Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

161.116

Verordnung der BK über die elektronische Stimmabgabe

(VEleS)

vom 13. Dezember 2013 (Stand am 1. Juli 2018)

Die Schweizerische Bundeskanzlei (BK),

gestützt auf die Artikel 27*c* Absatz 2, 27*e* Absatz 1, 27*f* Absatz 1, 27*g* Absatz 2, 27*i* Absatz 3 und 27*l* Absatz 3 der Verordnung vom 24. Mai 1978[1] über die politischen Rechte (VPR),

verordnet:

[1] SR **161.11**

Art. 1 Gegenstand und Begriffe

[1] Diese Verordnung legt die Voraussetzungen für die Zulassung der elektronischen Stimmabgabe fest.

[2] Es gelten die Begriffe nach Anhang Ziffer 1.3.

Art. 2 Allgemeine Voraussetzungen für die Zulassung der elektronischen Stimmabgabe pro Urnengang

Die Zulassung der elektronischen Stimmabgabe pro Urnengang wird erteilt, wenn folgende Voraussetzungen erfüllt sind:

a. Das System für die elektronische Stimmabgabe (System) ist so ausgestaltet und wird so betrieben, dass eine sichere und vertrauenswürdige Stimmabgabe gewährleistet ist (Anhang Ziff. 2 und 3).
b. Das System ist für die Stimmberechtigten einfach zu handhaben. Die besonderen Bedürfnisse möglichst aller Stimmberechtigten sind berücksichtigt.
c. Das System und die betrieblichen Abläufe sind so weit dokumentiert, dass sämtliche sicherheitsrelevanten technischen und organisatorischen Abläufe im Detail nachvollzogen werden können.

Art. 3 Risikobeurteilung

[1] Mit einer Risikobeurteilung muss der Kanton ausführlich und verständlich dokumentieren, dass sich jegliche Sicherheitsrisiken in einem ausreichend tiefen Rahmen bewegen. Die Beurteilung bezieht sich auf folgende Sicherheitsziele:

a. Korrektheit des Ergebnisses;
b. Schutz des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse;
c. Verfügbarkeit der Funktionalität;
d. Schutz der persönlichen Informationen über die Stimmberechtigten;
e. Schutz der Informationen für die Stimmberechtigten vor Manipulationen;
f. Ausschluss von Beweisen zum Stimmverhalten.

[2] Jedes Risiko muss mit Bezug auf die Sicherheitsziele, allfällige mit ihnen verbundene Datensätze, Bedrohungen, Schwachstellen und die Dokumentation zum System und zu dessen Betrieb identifiziert und klar beschrieben werden. Der Kanton muss auf dieser Grundlage begründen, weshalb er die Risiken als hinreichend gering einschätzt.

[3] Die Minimierung von Risiken darf sich nicht darauf abstützen, sicherheitsrelevante Informationen zum System und dessen Betrieb geheim zu halten.

Art. 4 Anforderungen an die Zulassung von mehr als 30 Prozent des kantonalen Elektorats

[1] Soll ein System für den Einbezug von mehr als 30 Prozent des kantonalen Elektorats zugelassen werden, so müssen die Stimmenden die Möglichkeit haben, zu erkennen, ob ihre Stimme auf der Benutzerplattform oder auf dem Übertragungsweg manipuliert oder abgefangen worden ist (individuelle Verifizierbarkeit, Anhang Ziff. 4.1 und 4.2).

[2] Zur individuellen Verifizierung muss die stimmende Person einen Beweis erhalten, dass das serverseitige System die Stimme so, wie sie die stimmende Person in die Benutzerplattform eingegeben hat, als systemkonform abgegeben registriert hat. Der Beweis muss für jede Teilstimme die korrekte Registrierung bestätigen.

[3] Wird das clientseitige Authentisierungsmerkmal elektronisch zugestellt, so müssen die Stimmberechtigten, die ihre Stimme nicht elektronisch abgegeben haben, nach der Schliessung des elektronischen Stimmkanals innert der gesetzlichen Beschwerdefristen einen Beweis anfordern können, dass das System keine Stimme registriert hat, die unter Verwendung ihres clientseitigen Authentisierungsmerkmals abgegeben wurde.

[4] Die Stichhaltigkeit eines Beweises darf nicht von der Vertrauenswürdigkeit der Benutzerplattform oder des Übertragungswegs abhängen.

[5] Sie darf auf folgenden Elementen basieren:

a. Vertrauenswürdigkeit des serverseitigen Systems;
b. Vertrauenswürdigkeit der besonderen technischen Hilfsmittel der Stimmenden; diese müssen besonders hohe Sicherheitsanforderungen erfüllen;
c. Vertraulichkeit von in Papierform zugestellten Daten; die Vertraulichkeit dieser Daten muss ausserhalb der Infrastruktur durch besondere Massnahmen sichergestellt sein.

Art. 5 Anforderungen an die Zulassung von mehr als 50 Prozent des kantonalen Elektorats

[1] Soll ein System für den Einbezug von mehr als 50 Prozent des kantonalen Elektorats zugelassen werden, so muss sichergestellt sein, dass Stimmende oder die Prüferinnen und Prüfer unter Einhaltung des Stimmgeheimnisses die Möglichkeit haben, jede Manipulation zu erkennen, die zu einer Verfälschung des Ergebnisses führt (vollständige Verifizierbarkeit, Anhang Ziff. 4.3 und 4.4).

[2] Die vollständige Verifizierbarkeit ist gegeben, wenn erweiterte Anforderungen an die individuelle Verifizierbarkeit (Abs. 3) und Anforderungen an die universelle Verifizierbarkeit (Abs. 4–6) erfüllt sind.

[3] Zur individuellen Verifizierung sind zusätzlich zu Artikel 4 die folgenden Anforderungen zu erfüllen:

a. Der Beweis muss den Stimmenden zusätzlich zur Bestätigung dienen, dass die für die universelle Verifizierung relevanten Daten den vertrauenswürdigen Systemteil (Abs. 6) erreicht haben.
b. Die stimmende Person muss nach der Schliessung des elektronischen Stimmkanals einen Beweis anfordern können, dass der vertrauenswürdige Systemteil nicht bereits eine Stimme registriert hat, die unter Verwendung ihres clientseitigen Authentisierungsmerkmals abgegeben wurde.
c. Die Stichhaltigkeit eines Beweises darf nicht von der Vertrauenswürdigkeit des gesamten serverseitigen Systems abhängen. Sie darf jedoch auf der Vertrauenswürdigkeit des vertrauenswürdigen Systemteils basieren.

[4] Zur universellen Verifizierung erhalten die Prüferinnen und Prüfer einen Beweis der korrekten Ergebnisermittlung. Sie müssen den Beweis in einem beobachtbaren Prozess auswerten. Dazu müssen sie technische Hilfsmittel verwenden, die vom Rest des Systems unabhängig und isoliert sind. Der Beweis muss bestätigen, dass das ermittelte Ergebnis:

a. alle systemkonform abgegebenen Stimmen, die durch den vertrauenswürdigen Systemteil registriert wurden, berücksichtigt;
b. ausschliesslich systemkonform abgegebene Stimmen berücksichtigt;
c. alle Teilstimmen gemäss des im Rahmen der individuellen Verifizierung generierten Beweises berücksichtigt.

[5] Die Stichhaltigkeit des Beweises darf nur von der Vertrauenswürdigkeit des

vertrauenswürdigen Systemteils und des zur Überprüfung eingesetzten technischen Hilfsmittels abhängen. Gleichzeitig dürfen die Gewährleistung des Stimmgeheimnisses und der Ausschluss vorzeitiger Teilergebnisse innerhalb der Infrastruktur nur von der Vertrauenswürdigkeit des vertrauenswürdigen Systemteils abhängen.

[6] Der vertrauenswürdige Systemteil umfasst entweder eine oder wenige Gruppen von durch besondere Massnahmen gesicherten, unabhängigen Komponenten (Kontrollkomponenten). Ihr Einsatz muss auch dann jeden Missbrauch erkennbar machen, wenn pro Gruppe nur eine der Kontrollkomponenten korrekt funktioniert und insbesondere nicht unbemerkt manipuliert wird. Für die Vertrauenswürdigkeit des vertrauenswürdigen Systemteils ist die unterschiedliche Ausgestaltung der Kontrollkomponenten sowie die Unabhängigkeit von deren Betrieb und deren Überwachung massgebend.

Art. 6 Zusätzliche Massnahmen zur Risikominimierung

Falls die Risiken trotz der ergriffenen Massnahmen nicht hinreichend klein sind, so müssen zur Risikominimierung zusätzliche Massnahmen ergriffen werden. Dies gilt insbesondere auch dann, wenn sämtliche Anforderungen nach Anhang Ziffer 2–4 bereits umgesetzt sind.

Art. 7 Anforderungen an die Überprüfung

[1] Die Kantone sorgen dafür, dass die Erfüllung der Voraussetzungen von unabhängigen Stellen überprüft wird. Die Überprüfung findet insbesondere statt, wenn das System oder sein Betrieb so geändert worden sind, dass die Erfüllung der Voraussetzungen für die Zulassung in Frage gestellt sein könnte.

[2] Falls mehr als 30 Prozent des kantonalen Elektorats zu einem Versuch zugelassen werden soll (Art. 4 und 5), so müssen das System und sein Betrieb hinsichtlich folgender Kriterien besonders eingehend geprüft werden:

a. kryptografisches Protokoll (Anhang Ziff. 5.1);
b. Funktionalität (Anhang Ziff. 5.2);
c. Sicherheit von Infrastruktur und Betrieb (Anhang Ziff. 5.3);
d. Schutz gegen Versuche, in die Infrastruktur einzudringen (Anhang Ziff. 5.5);
e. Anforderungen an Druckereien (Anhang Ziff. 5.6);
f.[2] bei Verwendung eines Systems mit der Eigenschaft der vollständigen Verifizierbarkeit nach Artikel 5: Kontrollkomponenten (Anhang Ziff. 5.4).

[3] Falls höchstens 30 Prozent des kantonalen Elektrorats zu einem Versuch zugelassen werden soll und das System die Eigenschaft der vollständigen Verifizierbarkeit nach Artikel 5 aufweist, so müssen das System und sein Betrieb hinsichtlich folgender Kriterien besonders eingehend geprüft werden:

a. kryptografisches Protokoll (Anhang Ziff. 5.1);
b. Funktionalität (Anhang Ziff. 5.2), wobei die Überprüfung die Software von Behördenportalen, die mit einem System verbunden sind, ausschliessen darf;
c. Sicherheit von Infrastruktur und Betrieb (Anhang Ziff. 5.3), wobei sich die Überprüfung auf diejenige Infrastruktur beschränken darf, die die Stimme registriert und den Beweis zu Handen der Stimmenden gemäss Artikel 4 Absatz 2 erstellt;
d. Schutz gegen Versuche, in die Infrastruktur einzudringen (Anhang Ziff. 5.5);
e. Kontrollkomponenten (Anhang Ziff. 5.4).[3]

[2] Fassung gemäss Ziff. I der V der BK vom 30. Mai 2018, in Kraft seit 1. Juli 2018 (AS **2018** 2279).

[3] Eingefügt durch Ziff. I der V der BK vom 30. Mai 2018, in Kraft seit 1. Juli 2018 (AS **2018** 2279).

Art. 7*a*[4] Offenlegung des Quellcodes

[1] Der Quellcode der Software des Systems muss offengelegt werden.

[2] Die Offenlegung findet statt, wenn das System die Eigenschaft der vollständigen Verifizierbarkeit nach Artikel 5 aufweist, und:

a. nach der Überprüfung nach Artikel 7 Absatz 2, falls mehr als 30 Prozent des kantonalen Elektorats zu einem Versuch zugelassen werden soll;
b. nach der Überprüfung nach Artikel 7 Absatz 3, falls höchstens 30 Prozent des kantonalen Elektorats zu einem Versuch zugelassen werden soll.

[3] Nicht offengelegt werden muss der Quellcode von:

a. Drittkomponenten wie Betriebssystemen, Datenbanken, Web- und Applikationsservern, Rechteverwaltungssystemen, Firewalls oder Routern, sofern diese weit verbreitet sind und laufend aktualisiert werden;
b. Behördenportalen, die mit einem System verbunden sind.

[4] Eingefügt durch Ziff. I der V der BK vom 30. Mai 2018, in Kraft seit 1. Juli 2018 (AS **2018** 2279).

Art. 7*b*[5] Modalitäten der Offenlegung des Quellcodes

[1] Der Quellcode muss nach besten Praktiken aufbereitet und dokumentiert werden.

[2] Er muss einfach und unentgeltlich über das Internet beziehbar sein.

[3] Eine Dokumentation zum System und zu dessen Betrieb muss die Relevanz der einzelnen Teile des Quellcodes für die Sicherheit der elektronischen Stimmabgabe erklären. Sie ist zusammen mit dem Quellcode offenzulegen.

[4] Jeder und jede darf den Quellcode zu ideellen Zwecken untersuchen, verändern, kompilieren und ausführen sowie dazu Studien verfassen und diese publizieren. Der Eigner des Quellcodes kann dessen Nutzung zu anderen Zwecken erlauben.

[5] Eingefügt durch Ziff. I der V der BK vom 30. Mai 2018, in Kraft seit 1. Juli 2018 (AS **2018** 2279).

Art. 8 Belege zu den Gesuchen

[1] Den nach den Artikeln 27*c* und 27*e* Absatz 1 VPR eingereichten Gesuchen sind beizulegen:

a. Belege oder Zertifikate, dass das System und dessen Betrieb hinsichtlich der gestellten Anforderungen geprüft worden sind und sämtliche Anforderungen wirksam erfüllen (Anhang Ziff. 6.1–6.3);
b. Belege, dass die Beurteilung der Risiken im Vorfeld eines Urnengangs vorgenommen wurde; aus diesen muss hervorgehen, weshalb sich die eingeschätzten Risiken in einem ausreichend tiefen Rahmen bewegen (Anhang Ziff. 6.4).

[2] Auf Belege, die die Bundeskanzlei bereits erhalten hat und die noch gültig sind, kann verwiesen werden.

Art. 9 Weitere Bestimmungen

[1] Die detaillierten technischen und administrativen Anforderungen an die elektronische Stimmabgabe sind im Anhang geregelt.

[2] Bis zum 30. Juni 2015 kann ein Kanton in Ausnahmefällen von der Umsetzung einzelner Anforderungen aus Anhang Ziffer 2 und 3 befreit werden, sofern:

a. nicht mehr als 30 Prozent des kantonalen Elektorats zugelassen werden sollen;
b. die nicht umgesetzten Anforderungen im Gesuch bezeichnet sind; und
c. der Kanton die alternativen Massnahmen beschreibt und mit Bezug auf die Risikobeurteilung begründet, weshalb er die Risiken als hinreichend gering einschätzt.

Art. 10 Inkrafttreten

Diese Verordnung tritt am 15. Januar 2014 in Kraft.

Anhang

(Art. 9 Abs. 1)

Technische und administrative Anforderungen an die elektronische Stimmabgabe[6]

[6] Der Text des Anhangs zu dieser Verordnung wird in der AS nicht publiziert (AS **2018** 2279). Er kann kostenlos abgerufen werden unter www.bk.admin.ch > Politische Rechte > E-Voting > Bundesrechtliche Anforderungen oder kostenlos bezogen werden bei der Bundeskanzlei, Sektion Politische Rechte, Bundeshaus West, 3003 Bern.