Interessensgruppe für sichere Abstimmungen (IsA)
Ringstrasse 2
CH–3629 Kiesen

Interessensgruppe für sichere Abstimmungen (IsA), Ringstrasse 2, CH–3629 Kiesen

Bundeskanzlei
Sektion Politische Rechte
Bundeshaus West
3003 Bern

16. August 2021

Vernehmlassung 2021/61: Änderung der Verordnung über die politischen Rechte (VPR) und der Verordnung der BK über die elektronische Stimmabgabe (VEleS)

Sehr geehrte Damen und Herren Bundesräte
Sehr geehrter Herr Bundeskanzler
Sehr geehrte Damen und Herren

Wir schreiben Ihnen als eine Gruppe von Personen, die sich mit der Sicherheit von Wahlen und Abstimmungen beschäftigen. Unsere Gruppe eint Kritiker und Befürworter der elektronischen Stimmabgabe.

Unsere Vernehmlassungsantwort haben wir gemeinsam auf einer Online-Plattform erarbeitet. Wir haben dieses Hilfsmittel *Plattform für Eidgenössische Vernehmlassungsantworten* (Plattform-EVA) genannt. Dort haben wir auch Dokumente, die wir mittels BGÖ-Gesuchen erhalten haben, publiziert.

Wir begrüssen einen Grossteil der vorgeschlagenen Änderungen im VEleS und VPR, sehen jedoch einige Kernpunkte ausgespart und weitere Fragen zu wenig klar adressiert. Als wesentlich möchten wir vorab folgende Punkte hervorheben:

- **Open-Source** muss gesetzlich verankert werden. Das schliesst auch einen offenen Entwicklungsprozess inkl. Publikation der Commit-History ein. Langfristig führt unserer Meinung nach kein Weg an Open-Source vorbei, um in der Gesellschaft Vertrauen in die elektronische Stimmabgabe wachsen zu lassen.
- **Der Anhang** zur VEleS kümmert sich in gewissen Punkten um ausgesprochen

implementationsspezifische Fragen, lässt jedoch wichtige Makro-Sichtweisen ausser Acht. Eine Nivellierung oder eventuell auch Glättung erscheint uns hier von Vorteil.

- **Die Klarheit der Terminologie** sollte verbessert werden. Der Artikel 2 der VEleS erfüllt seinen Zweck noch nicht und könnte sich als Achillesverse nicht nur für die Regulierung, sondern für die elektronische Stimmabgabe als Ganzes erweisen.

Detaillierte und gezielte Stellungnahmen, sowie einige Änderungsvorschläge finden Sie im angehängten Fragebogen, der Ihrer Vorlage folgt. Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassungsantwort und stehen für Fragen und eine weitere Zusammenarbeit zur Verfügung.

Mit freundlichen Grüßen

Interessensgruppe für sichere Abstimmungen (IsA)

Christian Folini
Christian Killer
Melchior Limacher
Simon Studer
Bernhard Tellenbach

Anhang:

- Fragebogen inkl. Antworten und detaillierten Kommentaren zu den Artikeln und Anhängen

Fragebogen

Teilrevision der Verordnung über die politischen Rechte und Totalrevision der Verordnung der BK über die elektronische Stimmabgabe (Neuausrichtung des Versuchsbetriebs)

Vernehmlassung vom 28. April 2021 bis zum 18. August 2021

Absender
Namen und Adresse des Kantons oder der Organisation:
Interessensgruppe für sichere Abstimmungen (IsA), Ringstrasse 2, CH-3692 Kiesen
Christian Folini, Christian Killer, Melchior Limacher, Simon Studer

Kontaktperson für Rückfragen (Name, E-Mail, Telefon):
Christian Folini, christian.folini@time-machine.ch, +41 (0) 31 301 60 71

---

1. Allgemeine Rückmeldungen

1.1. Befürworten Sie die Stossrichtungen und Zielsetzungen der Neuausrichtung des Versuchsbetriebs zur elektronischen Stimmabgabe?

☐ Ja ☒ Ja mit Vorbehalt ☐ Nein

Anmerkungen:

Wir begrüssen die kurz- und mittelfristige Beschränkung der elektronischen Stimmabgabe auf einen klar umrissenen Versuchsbetrieb.

Ebenfalls begrüssen wir, dass die Relevanz von Transparenz und Public Scrutiny erkannt wurde und breiten Eingang in die Verordnung gefunden hat.

Wir bemängeln aber gleichzeitig, dass eine offene Entwicklung und eine Publikation des Source Codes unter einer Open Source Lizenz nicht zu den Anforderungen an Systeme zur elektronischen Stimmabgabe zählt.

Die Regulierung geht sehr weit in der genauen Spezifikation eines möglichst transparenten Entwicklungsprozesses. Leider ist beispielsweise die Commit-History nicht Teil der zu veröffentlichenden Dokumentation. Dies erschwert es deutlich, Änderungen oder die Entwicklungsgeschichte von Komponenten oder die Abläufe bei der Softwareentwicklung nachzuvollziehen. Dies wäre aber ein wichtiger Beitrag zur Beurteilung der Qualität der Softwareentwicklung. Wir empfehlen, eine offene Entwicklung zu verordnen.

Dass im Widerspruch zur Empfehlung der einbezogenen Expertengruppe keine Open Source Lizenz verordnet wird, dürfte mittelfristig E-Voting in der Schweiz schwächen. Die Wichtigkeit von Public Scrutiny wird zwar anerkannt, aber die Schlüsse daraus wurden nicht hinreichend gezogen. Wird das System nicht unter einer Open Source Lizenz entwickelt, wird kaum eine nachhaltige internationale Community um die Schweizer E-Voting Systeme entstehen. Teilnahme in einer E-Voting Community erfordert Interesse, Engagement und Fachkompetenz, Voraussetzungen also, die nur ein kleiner Teil der Bevölkerung mitbringt. Es scheint unwahrscheinlich, dass die Schweiz genügend freiwillige Fachkräfte aufbringen kann, um mittels Public Scrutiny ein solides Sicherheitsniveau zu erreichen. Zumal der Verzicht auf eine gängige und eine in ihren Folgen gut bekannte Open Source Lizenz allfällige Interessenten eher abschreckt.

Als Kompromiss könnte eine Übergangslösung gefunden werden, die es der Post ermöglicht, den Versuchsbetrieb mit lizenzbelasteten Komponenten wieder aufzunehmen und so über Kantonsbeiträge die Weiterentwicklung finanziell zu unterstützen. Klare Vorgabe müsste jedoch sein, dass innerhalb einer Übergangsfrist die lizenzbelasteten Komponenten durch Open Source Kompontenten ersetzt werden. Ein solcher Hinweis fehlt aber sowohl in der Vorlage wie auch im erläuternden Bericht, so dass hier jegliche verbindliche Perspektive fehlt.

1.2. Weitere allgemeine Rückmeldungen zur Neuausrichtung des Versuchsbetriebs und der Vernehmlassungsvorlage:

Die technischen Ausführungsbestimmungen (Anhang VEleS) sind sehr, sehr detailliert. Wir sehen auf der einen Seite die Gefahr einer Überregulierung und auf der anderen Seite eine grosse Schwierigkeit, den Inhalt dieses Anhangs technisch beurteilen zu können. Dies könnte dazu führen, dass die Bundeskanzlei nur sehr wenig Rückmeldung zu diesem Anhang erhält und diesen Mangel in der Folge fälschlicherweise als Zustimmung zu einem überfrachteten Reglement versteht.

Sollte man beim entworfenen Detaillierungsgrad bleiben, sollte die Schlüsselgenerierung expliziter reguliert werden. Das Sicherstellen von genügend Entropie zur Schlüsselgenerierung ist eine für die Sicherheit der elektronischen Stimmabgabe äusserst kritische Anforderung, die im vorliegenden Entwurf nur summarisch mit viel Interpretationsspielraum ("Genügend Entropie") reguliert wird.

2. Fragen zu den Stossrichtungen der Neuausrichtung

2.1. Weiterentwicklung der Systeme

Die Sicherheitsanforderungen an E-Voting-Systeme und deren Betrieb werden in den Rechtsgrundlagen des Bundes wiedergegeben. Mit der Vernehmlassungsvorlage sollen die Qualitätskriterien für die Systeme und deren Entwicklungsprozess präzisiert werden und der Bund soll künftig nur noch vollständig verifizierbare Systeme zulassen.

2.1.1. Erachten Sie die unterbreiteten Rechtsgrundlagen als geeignet, um das Ziel der Weiterentwicklung der Systeme umzusetzen (insbes. Art. 27*i* E-VPR, Art. 5-8 E-VEleS und Anhang zur E-VEleS)?

☐ Ja ☒ Ja mit Vorbehalt ☐ Nein

Anmerkungen:

Die fehlende Verordnung einer Open Source Lizenz sowie die fehlende Forderung der Publikation der kompletten Commit History bedeutet, dass die Weiterentwicklung und die Beurteilung der Weiterentwicklung nicht unter optimalen Bedingungen passieren kann. Die fehlende Open Source Lizenz schöpft das Potential für Public Scrutiny nicht aus und die fehlende Commit History zwingt Auditierende, den Entwicklungsprozess zu rekonstruieren, anstatt ihn aus der Commit History herauslesen zu können.

2.2. Wirksame Kontrolle und Aufsicht

Die Zielsetzung besteht in einer aussagekräftigen Überprüfung der E-Voting-Systeme und ihres Betriebs. Bisher waren die Kantone dafür verantwortlich, diese durch akkreditierte Stellen zertifizieren zu lassen. Neu soll der Hauptteil der Überprüfungen von unabhängigen Expertinnen und Experten direkt im Auftrag des Bundes erfolgen. Die Ergebnisse der Überprüfungen sollen die Grundlage für den Zulassungsentscheid durch die Bundeskanzlei sowie für einen kontinuierlichen Verbesserungsprozess der elektronischen Stimmabgabe bilden.

2.2.1. Erachten Sie die unterbreiteten Rechtsgrundlagen, insbesondere die Anpassung der Zuständigkeiten bei der Prüfung der Systeme und deren Betrieb, als geeignet, um das Ziel der wirksamen Kontrolle und Aufsicht umzusetzen (insbes. Art. 27*l* E-VPR, Art. 10 E-VEleS und Ziff. 26 Anhang zur E-VEleS; auch Art. 27*i* E-VPR und Art. 4 E-VEleS)?

☐ Ja ☒ Ja mit Vorbehalt ☐ Nein

Anmerkungen:

Wir haben bei Artikel 10 der VEleS kleine Anmerkungen, erachten die Architektur der Prüfungen aber als hinreichend.
Artikel 26.4 "Prüfung des Schutzes gegen Versuche, in die Infrastruktur einzudringen" nennt als Mindestanforderung einen Web Applikation Penetration Test, was in klarem Widerspruch zum Titel des Artikels steht. Eine technische Sicherheitsprüfung der Infrastruktur darf sich nicht nur auf Web Applikationen beschränken sondern sollte im

Rahmen einer «Red Teaming» Übung mit möglichst offenem Scope durchgeführt werden.

2.3. Stärkung der Transparenz und des Vertrauens

E-Voting soll sich weiterhin im Versuchsbetrieb befinden. Dazu wird das zugelassene Elektorat auf kantonaler und auf nationaler Ebene limitiert. Zudem wollen Bund und Kantone vermehrt Transparenz schaffen und Anreize zur Mitwirkung interessierter Personen aus der Öffentlichkeit setzen. Als Grundlage für diese Zusammenarbeit sollen adressatengerechte Informationen öffentlich zugänglich sein. Dazu gehören insbesondere allgemeinverständliche Informationen über die Funktionsweise der elektronischen Stimmabgabe für Stimmberechtigte sowie Unterlagen für Fachpersonen. Für die Zusammenarbeit mit Fachpersonen sind finanzielle Anreize etwa mit einem ständigen Bug-Bounty-Programm zu setzen.

2.3.1. Erachten Sie die Limitierung des zugelassenen Elektorats als notwendig und wenn ja, wie beurteilen Sie die Höhe der gewählten Limiten (Art. 27*f* E-VPR)?

☒ Ja ☐ Ja mit Vorbehalt ☐ Nein

Anmerkungen:

In sich dürfte die elektronische Stimmabgabe nur dann zugelassen werden, wenn sie ihre Sicherheit dauerhaft unter Beweis gestellt und das öffentliche Vertrauen in diese Sicherheit erwiesen ist, denn oftmals reichen verhältnismässig wenig Stimmen aus, um ein Ergebnis zu kippen. Allerdings können die hohen Anforderungen nicht erreicht werden, ohne dass die elektronische Stimmabgabe tatsächlich erlaubt wird. Die Beschränkung auf kantonale und nationale Limiten erscheinen als tauglicher Kompromiss. Unschön ist freilich, dass die vorgeschlagenen kantonalen Limiten es Kantonen mit ungewöhnlicher Architektur der Wahlkreise (namentlich Basel Stadt und eventuell Glarus) sehr schwierig machen, Versuche mit der elektronischen Stimmabgabe durchzuführen.

Dazu kommt, dass die Privilegierung von Menschen mit Behinderung bei der Berechnung der Limiten sich in der Praxis wohl nur sehr schwer umsetzen lassen.

2.3.2. Erachten Sie die unterbreiteten Rechtsgrundlagen zur Offenlegung von Informationen und zum Einbezug der Öffentlichkeit als geeignet, um die Transparenz und das Vertrauen zu fördern (insbes. Art. 27*m* E-VPR; Art. 11-13 E-VEleS)?

☐ Ja ☐ Ja mit Vorbehalt ☒ Nein

Anmerkungen:

Die Rechtsgrundlagen sind mit hoher Wahrscheinlichkeit förderlich. Aber das Fehlen einer Forderung nach einer Open Source Lizenz und einer komplett öffentlichen Entwicklung vergibt ein grosses Potential.

Darüber hinaus fehlt ein Massstab für die Beurteilung des Erfolgs dieses Einbezugs, so dass sich die Verordnung darauf beschränkt, Anreize zu fordern anstatt den Erfolg dieser Anreize zu messen.

2.4. Stärkere Vernetzung mit der Wissenschaft

Der Wissenschaft wird für die Weiterentwicklung von E-Voting eine wichtige Rolle beigemessen. Bei der Erarbeitung der Grundlagen, der Begleitung und Auswertung der Versuche sowie bei der Überprüfung der Systeme sollen vermehrt unabhängige Expertinnen und Experten, insbesondere aus der Wissenschaft, einbezogen werden.

2.4.1. Erachten Sie die unterbreiteten Rechtsgrundlagen als geeignet, um das Ziel der stärkeren Vernetzung mit der Wissenschaft umzusetzen (insbes. Art. 27*m* E-VPR, Art. 27*o* E-VPR, Art. 11-13 E-VEleS)?

☒ Ja ☐ Ja mit Vorbehalt ☐ Nein

Anmerkungen:

Ja, wir erachten die unterbreiteten Rechtsgrundlagen hierfür als geeignet. Dies namentlich nach dem Expertendialog, der im Jahr 2020 durchgeführt wurde und den wir - für Sie wohl wenig überraschend - als Erfolg beurteilen. Dazu kommt, dass der Umgang der Schweiz mit der elektronischen Stimmabgabe und namentlich die Regulierung in der Wissenschaft international einen sehr guten Ruf geniessen.

Artikelweise Detailerörterung / Discussions, article par article du projet / Esame del progetto articolo per articolo

VPR ODP ODP	Nötig? Nécessaire? Necessaria?	Tauglich? Adéquat? Adeguata?	Praktikabel? Applicable? Realizzabile?	Änderungsvorschlag? Autre proposition? Proposta di modifica?	Bemerkungen Remarques Osservazioni
Art. 8*a* Abs. 1 art. 8*a* al. 1 art. 8*a* cpv. 1	Ja	Ja	Ja	-	-
Art. 8*d* Abs. 3 art. 8*d* al. 3 art. 8*d* cpv. 3	Ja	Ja	Ja	-	-
Art. 27*b* Bst. b art. 27*b* let. b art. 27*b* lett. b	Ja	Ja	Ja	-	Wir begrüssen die Vereinfachung des Verfahrens.
Art. 27*d* Bst. c art. 27*d* let. c art. 27*d* lett. c	Ja	Ja	Ja	-	Wir begrüssen die Flexibilisierung dieses Artikels. Allerdings sehen wir auch eine leichte Gefahr für die Planungssicherheit der Kantone / Systemanbieter.
Art. 27*e* Abs. 1-2 art. 27*e* al. 1 à 2 art. 27*e* cpv. 1-2	Ja	Ja	Ja	-	-
Art. 27*f* art. 27*f*	Ja	Nein	Teilweise	Abs. 3 "Die stimmberechtigten Auslandschweizer sowie Stimmberechtigte, die aufgrund einer Behinderung **ihre Stimme nur elektronisch autonom abgeben können**, werden bei der Berechnung der Limiten nicht mitgezählt."	Abs. 3: Der Text spezifiziert nicht, auf welchem Kanal die Menschen mit Behinderung die Stimme nicht autonom abgeben können. Ziel ist es ja wohl, den Menschen mit Behinderung den barrierefreien elektronischen Kanal zur Verfügung zu stellen. Eventuell liesse sich das besser formulieren. Die Idee, die Stimmen von Menschen mit Behinderung nicht zu den Limiten hinzuzuzählen, könnte sich in der Praxis als impraktikabel erweisen, da sie ja in ihrem Wahlkreis verbleiben dürften und eine separate Ausweisung der elektronischen Stimmen zu einer Identifikation von einzelnen Menschen mit Behinderung führen könnte.
Art. 27*i* Abs. 1 und 2 art. 27*i* al. 1 et 2 art. 27*i* cpv. 1 e 2	Ja	Ja	Ja	-	Wir begrüssen den Zwang zur Plausibilisierung und die Zuweisung der Verantwortung an die Kantone.

Art. 27*l* art. 27*l*	Ja	Ja	Ja	-	Wir begrüssen die Stärkung der technischen Kompetenzen der BK und die Abkehr von einem externen Zertifizierungsprozess.
Art. 27*m* art. 27*m*	Ja	Nein	Teilweise	1 Die Bundeskanzlei und die Kantone, die Versuche durchführen, sorgen für den Einbezug der Öffentlichkeit und der Fachkreise und setzen Anreize für die Mitwirkung. 2 Die Kantone, die Versuche durchführen, machen die Funktionsweise und die Sicherheitseigenschaften des Systems der elektronischen Stimmabgabe sowie die wesentlichen betrieblichen Abläufe öffentlich bekannt. **Sie legen die entsprechende Dokumentation offen, machen den Entwicklungsprozess transparent und veröffentlichen den Quellcode unter einer Open-Source Lizenz.** ~~Sie legen die entsprechende Dokumentation sowie den Quellcode der Software offen.~~ 3 Sie informieren die Stimmberechtigten allgemein verständlich über die Organisation, die Technik und das Verfahren der elektronischen Stimmabgabe. Sie zeigen, wie beim Auftreten von Problemen vorzugehen ist, und erklären, wie die Verifizierbarkeit funktioniert. 4 Alle wichtigen behördlichen Vorgänge bei der Abwicklung eines Urnengangs mit der elektronischen Stimmabgabe ~~und die entsprechende Dokumentation~~ müssen einer Vertretung der Stimmberechtigten zugänglich sein. **Die Dokumentation aller**	2 "Public Scrutiny" erfordert eine transparente Entwicklung (inkl. Commit-History) und Engagement einer grossen Community. Mit einer Open-Source Lizenz wird die Wahrscheinlichkeit grösser, dass andere Länder Schweizer E-Voting Quellcode ebenfalls einsetzen. Demzufolge würde mit einer Open-Source Lizenz die Community um das Schweizer System grösser und somit das System sicherer. Es zeichnet sich bereits jetzt ab, dass der Aufbau einer Community sehr herausfordernd - wenn nicht gar einer der grössten Knackpunkte für ein sicheres E-Voting - sein wird. Folglich sollte alles unternommen werden, um diesem Schwachpunkt zu begegnen. 4 Impliziert, dass die Dokumentation der Vorgänge einer Abstimmung nur einer Vertretung der Stimmberechtigten zugänglich sein müssen. Das ist nicht erwünscht. Diese Information muss öffentlich sein. 5 Der Hinweis auf das Stimmgeheimnis bei der Veröffentlichung der elektronischen Ergebnisse ist sinnvoll. Eventuell wäre es eine taugliche Umsetzung, die elektronischen Ergebnisse in einem Wahlkreis erst ab einer gewissen Zahl von elektronischen Stimmen separat auszuweisen.

Artikelweise Detailerörterung / Discussions, article par article du projet / Esame del progetto articolo per articolo

				wichtigen behördlichen Vorgänge wird veröffentlicht soweit die Veröffentlichung mit der sicheren Abwickung des Urnengangs vereinbar ist. 5 Die Kantone veröffentlichen bei eidgenössischen Wahlen und Abstimmungen die Ergebnisse der über den elektronischen Stimmkanal abgegebenen Stimmen. Das Stimmgeheimnis ist zu wahren.	
Art. 27*o* art. 27*o*	Ja	Ja	Ja	-	-
Anhang 3*a* Annexe 3*a* Allegato 3*a*	Ja	Nein	Ja	Ein maschinenlesbares Format definieren.	Mit Blick auf Digitalisierungsstrategien ist die vorgeschlagene Revision nicht zu vereinbaren.

VEleS OVotE OVE	Nötig? Nécessaire? Necessaria?	Tauglich? Adéquat? Adeguata?	Praktikabel? Applicable? Realizzabile?	Änderungsvorschlag? Autre proposition? Proposta di modifica?	Bemerkungen Remarques Osservazioni
Art. 1-2 art. 1-2	Ja	Nein (teilweise)	Ja	Keiner	Der Abschnitt "a. System" bezeichnet die Gesamtheit der Software und der Infrastruktur, scheint sich dann aber auf die "Durchführung" zu beschränken ohne dass hier klar gemacht wird, ob die Vor- und Nachbereitung der Wahlen und Abstimmungen auch Teil der Durchführung sind. Das wäre eventuell noch zu klären. Der Abschnitt "j. Software" ist deutlich zu eng gefasst. Nicht kryptographische Software muss eingeschlossen werden und auch Hilfssysteme sind einzubeziehen. Daneben sollte vermieden werden, dass untaugliche Teilsysteme von Extern übernommen werden, um sicher zu stellen, dass sie als externe Entwicklung nicht unter diese Definition fallen.
Art. 3 art. 3	Ja	Nein	Ja	b. Das System ist für die Stimmberechtigten einfach zu handhaben; ~~die besonderen Bedürfnisse möglichst aller Stimmberechtigten sind berücksichtigt~~. d. Der Öffentlichkeit werden ~~adressatengerechte~~ Informationen zur Funktionsweise des Systems und zu den betrieblichen Abläufen **in verständlicher Form** zugänglich gemacht ~~und Anreize zur Mitwirkung von fachkundigen Personen aus der Öffentlichkeit sind vorhanden~~. **Die vorhandenen Anreize führen nachweislich zu einer hinreichenden Mitwirkung von fachkundigen Personen aus der Öffentlichkeit.**	Artikel 3b: Der Nachsatz ist sehr offen und schwach formuliert. Wir denken, dass diese besonderen Bedürfnisse ohnehin durch verschiedene Vorgaben abgedeckt sind und deshalb hier nicht explizit erwähnt werden müssen. Der Artikel 3d beschränkt sich auf das Vorhandensein von Anreizen, ohne sie qualitativ oder quantitativ zu bestimmen. Angesichts des grossen Bedarfs nach Public Scrutiny scheint mir das nicht adäquat. Grob wird der Zwang zur Zertifizierung durch Public Scrutiny ersetzt. Weil die aber schlecht zu messen und zu beweisen ist, beschränkt sich dieser Absatz auf Anreize, die dann hoffentlich zu Public Scrutiny führen. Der Begriff "Mitwirkung" ist sehr stark. Wir sprechen uns dafür aus, ihn beizubehalten, auch wenn er über die Forderung in anderen Passagen der VEleS hinausgeht.
Art. 4 art. 4	Ja	Nein	Ja	3 Die Risikobeurteilungen beziehen sich auf folgende Sicherheitsziele: a. Korrektheit des Ergebnisses; b. Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse; c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals; d.	Artikel 4 Abs 1: Der Einbezug von Vertrauen und Akzeptanz der Öffentlichkeit ist sinnvoll. Es ist unklar, ob sich über diesen Absatz eine Bewilligung aufgrund fehlender Vertrauen und Akzeptanz in einem bestimmten Einzelkanton verweigern liesse. Wenn das nicht möglich ist, dann lässt dieser Abschnitt hier Fehlschlüsse zu und wenn es möglich sein soll, dann wäre das klar zu schrei-

				Schutz der persönlichen Informationen über die Stimmberechtigten; e. ~~Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen~~; **Sicherstellung der Vertraulichkeit und Integrität von für die Stimmberechtigten bestimmten Informationen.** f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten.	ben oder noch besser aus dem kantonalen Kontext herauszunehmen, da es sich dabei eher um eine nationale Frage handelt.
Art. 5 art. 5	Ja	Nein	Ja	1 Es ist sichergestellt, dass jede Manipulation, die zu einer Verfälschung des Ergebnisses führt, unter Wahrung des Stimmgeheimnisses erkannt werden kann (vollständige Verifizierbarkeit). Dies ~~ist~~ **gilt als** gegeben, wenn die Anforderungen an die individuelle und an die universelle Verifizierbarkeit erfüllt sind.	-
Art. 6 art. 6	Ja	Nein	Ja	-	Vieles hängt hier am Verständnis des Begriffes "Vertrauenswürdigkeit". Bei einer technischen Lesart des Begriffes funktioniert der Artikel. Wenn Vertrauen auch eine soziologische oder politologische Kategorie ist, dann ist der Artikel nicht mehr länger tauglich. Entweder muss die Lesart hier also spezifiziert oder aber "Vertrauenswürdigkeit" wird in Artikel 2 definiert.
Art. 7 art. 7	Ja	Ja	Ja	-	Zum Begriff "Vertrauenswürdigkeit" siehe auch Bemerkungen zu Artikel 6.
Art. 8 art. 8	Ja	Ja	Ja	-	-
Art. 9 art. 9	Ja	Ja	Ja	-	Dieser Artikel ermöglicht es der Bundeskanzlei laufend weitere Massnahmen zur Risikominimierung einzufordern. Dies untergräbt die Rechts- und Planungssicherheit der Lieferanten und der Kantone. Allerdings formalisiert es lediglich eine Praxis, welche schon früher (Public Intrusion Test) gespielt hat. Allenfalls wären Schranken zu setzen, wie und in welchem Rahmen die Bundeskanzlei hier Forderungen stellen kann.
Art. 10 art. 10	Ja	Nein	Ja	Ziffer 2 kann ersatzlos gestrichen werden. Die Prüfungen im Auftrag der	Es ist nicht klar, weshalb das ISMS des Systembetreibers durch den Kanton, der Rest des Betriebes aber

				Bundeskanzlei (1c) prüfen die Sicherheit von Infrastruktur und Betrieb. Es ist nicht vorstellbar, dass diese Prüfungen zu einem positiven Befund gelangen, wenn kein geprüftes ISMS vorhanden ist. 4 Die nach den Absätzen 1 und 2 für die Prüfungen zuständigen Behörden publizieren die ~~Belege~~ **Berichte** und die Zertifikate. Zusätzlich sind weitere Unterlagen zu publizieren, sofern sie für die Nachvollziehbarkeit relevant sind. Von einer vollständigen Publikation kann abgesehen werden, sofern eine begründete Ausnahme insbesondere gestützt auf das Öffentlichkeits- oder das Datenschutzrecht vorliegt. In diesem Fall ist eine teilweise Publikation zu ermöglichen.	durch den Bund zu prüfen ist. Absatz 4 sollte strenger formuliert werden. Es darf nicht genügen, lediglich einen Beleg für eine erfolgte Prüfung zu publizieren, da ein solcher Beleg wenig aussagt über die qualitativen Ergebnisse einer Überprüfung. Bekanntlich schaffte es die Post, den KPMG Prüfbericht vor der Bundeskanzlei und der Öffentlichkeit geheim zu halten. Dies darf sich nicht wiederholen.
Art. 11 art. 11	Ja	Nein	Ja	1 Der Kanton sorgt dafür, dass folgende Unterlagen offengelegt werden: a. der Quellcode der Software des Systems ~~einschliesslich der Dateien mit relevanten Parametern~~ **unter einer Open Source Lizenz. Die Publikation schliesst die detaillierte Entwicklungsgeschichte (Commit-History) sowie die Dateien mit relevanten Parametern mit ein.**; b. die Dokumentation der Software; c. Anleitungen und ergänzende Dokumentationen, die fachkundige Personen benötigen, um das System in der eigenen Infrastruktur kompilieren, in Betrieb nehmen und analysieren zu können; d. die Dokumentation der Prozesse für den Betrieb, die Wartung und die Sicherung des Systems; e. Informationen und Beschreibungen zu bekannten Mängeln, **namentlich Berichte zu Penetration Tests**. 2 Nicht offengelegt werden müssen: a. der Quellcode von Drittkomponenten wie	- Der Dialog mit der Wissenschaft hat eine deutliche Empfehlung für eine Publikation des Source Codes unter einer Open Source Lizenz abgegeben. Dies darf nicht übergangen werden. Zumal im begleitenden Bericht keinerlei Begründung hierfür angegeben wird. - Entscheidet sich die Bundeskanzlei wirklich dafür, keine Open Source Lizenz zu verlangen, dann sollte aber zumindest die komplette Commit History eingefordert werden. Damit lassen sich die folgenden Fragen diskutieren: Welche Accounts haben wann, in welchem Rhythmus, welche Code-Teile verändert. Gibt es Korrekturen, Nachbesserungen, welche Accounts arbeiten in weilen Bereichen des Codes, wie viele Accounts sind beteiligt, etc. Diese Informationen erlauben es der interessierten Öffentlichkeit, die Qualität des Entwicklungsprozesses besser zu beurteilen. - Die Definition von "Software" darf sich nicht nur auf kryptografische Implementierung beziehen.

				Betriebssystemen, Datenbanken, Web- und Applikationsservern, Rechteverwaltungssystemen, Firewalls oder Routern, sofern diese weit verbreitet sind und laufend aktualisiert werden; b. der Quellcode von Behördenportalen, die mit dem System verbunden sind; c. Dokumente, für die eine begründete Ausnahme von einer Publikation insbesondere gestützt auf das Öffentlichkeits- oder das Datenschutzrecht vorliegt.	
Art. 12 art. 12	Ja	Nein	Ja	-	12.1 "Möglichst einfach" könnte durch "nach gängiger Praxis" ersetzt werden. Das wäre etwas klarer. 12.5 Es ist nicht einzusehen, weshalb nur kommerzielle Verstösse gegen die Nutzungsbedingungen verfolgt werden dürfen. Ein Beispiel: Es wird eine Lizenz gewählt, die es erlaubt den Code zu kopieren, aber nur unter Angabe der Quelle. Wird der Code nun kopiert, aber die Quelle nicht angegeben, so verstösst das gegen die Nutzungsbedingungen / die Lizenz des Codes, aber gemäss 12.5 darf der Verstoss nicht verfolgt werden. Es wäre besser, wenn die Lizenz und damit die Nutzungsbedingungen festgelegt wird, anstatt die Ahndung von Lizenzverstössen einzuschränken.
Art. 13 art. 13	Ja	Ja	Ja	-	- Absatz 1.b impliziert zusammen mit "Art.2 Begriffe / a. System", dass die für E-Voting relevante kantonale Infrastruktur ebenfalls im Scope eines Bug-Bounty Programms sein muss. Wir begrüssen das. - Falls bei den öffentlichen Tests mit einem wiederkehrenden und nicht mit einem permanenten Test gearbeitet wird, so lässt die Verordnung (als auch der Bericht) offen, in welcher Dauer und in welcher Frequenz hier getestet werden soll. Das ist vermutlich gewollt, aber nicht unbedingt hinreichend.
Art. 14 art. 14	Ja	Nein	Nein	-	14.1 "Wichtige Aufgaben" und 14.2 "Aufgaben des technischen Betriebs" sind zu wenig klar definiert.
Art. 15 art. 15	Ja	Ja	Ja	-	-

Art. 16 art. 16	Ja	Nein	Ja	-	Es fehlen Belege für eine aktive Community, welche den Source Code untersucht hat resp. Belege dafür, dass Public Scrutiny tatsächlich spielt. Sollten sich solche Belege nicht beibringen lassen, dann sollten zumindest dafür Belege eingefordert werden, dass es einen redlichen Versuch gab, eine Community für Public Scrutiny aufzubauen.
Art. 17 art. 17	Ja	Ja	Ja	-	-
Art. 18 art. 18	Ja	Ja	Ja	-	-

Anhang VEIeS **Annexe OVotE** **Allegato OVE**	**Änderungsvorschlag** **Autre proposition** **Proposta di modifica**	**Bemerkungen** **Remarques** **Osservazioni**
Ziff. 2	Nach einer Bereinigung der Begriffsbestimmungen in Artikel 1 sollte 2.12.11 "Werden Stimmdaten importiert, so ist eine Setup-Komponente ..." ersatzlos gestrichen werden.	Der Begriff der Setup-Komponente ist irreführend. Der Umstand, dass für das Setup der Wahl und für die Auswertung der Wahl die gleiche Quellcode-Grundlage (Secure Data Manager im Fall des Post/Scytl-Systems) verwendet wird, darf nicht dazu führen, dass diese beiden fundamental verschiedenen Aufgaben in der Regulierung oder Spezifikation vermischt werden.
Ziff. 8	8.13 Die Prüferinnen und Prüfer werden zu Prozessen, denen die Korrektheit des Ergebnisses, die Einhaltung des Stimmgeheimnisses und das Fehlen vorzeitiger Teilergebnisse unterliegen (beispielsweise Schlüsselgenerierung, Druck des Stimmmaterials, Entschlüsselung und Auszählung), angemessen informiert und geschult. Sie sind in der Lage, die Vorgänge und ihre Bedeutung ~~in den Kernpunkten~~ zu verstehen.	Die Prüferinnen und Prüfer sind die Personen mit dem grössten Fachwissen auf Seiten des Kantons und bürgen für die Korrektheit eines Urnengangs. Es ist daher nicht ausreichend, wenn diese ihre Aufgabe lediglich "in den Kernpunkten" verstehen.
Ziff. 12	-	Es ist nicht klar, was 12.6 in der Praxis bedeutet. Die Post agiert als Systembetreiber und erhält mit den versandfertigen Abstimmungscouverts persönliche Daten aus dem Stimmregister.
Ziff. 13	Zwei zusätzliche Risikoszenarien: - Angreifer schüren in der Öffentlichkeit Zweifel an der Korrektheit des Ergebnisses. - Angreifer manipulieren mittels physischem Zugang die Setup-Komponente.	-

Ziff. 14	14.10 Durch einen vorgegebenen und dokumentierten Prozess werden ~~die~~ **alle** Teile des Systems ,~~die vom Internet erreichbar sind,~~ regelmässig aktualisiert, um bekanntgewordene Schwachstellen zu eliminieren.	Die Formulierung "von Internet erreichbar" ist nicht eindeutig. Im Extremfall würde das bedeuten, dass nur ein relativ kleiner Teil des Systems regelmässig aktualisiert werden müsste. Wir empfehlen, dass im Grundsatz alle bekannten Schwachstellen zu eliminieren sind und Abweichungen davon begründet, dokumentiert und in der Risikoanalyse berücksichtigt werden müssen.
Ziff. 16	~~16.2 Die Systeme sind vor Angriffen, unabhängig von der Art der Angriffe oder ihrer Herkunft, geschützt~~.	16.2 ist nicht erfüllbar und damit ersatzlos zu streichen. 16.3 lässt mit der Formulierung "klar getrennt" zu viel Interpretationsspielraum. Es ist z.B. nicht eindeutig, ob eine separate Datenbank in einem Datenbankcluster als "klar getrennt" von anderen Datenbanken betrachtet werden kann.
Ziff. 24	24.1.19 Es wird eine Konfigurationsliste erstellt, die die folgenden Elemente enthält: - die Software; - Nachweise der erforderlichen Überprüfungen zur Einhaltung der Sicherheit; - die Teile, aus denen die Software besteht; - den Quellcode; - **die Commit-History;** - Berichte über Sicherheitsmängel und über den Stand der Behebung. ~~Für jedes Element, das für Sicherheitsfunktionen relevant ist, wird die Entwicklerin oder der Entwickler genannt. Jedes Element wird eindeutig identifiziert.~~	Für die Nachvollziehbarkeit einer Konfiguration ist die Commit-History von Bedeutung, weil dieser entnommen werden kann, wer in welcher Reihenfolge welche Änderungen aus welchem Grund vorgenommen hat. Elemente einzelnen Entwicklern zuzuordnen erachten wir als unpraktisch, weil dadurch die Resilienz des Entwicklungsteams geschwächt werden kann und weil diese eindeutige Zuordnung auf Dauer, etwa nach personellen Änderungen im Entwicklungsteam, nicht aufrecht erhalten werden kann.
Ziff. 26	26.4.1 Gegenstand: Es wird geprüft, ob es den Expertinnen und Experten im Auftrag der Bundeskanzlei gelingt, im Rahmen eines Tests die Infrastruktur des Online-Systems **und Offline-Systems** einzudringen und sich Zugang zu wichtigen Daten zu verschaffen oder die Kontrolle über wichtige Funktionen zu übernehmen. Die Tests werden auf der Grundlage von potenziellen Schwachstellen durchgeführt, die nach einer methodischen Analyse der öffentlich zugänglichen Unterlagen, insbesondere nach Artikel 11, entdeckt wurden. ~~Die Expertinnen und Experten prüfen im Mindesten Schwachstellen, die im Open Web Application Security Project (OWASP) dokumentiert sind.~~	OWASP sollte in diesem Kontext nicht zitiert werden, da ein Infrastruktur-Penetrationstest weit über die Prüfung von Web-Applikationen hinausgeht. Die Webapplikation des Online-Systems neben dem Bug-Bounty einem zusätzlichen Penetration-Test zu unterziehen, würde kaum relevante neue Erkenntnisse bringen und wäre daher unnötige Geldverschwendung. Es sollten stattdessen möglichst methodenagnostische Red-Teaming Übungen durchgeführt werden, mit Phishing, lateralen Bewegungen und physischen Zugangsversuchen im Scope. Aufgrund der Kritikalität des Offline-Systems ist ausserdem wünschenswert, dass ein solcher Test auch bei diesem durchgeführt wird. Allenfalls müsste die Beauftragung im letzteren Fall durch den Kanton erfolgen.