Bayerischer Landtag

19. Wahlperiode 05.05.2026 Drucksache 19/11340

Schriftliche Anfrage

des Abgeordneten **Franz Schmid AfD**
vom 02.03.2026

Digitale U-18-Wahl

Die folgenden Fragen beziehen sich auf die digitale U-18-Wahl zu den Kommunalwahlen 2026 in Bayern.

Die Staatsregierung wird gefragt:

Antwort

des Staatsministeriums für Digitales
vom 31.03.2026

1.1 Welche Software bzw. welcher Anbieter wurde für die digitale U-18-Wahl eingesetzt?

1.2 Welche konkrete Produktlösung bzw. Version kam zum Einsatz?

1.3 Aus welchen Gründen wurde diese Lösung ausgewählt?

Die Fragen 1.1 bis 1.3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Bayerische Jugendring (BJR) hat mit Unterstützung des Staatsministeriums für Digitales (StMD) eine Markterkundung durchgeführt. Die Entscheidung wurde durch den BJR getroffen. Ausgewählt wurde POLYAS CORE 3 Verifiable in der Version 3.68.3. der POLYAS GmbH, Kassel.

2.1 Welche IT-Sicherheitsstandards lagen der digitalen Wahl zugrunde?

2.2 Gab es Zertifizierungen, externe Prüfungen oder Penetrationstests?

2.3 Falls ja, durch wen wurden diese durchgeführt (bitte auch Ergebnis nennen)?

Die Fragen 2.1 bis 2.3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Architektur des Wahlsystems entspricht den Anforderungen des Schutzprofils BSI-CC-PP-0121-2024. Betrieb und Entwicklung des Wahlsystems orientieren sich an ISO27001 und sind danach zertifiziert. Ein entsprechender Penetrationstest wurde von der Micromata GmbH, Kassel, durchgeführt. Es wurden keine sicherheitskritischen Risiken identifiziert (ISO27001: Datenschutz CERT).

3.1 Welche Maßnahmen wurden zum Schutz vor Manipulation getroffen?

3.2 Welche Vorkehrungen gab es gegen Cyberangriffe oder Datenlecks?

3.3 Wurden Notfall- oder Backup-Konzepte implementiert?

Die Fragen 3.1 bis 3.3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Manipulationsschutz wurde unter anderem durch die Kombination aus Ende-zu-Ende-Verschlüsselung, kryptografischen Signaturen auf jedem Stimmzettel, unveränderlichen Bulletin Boards, Zero-Knowledge-Proofs für jeden Verarbeitungsschritt sowie individueller und universeller Verifikation gewährleistet. Zudem wurden, hier in einer

nicht abschließenden Auflistung, auch Passwörter mit hoher Entropie gegen Brute-Force-Angriff, Monitoring und Identifikation von ungewöhnlichen Netzwerkaktivitäten und entsprechender Alarmierung sowie ISO27001-zertifiziertes-Hosting mit DDoS-Schutz unter regelmäßigen externen Penetrationstests verwendet. Die implementierten Notfall- und Backup-Konzepte waren an den Anforderungen der ISO27001 sowie an der BSI TR-03169 ausgerichtet.

4.1 Wie wurde sichergestellt, dass nur berechtigte Personen abstimmen konnten?

4.2 Welche Mechanismen verhinderten Mehrfachabstimmungen?

4.3 Wie wurde technisch garantiert, dass pro Person nur eine Stimme gezählt wird?

5.1 Wie erfolgte die Authentifizierung der Teilnehmenden (z. B. Einmal-Code, Altersprüfung etc.)?

5.2 Wurde ein Identitäts- oder Altersnachweis verlangt?

5.3 Gab es alternative Verfahren bei technischen Problemen?

Die Fragen 4.1 bis 5.3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Ein unabhängiger Registrar (Softwarekomponente) generiert für jede wahlberechtigte Person ein Passwort, das gleichzeitig als „Login-Credential“ und als kryptografischer „Private Key“ zum Signieren des für diese Person erzeugten digitalen Stimmzettels dient. Nur ein korrekt signierter Stimmzettel wird vom Wahlserver akzeptiert, personenbezogenen Daten werden dafür explizit nicht verwendet und nicht benötigt. Jeder digitale Stimmzettel einer wahlberechtigten Person wird nach erfolgreicher Stimmabgabe im Verzeichnis („Registry Board“) als „bereits gewählt“ markiert und kann danach nicht erneut zur Stimmabgabe verwendet werden. Technisch wird dies über den individuellen „Private Key“ jedes Stimmzettels sichergestellt. Auf dieser Basis können doppelt signierte oder doppelt eingehende Stimmzettel zweifelsfrei identifiziert und explizit als ungültig markiert und herausgefiltert werden.

Die teilnahmeberechtigten Wählerinnen und Wähler im Alter von 14 bis 17 Jahren wurden durch die teilnehmenden Pilotkommunen standardgemäß identifiziert. Anschließend wurden sie mit den entsprechenden Anmeldedaten analog zu einer Wahlbenachrichtigung angeschrieben. Für den Fall von technischen Problemen hätte (analog zu regulären politischen Wahlen) durch den Wahlausschuss beschlossen werden können, den Wahlzeitraum entsprechend zu verlängern, bis etwaige technische Probleme behoben sind. In diesem Pilotprojekt sind keine technischen Probleme aufgetreten.

6.1 Wie wurde der Datenschutz gemäß Datenschutz-Grundverordnung umgesetzt?

6.2 Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

6.3 Welche technischen und organisatorischen Maßnahmen (TOM) wurden angewandt?

7.1 Wo wurden die Daten gespeichert?

7.2 Wie lange werden die Daten gespeichert?

7.3 Wer hat bzw. hatte Zugriff auf die gespeicherten Daten?

Die Fragen 6.1 bis 7.3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die technischen Projektpartner haben bei der Wahldurchführung keine personenbezogenen Daten be-, verarbeitet oder gespeichert. Die Umsetzung des Datenschutzes erfolgte gemäß Datenschutz-Grundverordnung (DSGVO) systematisch durch die Kombination von rechtlichen, organisatorischen und technischen Maßnahmen. Im Vorfeld der digitalen U-18-Wahl wurde für die beteiligten Kommunen zudem ein Prüfungsprozess in Abstimmung mit dem örtlichen Datenschutz durchgeführt. Dabei wurden spezifische Datenschutzmaßnahmen definiert, um die Einhaltung der DSGVO sicherzustellen. Dies umfasste unter anderem die rechtskonforme Prüfung der digitalen U-18-Wahl, die Prüfung der verwendeten Plattform auf die technische Umsetzung und der DSGVO-konforme Datenverarbeitung, die zielgruppenspezifische Information über die Verwendung der Daten, die Trennung personenbezogener Daten zwischen Kommune und Plattform sowie die interne Verarbeitung der Daten innerhalb der Verwaltung.

8.1 Welche Gesamtkosten sind entstanden (Software, Betrieb, Personal, Kommunikation) bzw. wer hat diese getragen?

Für Software, Betrieb, Personal und Kommunikation sind beim StMD keine zusätzlichen Kosten entstanden.

8.2 Gab es laufende Lizenz- oder Wartungskosten?

Nein.

8.3 Wie hoch war die digitale Wahlbeteiligung im Vergleich zur analogen, gab es dokumentierte Probleme bzw. ist eine Evaluation bzw. ein Abschlussbericht vorgesehen oder bereits veröffentlicht?

Die Wahlbeteiligung in den digitalen Pilotkommunen betrug insgesamt 16,7 Prozent. Eine exakte Wahlbeteiligung in den analogen Kommunen ist nicht bekannt. Eine wissenschaftliche Begleitung des Projektes fand durch die Universität der Bundeswehr München statt. Die Ergebnisse werden nach Fertigstellung der Studie veröffentlicht.

Hinweise des Landtagsamts

Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

Zur Vereinfachung der Lesbarkeit können Internetadressen verkürzt dargestellt sein. Die vollständige Internetadresse ist als Hyperlink hinterlegt und in der digitalen Version des Dokuments direkt aufrufbar. Zusätzlich ist diese als Fußnote vollständig dargestellt.

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de/parlament/dokumente abrufbar.

Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de/aktuelles/sitzungen zur Verfügung.