Standeskanzlei Graubünden
Chanzlia chantunala dal Grischun
Cancelleria dello Stato dei Grigioni

KANTON LUZERN

Kanton St.Gallen
Staatskanzlei

Thurgau
Staatskanzlei

Vorfall in Basel-Stadt: Überprüfung Prozesse und Definition von Massnahmen

E-Voting Graubünden / Luzern / St.Gallen / Thurgau

Autoren	**E-Voting Beauftragter (GR)** **Projektleitung E-Voting (LU)** **Leitung der elektronischen Stimmabgabe (SG)** **Fachperson E-Voting (TG)**

Datum	17.04.2026
Version	1.0
Klassifizierung	Keine

Änderungskontrolle

Version	Datum	Beschreibung	Name
0.9	27.03.2026	Entwurf für das Zulassungsgesuch der Kantone GR, SG und TG für den Urnengang vom 14.06.2026	E-Voting Beauftragter (GR) Projektleitung E-Voting (LU) Leitung der elektronischen Stimmabgabe (SG) Fachperson E-Voting (TG)
1.0	17.04.2026	Überarbeitete Version für das definitive Gesuch um Erteilung Grundbewilligung für LU, Nachreichung der Kantone GR, SG und TG für den Zulassungsentscheid.	E-Voting Beauftragter (GR) Projektleitung E-Voting (LU) Leitung der elektronischen Stimmabgabe (SG) Fachperson E-Voting (TG)

Referenzierte Dokumente

Nr.	Dokument	Version
[1]	Konzept E-Voting	Aktuelle Version
[2]	Glossar	Aktuelle Version
[3]	Konzept Vollständige Verifizierbarkeit	Aktuelle Version
[4]	Richtlinie Informationssicherheit	Aktuelle Version
[5]	Hardware und Infrastruktur	Aktuelle Version
[6]	Konzept Schulungen und interne Information	Aktuelle Version

Inhaltsverzeichnis

1 Einleitung

Am 5. März 2026 meldete der Kanton Basel-Stadt der Krisenorganisation Vote électronique, dass er möglicherweise keinen Zugang mehr hat zum Administratoren-Passwort, das für die Entschlüsselung der elektronischen Urne für den Urnengang vom 8. März 2026 notwendig war. Die Kantone, die Schweizerische Post und die Bundeskanzlei haben umgehend die gemeinsame Krisenorganisation aktiviert. Die Bemühungen für einen Zugang zum Passwort waren leider nicht erfolgreich und der Kanton Basel-Stadt hat mit einer Medienmitteilung vom 7. März 2026 informiert, dass die 2048 elektronisch abgegebenen Stimmen im Kanton Basel-Stadt nicht entschlüsselt und entsprechend auch nicht gezählt werden konnten[1].

Am 10. März 2026 hat der Kanton Basel-Stadt angekündigt, die Umstände und Ursachen des Vorfalls extern analysieren zu lassen. Gleichzeitig hat er zur Kenntnis genommen, dass die Staatsanwaltschaft Basel-Stadt ein Strafverfahren eingeleitet hat. Der Kanton Basel-Stadt hat auch festgehalten, dass der Vorfall am Abstimmungswochenende vom 8. März 2026 nur im Kanton Basel-Stadt aufgetreten ist und auf die Handhabung einer externen Komponente (USB-Stick) zurückzuführen sei und nicht auf das E-Voting-System, welches die Schweizerische Post zur Verfügung stellt.

Am 11. März 2026 hat die Bundeskanzlei kommuniziert, dass sie als Sofortmassnahme vorsieht, dass alle E-Voting-Kantone ihre Prozesse zum Schutz der Schlüssel für die Entschlüsselung der elektronischen Urnen überprüfen. Welche weiteren Massnahmen zu ergreifen sind, soll im Rahmen der etablierten Prozesse im engen Austausch aller Akteure geprüft werden.

Ebenfalls am 11. März 2026 haben die Kantone Graubünden, St.Gallen und Thurgau angekündigt, dass sie an E-Voting festhalten wollen. Die Erfahrungen sind positiv. E-Voting befindet sich weiterhin im Versuchsbetrieb. Dieser ist bewusst darauf ausgerichtet, praktische Erfahrungen zu sammeln und Abläufe sowie Prozesse laufend zu verbessern und weiterzuentwickeln. Aus Sicht der drei Kantone ist es daher zweckmässig, diesen Versuchsbetrieb weiterzuführen.

Im vorliegenden Dokument beschreiben die Kantone Graubünden, Luzern, St.Gallen und Thurgau die bisherigen Prozesse im Zusammenhang mit der Entschlüsselung der Urne und legen dar, welche Überprüfungen in der Folge des Vorfalls in Basel-Stadt gemacht und welche Massnahmen getroffen werden.

Die Kantone nehmen den Vorfall, der im März 2026 in Basel-Stadt auftrat, sehr ernst. Es ist wichtig, dass daraus die richtigen Lehren gezogen werden. Die bisher vorhandenen Informationen zum Vorfall in Basel-Stadt sind eingeflossen. Allfällige zusätzliche Erkenntnisse aus der von Basel-Stadt in Auftrag gegebenen externen Untersuchung werden berücksichtigt, sobald sie vorliegen.

[1] Siehe Medienmitteilung vom 07.03.2026

2 Beschreibung des Prozesses im Zusammenhang mit der Entschlüsselung

Für die Übersicht über den E-Voting-Prozess verweisen die Kantone auf das Dokument «Konzept E-Voting» (siehe *referenziertes Dokument [1]*).

2.1 Grundprinzip für die Ver- und Entschlüsselung der elektronischen Stimmen

Bei der Vorbereitung des Urnengangs wird am sogenannten Tag 2 (D2) anhand von zwei Passwörtern (Passwort Admin-Board[2] / Passwort Electoral-Board[3]) ein Schlüsselpaar[4] generiert. Dieses Schlüsselpaar wird mit den Schlüsseln der Kontrollkomponenten kombiniert. Der kombinierte öffentliche Schlüssel wird vom Gerät der Stimmberechtigten verwendet, um die Stimme zu verschlüsseln.

Nach der Urnenschliessung am Samstag vor dem Abstimmungssonntag um 12:00 Uhr[5] erfolgt die Entschlüsselung der Stimmen. Die Stimmen können nur entschlüsselt werden, wenn alle Kontrollkomponenten die Stimmen mischen (und dabei die Stimmen teilentschlüsseln) und sowohl das Admin-Board wie auch das Electoral-Board ihre jeweiligen Passwörter eingeben, um den privaten Schlüssel wiederherzustellen. Mit dem privaten Schlüssel (der aus den beiden Passwörtern des Admin-Boards und des Electoral-Boards wiederhergestellt wurde) findet anschliessend die finale Entschlüsselung statt. Dadurch ist sichergestellt, dass die Stimmen end-to-end-verschlüsselt sind und erst durch das Zusammenwirken von Admin-Board und Electoral-Board entschlüsselt werden können. Fehlt eines der beiden Passwörter, ist keine Entschlüsselung möglich.

---

2 Begriff steht für die kantonalen Administratoren, die im 4-Augen-Prinzip den E-Voting-Prozess durchführen (siehe «Glossar», *referenziertes Dokument [2]*).

3 Begriff steht für die Personen, die nach kantonalem Recht für die Beaufsichtigung des ordnungsgemässen Ablaufs des elektronischen Urnengangs verantwortlich sind und die in der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS) vorgesehene Rolle der Prüferinnen und Prüfern übernehmen (siehe «Glossar» und «Konzept Vollständige Verifizierbarkeit», *referenzierte Dokumente [2] und [3]*).

4 Für mehr Informationen zum Sicherheitsschlüssel wird auf den *Abschnitt 4.2.2* der System Specification und auf die Fussnote 6 verwiesen.

5 Die Entschlüsselung ist «erst» nach 12:15 Uhr möglich. Der Kanton hat eine Karenzzeit von 15 Minuten definiert. Damit erhalten Stimmberechtigte, die sich kurz vor 12:00 Uhr eingeloggt haben, 15 Minuten Zeit, um ihre elektronische Stimmabgabe abzuschliessen. Ein Einloggen nach 12:00 Uhr ist nicht möglich (siehe «Konzept E-Voting», *referenziertes Dokument [1]*).

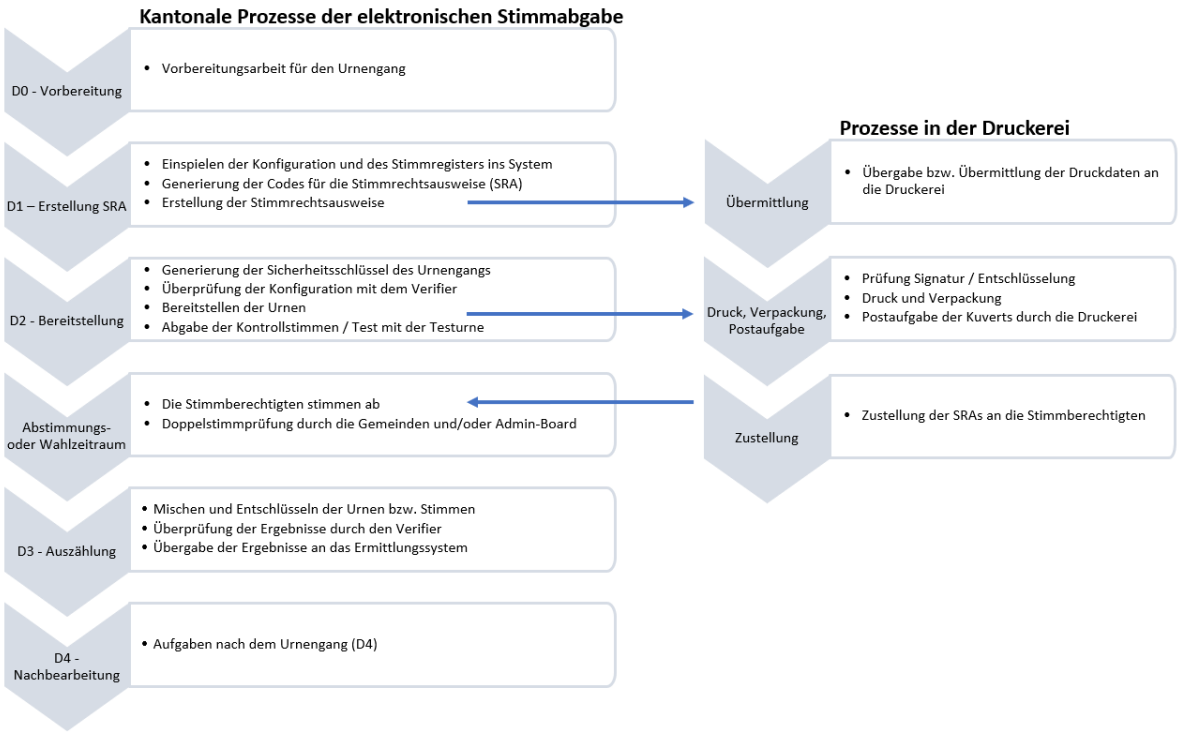

Abbildung 1: Grafik zum Prozess E-Voting aus dem «Konzept E-Voting» (siehe *referenzierte Dokumente [1]*)

2.2 Prozess für die Erstellung und sichere Aufbewahrung der beiden Passwörter

Nachfolgend werden die Prozesse für die Erstellung und Aufbewahrung der beiden Passwörter und die Handhabung der dafür notwendigen USB-Sticks beschrieben:

- **Generierung der beiden Passwörter am Tag 2 (D2) in einem klar definierten Prozess:** Die beiden Passwörter werden bei der Vorbereitung des Urnengangs am Tag 2 in Anwesenheit des Electoral-Boards in einem klar definierten Prozess festgelegt: Die beiden Passwörter werden auf einem Offline-Gerät (Setup Computer) mit der Software KeePass nach dem Zufallsprinzip mit genügender Entropie erstellt und haben je 50 Zeichen[6]. Der Prozess wird vom Admin-Board im 4-Augen-Prinzip durchgeführt und durch das Electoral-Board beobachtet und überwacht.

- **Speicherung auf je drei PIN-geschützten USB-Sticks:** Die beiden Passwörter werden ausschliesslich auf je drei PIN-geschützten USB-Sticks gespeichert, die nur für diesen Zweck eingesetzt werden. Somit gibt es pro Passwort je zwei Backups.

[6] Siehe dazu *Abschnitt 4.3* der «Richtlinie Informationssicherheit» (siehe *referenziertes Dokument [4]*) sowie *Abschnitt 4.2.2* der System Specification. Die Bit-Länge der Passwörter muss dem Sicherheitslevel entsprechen. Im E-Voting-System gilt ein Sicherheitslevel von 128 bits. Bei 7-bit pro Zeichen wäre somit bereits ein Passwort mit einer Länge von 19 Zeichen genügend. Die Passwörter werden im 4-Augen-Prinzip unter Aufsicht und Beobachtung des Electoral-Boards generiert. Es wurde bewusst eine Länge von 50 Zeichen gewählt, um sicherzustellen, dass niemand sich die beiden Passwörter merken kann.

- **Verwendete Sticks und deren Handhabung:** Die PIN-geschützten USB-Sticks werden an keine anderen Geräte angeschlossen als die Offline-E-Voting-Geräte. Die von den Kantonen verwendeten USB-Sticks sind im Dokument «Hardware und Infrastruktur» (siehe *referenziertes Dokument [5]*) festgehalten. Die USB-Sticks sind auf Hardware-Basis verschlüsselt. Es kann nur auf die darauf gespeicherten Daten (= das Passwort des Admin-Boards oder des Electoral-Boards) zugegriffen werden, wenn ein PIN-Code eingegeben wird. Durch die PIN-Eingabe wird der Stick geöffnet. Die USB-Sticks verfügen über einen Schutz vor Brute-Force-Attacken. Zehn falsche PIN-Eingaben führen zur unwiderruflichen Zerstörung der auf dem Stick gespeicherten Daten. Umso wichtiger sind daher die sorgfältige PIN-Definition und die sichere Aufbewahrung der Sticks.

    - Die **PIN-Codes für die drei USB-Sticks des Admin-Boards** (im Normallfall 6 bis 8 Zeichen) werden im 4-Augen-Prinzip definiert. Es muss entsprechend sichergestellt werden, dass beide Personen den PIN kennen und den Stick anhand der PIN-Codes öffnen können. Die Mitglieder des Admin-Boards merken sich den oder die PIN-Codes. Die PIN-Codes werden als Backup aufgeschrieben und sicher in der Verantwortung des Admin-Boards aufbewahrt. Das Öffnen des Sticks wird wiederholt getestet, auch die Öffnung anhand des notierten PIN-Codes.

    - Die **PIN-Codes für die drei USB-Sticks des Electoral-Boards** (im Normallfall 6 bis 8 Zeichen) werden durch die jeweiligen Personen selbst festgelegt. Die Mitglieder des Electoral-Boards merken sich den PIN-Codes. Die PIN-Codes werden als Backup aufgeschrieben und müssen sicher aufbewahrt werden. Das Öffnen des Sticks durch das jeweilige Mitglied des Electoral-Boards wird wiederholt getestet, auch die Öffnung anhand des notierten PIN-Codes.

- **Test-Entschlüsselung bei der Vorbereitung des Urnengangs (am Tag 2):** Am D2 wird eine Testurne entschlüsselt, um sicherzustellen, dass der Prozess ordnungsgemäss durchgeführt werden kann. Dazu wird genau der gleiche Prozess durchlaufen, wie bei der Entschlüsselung der Stimmen nach der Urnenschliessung. Für die Entschlüsselung müssen die zuvor generierten und gespeicherten Passwörter des Admin-Boards und des Electoral-Boards eingegeben werden. Um die beiden Passwörter eingeben zu können, wird je ein PIN-geschützter Stick des Admin-Boards und des Electoral-Boards mit dem jeweiligen PIN-Code geöffnet und das Passwort in den Tally Computer (Offline-Gerät) übertragen.

- **Aufbewahrung der beiden Passwörter bzw. der je drei PIN-geschützten USB-Sticks:** Das Passwort des Admin-Boards und dasjenige des Electoral-Boards werden getrennt voneinander aufbewahrt. Dies stellt sicher, dass niemand Zugriff auf beide Passwörter hat und dass die Urnen nur entschlüsselt werden können, wenn das Admin-Board und das Electoral-Board für die Entschlüsselung zusammenkommen.

    - Die Aufbewahrung der drei **USB-Sticks des Admin-Boards** erfolgt im Safe. Der Zugang zum Safe ist nur im strengen 4-Augen-Prinzip möglich. Das heisst, dass keine einzelne Person ohne die Mitwirkung einer anderen sich faktisch Zugriff verschaffen kann.

    - Die Aufbewahrung der **USB-Sticks des Electoral-Boards** variiert unter den Kantonen: Die Sticks werden sicher aufbewahrt, und in allen Kantonen wird sichergestellt, dass das Admin-Board nicht auf das Passwort des Electoral-Boards zugreifen kann und umgekehrt.

2.3 Beurteilung der Risiken

Die Kantone sind gemäss den Vorgaben der Verordnung der Bundeskanzlei über die elektronische Stimmabgabe (VEleS) verpflichtet, eine systematische Risikobeurteilung vorzunehmen und die in der VEleS festgehaltenen Bedrohungsszenarien zu analysieren. Entsprechend haben die Kantone auch die Risiken im Zusammenhang mit der Verfügbarkeit der beiden Passwörter analysiert und Massnahmen definiert, die Grundlage für den in *Abschnitt 2.2* beschriebenen Prozess waren. Die Risikoanalyse wurde aufgrund des Vorfalls in Basel-Stadt überprüft und ergänzt.

3 Überprüfung der Prozesse

3.1 Vorgehen

Die Kantone nehmen den Vorfall in Basel-Stadt sehr ernst. Unter Einbezug der Schweizerischen Post, der zukünftigen E-Voting-Kantone (Luzern, Neuenburg, Genf), der Bundeskanzlei sowie des Bundesamtes für Cybersicherheit (BACS) haben sie die Prozesse überprüft und Massnahmen definiert und teilweise bereits umgesetzt. Die Analyse hat sich nicht nur auf den in Basel-Stadt im Fokus stehenden Entschlüsselungsprozess beschränkt. Der Schwerpunkt lag auf der Frage, wie robust die Prozesse in den Kantonen, aber auch bei der Schweizerischen Post oder den Druckereien sind und wie die Resilienz erhöht werden könnte.

In zwei Workshops wurde bei der Überprüfung der Prozesse und der Definition von Massnahmen insbesondere folgenden Fragen nachgegangen:

- Bestehen irgendwo Schwachstellen oder blinde Flecken?
- Wie kann sichergestellt werden, dass die definierten Prozesse greifen, eingehalten und nicht (aus Fahrlässigkeit oder mit Vorsatz) umgangen werden?
- Wie kann das 4-Augen-Prinzip noch robuster gemacht werden?

Allfällige zusätzliche Erkenntnisse aus der von Basel-Stadt in Auftrag gegebenen externen Untersuchung werden berücksichtigt, sobald sie vorliegen.

3.2 Zusammenfassung der wichtigsten Erkenntnisse aus der Überprüfung der Prozesse

Es liegen keine Hinweise vor, die weitere Versuche mit E-Voting in Frage stellen würden. Die Prozesse sind gut, wenn sie eingehalten werden. Das 4-Augen-Prinzip ist dabei wesentlich für deren Einhaltung. Die Prozesse können punktuell verbessert und deren Einhaltung noch besser unterstützt werden (siehe *Abschnitt 4*). Es wurden keine neuen Bedrohungsszenarien ausgemacht.

4 Massnahmen

Wichtigster und wirkungsvollster Ansatzpunkt ist, die Einhaltung der Prozesse noch besser zu unterstützen. Stichworte sind Sensibilisierung / Awareness sowie Verbesserung von Anleitungen und Checklisten. Dazu gehören insbesondere auch die Sensibilisierung zur Bedeutung des 4-Augen-Prinzips und Massnahmen, um das 4-Augen-Prinzip noch robuster zu machen. Alle Kantone haben in diesem Zusammenhang den Zugriff auf den Safe überprüft. Der Zugriff auf den Safe ist gemäss den Anforderungen nur im strengen 4-Augen-Prinzip erlaubt. Das bedeutet, dass sichergestellt sein muss, dass nicht eine Person allein auf die darin aufbewahrten kritischen Daten zugreifen kann. Es muss zudem jeder Zugriff auf den Safe durch die betreffenden zwei Personen protokolliert werden. Im Fokus der Überprüfung standen mögliche Notschlüssel und Masterpasswörter für die Konfiguration der 4-Augen-Prinzip-Module.

Im nachfolgenden Abschnitt wird dokumentiert, welche kurzfristigen Anpassungen am Prozess für den nächsten Urnengang vorgenommen wurden. *Abschnitt 4.2* gibt einen Überblick über die von den Kantonen in Zusammenarbeit und im Austausch mit allen Akteuren erarbeiteten Massnahmen.

Die Kantone sind überzeugt, dass mit der Auseinandersetzung mit dem Vorfall in Basel-Stadt, der in diesem Zusammenhang erfolgten Überprüfung der Prozesse und den definierten Massnahmen viele Erkenntnisse gewonnen werden konnten und bereits viel erreicht wurde. Sie sind überzeugt, dass aus dem Vorfall die notwendigen Lehren gezogen werden und kein Grund besteht, weitere Versuche mit E-Voting in Frage zu stellen.

Die Kantone stehen untereinander, mit der Schweizerischen Post und auch mit der Bundeskanzlei in ständigem Austausch und werden die Weiterverfolgung der Massnahmen im Rahmen der bereits etablierten Gefässe sicherstellen.

4.1 Kurzfristige Anpassungen der Prozesse für den nächsten Urnengang

Die Überprüfung der Prozesse hat ergeben, dass diese grundsätzlich gut sind. Prozesse greifen jedoch nur, wenn sie eingehalten werden. Änderungen müssen sorgfältig und gezielt erfolgen, damit sie keine negativen Auswirkungen haben (d.h. eine Reduktion der Sicherheit durch eine überhastete und nicht wohlüberlegte Anpassung). Kurzfristig werden am Prozess in Ergänzung zu den sich bereits in Umsetzung befindenden oder bereits umgesetzten Massnahmen gemäss *Abschnitt 4.2* (namentlich im Bereich der Sensibilisierung) folgende Anpassungen vorgenommen:

- **(Teilweise) Erneuerung USB-Sticks:** Die Kantone Graubünden, St.Gallen und Thurgau hatten bis jetzt keine Probleme mit der Funktionstüchtigkeit der eingesetzten PIN-geschützten USB-Sticks für die Speicherung der zwei Passwörter. Als Vorsichtsmassnahme wurde dennoch entschieden, dass alle Kantone je einen der drei USB-Sticks durch einen neuen Stick ersetzen.

- **Zusätzliches Backup des Passworts der Administratoren:** Im Kanton Basel-Stadt bestand kein Zugang mehr auf das Passwort des Admin-Boards. Als kurzfristige Massnahme wird dieses Passwort in allen E-Voting-Kantonen als zusätzliche Sicherheitsmassnahme und im Sinn eines alternativen Speichermediums auf dem Setup Computer gespeichert (sowie weiterhin auf den drei USB-Sticks). Beim Setup Computer handelt es sich um ein

Offline-Gerät mit verschlüsselter Festplatte, das bei der Konfiguration des Urnengangs verwendet wird und bei der Entschlüsselung der Urne nicht mehr zum Einsatz kommt. Alle Geräte werden in der Verantwortung des Admin-Boards im Safe aufbewahrt. Auf den Safe kann nur im strengen 4-Augen-Prinzip zugegriffen werden.

- **Anpassung der Benutzeranleitung (Schritt-für-Schritt-Anleitung, die auch als Checkliste genutzt wird):** Im sogenannten Operational Guide ist das Erstellen der verschiedenen Sicherheitskopien bereits schrittweise dokumentiert. Gemeinsam mit der Schweizerischen Post wurde die Anleitung so optimiert, dass die Erstellung der je drei Backups bzw. USB-Sticks robuster wird und somit am Ende des Tag 2 (D2) Gewähr besteht, dass die Backups korrekt erstellt wurden, funktionieren und auch das Öffnen der Sticks durch die PIN-Eingabe gewährleistet ist.

4.2 Übersicht über die Massnahmen

Ein wesentliches Merkmal von E-Voting ist der kontinuierliche Verbesserungsprozess, der nie abgeschlossen sein wird. Entsprechend sind auch diverse der untenstehenden Massnahmen (wie z.B. die Awareness / Sensibilisierung) nie wirklich abgeschlossen und viel mehr als Daueraufgabe zu verstehen. Gemeint ist mit «abgeschlossen», dass die Massnahmen mit Blick auf den anstehenden Urnengang vom 14. Juni 2026 erledigt sind.

Nr.	Massnahme	Beschreibung	Zeitpunkt Umsetzung	Status
0 A	**Überprüfung Prozesse und bei Bedarf Definition von Massnahmen: Kantone**	Auch wenn der Vorfall in Basel-Stadt keinen Zusammenhang mit dem System der Schweizerischen Post oder mit den Druckereien hatte, so wurde trotzdem für alle Akteure die Frage gestellt, wie robust die Prozesse sind und wie die Resilienz erhöht werden könnte. Im Fokus standen dabei trotzdem die Kantone. Für die Schweizerische Post und die Druckereien gilt als Massnahme in Ergänzung zur Überprüfung, dass alle Beteiligten nochmals gezielt bezüglich der Einhaltung der Prozesse und insbesondere der Bedeutung des 4-Augen-Prinzips sensibilisiert werden.	kurzfristig	abgeschlossen
0 B	**Überprüfung Prozesse und bei Bedarf Definition von Massnahmen: Schweizerische Post**		kurzfristig	abgeschlossen
0 C	**Überprüfung Prozesse und bei Bedarf Definition von Massnahmen: Druckereien**		kurzfristig	weitgehend abgeschlossen (Sensibilisierung durch die Kantone erfolgt, Sensibilisierung aller involvierten Mitarbeitenden wird rechtzeitig für den Urnengang vom 14.06.2026 abgeschlossen).
1	**Risikoanalyse überprüfen**	Die Kantone überprüfen ihre Risikoanalyse im Zusammenhang mit dem Vorfall in Basel-Stadt. Die kontinuierliche Überprüfung der Risiken ist Teil der etablierten Prozesse und somit eine Daueraufgabe und entsprechend nie abgeschlossen.	kurzfristig	abgeschlossen
2 A	**Strenges 4-Augen-Prinzip überprüfen und bei Bedarf robuster machen (u.a. Zugang Safe)**	Die Kantone (und die Druckereien) überprüfen den Zugriff auf ihre Safes unter Berücksichtigung möglicher Notschlüssel / Masterpasswörter. Mittel- und längerfristig: Die Kantone überprüfen die Erkennbarkeit («tamper-evident»), wenn die definierten Massnahmen nicht mehr greifen. Zusätzlich wird der Zeitpunkt der Löschung kritischer Daten nochmals überprüft.	kurzfristig mittel- und längerfristig	abgeschlossen in Prüfung

3 A	**Einhaltung der Prozesse verbessern (insb. 4-Augen-Prinzip): Checklisten / Anleitungen**	Die Kantone prüfen, wie die Dokumentation / Anleitungen / Checklisten verbessert werden können, um sicherzustellen, dass die Prozesse eingehalten werden und nichts (auch nicht unter allfälligem Zeitdruck) vergessen geht. Kurzfristig: Operational Guide wird verbessert. Mittel- und längerfristig: Kantone und Schweizerische Post verbessern die Unterstützung bei der Einhaltung der Prozesse kontinuierlich (im Rahmen des bewährten kontinuierlichen Verbesserungsprozesses).	kurzfristig mittel- und längerfristig	abgeschlossen fortlaufend (KVP)
3 B	**Einhaltung der Prozesse verbessern (insb. 4-Augen-Prinzip): Applikatorische Unterstützung / Einforderung**	Die Kantone prüfen gemeinsam mit der Schweizerischen Post nochmals, ob und wie das 4-Augen-Prinzip applikatorisch noch besser unterstützt / eingefordert werden kann. Mittelfristig: Für den Release 1.6 (Publikation im Sommer 2026, Einsatz ab 2027) wird eine gezielte Verbesserung der Benutzeroberfläche bei der Festlegung der zwei Passwörter geprüft.	mittelfristig	in Prüfung (erste Ideen vorhanden)
4	**Anwendung 3-2-1-Prinzip (über)prüfen**	Die Kantone prüfen, ob und wie das 3-2-1-Prinzip verstärkt werden kann. Das 3-2-1-Prinzip ist eine bewährte Grundregel für den Schutz vor Datenverlust. Es besagt, dass wichtige Daten in mindestens drei Kopien vorliegen sollen, auf zwei unterschiedlichen Speichermedien, wobei eine Kopie an einem externen Standort aufbewahrt wird. Ziel ist es, nicht nur einzelne Ausfälle abzufangen, sondern auch systematische Risiken zu reduzieren. Der zentrale Gedanke dahinter ist Risikodiversifikation. Bereits jetzt werden pro Passwort drei Kopien erstellt, die USB-Sticks mit den Passwörtern sicher aufbewahrt und sichergestellt, dass die Passwörter nur zusammenkommen, wenn bei der Entschlüsselung der Urnen das Admin-Board und das Electoral-Board zusammenfinden. Die Kantone werden sich vertiefter mit diesem Prinzip auseinandersetzen. Da dies sorgfältig und wohlüberlegt erfolgen muss, werden mögliche Anpassungen nicht kurzfristig angestrebt. Kurzfristig wird für das Admin-Board-Passwort bereits eine Verbesserung umgesetzt. Es wird im Sinne eines zweiten Speichermediums zusätzlich auf dem Setup Computer des Admin-Boards gespeichert.	kurzfristig: Speicherung Passwort Amin-Board auf Setup Computer als zusätzliches Speichermedium mittel- und längerfristig	umgesetzt in Prüfung

5	**Sensibilisierung / Awareness generell und v.a. am Tag 2 (Erstellung und Speicherung Passwörter für die Entschlüsselung) erneuern / erhöhen**	Alle Involvierten müssen die wichtigsten Prinzipien und Sicherheitsmassnahmen (insb. 4-Augen-Prinzip) präsent haben und verstehen, warum sie wichtig sind. Die Sensibilisierung wird für den nächsten Urnengang gezielt erneuert. Mittel- und langfristig: Die Sensibilisierung und Awareness ist eine wichtige Daueraufgabe, die bereits entsprechend im «Konzept Schulungen und interne Information» (siehe *referenziertes Dokument [6])* dokumentiert ist. Die Kantone prüfen, ob und wie die Nachhaltigkeit und Wirkung der Massnahmen weiter verbessert werden können.	kurzfristig mittel- und längerfristig	abgeschlossen in Prüfung
6	**Life-Cycle überprüfen (USB-Sticks / weitere Hardware)**	Die Kantone Graubünden, St.Gallen und Thurgau haben bis jetzt keine Funktionsprobleme mit der Hardware (insb. den USB-Sticks) festgestellt. Kurzfristig soll trotzdem ein Teil der USB-Sticks erneuert werden. Mittel- und längerfristig prüfen die Kantone eine gemeinsame Policy für den Life-Cycle der zentralen Hardware.	kurzfristig mittel- und längerfristig	abgeschlossen in Prüfung
8	**Notwendigkeit Verwendung von PIN-geschützten USB-Sticks überprüfen**	Die Kantone haben die Verwendung der PIN-geschützten USB-Sticks überprüft. Gemäss den Anforderungen in der VEleS dürfen kritische Daten nur verschlüsselt auf Datenträgern abgespeichert werden. Technisch gäbe es theoretisch andere Lösungsmöglichkeiten. Diese sind aber mit Nachteilen verbunden und die Grundherausforderung bleibt (sichere Aufbewahrung des Schlüssels für die Entschlüsselung, damit nur Admin-Board und Electoral-Board gemeinsam die Entschlüsselung vornehmen können). Ein Verzicht auf die hardwareverschlüsselten USB-Sticks ist daher nicht möglich. Kurzfristig ändern die Kantone daher nichts an der Verwendung der USB-Sticks. Der zielführendere Ansatz sind die Massnahmen 5, 3A (und 3B). Es gilt mittelfristig sorgfältig zu überlegen, ob die bisherige Lösung gezielt verbessert werden kann.	kurzfristig mittel- und längerfristig	Überprüfung abgeschlossen, keine Massnahme in Prüfung
9	**Erkenntnisse aus der IT-forensischen Analyse berücksichtigen**	Die Kantone prüfen, ob sich aus der IT-forensischen Analyse der Schweizerischen Post und des Kantons Basel-Stadt Verbesserungsbedarf (z.B. für das Hardening und die Untersuchung von Vorfällen) ergeben. In einer ersten Einschätzung wurde kein Verbesserungsbedarf festgestellt, diese Analyse ist aber noch im Gang.	mittel- und längerfristig	in Prüfung

10	**Prüfung, welche USB-Sticks verwendet werden sollen**	Die Kantone setzen unterschiedliche Typen ein: USB-Sticks, bei denen die PIN-Eingabe auf dem Stick selbst erfolgt, und Sticks, bei denen die PIN-Eingabe nach dem Einstecken am Laptop erfolgt. Welche Sticks verwendet werden, ist im Dokument «Hardware und Infrastruktur» (siehe *referenziertes Dokument [5]*) festgehalten. Neben der Usability bei der Verwendung der Sticks ist es wichtig, mögliche Sicherheitslücken im Auge zu behalten. Kurzfristig wurde geprüft, dass die verwendeten USB-Sticks keine bekannten Sicherheitslücken aufweisen. Entsprechend wird kurzfristig an den bisher verwendeten Modellen festgehalten. Mittel- und längerfristig: Die Verwendung der USB-Sticks wird im Zusammenhang mit diversen anderen Massnahmen (z.B. Nr. 4) nochmals geprüft (inkl. Monitoring möglicher Sicherheitsmängel).	kurzfristig mittel- und längerfristig	Überprüfung abgeschlossen, keine Anpassungen in Prüfung
11	**Überprüfung und Anpassung Dokumentation**	Die Kantone überprüfen ihre bisherige Dokumentation mit dem Ziel, die aus dem Vorfall in Basel-Stadt gewonnenen Erkenntnisse und die Massnahmen abzubilden. Die Anpassung erfolgt in mehreren Ertappen: Kurzfristig (für die Zulassung des Urnengangs vom 14.06.2026) stehen punktuelle Anpassungen im Vordergrund. Weitere Anpassungen erfolgen unter Berücksichtigung des Zeitplans für die diversen Bewilligungsverfahren. Ziel ist es dabei, das vorliegende Dokument mittelfristig abzulösen bzw. die noch relevanten Inhalte in die bisherige Dokumentation zu integrieren.	kurzfristig mittel- und längerfristig	abgeschlossen in Prüfung
12	**Schulung / Einführung neue Mitarbeitende überprüfen und nötigenfalls verbessern**	Die Kantone überprüfen das bisherige Schulungskonzept (siehe *referenziertes Dokument [6]*). Ziel ist es, die Schulungen breiter abzustützen und die Erfahrungen und Synergien der verschiedenen Akteure noch besser zu nutzen. Erste Ideen sind bereits vorhanden (wie z.B. fixe Besuche bei anderen Kantonen vorsehen). Bereits beschlossen ist, dass die Bundeskanzlei zukünftig Schulungen mit Fokus auf die Anforderungen für neue Mitarbeitenden anbieten wird.	mittel- und längerfristig	in Prüfung

13	**Krisenmanagement zum Vorfall in Basel-Stadt auswerten und verbessern**	Für das Krisenmanagement bestehen etablierte Prozesse. Dazu gehört auch, dass die Kantone zusammen mit allen weiteren Akteuren das Krisenmanagement im Zusammenhang mit dem Vorfall in Basel-Stadt auswerten und bei Bedarf verbessern werden.	kurz- bis mittelfristig	in Prüfung