RECHT.NRW
Landesrecht Nordrhein-Westfalen

Ministerium des Innern
des Landes Nordrhein-Westfalen

Ministerialblatt für das Land Nordrhein-Westfalen

Ausgabe: MBl. NRW. 2022 Nr. 26
Veröffentlichungsdatum: 31.05.2022
Seite: 564

I

Verwaltungsvorschrift zur Zulassung von Anwendungen zur Bild-Ton-Übertragung sowie von Anwendungen zur Durchführung digitaler Abstimmungen im Rahmen von digitalen und hybriden Sitzungen kommunaler Gremien (Verwaltungsvorschrift Anwendungszulassung Digitalsitzungen – VV AnwendZulDigiSi)

2023

Verwaltungsvorschrift zur Zulassung von Anwendungen zur Bild-Ton-Übertragung sowie von Anwendungen zur Durchführung digitaler Abstimmungen im Rahmen von digitalen und hybriden Sitzungen kommunaler Gremien (Verwaltungsvorschrift Anwendungszulassung Digitalsitzungen – VV AnwendZulDigiSi)

Runderlass
des Ministeriums für Heimat, Kommunales, Bau und Gleichstellung
- 301-43.00 -

Vom 31. Mai 2022

Aufgrund des § 133 Absatz 2 der Gemeindeordnung für das Land Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 14. Juli 1994 (GV. NRW. S. 666), der zuletzt durch Artikel 15 des Gesetzes vom 23. Januar 2018 (GV. NRW. S. 90) geändert worden ist, und des § 12 Absatz 1 der Digitalsitzungsverordnung vom 27. April 2022 (GV. NRW. S. 711) erlässt das Ministerium für Heimat, Kommunales, Bau und Gleichstellung im Benehmen mit dem Beauftragten der Landesregierung Nordrhein-Westfalen für Informationstechnik folgende Verwaltungsvorschrift:

1
Anwendungsbereich

Diese Verwaltungsvorschrift ist bei der Prüfung und Zulassung von am Markt erhältlichen und kommunal eigenentwickelten Anwendungen zur Bild-Ton-Übertragung (Videokonferenzsysteme), Anwendungen zur Durchführung digitaler Abstimmungen (Abstimmungssysteme), sowie Anwendungen, die eine integrierte Lösung beider Elemente bieten, zu berücksichtigen, sofern diese Anwendungen für die Durchführung digitaler und hybrider kommunaler Gremiensitzungen nach der Digitalsitzungsverordnung vom 27. April 2022 (GV. NRW. S. 711) in der jeweils geltenden Fassung, im Folgenden DigiSiVO genannt, verwendet werden sollen. Sie beschreibt die Umsetzung des in § 47a Absatz 4 Satz 2 der Gemeindeordnung für das Land Nordrhein-Westfalen in der Fassung der Bekanntmachung vom 14. Juli 1994 (GV. NRW. S. 666) in der jeweils geltenden Fassung, im Folgenden GO NRW genannt, vorgesehenen und in § 11 DigiSiVO aufgrund von § 133 Absatz 4 Satz 3 GO NRW näher geregelten Zulassungsverfahrens und fasst auf dieser Grundlage die aus den kommunalrechtlichen Vorschriften sowie aus weiteren im Land Nordrhein-Westfalen geltenden Gesetzen und Verordnungen ableitbaren IT-sicherheitstechnischen, datenschutzrechtlichen und funktionalen Anforderungen zusammen, die die Anwendungen für eine Zulassung erfüllen müssen. Die technischen Voraussetzungen und die organisatorischen Vorkehrungen, die unter dem Gesichtspunkt der IT-Sicherheit, des Datenschutzes und der Sicherung eines reibungslosen Sitzungsablaufs beim Einsatz der Anwendungen von den Gemeinden und Gemeindeverbänden individuell in eigener Verantwortung zu schaffen beziehungsweise umzusetzen sind, sind nicht Gegenstand des Prüfungs- und Zulassungsverfahrens.

2
Zulassungsverfahren

2.1
Ziel des Zulassungsverfahrens

Das Zulassungsverfahren zielt darauf ab, sicherzustellen, dass Softwareanwendungen vor ihrer Verwendung für digitale und hybride kommunale Gremiensitzungen von fachkundiger Stelle daraufhin überprüft werden, ob sie die technischen und rechtlichen Anforderungen an eine geset-

zeskonforme Beratung und Beschlussfassung in digitalen und hybriden Sitzungsformaten erfüllen.

2.2
Aufgaben der Zulassungsstelle

Die erforderliche Zulassung von Anwendungen im Sinne von Nummer 1 für die Verwendung in digitalen und hybriden Gremiensitzungen obliegt gemäß § 11 Absatz 1 DigiSiVO der Gemeindeprüfungsanstalt als zuständige Stelle im Sinne von § 47a Absatz 4 Satz 2 GO NRW (Zulassungsstelle).

Die Zulassungsstelle ist für die Organisation und einheitliche Durchführung des Zulassungsverfahrens verantwortlich. Sie entwickelt aus den Vorgaben dieser Verwaltungsvorschrift einen Prüfkriterienkatalog beziehungsweise ein Prüfungshandbuch, legt das Prüfverfahren und die beizubringenden Nachweise fest und entscheidet auf Grundlage der Prüfergebnisse über die Zulassung einer zulassungspflichtigen Software-Anwendung, fertigt den Zulassungsbescheid und stellt gegebenenfalls eine Zulassungsbescheinigung aus.

2.3
Antragstellung

Die Stellung eines Antrags erfolgt regelmäßig durch den Hersteller oder Anbieter von Software-Anwendungen (hierunter fallen auch Software-as-a-Service-Lösungen) für Videokonferenzen, Online-Abstimmungen und Wahlen oder von integrierten Lösungen, die beide Komponenten umfassen, sowie durch Gemeinden oder Gemeindeverbände, die solche Softwareanwendungen selbst entwickelt haben. Eine Antragstellung durch eine Gemeinde oder einen Gemeindeverband für eine von Dritten hergestellte oder angebotene Anwendung kann ausnahmsweise unter der Voraussetzung zugelassen werden, dass alle erforderlichen Erklärungen und Auskünfte beigebracht werden und die Erfüllung der mit der Zulassung verbundenen Pflichten nachweislich sichergestellt ist.

Bei Anwendungen, die von mehreren Gemeinden oder Gemeindeverbänden eingesetzt werden sollen, genügt eine Zulassung, sofern nicht anbieterseitige gemeindespezifische Anpassungen der Anwendung wesentliche Abweichungen gegenüber dem zugelassenen Ausgangsprodukt aufweisen.

2.4
Mitwirkungspflichten der Antragstellenden

Die Antragstellerin beziehungsweise der Antragsteller ist für die frühzeitige Bereitstellung von Nachweisdokumenten und für die Richtigkeit und Aktualität der Angaben zu Produktinformationen verantwortlich.

Zu den Verantwortlichkeiten der Antragstellenden gehören insbesondere

a) die Einreichung von Nachweisdokumenten mit der Antragstellung und auf Anforderung während der Zulassungsprüfung,

b) die Mitwirkung am Zulassungsverfahren, unter aanderem durch Bereitstellung von Testsoftware und Benennung einer Ansprechperson,

c) gegebenenfalls die Gewährung des Zugangs zu den Betriebsräumen für Software-as-a-Service-Lösungen und

d) die Benachrichtigung der Zulassungsstelle über Produktänderungen.

2.5
Einzureichende Unterlagen

Folgende Angaben beziehungsweise Unterlagen sind mit dem elektronischen Antrag zu Beginn des Zulassungsverfahrens einzureichen:

a) Angaben zum Hersteller und Kontaktdaten einer oder mehrerer Ansprechpersonen gemäß Antragsformular,

b) Angaben zum Software-Produkt: Produktname, Module/Komponenten, Versionsnummer und Veröffentlichungsdatum gemäß Antragsformular und

c) Herstellernachweise und sonstige ausführliche Dokumentation, aus der die technischen Eigenschaften des zuzulassenden Software-Produktes klar und prüffähig hervorgehen.

Die Zulassungsstelle kann zum Nachweis der Erfüllung von Datenschutz- und IT- Sicherheits-Standards die Vorlage geeigneter Zertifikate von dritten Stellen (beispielsweise des TÜVs oder des Bundesamtes für Sicherheit in der Informationstechnik) verlangen. Die Antragstellerin beziehungsweise der Antragsteller kann seinerseits die Anerkennung vorhandener Zertifikate von dritten Stellen zum Nachweis der Erfüllung einzelner oder mehrerer Anforderungen beantragen. In diesen Fällen sind die Zertifikate inklusive des bestehenden Prüfberichts mit dem Antrag einzureichen.

Bei Bedarf hat die Antragstellerin beziehungsweise der Antragsteller nach Abstimmung mit der Zulassungsstelle eine testfähige Version der Softwareanwendung bereitzustellen. Dies umfasst

mindestens das installier- und testfähige Software-Produkt in dem Umfang und in der Version, für die die Antragstellung erfolgen soll, sowie eine hinreichende Dokumentation zum Software-Produkt und den dazugehörigen Modulen.

2.6
Vorbereitung der Prüfung

Zur Vorbereitung auf die Zulassungsprüfung soll vorab ein Informationsgespräch zwischen der Antragstellerin beziehungsweise dem Antragsteller und der Zulassungsstelle durchgeführt werden, um die Prüfschritte und die organisatorischen Rahmenbedingungen abzustimmen. Stellt eine Kommune den Antrag für eine von einem Dritten angebotene Softwarelösung, soll dieser Anbieter nach Möglichkeit in das Informationsgespräch einbezogen werden.

Nach Eingang der Antragsunterlagen erhält die Antragstellerin beziehungsweise der Antragsteller eine Eingangsbestätigung. Nach Sichtung der Unterlagen weist die Zulassungsstelle zeitnah auf fehlende Angaben oder Unterlagen hin. Sind die Unterlagen vollständig, erhält die Antragstellerin beziehungsweise der Antragsteller eine Bestätigung der Prüffähigkeit der Antragsunterlagen.

2.7
Durchführung der Prüfung

Die Zulassungsstelle kann sich für die Zulassungsprüfung oder Teile dieser einer externen sachkundigen Prüfdienststelle bedienen oder die Aufgaben der Prüfdienststelle selbst ausführen. Die Aufgaben der Prüfdienststelle sind

a) die Prüfung der Nachweisdokumente der Antragstellenden,

b) die Durchführung der Kriterienprüfung der Softwareanwendung mithilfe des bereitgestellten Prüfkriterienkatalogs und

c) die Erstellung eines nach Vorgaben der Zulassungsstelle standardisierten Prüfberichts nach Abschluss der Kriterienprüfung einschließlich einer Zulassungsempfehlung.

Die Prüfdienststelle trägt gegenüber der Zulassungsstelle die Verantwortung für die korrekte Durchführung der Zulassungsprüfung sowie für die Korrektheit der Prüfergebnisse beziehungsweise des Prüfberichts und der zugehörigen Dokumente.

Die Prüfdienststelle kann auch während des Prüfverfahrens weitere Nachweise und ergänzende Unterlagen anfordern, wenn die Erfüllung der Anforderungen auf Grundlage der vorliegenden Unterlagen nicht zweifelsfrei bestätigt werden kann.

Soll die Prüfung auf bereits vorhandene oder beizubringende Zertifikate von dritten Stellen gestützt werden, ist der Zulassungsprüfung im engeren Sinne eine Anerkennungsprüfung der Zertifikate vorgelagert. Die Informationen der vorgelegten oder beizubringenden Zertifikate und Prüfberichte müssen Rückschlüsse darauf zulassen, ob eine oder mehrere der in dieser Verwaltungsvorschrift konkretisierten technischen Anforderungen erfüllt sind. Ergebnis der Anerkennungsprüfung ist die Feststellung, welche Prüfkriterien auf Grundlage der vorgelegten Nachweise bereits als erfüllt angesehen werden können. In Form einer Differenzprüfung wird anschließend im Einzelnen geprüft, welche eigenen Prüfkriterien durch die dritte Stelle nicht behandelt wurden, die sodann Gegenstand der eigenen Prüfung werden.

Die Prüfung erfolgt am Sitz der Gemeindeprüfungsanstalt beziehungsweise der beauftragten Prüfdienststelle oder an einem Geschäftsstandort der Antragstellerin beziehungsweise des Antragstellers in einer geeigneten Testumgebung.

Die Prüfung und die darauf aufbauenden Entscheidungen erfolgen unter Beachtung des Vier-Augen-Prinzips.

2.8
Entscheidung über die Zulassung

Auf Grundlage des Prüfberichts entscheidet die Zulassungsstelle über die Zulassung der Anwendung. Geht aus dem Prüfbericht die Erfüllung der in Nummer 3 dieser Verwaltungsvorschrift konkretisierten technischen Anforderungen hervor, erfolgt eine positive Zulassungsentscheidung. Hierzu stellt die Zulassungsstelle den Antragstellenden einen Zulassungsbescheid einschließlich einer Zulassungsbescheinigung aus. Die Zulassungsbescheinigung wird zusätzlich auf der Internetseite der Gemeindeprüfungsanstalt veröffentlicht, sofern die Antragstellenden der Veröffentlichung nicht widersprechen.

Die Zulassungsentscheidung kann sich auch nur auf selbständig verwendbare Teile oder Komponenten einer Anwendung beziehen. Das gilt insbesondere für Anwendungen, die die Funktionalitäten einer Videokonferenzlösung und einer Online-Abstimmungslösung in sich vereinen. Der Teil, für den die Zulassung ausgesprochen wird, ist in diesem Fall in der Zulassungsentscheidung hinreichend genau zu bestimmen.

Die Zulassung wird regelmäßig verweigert, wenn das betrachtete Software-Produkt die Prüfkriterien nicht erfüllt und somit den technischen Anforderungen nach Nummer 3 dieser Verwaltungsvorschrift nicht entspricht. In diesem Fall werden der Antragstellerin beziehungsweise dem Antragsteller vor einer förmlichen Ablehnung des Zulassungsantrags die Gründe schriftlich mitgeteilt und ihr beziehungsweise ihm Gelegenheit gegeben, innerhalb einer angemessenen Frist die noch bestehenden Defizite durch Nachbesserungen zu beheben. Kann die Erfüllungslücke im Rahmen einer Nachprüfung nicht endgültig geschlossen werden, ergeht ein Ablehnungsbescheid, aus dem die Gründe der Ablehnung hervorgehen.

Die Gültigkeit der Zulassungen nach Absatz 1 ist an die vorgelegte Version der Anwendung gekoppelt und längstens auf fünf Jahre zu befristen. Die Zulassung kann mit weiteren Nebenbestimmungen versehen werden, insbesondere mit Auflagen, mit denen die Einhaltung von in dieser Verordnung konkretisierten technischen Anforderungen sichergestellt wird. Die Gültigkeit der Zulassung erlischt bei einer wesentlichen Änderung der zugelassenen Anwendung. Die Wesentlichkeit einer Änderung ist insbesondere dann anzunehmen, wenn die Erfüllung der Anforderungen dieser Vorschrift berührt wird. Die Zulassung kann für den Fall eines Verstoßes gegen Nebenbestimmungen des Zulassungsbescheides mit einem Widerrufsvorbehalt versehen werden.

2.9
Änderungen des Produktes

Die Antragstellerin beziehungsweise der Antragsteller ist verpflichtet, die Zulassungsstelle über vorgesehene Produktänderungen zu informieren. Anhand dieser Information prüft die Zulassungsstelle, ob die Voraussetzungen für die Zulassung weiterhin vorliegen. Die Zulassungsstelle entscheidet nach Bewertung der angezeigten Produktänderungen, ob es sich um eine wesentliche Änderung handelt und inwieweit eine erneute Zulassungsprüfung oder eine Teilprüfung erforderlich ist. Die Entscheidung wird auf der Internetseite der Gemeindeprüfungsanstalt veröffentlicht.

2.10
Gebühren

Für die Prüfung und Zulassung von Anwendungen zur Durchführung von digitalen und hybriden Gremiensitzungen, für die ihr durch § 11 Absatz 1 DigiSiVO in Verbindung mit § 133 Absatz 4 Satz 3 GO NRW die Zuständigkeit übertragen worden ist, erhebt die Gemeindeprüfungsanstalt Gebühren auf der Grundlage von § 10 Absatz 1 in Verbindung mit § 2a Absatz 4 des Gemeindeprüfungsanstaltsgesetzes vom 30. April 2002 (GV. NRW. S. 160), das zuletzt durch Artikel 6 des Gesetzes vom 13. April 2022 (GV. NRW. S. 490) geändert worden ist.

3
Technische Anforderungen an Anwendungen für die Nutzung in kommunalen Gremiensitzungen im Land Nordrhein-Westfalen

3.1
Allgemeine technische Anforderungen an die IT – Sicherheit

3.1.1
Das individuelle Rechte- und Rollenkonzept der Anwendung ermöglicht die Beschränkung des allgemeinen Zugangs zur Anwendung über eine Nutzerauthentifizierung mittels Benutzernamen und komplexem Passwort.

3.1.2
Die Anwendung stellt sicher, dass Stamm- und Bewegungsdaten, die in der Anwendung verarbeitet werden, vor unberechtigtem Zugriff geschützt sind. PINS, Passwörter und sonstige Autorisierungsdaten müssen dabei verschlüsselt hinterlegt werden.

3.1.3

Das individuelle Rechte- und Rollenkonzept der Anwendung schließt die Zugriffe auf Daten in der Anwendung ein.

3.1.4
Die Anwendung unterstützt die Einstellung differenzierter Zugriffsrestriktionen für die systematische Auswertung der im Rahmen der Datenprotokollierung anfallenden Informationen und verhindert deren nachträgliche Veränderung. Hierbei unterstützt das Programm die zeitraumbezogene Löschung historisierter beziehungsweise protokollierter Informationen.

3.1.5
Metadaten, die im Rahmen der Nutzung der Anwendung gesammelt werden, müssen verschlüsselt gespeichert oder mit vergleichbaren Sicherheitsmaßnahmen geschützt werden können.

3.1.6
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst unter anderem die Einstellung differenzierter Zugriffsrestriktionen für die oben genannten Metadaten.

3.1.7
Die Anwendung ermöglicht die individuelle Festlegung von Dateiablageorten.

3.1.8
Die Anwendung ermöglicht das Einrichten, Ändern und Entfernen von Benutzerkennungen und Berechtigungen. Dies darf über eine administrative Rolle durchführbar sein.

3.1.9
Die Anwendung ermöglicht die Übertragung der Daten über vertrauenswürdige Strecken; ist dies nicht möglich, erfolgt eine geeignete Verschlüsselung der Daten.

3.1.10
Bei einer webbasierten Anwendung muss das HTTPS-Protokoll verwendet werden.

3.1.11
Die Anwendung ermöglicht die Anzeige aller teilnehmenden Personen.

3.1.12
Für die Anwendung existiert ein dokumentiertes Verfahren zur Behebung von Anwendungs- und Dokumentationsfehlern unter Zugriff auf die Supportwege des Anwendungsentwicklers inklusive definierter Eskalationsoptionen im Fall des Misserfolgs. Die der Anwenderin beziehungsweise dem Anwender zur Verfügung gestellten Kommunikationswege sind dokumentiert.

3.1.13
Die Anwendung arbeitet in einer vom Hersteller empfohlenen Umgebung stabil, sodass eine anwenderübliche Nutzung gewährleistet ist. Die Funktionalitäten der Anwendung sind dokumentiert. Programmbedingte Fehlersituationen sind anwendergerecht dokumentiert.

3.1.14
Die Anwendung ermöglicht die Erstellung und Nutzung von Datensicherungen.

3.1.15
Die Anwendung unterstützt Möglichkeiten, mit angemessenem Aufwand die Daten wiederherzustellen, die durch Programmfehler, Systemabstürze, Stromausfälle und sonstige Ereignisse be-

schädigt werden. Anwenderinnen und Anwender werden durch die Dokumentation über das Verhalten bei Systemabstürzen und Fehlern informiert.

3.1.16
Das Frontend und die dargestellten Inhalte müssen über eine konsistent genutzte Sprache verfügen. Der Support für die Technologie der Benutzeroberfläche muss in Deutsch stattfinden.

3.1.17
Die Anwendung ermöglicht die Umsetzung eines individuellen Rechte- und Rollenkonzeptes, das den unterschiedlichen Berechtigungen der Mitwirkenden an kommunalen Gremiensitzungen flexibel Rechnung trägt.

3.1.18
Die Anwendung ermöglicht die Verschlüsselung von Daten auf einem Sicherheitsniveau, das demjenigen der Empfehlungen der technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" (BSI TR-02102) in der jeweils zum Zeitpunkt der Antragstellung gültigen Fassung entspricht.

3.1.19
Die Anwendung ermöglicht, Kommunikationsdateien während einer Sitzung durch eine Ende-zu-Ende-Verschlüsselung gegen unberechtigte Zugriffe zu schützen.

3.1.20
Die Anwendung ermöglicht eine revisionssichere Aufzeichnung der Tätigkeiten aller Anwendungsadministratoren.

3.1.21
Die Anwendung ermöglicht eine Trennung der Übertragung (Streaming) vom internen System, über das die digitale Sitzung durchgeführt wird.

3.1.22
Die Anwendung ermöglicht im Fall von öffentlich bekannten, kritischen Schwachstellen ein Anwendungsupdate innerhalb eines vorgeschriebenen Zeitraums.

3.1.23
Die Anwendung ermöglicht Schnittstellen für Monitoring-Lösungen am Markt. Dies umfasst unter anderem die Stabilitätsermittlung des Systems, das Diagnostizieren von Mängeln oder Ursachen sowie die Erkennung eines Verbesserungspotentials.

3.1.24
Die Anwendung ermöglicht eine Speicherung durch Zeitstempel bei jeder Änderung an Datensätzen oder Dokumenten.

3.1.25
Die Anwendung ermöglicht Daten in gängige Formate, zum Beispiel .pdf, .csv, .jpg, .png, .txt, zu exportieren, soweit dies nach Art und Umfang der Nutzung erforderlich ist.

3.1.27
Die Anwendung ermöglicht eine Unterstützung bei dem Versand von Einladungen mit den Zugangs- und Einwahldaten direkt oder über eine Schnittstelle, zum Beispiel zu einem E-Mail-Programm.

3.1.28
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst das Blockieren von Teilnehmerinnen und Teilnehmern vom Wiedereintritt sowie die Aufhebung einer solchen Blockierung durch autorisierte Rollen.

3.1.29
Die Anwendung ermöglicht das automatische Erstellen eines Anwesenheitsprotokolls beziehungsweise einer Anwesenheitsliste über alle Eintritte in die sowie Austritte aus der durchgeführten Sitzung unter Aufnahme ihrer jeweiligen Zeitpunkte.

3.2
Allgemeine technische Anforderungen an den Datenschutz

3.2.1
Die Anwendung verhindert eine Auswertung der bei der Nutzung protokollierten Daten durch Profiling-Systeme auf Benutzerebene.

3.2.2
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst notwendige Konfigurationseinstellungen, wie zum Beispiel 'kann aktiviert beziehungsweise deaktiviert werden', zur Aufzeichnung der digitalen Sitzung (Ton und beziehungsweise oder Bild).

3.2.3
Die Anwendung unterstützt eine Archivierung von Metadaten.

3.2.4
Die Anwendung unterstützt den Export von zum Beispiel Konfigurationen, Metadaten, Textnachrichten und Dokumenten.

3.3. Systemspezifische technische Anforderungen an Videokonferenzanwendungen

3.3.1 Systemspezifische technische Anforderungen an die IT-Sicherheit der Videokonferenzanwendung

3.3.1.1
Die Anwendung ermöglicht das Signalisieren des Eintritts neuer, berechtigter Personen zur laufenden Sitzung (barrierearm).

3.3.1.2
Die Anwendung muss darstellen, welche Videokameras oder Mikrofone aktiviert beziehungsweise deaktiviert sind.

3.3.1.3
Die Anwendung ermöglicht mit Hilfe von Standardprogrammen, gängige Dokumententypen zu öffnen und zu importieren beziehungsweise exportieren, zum Beispiel Präsentationen. Die Dokumente sind durch Drittanbieteranwendungen zu öffnen, zum Beispiel Outlook, Word, PDF-Viewer. Die Ausführung von Makros muss dabei deaktiviert oder deaktivierbar sein.

3.3.1.4
Das individuelle Rechts- und Rollenkonzept der Anwendung umfasst den Start und das Beenden eines Live-Streams.

3.3.1.5
Die Anwendung ermöglicht eine barrierearme Bild- und Tonaktivität. Dabei muss die zusätzliche Konfigurierung eines akustischen Signals möglich sein.

3.3.2 Systemspezifische technische Anforderungen an den Datenschutz der Videokonferenzanwendung

3.3.2.1
Die Anwendung unterstützt die Darstellung sitzungsrelevanter Hinweise im Rahmen der Gewährung des Zugangs zu einer Sitzung.

3.3.2.2
Das individuelle Rechte- und Rollenkonzept umfasst, dass ohne die Zustimmung der jeweiligen Sitzungsteilnehmerin beziehungsweise des Sitzungsteilnehmers die Sitzungsleitung deren beziehungsweise dessen Mikrofon und Kamera nicht aktivieren darf.

3.3.2.3
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst das Löschen von Unterhaltungen nach Beendigung der Sitzung. Bei privaten Chats ermöglicht die Anwendung kein Einsehen und keine Protokollierung durch unbeteiligte Dritte.

3.3.2.4
Funktionen zum Teilen von Bildschirminhalten müssen eine zuverlässige Auswahl der zu teilenden Inhalte, zum Beispiel gesamter Desktop oder nur bestimmte Fenster, Programme oder Dateien, ermöglichen.

3.3.2.5
Die Anwendung ermöglicht eine standardmäßige Deaktivierung bestehender Aufzeichnungsfunktionen (Ton und beziehungsweise oder Bild).

3.3.2.6
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst eine Aktivierung der Ton- und beziehungsweise oder Bildaufzeichnung der virtuellen Sitzung (nach erfolgter Einwilligung der betroffenen Personen) ausschließlich durch die Sitzungsleitung oder die Sitzungsassistenz.

3.3.2.7
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst unter anderem die Möglichkeit, dass Teilnehmerinnen und Teilnehmer während ihrer Kameraübertragung ihren Hintergrund durch das Ausgrauen oder Verwischen oder durch das Einblenden eines standardisierten Hintergrundbildes unkenntlich machen.

3.3.3
Systemspezifische funktionale Anforderungen an die Videokonferenzanwendung

3.3.3.1
Die Anwendung ermöglicht zur Durchführung von Sitzungen eine Bildübertragung. Dies muss über verbaute Kameras in Geräten und beziehungsweise oder extern angeschlossene Kameras sichergestellt sein.

3.3.3.2

Die Anwendung ermöglicht zur Durchführung von Sitzungen eine Tonübertragung. Dies muss über verbaute Mikrofone in Geräten und beziehungsweise oder extern angeschlossene Mikrofone sichergestellt sein.

3.3.3.3
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet unter anderem die eigenständige Aktivierung beziehungsweise Deaktivierung der Tonübertragung während einer Sitzung.

3.3.3.4

Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet unter anderem die eigenständige Aktivierung beziehungsweise Deaktivierung der Bildübertragung während einer Sitzung.

3.3.3.5
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet die Möglichkeit der Stummschaltung und Aufhebung der Stummschaltung einzelner, mehrerer oder aller Teilnehmerinnen und Teilnehmer, Gremienmitglieder oder berechtigter Personen während einer Sitzung durch eine berechtigte Rolle.

3.3.3.6
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet die Möglichkeit, berechtigte Teilnehmerinnen und Teilnehmer mit Rechten einer Moderatorin beziehungsweise eines Moderators auszustatten, um unter anderem einzelne Fenster beziehungsweise den gesamten Desktop für eine Bildschirmübertragung freizugeben und zu übertragen.

3.3.3.7

Das individuelle Rechte- und Rollenkonzept beinhaltet die Möglichkeit, Rechte von Teilnehmerinnen und Teilnehmern auf eine rein zuhörende und zuschauende Rolle zu beschränken. Dies muss auch während der laufenden Sitzung erfolgen können.

3.3.3.8
Die Anwendung ermöglicht berechtigten Teilnehmenden die Ankündigung einer Wortmeldung.

3.3.3.9
Die Anwendung ermöglicht, dass die oben genannten Wortmeldungen für alle Teilnehmenden erkennbar sind.

3.3.3.10
Die Anwendung fokussiert die jeweils sprechende Sitzungsteilnehmerin beziehungsweise den Sitzungsteilnehmer. Das Bild und der Ton der aktiven Sitzungsteilnehmerin beziehungsweise des Sitzungsteilnehmers sind für alle Teilnehmenden sichtbar.

3.3.3.11
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet die Möglichkeit einer ausschließlichen Zulassung zur Live-Stream-Verfolgung.

3.3.3.12
Die Anwendung ermöglicht das Erstellen von virtuellen Sitzungen im Vorfeld der eigentlichen Durchführung.

3.3.3.13
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst den Start der Sitzung mit der Einwahl der Sitzungsleitung.

3.3.3.14
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst den Rollenwechsel der Sitzungsleitung (im Sinne einer Übergabe) während der Sitzung manuell sowie auf Grundlage voreingestellter Stellvertretungsfunktionen.

3.3.3.15
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst die Möglichkeit der Entfernung von Teilnehmerinnen und Teilnehmern.

3.3.3.16
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst das Beenden einer Sitzung und eventuellen Aufzeichnung sowie die Entfernung aller Anwendungsteilnehmerinnen und Anwendungsteilnehmer aus der Sitzung.

3.3.3.17
Die Anwendung ermöglicht den Export von Dateien in externe definierte Dateiablagen.

3.3.3.18
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst die Erstellung von Zugangs- und Einwahldaten.

3.3.3.19
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst die Möglichkeit, die laufende Sitzung verlassen zu können. Dabei muss die Person automatisch aus allen aktiv genutzten Anwendungen der jeweiligen Sitzung entfernt werden.

3.3.3.20
Das individuelle Rechte- und Rollenkonzept der Anwendung ermöglicht das Verbleiben in einem Warteraum bis zur manuellen Zulassung zur Sitzung.

3.3.3.21
Die Anwendung ermöglicht, dass Anwendungsaufzeichnungen in einem gängigen Format gespeichert werden.

3.3.3.22
Die Anwendung ermöglicht es, Sitzungen als Live-Stream zu übertragen.

3.3.3.23
Die Anwendung ermöglicht die Umsetzung eines individuellen Rechte- und Rollenkonzeptes. Dies beinhaltet unter anderem das Anzeigen von Namen und Rollen aller an der Sitzung teilnehmenden Personen.

3.3.3.24
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst unter anderem das Pausieren und Unterbrechen einer laufenden Sitzung.

3.3.3.25
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet unter anderem das ad-hoc Erstellen nicht-öffentlicher Sitzungsräume für Beratungen, für die jeweils Rollen als Sitzungsleitung definiert werden können.

3.3.3.26
Die Anwendung ermöglicht eine gleichzeitige Übertragung von Bildern aller Teilnehmenden, die ihre Videokameras aktiviert haben.

3.3.3.27
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet unter anderem das Fortsetzen pausierter oder unterbrochener Sitzungen.

3.3.3.28
Die Anwendung ermöglicht eine zusätzliche Einwahl per Telefon.

3.4
Systemspezifische technische Anforderungen an Abstimmungsanwendungen

3.4.1
Systemspezifische technische Anforderungen an die IT-Sicherheit der Abstimmungsanwendung

3.4.1.1
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst unter anderem eine Authentifizierung und Autorisierung berechtigter Gremienmitglieder vor der Abstimmung beziehungsweise Wahl, zum Beispiel durch eine Multi-Faktor-Authentifizierung.

3.4.1.2
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet, dass der Zugang zur Anwendung über eine Nutzerauthentifizierung mittels einer Multi-Faktor-Authentifizierung zur eindeutigen Authentifizierung erfolgt.

3.4.2
Systemspezifische funktionale Anforderungen an die Abstimmungsanwendung

3.4.2.1
Das individuelle Rechte- und Rollenkonzept der Anwendung umfasst die Erstellung und Durchführung von namentlicher, offener oder geheimer Abstimmung beziehungsweise Wahl.

3.4.2.2
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet die Erstellung von Einladungen mit Zugangsdaten für eine Abstimmung beziehungsweise Wahl.

3.4.2.3
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet die Erstellung einer Abstimmung beziehungsweise Wahl nach den einschlägigen Kriterien der GO NRW.

3.4.2.4
Das individuelle Rechte- und Rollenkonzept der Anwendung beinhaltet den Start einer namentlichen, offenen oder geheimen Abstimmung beziehungsweise Wahl.

3.4.2.5
Die Anwendung ermöglicht die Ergänzung von Wahlvorschlägen während der Sitzung unmittelbar vor Wahlbeginn.

3.4.2.6
Die Anwendung ermöglicht eine Abstimmung mit namentlicher Stimmzählung.

3.4.2.7
Die Anwendung ermöglicht eine Abstimmung beziehungsweise Wahl mit einfacher Zählung der Ja-, Nein- und Enthaltungsstimmen. Bei mehreren Wahlalternativen müssen Nein-Stimmen auszuschließen sein.

3.4.2.8
Die Anwendung muss die Durchführung einer geheimen Abstimmung beziehungsweise Wahl mit geheimer Stimmzählung ermöglichen.

3.4.2.9
Die Anwendung ermöglicht eine automatisierte Auswertung der abgegebenen Stimmen nach Beendigung des Vorgangs. Bei der offenen Abstimmung beziehungsweise Wahl muss dabei erkennbar sein, wer wie abgestimmt hat. Bei der namentlichen Abstimmung beziehungsweise Wahl muss ein entsprechendes Protokoll unterstützt werden.

3.4.2.10
Die Anwendung ermöglicht die Definition eines Zeitfensters zur Durchführung einer Abstimmung beziehungsweise Wahl.

3.4.2.11
Die Anwendung ermöglicht bei einer offenen oder namentlichen Abstimmung das Anzeigen der Namen im Abstimmungsergebnis.

3.4.2.12
Die Anwendung ermöglicht die rechtlich zulässige Nachvollziehbarkeit aller Schritte von Wahlhandlungen zu Prüfzwecken gemäß Artikel 38 in Verbindung mit Artikel 20 Absatz 1 und Absatz 2 des Grundgesetzes. Dieser gebietet, dass alle wesentlichen Schritte der Wahl (Integrität der Stimmabgabe und der Stimmauszählung) öffentlicher Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen. Dies genügt nur dann den verfassungsrechtlichen Anforderungen, wenn die Anwendung die Überprüfung wesentlicher Schritte von Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnis ermöglicht.

3.4.2.13
Die Anwendung schließt zuverlässig aus, dass bei geheimen Abstimmungen durch zusätzliche erfasste Merkmale der Abstimmenden, zum Beispiel die Fraktionszugehörigkeit, Rückschlüsse auf das Stimmverhalten während geheimer Abstimmungen möglich werden.

3.4.2.14
Die Anwendung ermöglicht je nach Abstimmung beziehungsweise Wahl die Konfiguration der abzugebenden Stimmen. Es muss sichergestellt sein, dass nur die Anzahl der jeweils möglichen Stimmen, je Gremienmitglied und insgesamt, verarbeitet wird.

3.4.2.15
Das individuelle Rechte- und Rollenkonzept ermöglicht abstimmungsbezogene Änderungen der Stimmberechtigten in einer Sitzung.

3.4.2.16
Die Anwendung ermöglicht eine Kenntlichmachung von offenen, namentlichen und geheimen Abstimmungen.

3.4.2.17
Die Anwendung ermöglicht die Umsetzung eines individuellen Rechte- und Rollenkonzeptes. Dies beinhaltet unter anderem einen Wechsel von offenen oder namentlichen Abstimmungen zu geheimen Abstimmungen.

3.4.2.18
Die Anwendung ermöglicht, offene und namentliche Abstimmungs- oder Wahlergebnisse nach Fraktionszugehörigkeit anzuzeigen.

3.5
Besondere Anforderungen für Software-as-a-Service-Lösungen

3.5.1
In dem Fall von fremdgehosteten Diensten hat der Anbieter eine Dokumentationspflicht gegenüber dem Betreiber. Dies umfasst eine Beschreibung an welchen Lokationen Daten gespeichert und verarbeitet werden.

3.5.2
Die Anwendung ermöglicht eine Deaktivierung oder Deinstallation nicht benötigter sicherheitskritischer Dienste und Funktionen.

3.5.3
In einer vom Anbieter vorgegebenen oder empfohlenen Systemumgebung dürfen die durchschnittlichen Antwortzeiten nicht zu einer dauerhaften Latenzzeit bei Bild- und Tonübertragung führen, die mehr als 120 Millisekunden beträgt.

3.5.4
Der Anbieter und beziehungsweise oder der Anwendungshersteller verpflichten sich, in vertraglich definierten regelmäßigen Abständen sowie anlassbezogen bei Auftreten von Sicherheitsschwierigkeiten Sicherheitsupdates für die Anwendung bereitzustellen.

3.5.5
Der Anbieter und beziehungsweise oder der Anwendungshersteller verpflichten sich, unverzüglich über bekannt gewordene Schwachstellen zu informieren und mögliche Umgehungswege an den Betreiber zu übermitteln.

3.5.6
Der Anbieter stellt eine Bedienungsanleitung für Betreiber und Anwender in deutscher Sprache zur Verfügung, zum Beispiel in Form einer Programmdokumentation für Administratoren und ein Benutzerhandbuch für Betreiber. Dies muss kommunalindividuell anpassbar sein.

3.5.7
Bei einer Software-as-a-Service-Lösung muss sichergestellt sein, dass sich der Serverstandort des Anbieters innerhalb der Europäischen Union befindet. Hierzu muss der Anbieter eine Aussa-

ge darüber treffen, wo die Daten verarbeitet werden, und sich verpflichten, Änderungen unaufgefordert und umgehend mitzuteilen.

3.5.8
Der Anbieter stellt technisch sicher, dass von ihm Beauftragte und beziehungsweise oder sonstige Dritte keinen Zugriff auf die verarbeiteten Daten erhalten, auch nicht auf einzelne Teile wie Nutzungsdaten. Hierzu muss der Anbieter eine Aussage darüber treffen, wo die Daten verarbeitet werden.

4
Inkrafttreten, Außerkrafttreten

Dieser Runderlass tritt am Tag nach der Veröffentlichung in Kraft und am 1. Juni 2027 außer Kraft.

- MBl. NRW. 2022 S. 564