhaltensnahen Outcome-Daten (z. B. Verhaltensänderung, Klick- oder Meldequoten, Vorher-Nachher-Messungen) vor.	EU / international; von ENISA für öffentliche Stellen, kritische Infrastrukturen und Unternehmen entwickelt, konzeptionell gut auf Schweizer Behörden und Organisationen übertragbar als Game-Baustein in Awareness-Programmen, jedoch ohne spezifische Evaluationsdaten zur Wirksamkeit.
91	ENISA (2022): European Cybersecurity Skills Framework (ECSF)	Europäischer Kompetenz- und Rollenrahmen mit 12 typischen Cybersecurity-Rollenprofilen (z. B. Cybersecurity Educator, Cybersecurity Risk Manager, Cybersecurity Auditor), der für jede Rolle Mission, Aufgaben sowie benötigte Kenntnisse, Fertigkeiten und Kompetenzen beschreibt und diese mit bestehenden Referenzrahmen (z. B. e-CF, EQF) verknüpft.	Konzeptioneller Referenzrahmen ohne eigene Wirksamkeitsstudie; systematische Strukturierung von Rollen, Aufgaben, Skills und Kompetenzen, ergänzt um Mapping zu bestehenden europäischen Qualifikations- und Kompetenzrahmen, jedoch ohne verhaltensbezogene Outcome-Messgrössen.	nein – Dient als Struktur- und Referenzrahmen zur Beschreibung und Harmonisierung von Rollen und Kompetenzen in der Cybersecurity und unterstützt indirekt die Gestaltung von Education-, Training- und Awareness-Programmen, enthält aber keine eigenen Wirksamkeitskennzahlen oder Vorher-	EU / international; strategisch wichtig für Schweizer Verwaltung und Organisationen, um Rollen, Skills und SETA-Programme an europäischen Best Practices auszurichten und eine gemeinsame Sprache zwischen HR, Bildungsträgern und Fachbereichen zu etablieren, ohne selbst als Evaluationsinstrument für

				Nachher-Analysen zu konkreten Awareness-Initiativen.	Awareness-Massnahmen zu fungieren.
92	ENISA (2024): Awareness Raising in a Box (AR-in-a-Box)	Do-it-yourself-Toolkit der EU-Agentur ENISA zur Planung, Umsetzung und Evaluation von Cybersicherheits-Awareness-Programmen; bündelt Leitfäden, Checklisten und Vorlagen für interne Programme und externe Kampagnen (u. a. Zielgruppenanalyse, Kanalwahl, Kommunikationsstrategie, KPI-Definition) sowie Gamification-Elemente wie Quiz und ein Cyber Awareness Game über die EU Academy.	Konzeptionelles Toolkit ohne eigene empirische Primärstudie; beschreibt strukturierte Vorgehensweisen, Rollen, Planungs- und Kommunikationsprozesse, KPI-Auswahl und -Messung sowie – in der aktualisierten Version 2024 – einen Leitfaden für interne und externe Cyber-Krisenkommunikationspläne, basierend auf Pilotierungen mit nationalen Partnern.	nein – Liefert einen strukturierten Methoden- und KPI-Rahmen für Awareness-Programme (inkl. Hinweisen zur Auswahl und Bewertung von Kennzahlen), berichtet jedoch keine systematischen Outcome-Studien zur tatsächlichen Verhaltenswirkung von mit AR-in-a-Box umgesetzten Programmen (keine publizierten Vorher-Nachher-Daten zu Klick- oder Meldequoten).	EU; generisches Toolkit für öffentliche Stellen, kritische Infrastrukturen und Unternehmen, direkt nutzbar für Schweizer Behörden und Organisationen zur Strukturierung und Professionalisierung von Awareness-Programmen (inkl. Krisenkommunikation), jedoch ohne eigene Schweizer Wirksamkeitsdaten oder verhaltensnahe Evaluationsstudien.
93	ENISA (2024): Best Practices for Cyber Crisis Management	Best-Practice-Studie zum operativen Cyber-Krisenmanagement in der EU im Auftrag von EU-CyCLONe; definiert Begriffe, Rollen und Strukturen auf EU- und Mitgliedstaatenebene (ENISA, EU-CyCLONe, CSIRTs, nationale Behörden) und beschreibt 15 Best Practices entlang der Phasen Prävention, Preparedness, Response und Recovery im Lichte von NIS2.	Qualitative Studie auf Basis von Desk Research und Konsultationen von Fachpersonen (Workshops, Interviews mit Mitgliedern von EU-CyCLONe); systematische Aufbereitung von Rollen, Prozessen und Best Practices im Cyber-Krisenmanagement, ohne standardisierte Vorher-Nachher-Messung oder verhaltensbezogene Outcome-Daten.	nein – Stellt einen Rahmen und einen Katalog von Best Practices (inkl. Empfehlungen zu Übungen, Trainings- und Kommunikationsmassnahmen) bereit, enthält aber keine quantitativen Wirksamkeitsevaluationen oder verhaltensnahen Kennzahlen (z. B. Vergleich von Organisationen mit/ohne Übungen, Vorher-Nachher-Messungen).	EU; relevanter Referenzrahmen für die Ausgestaltung von Cyber-Krisenmanagement, Übungen und Krisenkommunikation auch in der Schweiz (insbesondere für Bund und Kantone); liefert konzeptionelle Leitplanken und Praxisbeispiele, aber keine direkten Wirksamkeitsnachweise für Awareness- oder Trainingsmassnahmen.
94	ENISA (2024): Cybersecurity Awareness Conference – «Reframing	1st Cybersecurity Awareness Raising Conference von ENISA und SI-CERT am 27. November 2024 in Ljubljana; richtet sich an Fachpersonen aus öffentlichem und privatem Sektor, die für Cybersecurity-	Kein formales Studiendesign; Fachkonferenz mit Keynotes, Panels und Praxis-Sessions, deren Inhalte und Beispiele über Agenda, Eventseiten und News-Beiträge dokumentiert sind,	nein – Vermittelt Konzepte, Methoden und Best Practices zur Neuausrichtung von Awareness-Kommunikation und zum Human Factor, berichtet aber keine verhaltensnahen Outcome-Daten oder	EU; europäische Fachkonferenz mit Beteiligung von Schweizer Stellen (u. a. SWITCH), konzeptionell sehr relevant für die Weiterentwicklung schweizerischer Awareness-Strategien

	Cybersecurity Awareness Raising»	Awareness verantwortlich sind, und fokussiert auf Human Factor, Psychologie, Best Practices und Gamification (z. B. Crime Prevention, AR-in-a-Box, Cyber Safety for Older Adults, «Beyond Fear», Escape Room, Treasure Hunt, Roleplay, Videogame).	ohne systematische Erhebung verhaltensbezogener Kennzahlen oder Vorher-Nachher-Messungen bei Teilnehmenden.	Evaluationsstudien zur Wirksamkeit der vorgestellten Ansätze.	(Human-Factor-Perspektive, Gamification, C-Level-Awareness), jedoch ohne direkte Wirksamkeitskennzahlen.
95	ENISA (2024): How to Promote Cyber Security Awareness to C-Level	Praxisleitfaden im Rahmen des ENISA-Toolkits AR-in-a-Box mit dem Ziel, C-Level-Unterstützung für Cybersecurity-Awareness-Programme zu gewinnen und zu halten; beschreibt ein 3-Phasen-Vorgehen von der Analyse des Reifegrads über die Übersetzung von Cyberrisiken in Geschäftsziele bis zur langfristigen Einbindung der Führungsebene.	Konzeptioneller Leitfaden ohne eigene empirische Studie; strukturiert Vorgehen, Rollen und Interaktion mit C-Level, konkretisiert Typen von C-Level-Support (Strategie, Ressourcen, Training, Kommunikation/Kultur) und schlägt KPIs sowie Reporting-Formate vor, gestützt auf Praxis- und Umfrageergebnisse.	nein – Bietet ein strukturiertes Rahmenwerk, Rollenbilder sowie Vorschläge für KPIs und Reporting zur Einbindung von C-Level in Awareness-Programme, stellt aber keine systematische Evaluation der Wirksamkeit spezifischer Awareness- oder C-Level-Interventionsstrategien bereit (keine Vorher-Nachher-Messungen, keine verhaltensbezogenen Outcome-Daten).	EU; hohe praktische Relevanz für Schweizer Behörden und Organisationen, die C-Level-Unterstützung für Awareness-Programme aufbauen wollen, da Governance- und Kommunikationsleitplanken bereitgestellt werden, jedoch ohne empirische Wirksamkeitsevaluation der vorgeschlagenen Ansätze.
96	ENISA (2024): 2024–2026 Single Programming Document – Condensed work programme 2024	Mehrjahres- und Jahresarbeitsprogramm von ENISA; Activity 9 «Outreach and education» bündelt Massnahmen zur Erhöhung der Awareness für Cyberrisiken und zur Förderung cybersicheren Verhaltens, u. a. durch Outreach-Kampagnen, Best-Practice-Leitfäden, Koordination der Awareness-Aktivitäten der Mitgliedstaaten und Massnahmen im Rahmen der Cybersecurity	Strategisches Planungs- und Steuerungsdokument ohne eigene empirische Wirksamkeitsstudie; definiert Ziele, Aktivitäten und Leistungsindikatoren (z. B. Staff Awareness, SME- und nationale Cybersecurity-Kultur, Anteil der Vorfälle mit Human Error als Root-Cause, Zielgrösse von mindestens 200’000 ausgebildeten Cybersecurity-Fachpersonen bis 2025), jedoch	nein – Legt Zielindikatoren und Zielwerte für Awareness-, Bildungs- und Skills-Programme fest, evaluiert aber keine konkreten Awareness- oder Trainingsmassnahmen (keine ausgewerteten Verhaltensdaten, keine empirische Wirkungsmessung einzelner Kampagnen oder Programme).	EU; wichtiger Orientierungsrahmen für Schweizer Behörden und Verwaltung bei der Definition von Zielen, KPIs und Programmen im Bereich Awareness, Bildung und Cybersecurity-Skills, ersetzt aber keine Wirksamkeitsstudien zu konkreten Trainings- oder Kampagnenmassnahmen.

		Skills Academy (Ausbildung, Zertifikate, Skills-Indikatoren).	ohne Vorher-Nachher-Design oder verhaltensbezogene Datenerhebung.		
97	ENISA (2025): European Cybersecurity Month 2025 – «Off the Hook – Don't be Phished»	EU-weite Sensibilisierungskampagne «European Cybersecurity Month» (ECSM) 2025 im Oktober unter dem Motto «Off the Hook – Don't be Phished», durchgeführt von ENISA und der Europäischen Kommission; im Fokus stehen Phishing und Social Engineering, unterstützt durch ein Media-Toolkit mit Messaging-Guides, Visuals, Social-Media-Assets und Vorlagen für Veranstaltungen, das von Partnerorganisationen in den Mitgliedstaaten genutzt werden kann.	Kein formales Evaluationsdesign; öffentlich zugängliche Informationen beschreiben Ziele, Schwerpunkte, Materialien und Beteiligungsmöglichkeiten der Kampagne, ohne systematische Vorher-Nachher-Messung oder verhaltensbezogene Outcome-Kennzahlen (z. B. Klick- oder Meldeverhalten).	nein – Legt inhaltliche Schwerpunkte und Unterstützungsangebote für Partnerorganisationen dar, berichtet jedoch keine verhaltensnahen Wirkungskennzahlen oder empirischen Evaluationsdaten zur tatsächlichen Verhaltensänderung der Zielgruppen.	EU; Kampagne für Bevölkerung, Unternehmen und öffentliche Stellen mit hoher Referenzrelevanz für nationale Initiativen (z. B. Cyber Security Month Schweiz), insbesondere zur Einordnung von Phishing- und Social-Engineering-Schwerpunkten, jedoch ohne spezifische Schweizer Beteiligungs- oder Wirkungsdaten.
98	ENISA (2025): NIS2 Technical Implementation Guidance	Umsetzungsleitlinie zur Durchführungsverordnung (EU) 2024/2690 für die NIS2-Richtlinie; konkretisiert technische und organisatorische Anforderungen an Cybersicherheits-Risikomanagementmassnahmen in 13 Bereichen (u. a. Policy, Incident Handling, Business Continuity, Supply Chain, Effektivitätsmessung, Cyberhygiene und Security-Training, HR-Security, Access Control, Asset Management).	Konzeptionelle Guidance ohne eigene empirische Primärstudie; beschreibt für jedes Anforderungselement praxisnahe Umsetzungshinweise, Beispiele für Nachweise («examples of evidence»), Monitoring- und Review-Zyklen sowie beispielhafte KPIs (u. a. Teilnahme/Abschluss von Security-Trainings, Vorfallzahlen, Reaktionszeiten, Non-Compliance-Fälle) und mappt diese auf etablierte Standards (z. B. ISO/IEC 27001/27002, NIST CSF).	nein – Definiert Anforderungen, Beispiele für Nachweise und KPIs zur Effektivitätsmessung von Sicherheitsmassnahmen (inkl. Awareness-, Cyberhygiene- und Trainingsprogrammen), evaluiert aber keine konkreten Programme und berichtet keine Vorher-Nachher-Daten oder verhaltensnahen Outcome-Kennzahlen realer Interventionen.	EU; wichtiger Referenzrahmen für Risikomanagement, Governance und KPI-Definition, an dem sich Schweizer Behörden und Betreiber kritischer Infrastrukturen bei der Ausgestaltung eigener Awareness-, Trainings- und Messkonzepte orientieren können, ohne dass selbst Wirksamkeitsstudien zu Awareness-Massnahmen enthalten sind.

99	ENISA (o. J.): European Cybersecurity Month – Overview & Media Toolkit	Überblicks- und Toolkit-Seite zum European Cybersecurity Month (ECSM) als jährliche EU-weite Awareness-Kampagne im Oktober; stellt ein Media-Toolkit mit Key Messages, Visuals, Social-Media-Assets, Logos und Leitfäden bereit, damit Behörden, Organisationen und Unternehmen eigene ECSM-Aktivitäten zu Themen wie Phishing, Social Engineering, Ransomware oder Cyberhygiene planen und kommunizieren können.	Kein formales Studiendesign; Beschreibung von Zielsetzung, Struktur und Materialien des ECSM sowie der Rolle von ENISA und der Europäischen Kommission als Koordinationsstelle, ohne systematische Erhebung von Verhaltenskennzahlen.	nein – Unterstützt Partnerorganisationen mit wiederverwendbaren Kommunikationsmaterialien und Kampagnenguides, enthält jedoch keine systematischen Outcome-Kennzahlen oder evaluativen Studien zur Wirksamkeit (z. B. Verhaltensänderungen, Klick- oder Meldequoten, Vorher-Nachher-Messungen).	EU; Referenzrahmen für europaweite Awareness-Kampagnen und Materialquelle für nationale Initiativen (z. B. Cyber Security Month Schweiz), fachlich relevant für die Ausgestaltung von Kampagnen, aber ohne eigene Wirksamkeitsdaten oder spezifische Schweizer Outcome-Daten.
100	Geppert et al. (2025): Phishing Awareness Training – A Technology Adoption Perspective	Technologie-Adoptionsstudie zu Phishing Awareness Training (PAT) mit Fokus auf Schweizer Organisationen; auf Basis von Literatur und Praxisinterviews wird ein TOE-basiertes Rahmenwerk (Technology–Organization–Environment) für Design, Einführung und Nutzung von PAT entwickelt.	Kombination aus systematischer Literaturanalyse (73 Quellen) und acht halbstrukturierten Interviews mit Fachpersonen in der Schweiz; qualitative Auswertung der Faktoren in den Dimensionen Technologie, Organisation und Umwelt und Mapping auf die Phasen der PAT-Einführung.	nein – Entwickelt ein Adoptions- und Implementierungsframework für PAT und identifiziert Einflussfaktoren, evaluiert jedoch keine konkreten Trainingsprogramme hinsichtlich verhaltensnaher Outcomes (z. B. Klick-/Meldequoten oder Vorher-Nachher-Vergleiche).	Schweiz; hohe Relevanz für Behörden und Organisationen, da das Framework direkt für die Planung und Einführung von Phishing-Awareness-Trainings im Schweizer Kontext genutzt werden kann, ohne eigenen Wirksamkeitsnachweis der Trainings.
101	Gundu (2024): Adaptive Cybersecurity Culture Model	Konzeptstudie, die ein zyklisches «Adaptive Cybersecurity Culture Model» (ACCM) vorstellt: Aufbau einer Sicherheitskultur nach den Prinzipien «Learn, Unlearn, Relearn» mit Fokus auf kontinuierlichem Lernen, gezieltem Verlernen veralteter Praktiken, kognitiver Flexibilität und einer	Konzeptionelle Rahmenarbeit ohne empirische Primärdatenerhebung; beschreibt ein Kulturmodell und leitet strategische Handlungsfelder und organisationale Hebel für eine adaptive Sicherheitskultur ab, ohne standardisierte	nein – Entwirft ein Rahmenmodell und Strategien zur Gestaltung einer adaptiven Sicherheitskultur und weist explizit auf zukünftigen Bedarf für quantitative Metriken und Wirksamkeitsmessungen hin, berichtet jedoch keine verhaltensnahen Outcome-Daten zu konkreten	International; branchenübergreifendes Kulturmodell, konzeptionell sehr relevant für Schweizer Verwaltung und Organisationen als Orientierungsrahmen für langfristige Awareness- und Kulturprogramme, ohne eigenen empirischen Wirksamkeitsnachweis.

		wachstumsorientierten Haltung, unterstützt durch Führungs-, Kommunikations- und Anreizstrukturen.	Messgrössen oder Vorher-Nachher-Design.	Awareness- oder Trainingsmassnahmen.	
102	Hielscher et al. (2024): Selling Satisfaction	Qualitative Markt- und Inhaltsanalyse von Security-Awareness- und Training-Anbietenden (SAT); aus Suchbegriffen von 30 Awareness-Verantwortlichen werden 156 Websites von 59 SAT-Anbietenden identifiziert und deren Marketingaussagen zu Nutzen, KPIs und «Human Risk» untersucht.	Qualitative Inhaltsanalyse von 2'476 marketingnahen Aussagen, die per Web-Scraping erhoben und inhaltsstrukturierend sowie thematisch codiert werden; Fokus auf Nutzenversprechen, KPI-/ROI-Narrativen und der Darstellung der Rolle von Mitarbeitenden in Awareness-Programmen.	nein – Analysiert, wie SAT-Anbietende Wirksamkeit, KPIs und «human risk scores» vermarkten und zeigt eine Lücke zwischen Marketingversprechen und nachweisbarer Wirkung, evaluiert jedoch keine konkreten Trainingsprogramme und berichtet keine verhaltensnahen Outcome-Daten.	EU / international; Meta-Perspektive auf den SAT-Markt, direkt relevant für Schweizer Behörden und Organisationen bei der Auswahl von Awareness-Lösungen, da die Ergebnisse dafür sprechen, Vendor-Versprechen kritisch zu prüfen und auf evidenzbasierte, unabhängig evaluierte Massnahmen zu setzen.
103	HSLU / EBAS (o. J.): «eBanking – aber sicher!» – Informations- und Schulungsangebot	Schweizer Informations- und Awareness-Plattform «eBanking – aber sicher!» (EBAS) der Hochschule Luzern – Informatik, seit 2009 in Betrieb und von zahlreichen Finanzinstituten unterstützt; bietet eine mehrsprachige Website mit Ratgeberinhalten zu sicherem E-Banking und digitaler Sicherheit, einen Phishing-Selbsttest, ein Ransomware-Game sowie öffentliche Grund- und Spezialkurse für Bankkundschaft, KMU und Bankmitarbeitende.	Kein formales Evaluationsdesign; Dienstleistungs- und Präventionsangebot mit laufender Bereitstellung von Online-Informationen, Selbsttests, Games und Kursen, teils ergänzt um Nutzungszahlen (z. B. Websitebesuche, Anzahl Kursteilnehmende), jedoch ohne standardisierte Vorher-Nachher-Messung oder systematische Erhebung verhaltensbezogener Kennzahlen.	nein – Dokumentiert Angebot, Formate und Zielgruppen (inkl. Phishing-Selbsttest und Schulungen), liefert aber keine publizierten verhaltensnahen Outcome-Daten zu Wirksamkeit (z. B. Veränderung von Phishing-Klick- oder Meldeverhalten oder sicherheitsrelevanten Nutzungsindikatoren).	Schweiz; etabliertes und breit genutztes Awareness- und Schulungsangebot mit direkter Relevanz für Banken, Bankkundschaft und Beratende, zentrale Referenz für E-Banking-Sensibilisierung im Schweizer Kontext, jedoch ohne veröffentlichte Wirksamkeitsstudien.
104	iBarry / Swiss Internet Security Alliance (o. J.): Internet-	Nationale Internet-Sicherheitsplattform des Vereins Swiss Internet Security Alliance (SISA); iBarry.ch bietet der Schweizer Bevölkerung und Unternehmen frei zugängliche Inhalte	Kein formales Evaluationsdesign; dauerhaftes Präventions- und Informationsangebot mit kuratierten Inhalten eines Advisory Boards und regelmässig	nein – iBarry.ch ist als zentrale Präventions- und Awareness-Plattform beschrieben, es liegen aber keine veröffentlichten, systematischen Evaluationsdaten zur	Schweiz; zentrale Plattform für die Sensibilisierung der Bevölkerung und Organisationen, wichtiger Infrastrukturbaustein für staatliche und privatwirtschaftliche

	Sicherheitsplattform iBarry.ch	zu Cyberrisiken, thematische Dossiers (z. B. Phishing, Deepfakes, Ransomware), Schritt-für-Schritt-Hilfen, Online-Sicherheitschecks, Erste-Hilfe-Anleitungen bei Cybervorfällen sowie mehrsprachige Erklärinhalte.	aktualisierten Online-Ressourcen, teils ergänzt um Nutzungszahlen (z. B. Reichweite, Kursangebote), jedoch ohne standardisierte Vorher-Nachher-Messungen oder systematische Erhebung verhaltensbezogener Kennzahlen.	Wirksamkeit im Sinne von Verhaltensänderungen vor (z. B. Veränderung von Klick- oder Meldeverhalten, Sicherheitsroutinen nach Nutzung der Plattform).	Awareness-Initiativen (u. a. S-U-P-E-R.ch, NCSC-Kampagnen), jedoch ohne veröffentlichte Wirksamkeitsstudien.
105	ISO/IEC (2022): ISO/IEC 27002:2022 – Information security controls	Internationaler Referenz-Kontrollkatalog mit 93 Informationssicherheits-Controls, gegliedert in die Bereiche Organizational, People, Physical und Technological Controls; zu jedem Control werden Zweck, Umsetzungshinweise und Control-Attribute beschrieben. Für Awareness ist insbesondere People Control 6.3 «Information security awareness, education and training» zentral, das angemessene Sensibilisierung, Ausbildung und Schulung sowie die Überprüfung des Verständnisses nach Trainingsaktivitäten fordert.	Normatives Referenzdokument ohne empirische Primärstudie; definiert Controls, Ziele, Implementierungsleitlinien und Control-Attribute und verweist für Messfragen konzeptionell auf ISO/IEC 27004, ohne eigene verhaltensbezogene Outcome-Messgrössen zu erheben.	nein – Beschreibt Best-Practice-Controls und Leitlinien für Awareness, Schulung und Training, liefert aber keine empirischen Wirksamkeitsdaten zu konkreten Awareness-Programmen (keine Vorher-Nachher-Verhaltenskennzahlen wie Klick- oder Meldequoten).	International; zentrale Referenznorm für Informationssicherheits-Controls, die auch im Schweizer Verwaltungs- und Unternehmenskontext breit eingesetzt wird und einen Gestaltungsrahmen für Awareness-Programme bietet, jedoch ohne eigene Wirksamkeitsstudien.
106	Jayakrishnan et al. (2022): Housie – A Multiplayer Game for Cybersecurity Training	Online-Serious-Game im Multiplayer-Format für den Unternehmenskontext; «Housie» ergänzt klassische textbasierte Unterlagen und Quizze durch ein Frage-und-Antwort-Spiel zu Cybersecurity-Themen, das Wissen spielerisch vermittelt und Engagement durch	Konzeptionelle Beschreibung einer Desktop-Anwendung mit Fokus auf Spielmechanik, didaktischen Zielen und Einsatzszenarien; es wird kein formales Vorher-Nachher-Design oder eine standardisierte verhaltensbezogene	nein – Beschreibt Design und intendierte Lernziele des Multiplayer-Serious-Games, liefert aber keine publizierten Wirksamkeitskennzahlen (z. B. Vorher-Nachher-Vergleiche, Fehlerquoten oder Klick-/Melde-KPIs) zur tatsächlichen Verhaltensänderung.	International (Unternehmenskontext); der Multiplayer- und Gamification-Ansatz ist konzeptionell gut auf Schweizer Organisationen übertragbar, dient aber in dieser Übersicht primär als Ideen- und Designbeispiel ohne belastbaren Wirksamkeitsnachweis.

		Wettbewerbs- und Gamification-Elemente erhöhen soll.	Wirkungsmessung berichtet.		
107	Kelleci (2023): Phishing Awareness Training Framework for Remote Workers	Masterarbeit mit systematischer Literaturanalyse zu Phishing-Awareness-Interventionen mit Fokus auf remote arbeitende Mitarbeitende; zentrale Herausforderungen der Remote-Arbeit (technologische und organisatorische Rahmenbedingungen im Homeoffice) werden herausgearbeitet und in ein Gestaltungsmodell für Phishing-Awareness-Trainings überführt.	Systematische Literaturarbeit ohne eigene Primärdatenerhebung; Auswertung bestehender Studien zu Phishing-Awareness und Verdichtung ihrer Ergebnisse in einem Trainings-Framework für Remote-Settings, ohne standardisierte Vorher-Nachher- oder Verhaltensmessungen.	nein – Verdichtet vorhandene Evidenz zu überwiegend positiven, aber kontextabhängigen Effekten von Phishing-Awareness-Interventionen in ein Framework für Remote-Beschäftigte, erhebt jedoch keine neuen verhaltensnahen Wirksamkeitsdaten (keine Klick- oder Melde-KPIs, keine eigenen Vorher-Nachher-Messungen).	Schweiz; Masterarbeit an der Hochschule für Wirtschaft FHNW mit explizitem Bezug zu Schweizer Unternehmen und Remote-Beschäftigten, liefert ein direkt anschlussfähiges Gestaltungsmodell für Phishing-Awareness-Trainings im Schweizer Kontext, jedoch ohne eigene Outcome-Evaluation.
108	Leijman & Svensson (2025): Designing a Security Awareness Program against Phishing Attacks	Bachelorarbeit, die auf Basis einer systematischen Literaturrecherche und semi-strukturierten Interviews mit Cybersicherheits-Mitarbeitenden bei Verisure ein Konzept für ein automatisiertes Sicherheitsbewusstseinsprogramm gegen Phishing in Organisationen entwickelt (u. a. simulierte Phishing-Angriffe, kontinuierliche Trainingsbausteine, Feedback-Mechanismen, jährliche Trainingstage).	Kombination aus systematischer Literaturrecherche der letzten fünf Jahre und semi-strukturierten Interviews; qualitative Auswertung der Best Practices und Einschätzungen der Fachpersonen, ohne standardisierte Vorher-Nachher-Messung oder verhaltensbezogene Kennzahlen.	nein – Fasst bestehende Best Practices zusammen und leitet ein Programmdesign für Phishing-Awareness ab, evaluiert das vorgeschlagene Programm jedoch nicht empirisch (kein Vorher-Nachher-Vergleich, keine eigenen Klick- oder Meldekennzahlen).	International (schwedische Bachelorarbeit mit Praxispartner); inhaltlich gut anschlussfähig für das Design von Awareness-Programmen in Schweizer Organisationen, jedoch ohne eigenen Wirksamkeitsnachweis.
109	Löffler et al. (2021): CySecEscape 2.0 – Virtual Escape Room	Virtueller Escape Room für KMU und Studierende: ca. 40-minütiges Online-Spiel in einer comicartigen Büro-Umgebung mit Rätseln zu physischer Sicherheit, Passworthygiene, Quellcode-Sicherheit, Informationsentsorgung,	Zwei kleine Testrunden mit insgesamt 4 Spielenden sowie drei Online-Klassen mit 81 Rückmeldungen; Erhebung von Einschätzungen zum Spielerlebnis und zur wahrgenommenen Eignung für Sensibilisierung, ohne	nein – Die Evaluation fokussiert auf das Spielerlebnis (z. B. 47 % «good»/«great», 33 % «ok») und liefert keinen belastbaren Wirksamkeitsnachweis im Sinne verhaltensnaher Kennzahlen (keine Klick-/Melde-KPIs, keine	Schweiz / international; FHNW-Projekt mit Fokus auf Schweizer KMU, konzeptionell gut auf Verwaltung und andere Organisationen übertragbar als Serious-Game-Baustein, bisher

		Identitätsdiebstahl, Phishing und Online-Banking, spielbar im Browser mit Briefing und Debriefing.	standardisierte Vorher-Nachher-Messung von Wissen oder Verhalten.	Vorher-Nachher-Verhaltensmessung).	jedoch ohne verhaltensnahe Wirksamkeitsdaten.
110	Meguro & Chong (2025): AdaPhish – AI-Powered Adaptive Defense and Education Resource	KI-gestützte Phish-Bowl-Plattform «AdaPhish», die eingereichte Phishing-E-Mails automatisiert anonymisiert, analysiert und organisationsübergreifend als geteilte Fallbibliothek bereitstellt; ermöglicht Trendanalysen, Reports und die Nutzung realer Phishing-Beispiele als edukative Ressource für Cybersicherheitstrainings.	Technische Konzept- und Evaluationsstudie mit Fokus auf der Leistungsfähigkeit der Plattform (u. a. Anonymisierung und KI-gestützte Analyse), ohne standardisierte Vorher-Nachher-Messung des Verhaltens von Nutzenden oder Trainingswirkung.	nein – Berichtet technische Leistungskennzahlen und argumentiert für den Einsatz von AdaPhish zur Unterstützung von Detection und Education, weist jedoch keine empirischen Wirksamkeitsdaten als Awareness- oder Trainingsmassnahme aus (keine Veränderungen von Klick- oder Meldequoten).	International; technische und edukative Plattform, konzeptionell sehr relevant für Schweizer Organisationen, die realistische Phishing-Beispiele sicher aggregieren, analysieren und für Awareness-Formate nutzen wollen, aber ohne direkten Wirksamkeitsnachweis im Sinne verhaltensnaher Kennzahlen.
111	NIST (2024): SP 800-50 Rev. 1 – Building a Cybersecurity & Privacy Learning Program	Rahmenwerk zum Aufbau eines Cybersecurity & Privacy Learning Program (CPLP) über den gesamten Lebenszyklus: von Planung und Strategie (Governance, Rollen, Ziele, Risikobezug) über Analyse & Design (Zielgruppen- und Rollenanalysen, Lernziele, Inhaltsarchitektur) und Entwicklung & Implementierung (Formate wie E-Learning, Micro-Learning, Simulationen, Prozessintegration) bis zu Assessment & Improvement (Messgrössen, Feedbackschlaufen, kontinuierliche Verbesserung).	Methoden- und Governance-Leitfaden ohne eigene empirische Primärstudie; beschreibt Prozessschritte, Rollenmodelle, mögliche Lern-, Verhaltens- und Kulturmetriken sowie die Verknüpfung mit NIST CSF 2.0, SP 800-53 und dem NIST Privacy Framework, jedoch ohne standardisierte Vorher-Nachher-Messung konkreter Programme.	nein – Beschreibt, wie ein systematisches Cybersecurity- und Privacy-Learning-Programm aufgebaut, gesteuert und mit geeigneten Metriken begleitet werden kann, stellt aber keine eigenen verhaltensbezogenen Outcome-Daten oder Programmevaluationen bereit; vorgeschlagene Metriken dienen als Orientierungs- und Designgrundlage, nicht als Wirksamkeitsnachweis.	International; Referenzrahmen aus den USA, der sich direkt auf Schweizer Organisationen und Behörden übertragen lässt, insbesondere für die strukturierte Planung von Awareness- und Privacy-Trainings, die Definition von Rollen und Verantwortlichkeiten sowie die Ausgestaltung von Kennzahlen und Verbesserungsprozessen, ohne selbst Outcome-KPIs zu liefern.
112	NIST CSRC (2024): Phishing – Human-	Ressourcen-Hub der NIST-Initiative Human-Centered Cybersecurity zum Thema	Konzeptionelle Ressourcensammlung ohne eigene Primärdatenerhebung; stellt	nein – Die Ressourcenseite bietet die Phish Scale als Mess- und Analysewerkzeug	International; weit verbreitetes Messverfahren, das Organisationen –

	Centered Cybersecurity (Phish Scale resources)	Phishing; bündelt sämtliche Materialien zur NIST Phish Scale als Verfahren zur Bewertung der menschlichen Erkennungsschwierigkeit von Phishing-E-Mails, inklusive User Guide, Beispielen, Worksheets, Poster, Präsentationen und Videos.	den NIST Phish Scale User Guide (Technical Note 2276) und weitere Materialien bereit, mit denen Organisationen E-Mails entlang der Dimensionen sichtbare Message Cues und Premise/Workplace Alignment einstufen und Klick- sowie Melderaten aus Phishing-Simulationen besser interpretieren können.	für bestehende Phishing-Awareness-Programme und verlinkt Forschungsarbeiten, die die Skala nutzen, liefert jedoch selbst keinen zusammenhängenden verhaltensnahen Wirksamkeitsnachweis dafür, dass Awareness-Trainings oder Kampagnen durch den Einsatz der Skala nachweislich wirksamer werden.	einschliesslich Schweizer Behörden und Unternehmen – bei der Einordnung von Klick- und Melderaten aus Phishing-Simulationen unterstützt, indem es die Schwierigkeit eingesetzter Mails systematisch klassifiziert, ohne selbst als Evaluationsstudie für Awareness-Massnahmen zu fungieren.
113	OECD (2024): New Perspectives on Measuring Cybersecurity	Konzeptionelles Mess- und Indikatoren-Framework für Cybersecurity auf Landes- und Sektorebene; bietet eine Checkliste für Cybersecurity-Messung und unterscheidet systematisch zwischen offiziellen Datenquellen (z. B. Erhebungen, Verwaltungsdaten, CSIRT-Statistiken) und nicht-offiziellen Quellen (z. B. Medienberichte, Anbieterstatistiken, Such- und Versicherungsdaten), ergänzt um zwei Proof-of-Concept-Indizes zur «Cybersecurity-Uncertainty».	Konzeptioneller Policy- und Methodenbericht ohne eigene Interventionsstudie; entwickelt ein Mess-Framework, strukturiert Datenquellen und konstruiert beispielhafte Uncertainty-Indizes als Demonstratoren, ohne standardisierte verhaltensbezogene Outcome-Messung von Awareness-Trainings oder Kampagnen.	nein – Entwickelt ein Mess-Framework und Beispielindikatoren für Cybersecurity, liefert aber keine verhaltensbezogenen Outcome-Daten zu Awareness- oder Trainingsmassnahmen; die Uncertainty-Indizes illustrieren Machbarkeit und Datenkombination, sind jedoch kein Evaluationsnachweis für konkrete Sensibilisierungsprogramme oder Verhaltensänderungen.	International; bietet einen Orientierungsrahmen, wie nationale Messsysteme (inkl. Meldestatistiken, Surveys, CSIRT-Daten) aufgebaut und kombiniert werden können; für die Schweiz relevant zur Einbettung von BACS-/NCSC-Kennzahlen und zur Diskussion, wie Awareness- und Sicherheitsindikatoren künftig standardisierter und international vergleichbar gemessen werden könnten.
114	OECD (2025): Economic Security in a Changing World – Kap. 6 «Cybersecurity»	Analytisch-strategisches Kapitel zum Beitrag der Cybersecurity zur wirtschaftlichen Sicherheit; beschreibt ökonomische und gesellschaftliche Dimensionen digitaler Sicherheit, skizziert einen risikobasierten Ansatz für Digital-Security-Risikomanagement und ordnet	Policy- und Governance-Kapitel ohne eigene Interventionsstudie; nutzt bestehende Empfehlungen, Beispiele und Indikatoren zu Vorfällen und umgesetzten Digital-Security-Massnahmen, ohne standardisierte verhaltensbezogene	nein – Bietet einen Policy- und Governance-Rahmen mit Hinweisen auf Messinitiativen und Indikatoren, evaluiert jedoch keine konkreten Awareness-Programme und liefert keine verhaltensbezogenen Outcome-Kennzahlen (keine Klick-/Meldequoten	International; Orientierungsrahmen der OECD mit hoher Relevanz für OECD-Staaten inklusive Schweiz als strategische Leitplanke für nationale Cybersecurity-Politik, Risikomanagement und Governance, jedoch ohne

		zentrale OECD-Instrumente sowie Governance-, Regulierungs- und Standardisierungsfragen (u. a. Zero Trust, Lieferkettensicherheit, Schutz kritischer Aktivitäten und Netze) ein.	Outcome-Messung von Awareness-Trainings oder Kampagnen.	oder Vorher-Nachher-Vergleiche).	direkte Evaluation von Awareness-Massnahmen.
115	Reeves, Delfabbro & Calic (2021): Encouraging Employee Engagement With Cybersecurity	Narratives Review zu «Cybersecurity Fatigue» als spezieller Form von Arbeitsdisengagement; entwickelt ein Vier-Komponenten-Modell, das unterschiedliche Ressourcentypen («advice-related» vs. «action-related») und Fatiguetypen («attitudinal» vs. «cognitive») beschreibt und anhand von Fallvignetten typische Organisationssituationen illustriert.	Narratives Review auf Basis von Literatur aus Management, Psychologie und Informationssystemen, ergänzt um drei Fallvignetten; es werden keine eigenen quantitativen Daten erhoben und keine standardisierten Verhaltens- oder Vorher-Nachher-Messungen durchgeführt.	nein – Zeigt auf, dass Umfang und Belastung durch SETA-Programme mitunter schwach oder sogar negativ mit Sicherheitsverhalten zusammenhängen können und führt dies konzeptionell auf Cyberfatigue zurück, berichtet jedoch keine eigene empirische Evaluation konkreter Awareness- oder Trainingsmassnahmen und keine verhaltensnahen Wirksamkeitskennzahlen.	International; allgemeiner Organisationskontext, konzeptionell sehr wichtig für Schweizer Organisationen, um Awareness-Programme so zu gestalten, dass Ermüdung und Überforderung vermieden und Engagement für Cybersecurity langfristig erhalten bleiben.
116	SANS Institute (2024): SANS 2024 Security Awareness Report – Embedding a Strong Security Culture	Jährlicher globaler Benchmark- und Trendreport zu Security-Awareness-Programmen und Sicherheitskultur; 2024 fliessen Antworten von über 1’000 Security-Awareness-Verantwortlichen aus mehr als 70 Ländern ein, die Programme anhand des Security Awareness Maturity Model® nach Reifegraden einordnen und Kennzahlen zu Teamgrössen, Budget, Verankerung und Top-Human-Risks liefern.	Standardisierte Online-Befragung von Awareness-Verantwortlichen mit Auswertung von Programmmetriken (Reifegrad, Ressourcen, Governance, Risikobild) anhand des Maturity Models, ohne Erhebung individueller Vorher-Nachher-Verhaltensdaten von Mitarbeitenden.	nein – Der Report zeigt Korrelationen (z. B. dass Programme mit messbarer Verhaltensänderung im Mittel rund 1,8 FTE und Programme mit Kultur- und Metrikfokus etwa 4,2 FTE benötigen) und beschreibt wahrgenommene Herausforderungen, liefert jedoch keine verhaltensbezogenen Outcome-Kennzahlen zu spezifischen Trainings- oder Kampagnenmassnahmen.	International; hoher Orientierungswert für Schweizer Behörden und Organisationen zur Einordnung der eigenen Awareness-Programme hinsichtlich Reifegrad, Ressourcenausstattung und Prioritäten, ohne direkten Wirksamkeitsnachweis einzelner Trainings- oder Kampagnenformate.
117	SANS Institute (2025): SANS	Jährlicher globaler Benchmark- und Trendreport zu	Standardisierte Online-Befragung von Awareness-	nein – Bietet Survey-basierte Benchmarks,	International; hoher Orientierungswert für Schweizer

	2025 Security Awareness Report	Security-Awareness-Programmen und Sicherheitskultur, basierend auf Antworten von über 2'700 Security-Awareness-Verantwortlichen aus mehr als 70 Ländern; liefert Kennzahlen zu Programmreife, Teamgrössen, Budget, Governance und Verankerung sowie Einschätzungen zu menschenbezogenen Risiken (u. a. Social Engineering als Top-Risiko).	Verantwortlichen mit Auswertung von Programmkennzahlen (Reifegrad, Ressourcen, Governance, Kulturintegration) und wahrgenommenen Risiken; keine Primärmessung des Verhaltens von Mitarbeitenden oder Vorher-Nachher-Designs.	Reifegradmodelle und Einschätzungen zu Ressourcenbedarf für Verhaltens- und Kulturveränderung, liefert jedoch keine verhaltensbezogenen Outcome-Evaluationen einzelner Trainings- oder Kampagnenprogramme (keine Klick-/Meldequoten oder Kontrollgruppenvergleiche).	Organisationen und Verwaltungen, um eigene Awareness-Programme hinsichtlich Reifegrad, Ressourcen und Risikobild mit globalen Benchmarks zu vergleichen, ohne direkten Wirksamkeitsnachweis für konkrete Trainingsmassnahmen.
118	Schaltegger et al. (2025): Human behavior in cybersecurity	Perspektiven- und Framework-Artikel, der Konzepte der Risikoforschung systematisch auf Cybersecurity überträgt; diskutiert unterschiedliche Formen von Unsicherheit (aleatorisch vs. epistemisch), Heuristiken und Risk Compensation, Mental-Models-Ansätze für zielgruppenspezifische Risikokommunikation sowie das Social Amplification of Risk Framework (SARF) und kritisiert das klassische Knowledge-Deficit-Modell.	Konzeptioneller Beitrag auf Basis bestehender Literatur und theoretischer Modelle; entwickelt einen argumentativen Rahmen für die Analyse menschlichen Verhaltens in der Cybersecurity, ohne eigene Feldstudien oder standardisierte verhaltensbezogene Messgrössen (z. B. Klick- oder Meldequoten) zu erheben.	nein – Entwickelt ein Forschungs- und Argumentationsprogramm sowie Implikationen für Policy, Kommunikation, Messung und Gestaltung von Cybersecurity-Massnahmen, liefert aber keine eigenen verhaltensbezogenen Outcome-Daten oder Vorher-Nachher-Evaluationen konkreter Awareness- oder Trainingsinterventionen.	Schweiz; Forschungsteam mit starkem Bezug zu Schweizer Hochschulen, konzeptionell sehr relevant für Behörden und Organisationen, die risikowissenschaftliche Konzepte gezielt in Awareness-, Kommunikations- und Messstrategien integrieren wollen, ohne direkte Wirksamkeitsnachweise zu bieten.
119	Schwab et al. (2025): What Makes Phishing Simulation Campaigns (Un)Acceptable?	Prä-registriertes Vignettenexperiment zu simulierten Phishing-Kampagnen, in denen jeweils vorherige Einwilligung der Mitarbeitenden, finanzielle Anreize in der Phishing-E-Mail (Bonus vs. kein Bonus) und Konsequenzen bei Klick (z. B. keine	Prä-registriertes Vignettenexperiment mit N = 793 Personen; Bewertung mehrerer Szenarien hinsichtlich Akzeptabilität der beschriebenen Phishing-Simulation und selbstberichteter Manipulationsintention (z. B.	nein – Untersucht Akzeptanz und Manipulationsintention, nicht Trainingswirksamkeit; zeigt, dass vorherige Einwilligung die Akzeptanz signifikant erhöht und harte Konsequenzen (v. a. Gespräch mit Vorgesetzten, Kündigung) sie deutlich senken, während	EU / international; liefert zentrale Hinweise für die ethische und akzeptanzorientierte Gestaltung von Phishing-Simulationen in Organisationen (inkl. Verwaltungen) und stützt die Forderung nach informierter Einwilligung und

		Konsequenz, Gespräch mit Vorgesetzten, zusätzliches Training, Kündigung) systematisch variiert werden.	bewusst falsch klicken, Kampagne nicht ernst nehmen).	sich für Manipulationsintention keine signifikanten Effekte zeigen und nur wenige Personen überhaupt Manipulationsabsichten angeben.	verhältnismässigen Konsequenzen, ohne selbst verhaltensnahe Trainingswirksamkeit zu messen.
120	Sommestad & Karlzén (2024): The unpredictability of phishing susceptibility	Repeated-measures-Feldexperiment ohne spezifische Awareness- oder Trainingseingriffe, in dem 102 Personen über einen gewissen Zeitraum insgesamt 2’294 potenziell schädliche E-Mails erhalten; untersucht wird, wie unterschiedliche Nachrichtenmerkmale zur individuellen Phishing-Suszeptibilität beitragen.	Repeated-measures-Feldexperiment mit Mehrebenenmodellierung; gemessen werden Link-Klicks (N ≈ 1’953) und das Ausführen von Dateien/Programmen (N ≈ 2’199) in Abhängigkeit von Scam-Typ, Grad der Adaption an die empfangende Person und eingesetzten Einfluss-/Persuasionstechniken.	nein – Zeigt, dass der Scam-Typ rund 6 % der Varianz bei Link-Klicks und etwa 3 % beim Ausführen von Dateien erklärt, während Personalisierung und weitere Einfluss-Techniken – kontrolliert für den Scam-Typ – keine robusten zusätzlichen Effekte zeigen; es werden jedoch keine Awareness- oder Trainingsprogramme getestet und somit keine Wirksamkeit von Massnahmen bewertet.	EU / international; liefert wichtige Hintergrund-Evidenz zu Angriffsmerkmalen und deren Beitrag zur Suszeptibilität und ist damit indirekt relevant für die Gestaltung von Awareness-Inhalten in Schweizer Organisationen, ohne direkt Trainingswirksamkeit zu beurteilen.
121	Steves, Greene & Theofanos (2020): Categorizing human phishing difficulty – A Phish Scale	Einführung der Phish Scale als Messmethode zur Bewertung der menschlichen Erkennungsschwierigkeit von Phishing-E-Mails; die Skala kombiniert sichtbare Message Cues (z. B. Tippfehler, ungewöhnliche Absender, Links) mit dem Premise / Workplace Alignment, also der Passung der Story zum Arbeitskontext der Zielgruppe, und wird auf zehn betriebliche Phishing-Übungen angewendet.	Analyse von Daten aus zehn realen Phishing-Simulationen: E-Mails werden entlang der beiden Dimensionen (Message Cues, Premise Alignment) geratet und in Schwierigkeitskategorien eingeteilt; diese Ratings werden mit den beobachteten Klickraten verglichen, um die Aussagekraft der Skala zu prüfen, ohne ein spezifisches Awareness-Training zu testen.	nein – Die Studie entwickelt und validiert ein Bewertungs-Framework und zeigt, dass höhere Schwierigkeitsstufen tendenziell mit höheren Klickraten einhergehen; dies dient der Validierung der Phish Scale, liefert aber keinen Vorher-Nachher-Nachweis der Wirksamkeit eines Trainingsprogramms.	International; grundlegendes Framework, das sich direkt in Schweizer Phishing-Simulationen integrieren lässt, um Klick- und Meldequoten nach Schwierigkeitsgrad der Mails zu interpretieren, ohne selbst einen Wirksamkeitsnachweis für Awareness-Trainings zu erbringen.
122	Sutton & Tompson (2025): Towards a Cybersecurity	Rapid Evidence Review zu Cybersecurity Culture (CSC) mit 1’768 Treffern in der Suche und 59 Studien in der finalen	Rapid Evidence Review mit systematischer Literaturrecherche und qualitativer Synthese; Ableitung eines	nein – Konzeptioneller und reviewbasierter Beitrag, der ein Rahmenmodell für die Verknüpfung von	EU / international; wichtiges theoretisches Fundament für Organisationen – einschliesslich Schweizer

	Culture–Behaviour Framework	Synthese; bündelt definitorische und empirische Arbeiten und leitet ein integriertes Rahmenmodell mit drei Ebenen ab (kulturelle Werte und Organisationskultur, Kultur-zu-Verhalten-Mechanismen, konkretes sicherheitsrelevantes Verhalten).	mehrdimensionalen Kultur–Verhalten-Rahmens und Identifikation zentraler CSC-Dimensionen (u. a. Einstellungen, Policy-Compliance, Security Education/Training/Awareness, Monitoring, Management Commitment), ohne eigene Primärdatenerhebung oder Vorher-Nachher-Design.	Cybersecurity-Kultur und Verhalten entwickelt, aber keine spezifischen Awareness- oder Trainingsprogramme empirisch evaluiert und keine verhaltensbezogenen Outcome-Daten berichtet.	Verwaltung –, um Cybersecurity-Kultur, Verhalten und Awareness-Programme systematisch zu verzahnen und spätere Wirksamkeitsmessungen konzeptionell sauber aufzusetzen, ohne selbst direkte Wirkungsnachweise konkreter Massnahmen zu liefern.
123	SWITCH (2024): Report 2024 .ch/.li – «Security awareness – iBarry and SISA»	Abschnitt des Jahresberichts der Registry für die ccTLDs .ch und .li, der die Zusammenarbeit mit der Swiss Internet Security Alliance (SISA) und der Plattform iBarry.ch beschreibt, inklusive drei Informationskampagnen 2024 (Passkeys, revDSG, Deepfakes), begleitenden Online-Inhalten und Tools wie checkawebsite.ibarry.ch sowie der Ankündigung eines iBarry-Newsletters.	Berichts- und Monitoring-Format ohne eigenes Interventionsdesign; fasst Themen, Kampagnen und Plattform-Aktivitäten von iBarry/SISA im Jahr 2024 zusammen, erhebt aber keine standardisierten verhaltensbezogenen Messgrössen wie Vorher-Nachher-Befragungen oder Klick-/Meldequoten.	nein – Hebt Themen, Kampagnen und Reichweiteninstrumente hervor, liefert jedoch keine verhaltensnahen Outcome-Kennzahlen zur Wirksamkeit der iBarry-/SISA-Aktivitäten (z. B. Veränderungen im Sicherheitsverhalten, Klick- oder Meldequoten).	Schweiz – auf die Schweizer Bevölkerung und Organisationen ausgerichtete Awareness-Aktivitäten; wichtige Referenz für öffentlich-private Zusammenarbeit (SWITCH, SISA, iBarry) in der Sensibilisierung, jedoch ohne veröffentlichte Wirksamkeitsdaten.
124	SWITCH (2025): Swiss Security Awareness Day (Bern, 11.09.2025)	Jährliche Fachtagung von SWITCH in Bern (u. a. mit Partnern wie SISA/iBarry), die sich auf Human-Centred Security und Security Awareness in Organisationen fokussiert und Fachpersonen aus Bildung, Kommunikation, IT, Security und Marketing mit Keynotes, Praxis-Talks, Best-Practice-Beispielen und Networking zusammenbringt.	Konferenz- und Community-Format ohne Interventionsdesign; es werden Inhalte, Praxisbeispiele und Austauschformate angeboten, aber keine standardisierten Messgrössen zu Verhaltensänderungen (z. B. Klick-/Meldequoten oder Vorher-Nachher-Vergleiche) erhoben.	nein – Der Anlass fungiert als zentrale Community- und Wissensplattform für Security Awareness in der Schweiz, es liegen jedoch keine publizierten Evaluationsstudien oder verhaltensbezogenen Outcome-Kennzahlen zur Wirksamkeit im Sinne von Verhaltensänderungen vor.	Schweiz; Leitveranstaltung zu Security Awareness mit direkter Relevanz für Hochschulen, Verwaltung, kritische Infrastrukturen und Unternehmen, primär zur Vernetzung, Wissensvermittlung und Inspiration, nicht zur formalen Wirksamkeitsmessung von Massnahmen.

125	van Steen (2025): Developing a behavioural cybersecurity strategy	Konzeptionelles Fünf-Schritte-Framework für eine verhaltensorientierte Cybersecurity-Strategie in Organisationen: von der Diagnose und Definition konkreter Zielverhaltensweisen (u. a. mit COM-B, Behaviour Change Wheel) über die Auswahl technischer, organisatorischer, policybasierter und verhaltensbezogener Interventionen bis zum Aufbau von Feedback- und Messschleifen sowie iterativer Anpassung.	Theoretisch-strategischer Beitrag auf Basis bestehender verhaltenswissenschaftlicher Modelle und Literatur; es werden keine eigenen Feldstudien durchgeführt und keine standardisierten verhaltensbezogenen Messgrössen (z. B. Klick- oder Meldequoten) erhoben, sondern ein Rahmen zur Planung, Umsetzung und Messung von Behaviour-Change-Massnahmen vorgeschlagen.	nein – Entwickelt einen verhaltensorientierten Strategie- und Evaluationsrahmen, stellt aber keine eigenen Vorher-Nachher-Daten oder Outcome-Kennzahlen zur Wirksamkeit konkreter Awareness- oder Behaviour-Change-Programme bereit.	EU / international; hohe strategische Relevanz für Organisationen, inklusive Schweizer Verwaltung, die klassische Awareness-Kampagnen um verhaltenswissenschaftlich fundierte Massnahmen erweitern und systematisch mit Mess- und Feedbackschleifen verknüpfen wollen, ohne dass der Ansatz bereits empirisch validiert ist.
126	Veneruso et al. (2020): A game-based learning experience for improving cybersecurity awareness	VR-basiertes Serious Game «CyberVR» mit sechs Mini-Games zu grundlegenden Cybersecurity-Themen (u. a. Informationsflüsse, Code Injection, Patch Management, Privilege Escalation, Kryptografie), in dem sich Spielende in einer virtuellen IT-System-Umgebung bewegen und schrittweise ein fiktives System absichern.	Design-Science-/Prototypenstudie, in der das Spielkonzept und die Mini-Games beschrieben werden; im Kurzpaper werden keine standardisierten Vorher-Nachher-Messungen von Wissen, Verhalten oder anderen verhaltensnahen Kennzahlen berichtet.	nein – Das Paper stellt das VR-Spiel und seine didaktische Anlage vor, verweist zwar auf eine erweiterte Fassung mit Evaluation, enthält jedoch selbst keine verhaltensnahe Wirksamkeitsmessung.	Internationaler Hochschul- und Ausbildungskontext; konzeptionell gut auf Schweizer Hochschulen und spezialisierte Awareness-Formate übertragbar, aber ohne eigenen empirischen Wirksamkeitsnachweis.
127	Volkamer, Sasse & Boehm (2020): Analysing simulated phishing campaigns for staff	Konzeptioneller Analyse- und Entscheidungsrahmen für simulierte Phishing-Kampagnen in Organisationen; beschreibt typische Ziele (Awareness, «teachable moments», Evaluation), Varianten der Durchführung (interne vs. externe Provider, Häufigkeit, Trainingsseiten) sowie Fragen zur	Theoretischer Übersichts- und Diskussionsbeitrag ohne eigenes Interventionsdesign; systematisiert Erfahrungswissen, Praxisbeispiele und Argumente zu Nutzen, Grenzen und Risiken von Simulated-Phishing-Kampagnen, erhebt aber keine	nein – Bietet eine kritische Einordnung von Simulated Phishing, zeigt mögliche Nebenwirkungen (u. a. auf Vertrauen, Selbstwirksamkeit, Verantwortungszuschreibung) auf und warnt vor einer einseitigen Fokussierung auf Klick-Raten, liefert jedoch keinen empirischen	EU / international – hoher Orientierungswert für Schweizer Behörden und Organisationen, die simulierte Phishing-Kampagnen planen oder bereits einsetzen; unterstützt dabei, Kampagnen in ein umfassenderes Sicherheits- und Reportingkonzept einzubetten und

		Datenvalidität, zu Nebenwirkungen und zur Einbettung in andere Awareness-Formate.	standardisierten verhaltensbezogenen Messgrössen (z. B. Vorher-Nachher-Klickraten, Meldequoten).	Wirksamkeitsnachweis konkreter Trainingsprogramme.	Klick-Raten nicht als einzigen Wirkungsindikator zu verwenden.
128	Wang, Guo & Yang (2022): Effectiveness of cyber security awareness in ICS risk assessment frameworks	Modellstudie im Kontext industrieller Steuerungssysteme (ICS), in der ein bestehender Incident-Response-Rahmen mit der MP²DR²-Risikokontrollmatrix erweitert wird: Sicherheitsbewusstsein wird als zusätzliche Kontrollmassnahme neben technischen und organisatorischen Kontrollen eingeführt und in verschiedenen Bedrohungs- und Asset-Szenarien berücksichtigt.	Quantitatives Modellierungs- und Bewertungsdesign ohne reale Intervention: Die Effektivität von Kontrollen wird für mehrere Szenarien mit und ohne Awareness rechnerisch verglichen; es werden keine empirischen Verhaltens- oder Vorher-Nachher-Daten (z. B. Fehlerraten von Mitarbeitenden) erhoben.	nein – Die Berechnungen zeigen, dass Sicherheitsbewusstsein in mehreren Szenarien ähnlich hohe oder höhere Effektivitätswerte wie andere Kontrollen erreicht und die Priorisierung der Kontrollen verändert, bleiben aber rein modellbasiert ohne Nachweis realer Verhaltensänderungen durch Awareness-Massnahmen.	Internationaler ICS- und Kritische-Infrastrukturen-Kontext; konzeptionell relevant für Betreiber kritischer Infrastrukturen in der Schweiz, um Sicherheitsbewusstsein als eigene Kontrollmassnahme in Risikomodelle einzubeziehen, jedoch ohne direkte Evaluation konkreter Awareness-Trainings oder Kampagnen.

Tabelle 3: Evidenztabelle – Quellen ohne direkte verhaltensnahe Evidenz («nein») (eigene Darstellung, basierend auf Literaturrecherche 2020–2025).

Anhang B – Interviewleitfaden und schriftliche Befragung

B1 – Hinweis zur Befragung und Interviewleitfaden

Im Rahmen der empirischen Analyse dieser Arbeit wurden ausgewählte Fachpersonen im Zeitraum Anfang bis Mitte Dezember 2025 per E-Mail zu einer schriftlichen Befragung eingeladen. Die angefragten Fachpersonen erhielten eine kurze Beschreibung von Ziel und Kontext der Arbeit sowie einen strukturierten Fragenkatalog. Die Auswertung der Antworten erfolgt anonymisiert und die Ergebnisse werden ausschliesslich für wissenschaftliche Zwecke verwendet.

Die schriftlichen Fragen wurden je nach Funktion der angefragten Personen leicht angepasst (z. B. Bezugnahme auf die Rolle in einer Gemeindeexekutive, im Stadtparlament, in der Politikberatung oder in Projekten zur digitalen Demokratie). Nicht alle Personen erhielten denselben Fragenkatalog. Der nachfolgende Anhang B2 dokumentiert alle verwendeten Fragen in den versendeten Fragekatalogen.

Insgesamt wurden sechs Fachpersonen angefragt. Vier Personen haben schriftlich geantwortet (vgl. Anhang B3.1–B3.4), zwei Fachpersonen haben die Teilnahme abgelehnt. Entsprechend enthält Anhang B3 ausschliesslich die vier eingegangenen Antworten.

B2 – Verwendete Fragen in der schriftlichen Befragung

Die nachfolgende Übersicht enthält alle Fragen, die in den Fragekatalogen an die Fachpersonen verwendet wurden. Nicht jede Frage wurde allen Fachpersonen gestellt.

Frage-Set 1 – Gemeinderätin (Sicherheit/Finanzen)

- **Erlebte Situationen rund um Unterschriften und politische Rechte:** Aus Ihrer Erfahrung als Gemeinderätin: In welchen Situationen rund um Unterschriftenlisten, Stimmrechtsbescheinigungen oder andere Abläufe zu politischen Rechten haben Sie das Gefühl, dass Integrität besonders gefordert oder potenziell gefährdet ist?
- **Umgang mit Grauzonen und heiklen Fällen in der Gemeinde:** Wie geht Ihre Gemeinde mit solchen Grauzonen oder heiklen Fällen konkret um? Gibt es typische Vorgehensweisen, interne Absprachen oder «Da schauen wir besonders genau hin»-Momente im Umgang mit Unterschriftenlisten und politischen Rechten?
- **Unterstützung durch Bund/Bundeskanzlei aus Gemeindesicht:** Wenn Sie der Bundeskanzlei bzw. dem Bund einen Wunschzettel schreiben könnten: Welche 2–3 Dinge würden Ihnen helfen, Integrität bei Unterschriftensammlungen und im Umgang mit Unterschriften besser zu sichern (z. B. klarere Hinweise, Beispiele, Schulungsangebote, Checklisten)? Gibt

es umgekehrt Bereiche, in denen Sie finden: «Hier sollte der Bund eher zurückhaltend sein, das gehört in die Verantwortung der Gemeinden»?

Frage-Set 2 – Ehemaliger Chef der Kriminalpolizei und aktiver Kommunalpolitiker

- **Integritätsrisiken/Versuchungen:** Aus Ihrer Erfahrung als ehemaliger Chef der Kriminalpolizei und als aktiver Kommunalpolitiker: In welchen Situationen rund um Unterschriftensammlungen oder politische Kampagnen sehen Sie die grössten Integritätsrisiken oder Versuchungen, Grenzen zu überschreiten?
- **Grenze zwischen «hart, aber legitim» und «manipulativ»:** Wenn Sie fair geführte und problematische Sammelpraktiken oder Kampagnen vergleichen: Woran machen Sie persönlich die Grenze fest zwischen «hart, aber noch legitim» und «nicht mehr akzeptabel/manipulierend»? Gibt es Kriterien oder typische Merkmale, die Ihnen dazu einfallen?
- **Rolle der Bundeskanzlei/realistische Hebel:** Angenommen, die Bundeskanzlei möchte Komitees und Sammelnde mit einfachen Materialien zur Integrität unterstützen: Welche 2–3 Massnahmen oder Botschaften würden aus Ihrer Sicht in der politischen Praxis tatsächlich etwas bewirken – und wo sehen Sie klare Grenzen für den Bund (z. B. politische Neutralität, Eigenverantwortung der Komitees)?

Frage-Set 3 – Einwohnerrat/Kommunalpolitiker

- **Integritätsrisiken aus Kampagnen- und Praxissicht:** Aus Ihrer Erfahrung als Einwohnerrat und Kommunalpolitiker: In welchen Situationen rund um Unterschriftensammlungen oder politische Kampagnen sehen Sie die grössten Integritätsrisiken oder Versuchungen, Grenzen zu überschreiten?
- **Grenze zwischen «hart, aber legitim» und «manipulativ»:** Wenn Sie fair geführte und problematische Sammelpraktiken oder Kampagnen vergleichen: Woran machen Sie persönlich die Grenze fest zwischen «hart, aber noch legitim» und «nicht mehr akzeptabel/manipulierend»? Gibt es Kriterien oder typische Merkmale, die Ihnen dazu einfallen?
- **Was Komitees tatsächlich annehmen würden/Rolle der Bundeskanzlei:** Angenommen, die Bundeskanzlei möchte Komitees und Sammelnde mit einfachen Materialien zur Integrität unterstützen (z. B. kurze Leitlinien, Beispiele, Checklisten): Welche 2–3 Massnahmen oder Botschaften würden aus Ihrer Sicht in der politischen Praxis tatsächlich genutzt und ernst genommen – und was würde eher als moralisierend oder realitätsfremd wahrgenommen?

Frage-Set 4 – Fachperson digitale Demokratie (E-Collecting, E-ID)

- **Analoge vs. digitale Integritätsrisiken:** Aus Ihrer Erfahrung mit Projekten im Bereich digitaler Demokratie (z. B. E-Collecting, E-ID): Wo sehen Sie die wichtigsten Integritätsrisiken im heutigen analogen Unterschriftensammeln – und welche neuen Risiken entstehen oder verschieben sich, wenn man Sammelprozesse digitalisiert?
- **Designprinzipien für vertrauenswürdige Sammelprozesse:** Welche 2–3 Gestaltungsprinzipien halten Sie für zentral, damit Sammelprozesse – analog oder digital – als legitim und vertrauenswürdig wahrgenommen werden (z. B. Transparenz, Nachvollziehbarkeit, Usability, Inklusion, offene Standards)? Gibt es Designentscheide, bei denen Sie sagen würden, dass sie Vertrauen untergraben und Vorwürfe von Manipulation begünstigen können?
- **Rolle der Bundeskanzlei zwischen Infrastruktur und Sensibilisierung:** Die Bundeskanzlei bewegt sich zwischen technischer Infrastruktur (z. B. künftige E-Collecting-Lösungen) und eher «weichen» Massnahmen wie Sensibilisierung und Leitlinien für Komitees und Sammelnde. Welche Rolle halten Sie für eine Bundesbehörde hier für sinnvoll und tragfähig – und wo sehen Sie Grenzen, damit nicht der Eindruck einer technokratischen oder bevormundenden Steuerung politischer Prozesse entsteht?

Frage-Set 5 – IT-/Security-Verantwortlicher (Software, Plattformen, Security)

- **Typische «Risk-Momente» aus Security- und Praxissicht:** Aus Ihrer Erfahrung in der Entwicklung und im Betrieb von Software, Plattformen und sicherheitsrelevanten IT-Systemen: In welchen Situationen verhalten sich Menschen erfahrungsgemäss besonders leicht unsicher oder unvorsichtig (z. B. bei Phishing, Freigaben, Zugriffsanfragen, Umgang mit sensiblen Daten)?
- **Was Awareness wirklich verhaltenswirksam macht:** Viele Organisationen setzen Security-Awareness-Programme ein, aber nicht alle führen zu einem anderen Verhalten. Welche 2–3 Gestaltungsprinzipien haben sich aus Ihrer Sicht als besonders wirksam erwiesen, wenn es darum geht, Verhalten tatsächlich zu verändern (nicht nur Wissen zu vermitteln) – gerade bei Nutzenden, die wenig Zeit haben und nicht primär «Security» im Kopf haben?
- **Übertragung auf Unterschriftensammlungen/Rolle einer Behörde:** Wenn Sie diese Erfahrungen auf einen anderen Kontext übertragen – etwa Unterschriftensammlungen im politischen Bereich: Welche Art von Sensibilisierung oder Unterstützung durch eine Behörde wie die Bundeskanzlei halten Sie grundsätzlich für realistisch und wirksam, um faires Verhalten zu fördern? Und wo sehen Sie Grenzen dessen, was man mit Awareness und Guidelines überhaupt erreichen kann?

Frage-Set 6 – Politikberatung

- **Integritätsrisiken aus Sicht der Politikberatung:** Aus Ihrer Erfahrung als Politikberater: Wo sehen Sie im Umfeld politischer Kampagnen und Unterschriftensammlungen die grössten Integritätsrisiken oder Versuchungen zur Grenzüberschreitung?
- **Grenze zwischen legitimer Überzeugung und Manipulation:** Wenn Sie zwischen legitimer politischer Überzeugungsarbeit und Manipulation unterscheiden: Woran würden Sie in der Praxis festmachen, dass eine Unterschriftensammlung oder Kampagnenkommunikation noch «hart, aber legitim» ist – und ab wann sie problematisch erscheint? Gibt es Kriterien, die Ihnen dabei besonders wichtig sind?
- **Rolle und Grenzen des Staates bei Sensibilisierung:** Angenommen, die Bundeskanzlei möchte Komitees und Sammelnde mit einfachen Materialien zur Integrität unterstützen (z. B. kurze Leitlinien, Beispiele, Checklisten): Welche 2–3 Prinzipien wären Ihnen in einem freiheitlich-demokratischen System wichtig, damit ein solches Sensibilisierungskonzept politisch und normativ vertretbar ist? Und wo sehen Sie Grenzen dessen, was der Bund in Bezug auf Sensibilisierung und Verhaltenssteuerung tun sollte?

B3 – Vollständige Antworten der Befragten

Die nachfolgenden Unterabschnitte enthalten die vollständigen schriftlichen Rückmeldungen aus der Befragung (vgl. Abschnitt 4.4). Die Antworten werden im Wortlaut wiedergegeben. Personenangaben wurden anonymisiert. Auf die Wiederholung der Fragen wird verzichtet. Diese sind in Anhang B2 dokumentiert.

B3.1 – Antwort eines Kommunalpolitikers (ehemaliger Chef einer kantonalen Kriminalpolizei)

Die folgende Rückmeldung ging als schriftliche Antwort auf Frage-Set 2 ein. Sie stammt von einem Kommunalpolitiker einer mittelgrossen aargauischen Stadt mit früherer Tätigkeit als Chef einer kantonalen Kriminalpolizei. Orthografie und Formatierung wurden leicht an den Stil der Arbeit angepasst. Begrüssung, Grussformel und Namensnennung wurden weggelassen. Der Wortlaut der Rückmeldung wurde inhaltlich unverändert übernommen.

In Sachen Integrität bei Unterschriftensammlungen bin ich in keiner Art und Weise «Experte», und habe mich weder in meiner beruflichen noch in meiner politischen Tätigkeit näher mit dieser Thematik befasst und/oder mit derartigen Fällen zu tun gehabt. Ich gestatte mir dennoch, Ihnen in aller Kürze und unabhängig von Ihren Fragen einige Stichworte zu liefern:

- Ich erachte die Integrität bei Unterschriftensammlungen in der Schweiz im Unterschied zu vielen anderen Staaten als wenig problematisch und in aller Regel als befriedigendem Masse vorhanden.
- Ich erachte es als durchaus legitim, bei Unterschriftensammlungen und politischen Kampagnen die eigenen Argumente klar und deutlich (sogar auch etwas plakativ) ins Zentrum der Kampagne zu stellen.
- «Gegnerische» Argumente müssen meines Erachtens bei solchen Kampagnen nicht erwähnt werden.
- Eigentliche Lügen dürfen unter keinen Umständen in die Kampagne einfliessen. Auch Halbwahrheiten sind zu vermeiden.
- Werbung «in eigener Sache» zu machen, z. B. durch Medienberichte, Standaktionen oder Hausbesuche, ist meines Erachtens zulässig.
- Gegen «motivierende Überzeugungsarbeit» im Verwandten- und Bekanntenkreis im Vorfeld von Kampagnen ist nichts einzuwenden.
- Das Ausfüllen von Unterschriftenbogen für andere Personen ist meines Erachtens dann zulässig, wenn diese Personen transparent informiert sind und genau wissen, unter welche Kampagne sie schlussendlich ihre Unterschrift setzen.
- Die Sammlung von Unterschriften bei Personen, die nicht oder nur bedingt in der Lage sind, die Thematik der Kampagne zu erfassen, ist grenzwertig und aus meiner Sicht nicht zulässig.
- Die Fälschung von Unterschriften ist verboten und unter Strafe gestellt.

Ich hoffe, dass ich Sie mit diesen kurzen Angaben bei Ihrer Arbeit ein kleines bisschen unterstützen konnte.

B3.2 – Antwort eines weiteren Kommunalpolitikers

Die folgende Rückmeldung ging als schriftliche Antwort auf Frage-Set 3 ein. Sie stammt von einem weiteren Kommunalpolitiker einer mittelgrossen aargauischen Stadt. Orthografie und Formatierung wurden leicht an den Stil der Arbeit angepasst. Begrüssung, Grussformel und Namensnennung wurden weggelassen. Der Wortlaut der Rückmeldung wurde inhaltlich unverändert übernommen.

Einleitend könnte die Bundeskanzlei generelle Richtlinien, evtl. in Form einer Checkliste, hinausgeben, welche die Initianten auf den sachlichen Ablauf und die Datenintegrität aufmerksam macht.

Zum sachlichen Ablauf gehört ein Aufruf zur Prüfung der Fähigkeit eines Begehrens, dies muss inhaltlich und formell Sinn machen.

Es sollte alles im Sinne des Landes beurteilt werden nach der Prämisse:

- Ist das Anliegen gesetzmässig?
- Ist die Verhältnismässigkeit gegeben?
- Ist das Anliegen wirtschaftlich, das heisst sparsam umsetzbar, und gibt es einen Mehrwert für unser Volk?

Die Initianten könnten z. B. auch sensibilisiert werden über die Möglichkeit zum Nachschauen, welche ähnlichen Vorstösse bereits stattgefunden haben.

Dann geht es darum, die Möglichkeiten aufzuzeigen, wie ein sicheres E-Collecting stattfinden kann und wie dadurch das Vertrauen der Stimmenden sichergestellt werden kann (E-ID).

Auf welchen Systemen laufen diese Programme? Wo liegen die Daten? Wie wird mit den persönlichen Daten umgegangen? Wie lange bleiben diese Daten gespeichert? Durch wen sind diese einsehbar? Wer wertet diese aus?

Wie sieht ein standardisierter Prozess aus und die garantierte Qualitätssicherung? Wie sind die Restriktionen bei einem Datenmissbrauch? Wie sieht die gesetzliche Grundlage aus? Wie gehen Stimmberechtigte im Ausland damit um? Dürfen diese auch unterschreiben?

Ist die Hürde für die nötige Anzahl Unterschriften noch angemessen, oder ist diese zu tief?

Gerne nehme ich wie folgt Stellung zu Ihren Fragen:

Integritätsrisiken aus Kampagnen- und Praxissicht

Es wollen alle wissen, wo sind die Daten, was passiert mit den Daten, was wäre im Worstcase, wenn alles gehackt würde? Wer wertet aus? Wenn alles sicher funktioniert, wird es vermutlich zuerst eine Zeit lang hybrid nötig sein, Unterschriften zu sammeln. Auf welcher gesetzlichen Grundlage ist es möglich, E-Collecting zu betreiben?

Grenze zwischen «hart, aber legitim» und «manipulativ»

Der Inhalt des Begehrens muss nachvollziehbar sein, die Vor- und Nachteile für das Land müssen klar erörtert werden. Der Stimmberechtigte muss eine Risikoabschätzung vornehmen können. Das Parlament muss dies zwingend vorberaten und eine Empfehlung abgeben.

Was Komitees tatsächlich annehmen würden / Rolle der BK

Ich denke, Komitees würden eine entsprechende Sensibilisierung aufnehmen, in welcher sie sachlich gefragt werden über die oben erwähnten Punkte und eine Empfehlung, wie das Sammeln stattfinden soll.

Ich wünsche Ihnen viel Erfolg bei Ihrer Bachelorarbeit.

B3.3 – Antwort eines Unternehmers im Bereich digitaler Demokratie und E-Collecting

Die folgende Rückmeldung ging als schriftliche Antwort auf Frage-Set 4 ein. Sie stammt von einem Absolventen einer Schweizer Hochschule, der sich in einer Abschlussarbeit mit Fragen der digitalen Demokratie und des E-Collecting befasst hat und heute unternehmerisch in diesem Feld tätig ist. Orthografie und Formatierung wurden leicht an den Stil der Arbeit angepasst. Begrüssung, Grussformel und Namensnennung wurden weggelassen. Der Wortlaut der Rückmeldung wurde inhaltlich unverändert übernommen.

Analoge vs. digitale Integritätsrisiken

Wichtigste Punkte beim heutigen analogen Unterschriftensammeln:

- Auf der Strasse oder an der Haustür wird faktisch nicht verlässlich geprüft, ob jemand stimmberechtigt für das Begehren ist (Gemeinde, Alter, Stimmrecht). Die Kontrolle passiert erst bei der kommunalen Bescheinigung. Das schafft Raum für ungültige Unterschriften (z. B. falsche Gemeinde, nicht stimmberechtigt etc. gemäss Liste der Bundeskanzlei mit Kurzbegründungskennzeichen).
- Fehlanreize durch bezahltes Sammeln:
    - Falschangaben beim Ansprechen («Worum es wirklich geht»).
    - Druck oder Belästigung (Grenze zur unzulässigen Beeinflussung).
    - Fälschungen, insbesondere wenn Kontrolle und Nachvollziehbarkeit (Traceability) der Bögen schwach sind.
- Manipulation der Bögen: Papier kann verloren gehen, nachträglich ergänzt, ausgetauscht oder selektiv eingereicht werden.
- Intransparenz über Sammelqualität und -praktiken: Die Öffentlichkeit sieht das Resultat (eingereichte Zahl), aber kaum, wer gesammelt hat, unter welchen Regeln, wie Daten behandelt wurden oder wie Fehler korrigiert wurden.
- Besonders kritisch ist die Frage: Welche Bögen hat die Bundeskanzlei nachträglich aus welchen Gründen für ungültig erklärt? (aktuelles Beispiel: Dossier «amtlich gestrichene Unterschriften» auf demokratie.ch).
- «Unterschriftenroboter» als Wake-up-Call (vgl. entsprechende Debatte, z. B. auf LinkedIn).

Wichtigste Punkte beim digitalen Sammeln (E-Collecting):

- Skalierung und Geschwindigkeit: Das Kernrisiko digital ist weniger, ob Manipulation möglich ist, sondern dass sie bei Erfolg sofort sehr viele Stimmen oder Unterschriften betreffen kann

(schnelle, massenhafte Einreichung; Kampagnen können in Stunden statt Wochen eskalieren).

- Identitäts- und Authentisierungsrisiken verlagern sich:
  - Analog: «Ist diese Unterschrift echt?» – kann analog sowieso nicht zuverlässig geprüft werden und trägt auch nicht zur Identifizierung bei (vgl. Braun Binder).
  - Digital: «Ist diese Person korrekt authentisiert und handelt sie selbst?» (Account-Übernahme, Social Engineering, Malware, SIM-Swap, Phishing). Die E-ID beziehungsweise Authentisierung wird damit zum kritischen Single Point of Failure.
- Systemische Risiken (Infrastruktur und Anbieter):
  - Abhängigkeit von Plattformen, Zertifikaten, Cloud-Anbietern.
  - Fehler in Implementierung oder Updates können die Integrität stärker bedrohen als Einzelbetrug im Analogen.
- Nachweisbarkeit versus Geheimhaltung:
  - Für Unterschriften gibt es kein Stimmgeheimnis wie beim Urnengang, aber es gibt Datenschutz und politische Sensibilität.
  - Faktisch gibt es ein «Unterschriftengeheimnis», das auf dem digitalen Kanal eher eingefordert wird als im analogen Kanal.
- «Interface-Manipulation» und Dark Patterns:
  - Digital kann das UI/UX die Entscheidung stärker beeinflussen (voreingestellte Zustimmung, irreführende Formulierungen, Klickstrecken).
  - Risiko der falschen Attribution («Ich dachte, ich habe nur Infos bestellt.»).
- Ungleichheiten verschieben sich:
  - Analog benachteiligt teils Personen mit wenig Zeit oder Präsenz im öffentlichen Raum.
  - Digital benachteiligt Personen ohne digitale Mittel oder Kompetenzen oder mit höherer Skepsis gegenüber E-ID.
  - Daraus folgt ein Legitimitätsrisiko, wenn E-Collecting faktisch «pay-to-play» via digitale Kampagnenoptimierung wird.

Designprinzipien für vertrauenswürdige Sammelprozesse

Nachvollziehbarkeit und Prüfbarkeit (Auditability):

- Es muss für Behörden und – in angemessenem Rahmen – für Öffentlichkeit und Beobachtende überprüfbar sein, dass Prozesse korrekt ablaufen.
- Digital bedeutet das: nachvollziehbare Logs, klare Prüfschritte, unabhängige Audits, reproduzierbare Auswertungen.

- Analog bedeutet das: klare Verantwortlichkeiten, nummerierte Bögen, dokumentierte Übergaben, stichprobenfähige Kontrollen.
- Vertrauensbildend sind Open-Source-Lösungen, öffentliche Bug-Bounty-Programme und freie Lizenzen der Systeme (FLOSS).

Transparenz über Rollen, Regeln und Datenflüsse:

- Wer betreibt die Infrastruktur? Wer ist rechtlich verantwortlich? Welche Daten werden erhoben, wie lange gespeichert, wofür verwendet?
- Besonders vertrauensbildend ist eine klare Trennung zwischen politischem Komitee, technischer Plattform und staatlicher Prüfstelle (keine Vermischung der Rollen).
- E-Collecting ändert grundlegend die Verantwortlichkeiten im Sammelprozess: Wo vorher Komitees im Zentrum standen, ist neu eine Plattform. Die Frage, wer der Plattform vertraut und wie sie betrieben wird, wird zentraler.

Inklusion und niedrige Fehlerrate:

- Prozesse müssen so gestaltet sein, dass gutwillige Stimmberechtigte nicht unnötig scheitern (falsche Gemeinde, abgebrochene Authentisierung, missverständliche Schritte).
- Gute Usability ist nicht nur Komfort, sondern Integrität: Je weniger Fehler, desto weniger Angriffsfläche und desto weniger Zweifel an der Legitimität.
- Barrierefreiheit ist ein zentrales Element vertrauenswürdiger Sammelprozesse.

Rolle der Bundeskanzlei zwischen Infrastruktur und Sensibilisierung

- Es sollte keine Staatsplattform entstehen: Es darf nicht der Eindruck entstehen, dass eine staatliche Plattform den politischen Prozess dominiert.
- Daten und Prozesse sollen möglichst transparent und dezentral bei den Stimmberechtigten liegen.

B3.4 – Antwort eines Unternehmers im Bereich Software- und IT-Sicherheit

Die folgende Rückmeldung ging als schriftliche Antwort auf Frage-Set 5 ein. Sie stammt von einem Unternehmer im Bereich Software- und IT-Sicherheit, der u. a. für Lernplattformen und sicherheitsrelevante IT-Infrastrukturen Verantwortung trägt. Orthografie und Formatierung wurden leicht an den Stil der Arbeit angepasst. Begrüssung, Grussformel und Namensnennung wurden weggelassen. Der Wortlaut der Rückmeldung wurde inhaltlich unverändert übernommen.

Typische «Risk-Momente» aus Security- und Praxissicht

Autorität und Glaubwürdigkeit:

- Loyalität vortäuschen: als Kollege oder Vorgesetzter auftreten.
- Pretexting: eine Geschichte mit scheinbar tiefem Wissen über die betroffene Person erfinden.
- «Chefhaftigkeit» zeigen: Sicherheit, Eloquenz, Fachwissen und scheinbare Rechtsfragen demonstrieren.
- Kollegialität: Druck aufgrund einer persönlichen Beziehung zur betroffenen Person aufbauen.

Schweizer Pflichtbewusstsein:

- Menschen in der Schweiz haben den Zwang, Formulare und Anfragen vollständig auszufüllen.
- Menschen in der Schweiz haben den Zwang, Anfragen um (fast) jeden Preis zu erfüllen und es «richtig» zu machen.

Zugzwang, Zeitzwang, Ausnützung von Impulsen:

- Künstliche Verknappung der Zeit, um einen fundierten Entscheid zu treffen.

Projektion:

- Umleiten von Ärger des Kunden in eine davon eigentlich losgelöste Aktion.

MICE (Money, Ideology, Coercion/Compromise, Ego):

- Mitarbeitende unterliegen den Versuchungen oder Zwängen von MICE und handeln oft nicht nur in ihrem eigenen Interesse. Sie werden geführt oder gezwungen.

Wenn keine festen Kontrollmechanismen oder «Auswege» vorliegen, auf die sich Mitarbeitende berufen können:

- Peerfunktionen einführen: Eine Peer- oder Supervisor-Funktion muss zustimmen.
- Automatische Protokollierung von Gesprächen und Zugriffen einführen: «Das kann ich nicht machen, das wird protokolliert.»
- Befugnisse aufteilen: «Da habe ich keinen Zugriff.»
- Systemgestützte Verifizierung durch mehrere Faktoren einführen: «Ohne Ihre PIN oder ID-Nummer kann ich nicht auf das System zugreifen.»

Was Awareness wirklich verhaltenswirksam macht

Training in der Anwendung:

- Awareness ist mehr als nur «Durchsprechen». Verinnerlichen braucht Wiederholung und sichere Anwendung.
- Regelmässige Überprüfung mit variierenden Aktionen hilft.
- Schulung unterstützt die allgemeine Modellbildung, aber der einzelne Fall kann sich stark von der Schullösung unterscheiden.
- Um Sicherheit zu gewährleisten, muss die Person verschiedenen Variationen eines Tatbestands ausgesetzt werden.

Belohnung und Strafe:

- Intrinsisch motivierte Mitarbeitende reagieren auf Awareness und Sicherheit in der Anwendung.
- Unmotivierte Mitarbeitende ohne Konsequenzen hingegen nicht. Sie sehen keinen Grund für Mehraufwand, wenn dieser keinen Mehrertrag bringt oder keine Ertragsminderung verhindert.

Übertragung auf Unterschriftensammlungen und Rolle einer Behörde

- Die Unterschriftensammlung als demokratisches Mittel muss einfach und zugänglich sein.
- Die Motivation der Initianten hilft ihnen, möglichst viele Unterschriften zu sammeln. Dafür nutzen sie alle Überzeugungsmittel aus der ersten Frage.
- Es ist schwierig, die Sammlung zu erschweren, ohne demokratische Mittel zu entwerten und ohne proaktiv gegen alle zukünftigen «Marketing-Ideen» bereits Mittel und Strafen festzulegen. Sonst würde man vorschlagen: Unterschriften müssen persönlich auf einem Amt beigebracht werden, wie bei allen beglaubigten Aktionen.
- Um dem Druck bei einer Sammelaktion entgegenzuwirken, sollte die unterschreibende Person die Relevanz ihres Konsenses verstehen und diesen unabhängig von den Sammelaktivitäten bestätigen können – ähnlich wie beim Double-Opt-in im Marketing.
- Die Bundeskanzlei sollte Unterschreibende auf dem Postweg oder per E-Voting-App kontaktieren und ihren Konsens einholen.
- Die Bundeskanzlei verifiziert die Unterschriften über das Wählerverzeichnis und auf dem (E-)Postweg, und die unterschreibende Person kann ihre Zustimmung widerrufen, falls sie ohne ihr Wissen oder unter Druck erfolgt ist.

Anhang C – Prototypische Sensibilisierungsmaterialien (Paket B)

C.1 Ziel und Einordnung

Dieser Anhang enthält prototypische Textvorschläge für die in Abschnitt 7.3 beschriebenen Hilfsmittel aus Paket B. Die Materialien richten sich an Komitees und Sammelnde und sollen die Integrität von Unterschriftensammlungen praxisnah unterstützen. Sie übersetzen die in Kapitel 5 identifizierten Wirkungshebel sowie die in Kapitel 6 sichtbaren Praxisperspektiven in konkrete, leicht nutzbare Formate.

Die vorgeschlagenen Texte sind bewusst neutral formuliert und dienen als Vorlagen. Sie können von der BK oder von Komitees inhaltlich und sprachlich an spezifische Bedürfnisse, Zielgruppen und das jeweils verwendete Corporate Design angepasst werden. Die Bundeskanzlei entscheidet im Rahmen ihrer Rolle, ob und in welcher Form sie diese Vorlagen zur Verfügung stellt und übernimmt keine Verantwortung für deren Umsetzung in einzelnen Kampagnen. Die Verantwortung für die konkrete Ausgestaltung, den Einsatz und allfällige Anpassungen liegt bei den Komitees.

Die Materialien sind in drei Bausteine gegliedert:

3. Integritäts-Check für Komitees (C.2)
4. Einseiter «Faires Sammeln» für Sammelnde (C.3)
5. Kurz-Checkliste «Heikle Situationen und rote Linien» (C.4)

C.2 Integritäts-Check für Komitees (A4)

Titel: Integritäts-Check für Komitees – Selbstreflexion zur Unterschriftensammlung

Zweck und Nutzung: Dieser Integritäts-Check dient Komitees als Grundlage für eine gemeinsame Standortbestimmung zur Integrität der Unterschriftensammlung. Er kann zu Beginn einer Kampagne, bei wichtigen Meilensteinen oder beim Eintritt neuer Schlüsselpersonen eingesetzt werden. Die Aussagen und Fragen sollen im Komitee gemeinsam besprochen werden. Aus offenen Punkten können konkrete Vereinbarungen und Massnahmen abgeleitet werden.

Layout-Hinweis für die Umsetzung: In der Praxis bietet sich eine Tabelle mit zwei Spalten an: links «Aussage/Frage», rechts «Bemerkungen/Vereinbarte Massnahmen».

Vorschlag für den Inhalt:

Aussage/Frage 1 – Rollen und Zuständigkeiten: Wir haben im Komitee klar festgelegt, wer Sammelnde instruiert und bei Fragen zu Integrität ansprechbar ist.

Aussage/Frage 2 – Grundverständnis von Integrität: Wir haben im Komitee besprochen, welche Sammelpraktiken wir bewusst nicht einsetzen wollen – selbst wenn sie formal zulässig wären.

Aussage/Frage 3 – Zusammenarbeit mit Sammelorganisationen: Wir haben klare Kriterien definiert, nach denen wir Angebote externer Sammelorganisationen prüfen (z. B. Transparenz zu Arbeitsbedingungen, Entschädigungsmodellen und Sammelmethoden).

Aussage/Frage 4 – Umgang mit Drucksituationen: Wir haben im Komitee besprochen, wie Sammelnde mit Drucksituationen umgehen sollen (z. B. wenn Personen sich bedrängt fühlen oder wenn Sammelziele sehr ambitioniert sind).

Aussage/Frage 5 – Sensible Personengruppen: Wir haben uns Gedanken gemacht, wie wir mit Personen umgehen, deren Urteilsfähigkeit eingeschränkt sein könnte (z. B. in Pflegeeinrichtungen oder bei Personen mit kognitiven Einschränkungen).

Aussage/Frage 6 – Kommunikationsmaterialien für Sammelnde: Unsere schriftlichen Materialien für Sammelnde (Instruktionen, E-Mails, Chat-Nachrichten) enthalten klare Hinweise auf faires Sammeln und rote Linien.

Aussage/Frage 7 – Meldemöglichkeiten: Sammelnde wissen, an wen sie sich im Komitee wenden können, wenn sie unsichere oder heikle Situationen erleben oder von problematischen Praktiken erfahren.

C.3 Einseiter «Faires Sammeln» für Sammelnde

Titel: Faires Sammeln – Leitlinien für Sammelnde

Zweck und Zielgruppe: Dieser Einseiter richtet sich an alle Personen, die im Auftrag eines Komitees Unterschriften sammeln – unabhängig davon, ob sie ehrenamtlich oder entgeltlich tätig sind. Er vermittelt auf einer Seite die wichtigsten Grundsätze für faires Sammeln in einfacher, verständlicher Sprache.

Layout-Hinweis für die Umsetzung: Die Formulierungen verwenden bewusst die Du-Form, da sie für viele Sammelkontexte (z. B. Strassensammlung, Vereinsumfeld) unmittelbar anschlussfähig ist. Komitees können die Ansprache bei Bedarf auf die Sie-Form umstellen.

Vorschlag für den Inhalt:

Warum Integrität beim Sammeln wichtig ist: Mit Deiner Unterstützung trägst du dazu bei, dass die direkte Demokratie in der Schweiz funktioniert. Integrität bei der Unterschriftensammlung bedeutet, dass jede Unterschrift freiwillig, informiert und ohne unzulässigen Druck zustande kommt. Die

folgenden Leitlinien helfen Dir, fair zu sammeln – im Interesse der unterzeichnenden Personen, des Komitees und der Glaubwürdigkeit des Volksbegehrens.

Leitlinien für faires Sammeln:

6. **Keine Unterschriften ohne Einverständnis:** Sammle keine Unterschriften für Personen, die nicht klar zugestimmt haben. Unterschriften dürfen nicht ohne Wissen und Wollen der betroffenen Person geleistet werden.
7. **Keine irreführenden Aussagen:** Erkläre kurz und ehrlich, worum es in der Vorlage geht. Versprich nichts, was die Vorlage nicht leisten kann, und verschweige keine zentralen Punkte.
8. **Besondere Vorsicht bei vulnerablen Personen:** Sei zurückhaltend bei Personen, deren Urteilsfähigkeit eingeschränkt sein könnte (z. B. in Pflegeeinrichtungen). Wenn du unsicher bist, verzichte im Zweifel auf eine Unterschrift.
9. **Transparenz beim Ausfüllen für Dritte:** Wenn du einer Person beim Ausfüllen hilfst, lies alle Angaben vor und frage nach, ob alles so gewollt ist. Fülle keine Unterschriftenzeilen ohne ausdrückliche Zustimmung aus.
10. **Kein unzulässiger Druck:** Setze niemanden unter Druck, um eine Unterschrift zu bekommen – auch nicht durch Gruppendruck, Beschämung oder das Schüren von Angst.
11. **Fragen statt improvisieren:** Wenn Du in eine Situation kommst, in der Du unsicher bist (z. B. ungewöhnliche Angebote, Sammeln gegen Geld, Unterschriftenstapel ohne persönlichen Kontakt), brich die Situation ab und frage im Komitee nach.

Deine Ansprechperson im Komitee

Bei Fragen oder wenn Du heikle Situationen erlebst, wende Dich an:

Name: _____

Telefon/E-Mail: _____

C.4 Kurz-Checkliste «Heikle Situationen und rote Linien»

Titel: Heikle Situationen und rote Linien – Kurz-Checkliste für Sammelnde

Zweck und Nutzung: Einige Situationen sind besonders sensibel und können die Integrität der Unterschriftensammlung gefährden. Die folgende Checkliste nennt typische Konstellationen und gibt Hinweise, wie Du fair damit umgehen kannst. Sie eignet sich für kurze Briefings zu Beginn einer Sammelaktion oder zur Nachbesprechung konkreter Erfahrungen.

Layout-Hinweis für die Umsetzung: In der Praxis bietet sich eine dreispaltige Tabelle an: «Situation» – «Woran erkenne ich, dass es heikel wird?» – «Was ist ein fairer Umgang?». Der Text unten ist direkt tabellarisch umsetzbar.

Situation 1: Sammeln im Freundes- und Bekanntenkreis

Woran erkenne ich, dass es heikel wird? Personen unterschreiben vor allem, um Dir einen Gefallen zu tun, ohne den Inhalt wirklich zu kennen oder überzeugt zu sein.

Was ist ein fairer Umgang? Gib Deinem Gegenüber Zeit, sich zu informieren, und akzeptiere ein Nein ohne Diskussion. Mach klar, dass es Dir wichtiger ist, dass sie überzeugt sind, als dass Du möglichst viele Unterschriften bekommst.

Situation 2: Sammeln bei Personen mit möglicher Einschränkung der Urteilsfähigkeit

Woran erkenne ich, dass es heikel wird? Du hast den Eindruck, dass eine Person den Inhalt oder die Tragweite der Vorlage nicht versteht.

Was ist ein fairer Umgang? Verzichte im Zweifel auf eine Unterschrift. Wenn eine Betreuungsperson anwesend ist, kann diese unterstützen – trotzdem gilt: «keine Unterschrift ohne ausdrückliche Zustimmung».

Situation 3: Haustürbesuche und Sammeln im privaten Umfeld

Woran erkenne ich, dass es heikel wird? Personen wirken unter Zeitdruck oder sagen mehrmals Nein, während Du oder andere weiter nachfragen.

Was ist ein fairer Umgang? Stelle Dich kurz vor, erkläre das Anliegen in wenigen Sätzen und akzeptiere ein Nein. Vermeide Drucksituationen und beende das Gespräch freundlich.

Situation 4: Sammeln an Orten mit starkem sozialen Druck (z. B. im Verein oder am Arbeitsplatz)

Woran erkenne ich, dass es heikel wird? Jemand unterschreibt nur, weil andere zuschauen oder die Stimmung erwarten lässt, dass alle mitmachen.

Was ist ein fairer Umgang? Biete die Möglichkeit, sich in Ruhe und ohne Öffentlichkeit zu entscheiden (z. B. Informationsmaterial mitgeben). Mach klar, dass eine Unterschrift freiwillig ist und keine Konsequenzen bei einem Nein entstehen.

Situation 5: Angebote, Unterschriften «am Stück» zu liefern

Woran erkenne ich, dass es heikel wird? Dir werden Unterschriftenlisten angeboten, bei denen unklar ist, wie die Unterschriften zustande gekommen sind, oder es werden ungewöhnlich hohe Stückzahlen in kurzer Zeit versprochen.

Was ist ein fairer Umgang? Nimm solche Angebote nicht einfach an. Kläre im Komitee ab, wie damit umzugehen ist, und verzichte im Zweifel darauf.

Hinweis zum Schluss: Wenn Du in einer anderen Situation ein ungutes Gefühl hast, gilt dasselbe Prinzip: Im Zweifel nachfragen, statt allein zu entscheiden. Integrität heisst auch, heikle Situationen ernst zu nehmen und gemeinsam nach fairen Lösungen zu suchen.