

GOB Legal Rechtsanwaltsgesellschaft mbH
Balzacstraße 3 · 04105 Leipzig

Intevation GmbH
Neuer Graben 17

49074 Osnabrück

GOB Legal Rechtsanwaltsgesellschaft mbH
Balzacstraße 3
D-04105 Leipzig

Tel. +49 341 64953-12
Fax +49 341 64953-22
E-Mail w.tetzel@gob-legal.de

Aktenzeichen: 000038-2021

Datum: 25.03.2021

Gutachten

Betrieb von OpenSlides 3 für Veranstaltungen mit geheimen Abstimmungen und Wahlen

Im Auftrag der Intevation GmbH haben wir die in der **Anlage 1** beigefügte Dokumentation für den Betrieb von OpenSlides 3 durch die Intevation GmbH geprüft.

Ich bestätige, dass OpenSlides 3 auf Basis der beiliegenden Dokumentation für Veranstaltungen mit geheimen Abstimmungen und Wahlen rechtswirksam eingesetzt werden kann.

Insbesondere erfüllt die Software im Betrieb folgende Anforderungen:


1. Nur stimmberechtigte Personen können Stimmen abgeben.
2. Personen können nicht unberechtigt mehrfach abstimmen.
3. Die Stimmen werden nur anonymisiert gespeichert. Die Stimmabgaben werden durch das Hosting nicht protokolliert. Insbesondere sind Server-Logs (für IP-Adressen u. a.) deaktiviert.

Unsere Bestätigung steht unter den folgenden Vorbehalten:

1. OpenSlides 3 enthält keine bekannten Programmierfehler und das Hosting wird ordnungsgemäß konfiguriert. Es gibt keine bisher nicht bekannten Sicherheitslücken.

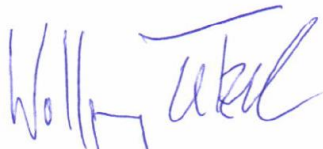
Saalesparkasse
IBAN: DE 238 005 376 218 940 095 99
BIC: NOLADE21HAL

Geschäftsführer:
Rechtsanwalt Wolfgang Tetzel, Leipzig
StB Dipl.-Betriebsw. (FH) Antje Bissinger, Aschersleben


Sitz der Gesellschaft: Leipzig
AG Leipzig, HRB 34676
St.-Nr. 231/109/12706

2. Die für das Hosting verantwortlichen Mitarbeitenden betreiben OpenSlides 3 bestimmungsgemäß und ohne Manipulationen am Programm selbst oder an Komponenten des Hostings. Sie nehmen nur in der Dokumentation vorgesehene Zugriffe und Protokollierungen vor.
3. Die für die jeweilige Veranstaltung gültigen Rechtsvorschriften, insbesondere die Satzungen oder Gesellschaftsverträge der Organisationen gestatten die Durchführung geheimer elektronischer Abstimmungen und Wahlen nach dem Stand der Technik. Hierbei muss der Betrieb des Wahlsystems durch einen externen Dienstleister zulässig sein. Erforderlich ist ein Dienstleistungsvertrag mit qualifizierter Verschwiegenheitsklausel.

Für die Einzelheiten verweisen wir auf den in **Anlage 2** beiliegenden Bericht, der untrennbarer Bestandteil unserer obigen Bestätigung ist.



Wolfgang Tetzl
Rechtsanwalt

Anlage 1: Dokumentation für den Betrieb von OpenSlides 3 durch die Intevation GmbH

1. Allgemeines

OpenSlides ist ein digitales Antrags- und Veranstaltungssystem, das zur Begleitung von Präsenz-, Hybrid- und Onlineveranstaltungen eingesetzt wird. In OpenSlides können u. a. Tagesordnung, Anträge und Wahlen von Veranstaltungen verwaltet werden. OpenSlides unterstützt insbesondere den Willensbildungsprozess der stimmberechtigten Teilnehmenden durch das Antrags- und Wahlsystem sowie durch digitale Abstimmungen und Wahlen.

OpenSlides ist eine webbasierte Server-Client-Anwendung. Jeder Benutzer ruft mit einem Webbrowser eine für jede OpenSlides-Instanz individuelle URL auf. Der Server übersendet den Programmcode für die Clientanwendung, die im Webbrowser des Benutzers ausgeführt wird (HTML, CSS, JavaScript). Clientanwendung und Server stehen danach im ständigen Datenaustausch, bis der Benutzer das Browserfenster schließt oder in diesem Fenster eine andere Webseite auswählt. Je nach Einstellung des Browsers können Webseiten-Daten auch nach dem Schließen des Browserfensters auf dem Gerät des Benutzers gespeichert bleiben. Der Übertragungsweg zwischen Client und Server ist TLS-verschlüsselt.

Gegenstand der folgenden Dokumentation ist OpenSlides in der Version 3 (aktuelle Betriebsversion) und die Anwendung nicht-namentlicher Abstimmungen und Wahlen.

Kunde im Sinne der folgenden Dokumentation ist die Organisation, die die Intevation GmbH mit dem Hosting einer OpenSlides-Instanz beauftragt. Die Intevation GmbH ist dabei gegenüber dem Kunden vertraglich verpflichtet, die Software und das Hosting nach der folgenden Dokumentation zu betreiben.

2. Hosting

OpenSlides wird von der Intevation GmbH auf mehreren dedizierten Servern in einem Cluster betrieben. Diese Server befinden sich in Deutschland. Konkret werden die Server in Rechenzentren der Hetzner Online GmbH und der Hostway Deutschland GmbH betrieben, die nach ISO/IEC 27001 zertifiziert sind. Die Betreiber der Rechenzentren sind gegenüber der Intevation GmbH vertraglich verpflichtet, dass das Informationssicherheitsmanagementsystem die Anforderungen der Zertifizierung erfüllt.

Die auf den dedizierten Servern eingesetzte Software wird ausschließlich von Mitarbeitenden der Intevation GmbH administriert und entspricht den aktuellen Sicherheitsanforderungen. Insbesondere erfolgt der Zugang zu den Servern ausschließlich von sicherheitsgepflegten Endgeräten über SSH-Schlüssel mit einer Schlüssellänge gemäß der jeweils aktuellen technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik.

Jede OpenSlides-Instanz einschließlich der von dieser Instanz verwendeten Datenbanken ist über ein eigenes virtualisiertes Netzwerk von anderen Instanzen getrennt.

Es existieren zusätzliche Standby-Systeme und Backups, die im Falle eines Ausfalls des Systems die zeitnahe Fortsetzung des Betriebs gewährleisten.

3. Mitarbeitende

Die Mitarbeitenden der Intevation GmbH, welche administrativen Zugriff auf die Server und/oder die OpenSlides-Instanzen haben, sind durch die Intevation GmbH arbeits- oder dienstvertraglich verpflichtet, die Server und die Software bestimmungsgemäß und nach den jeweils aktuellen Sicherheitsanforderungen zu betreiben. Alle Mitarbeitenden sind nach Qualifikation und Erfahrung sorgsam ausgewählt und werden in regelmäßigen Abständen über IT-Sicherheit geschult und durch die Geschäftsführung überwacht. Die Mitarbeiter sind darüber hinaus über die Folgen von vorsätzlichen oder fahrlässigen Pflichtverstößen belehrt, insbesondere darüber, dass unbefugte Eingriffe und Veränderungen von Daten zivil- und strafrechtlich verfolgt werden können.

4. Zugang zu OpenSlides, Teilnehmendenverwaltung

In OpenSlides verfügen alle Teilnehmenden (stimmberechtigte oder nicht stimmberechtigte Teilnehmende) über einen jeweils eigenen Benutzerzugang mit einem Benutzernamen und einem Passwort. Beim erstmaligen Anlegen einer OpenSlides-Instanz wird ein Konto für einen Administrator des Kunden erstellt. Die Zugangsdaten erzeugt die Intevation GmbH und stellt sie dem Kunden auf einem von ihm gewählten Übermittlungsweg zur Verfügung. Der Versand über verschlüsselte E-Mail, per Brief oder Telefon ist möglich. Der Versand per E-Mail erfolgt mindestens mit einer aktuell gebräuchlichen Transportverschlüsselung.

Die Benutzernamen und die initialen Passwörter der Teilnehmenden legt der Kunde selbst fest. Der Kunde kann dabei einstellen, ob die Teilnehmenden die Zugangsdaten aus OpenSlides heraus per E-Mail (mit aktuell gebräuchlicher Transportverschlüsselung) erhalten sollen oder ob der Kunde die Zustellung selbst organisiert (z. B. per Briefpost).

Jeder Teilnehmende hat jederzeit die Möglichkeit, das eigene Passwort selbst zu ändern. Für Teilnehmende, bei denen der Kunde die Berechtigungen so eingestellt hat, dass sie ihr Passwort nicht selbst ändern können (z. B. Konten für Gäste und Pressevertreter), ist eine nicht-namentliche elektronische Abstimmung oder Wahl nicht zulässig. Hierauf wird der Kunde in den FAQs hingewiesen.

Nach der Anmeldung wird im Browser des Benutzers ein Session-Cookie gespeichert. Der Session-Cookie ist gültig, bis der Benutzer das Browserfenster schließt oder sich abmeldet (Logout).

Der Kunde hat die Möglichkeit, die Teilnehmenden einzelnen Gruppen zuzuweisen und diesen Gruppen im System nach einem abgestuften Rollenkonzept Berechtigungen zuzuweisen. Insbesondere kann der Kunde einstellen, welche Teilnehmende bei einzelnen Abstimmungen oder Wahlen stimmberechtigt sind und welche nicht. Die Rechteverwaltung kann nur von Personen vorgenommen werden, denen vom Kunden die entsprechende Administrationsberechtigung eingeräumt wurde, was nur unmittelbar oder mittelbar mit Hilfe des o. g. Administratorzugangs möglich ist.

Der Kunde kann auch einstellen, dass nicht angemeldete Gast-Benutzer OpenSlides benutzen können. Solche Benutzer sind bei namentlichen oder nicht-namentlichen Abstimmungen und Wahlen stets nicht stimmberechtigt.

Mitarbeitende der Intevation GmbH erhalten in einer OpenSlides-Instanz nur dann einen zusätzlichen Administratorzugang, wenn der Kunde dem zustimmt.

5. Funktionsweise elektronischer Abstimmungen und Wahlen

Abstimmungen über Anträge und Wahlen von Personen werden in OpenSlides von einer entsprechend berechtigten Person angelegt. Dabei kann je nach Einstellung auch eine digitale Abstimmung bzw. einen digitalen Wahlgang angelegt werden. Beim Anlegen muss angegeben werden, welche Gruppen von Teilnehmenden bei der Abstimmung oder Wahl stimmberechtigt sind. Möglich ist dies nur für namentlich bekannte Teilnehmende und nicht für anonyme Gast-Benutzer.

Eine Person mit entsprechender Berechtigung kann eine digitale Abstimmung bzw. Wahl starten. Sodann informiert der Server alle im Webbrowser angemeldeten Benutzer über den Beginn der Abstimmung bzw. Wahl und fordert die Benutzer zur Stimmabgabe auf, wenn es sich um stimmberechtigte Teilnehmende handelt.

Die Oberfläche zeigt dem Benutzer die einzelnen Entscheidungsoptionen an (z. B. Ja, Nein oder Enthaltung oder die Namen der Kandidaten im Wahlgang). Der Benutzer kann unter diesen Optionen auswählen und seine Stimme eingeben. Ein abschließender Bestätigungsdialog ermöglicht dem Benutzer, falsche Eingaben zu korrigieren. Danach sendet der Benutzer die Stimme ab. In technischer Hinsicht wird eine Mitteilung (Request) an den Server übersandt. Die Mitteilung enthält die konkrete Stimmabgabe und den Session-Cookie. Die Stimmabgabe wird auf dem Endgerät des Benutzers nicht gespeichert.

Der Server nimmt die Mitteilung entgegen, protokolliert jedoch die eingehende Mitteilung nicht. Es werden an dieser Stelle weder die IP-Adresse, noch der Session-Cookie, noch der Inhalt der Mitteilung mit den Informationen zur Stimmabgabe gespeichert.

OpenSlides ermittelt nun mit Hilfe des Session-Cookie den jeweiligen Teilnehmenden und verarbeitet die Stimme wie folgt weiter:

OpenSlides unterscheidet zwischen namentlichen und nicht-namentlichen digitalen Abstimmungen und Wahlen.

Bei **namentlichen Abstimmungen und Wahlen** wird die Stimmabgabe des Teilnehmenden unter Beibehaltung der Verknüpfung von Stimme und Benutzerkonto in der Datenbank gespeichert. Zuvor wird geprüft, dass der Teilnehmende nicht bereits abgestimmt bzw. gewählt hat. Nach Ende der Abstimmung bzw. Wahl kann sowohl die Zusammenfassung des Gesamtergebnisses als auch die Liste aller einzelnen Stimmen abgerufen werden. An Hand dieser Zusammenfassung kann nachvollzogen werden, dass nur stimmberechtigte Personen an der Abstimmung bzw. Wahl teilgenommen und Stimmen abgegeben haben.

Bei **nicht-namentlichen Abstimmungen und Wahlen** wird für jeden Teilnehmenden geprüft, ob dieser bereits abgestimmt bzw. gewählt hat. Ist dies nicht der Fall, wird die Stimme des Teilnehmenden in der Datenbank gespeichert. Zu dieser Stimme wird jedoch keine Zuordnung zum Teilnehmenden mitgespeichert. Die entsprechenden Datenbankfelder werden mit einem Null-Wert beschrieben. Stattdessen wird der Stimmabgabe ein zufällig generierter Token zugeordnet. In einer separaten Datenbank-Tabelle wird hinterlegt, dass der Teilnehmende nun an der Abstimmung bzw. Wahl teilgenommen hat. Es ist über die Datenbank-Transaktionslogik sichergestellt, dass ein Teilnehmender nicht gleichzeitig mehrere Stimmabgaben vornehmen und so die Prüfung umgehen kann, ob er bereits abgestimmt hat. Die Antwort des Servers sowie die danach an die Clients verteilten Mitteilungen enthalten nur den Hinweis, dass ein Teilnehmender nun abgestimmt bzw. gewählt hat, nicht jedoch den Inhalt der Stimmabgabe. Auch der Teilnehmende erhält vom Server nicht den mit seiner Stimmabgabe verbundenen Token übermittelt. Nach Abschluss der Abstimmungsmitteilung werden alle nicht in der Datenbank abgelegten Informationen aus dem Arbeitsspeicher gelöscht. Nach Ende der Abstimmung bzw. Wahl kann die Zusammenfassung des Gesamtergebnisses abgerufen werden. Es kann auch die Liste aller einzelnen Stimmen abgerufen werden, wobei diese Liste jedoch keine Zuordnung der einzelnen Stimmen zu den Teilnehmenden enthält, sondern nur die Tokens, die jedoch den Abstimmenden nicht zugeordnet werden können. Dies entspricht im übertragenen Sinne der Gesamtheit der in der Wahlurne enthaltenen Stimmzettel. Es kann außerdem abgerufen werden, wer an der Abstimmung bzw. Wahl teilgenommen hat. Dadurch ist überprüfbar, dass nur stimmberechtigte Personen an der Abstimmung bzw. Wahl teilgenommen und Stimmen abgegeben haben. Während der laufenden Abstimmung bzw. Wahl kann die Liste indes nicht abgerufen werden.

Beim oben beschriebenen Betrieb ist ausgeschlossen, dass ein Benutzer in OpenSlides gleich mit welchen Rechten die einzelnen Stimmabgaben der Teilnehmenden verändert. Es ist weiter ausgeschlossen, dass er im Falle der nicht-namentlichen Stimmabgabe die einzelnen Stimmabgaben der Teilnehmenden einsehen oder sonst abrufen kann. Es ist weiter ausgeschlossen, dass der Teilnehmende aus dem System eine Quittung über den Inhalt seiner Stimmabgabe abrufen kann.

Ein Mitarbeitender der Intevation GmbH kann ebenfalls keine einzelnen Stimmabgaben verändern, einsehen oder abrufen. **Dies gilt nicht, wenn er entgegen der obigen Beschreibung das Hosting manipuliert, zusätzliche Protokollierungen konfiguriert oder einen manipulierten Programmcode von OpenSlides verwendet.**

6. Vorbehalt von Fehlern

Die obige Beschreibung steht unter dem Vorbehalt, dass keine bekannten Programm- oder Konfigurationsfehler oder bisher nicht bekannte Sicherheitslücken vorliegen. Die Intevation GmbH hat sich für den Fall des Bekanntwerdens solcher Fehler oder Lücken gegenüber dem Kunden verpflichtet, diese unverzüglich zu beheben.

Anlage 2: Bericht über die Prüfung des Betriebs von OpenSlides 3 für Veranstaltungen mit geheimen Abstimmungen und Wahlen

1. Allgemeine Anforderungen

Die Rechtsordnung kennt eine Vielzahl unterschiedlicher Organisationsformen und eine vielschichtige Ausgestaltung der Formen der Willensbildung ihrer Mitglieder und Organe.

Maßgeblich für die Frage, ob in einer Organisation elektronische Abstimmungen und Wahlen nach dem Stand der Technik möglich sind, sind die jeweils einschlägigen Rechtsvorschriften (Gesetze, Verordnungen, Satzungen, Gesellschaftsverträge etc.), die die Verfassung der jeweiligen Organisation bestimmen.

Soweit diese Vorschriften die Durchführung von geheimen elektronischen Abstimmungen Wahlen nach dem Stand der Technik zulassen, ohne jedoch hierzu nähere Regelungen zu treffen, muss das Wahlsystem mindestens folgende Anforderungen erfüllen (vgl. zu den Anforderungen etwa für Vereine als Grundform aller zivilrechtlichen Vereinigungen *Schindler/Schaffner*, in: Schindler/Schaffner, Virtuelle Beschlussfassung in Kapitalgesellschaften und Vereinen 1. Auflage 2021, § 4 Rn. 693 ff. m. w. N.; vgl. auch das vom *Bundesamt für Sicherheit in der Informationstechnik* herausgegebene Common Criteria Schutzprofil für Basissatz von Sicherheitsanforderungen an Online-Wahlprodukte, Version 1.0, 18. April 2008, BSI-CC-PP-0037-2008, dort Rn. 16):

- Das Wahlsystem muss dem Stimmberechtigten ermöglichen, seine Stimme ohne Kenntnisnahme durch einen anderen eingeben und die Eingabe vor einer endgültigen Bestätigung korrigieren zu können.
- Das Wahlsystem muss sicherstellen, dass nur stimmberechtigte Personen Stimmen abgeben können.
- Das Wahlsystem muss ausschließen, dass Stimmberechtigte unberechtigt mehrfach abstimmen.
- Das Wahlsystem muss die Stimmen anonymisiert speichern.
- Keine stimmberechtigte Person darf in der Lage sein, seine Stimmenscheidung zu beweisen. (Dabei bleiben Einwirkungsmöglichkeiten auf den Abstimmenden, die außerhalb des Wahlsystems liegen, wie Eingabeprotokolle oder Screenshots auf dem Endgerät des Abstimmenden, ein Abfilmen des Bildschirms etc. außer Betracht.)
- Während der Abstimmung oder Wahl darf kein Zwischenergebnis ermittelt werden.

Zusätzlich wird unsererseits für erforderlich gehalten, dass der Betrieb des Wahlsystems nicht durch die Organisation selbst erfolgt, sondern damit ein externer

Dienstleister beauftragt wird. Mit diesem muss u. a. eine vertragliche Vereinbarung bestehen, nach der der Dienstleister auch gegenüber den gesetzlichen Vertretern der Organisation dauerhaft berechtigt und verpflichtet ist, Stillschweigen über Tatsachen zu bewahren, die ihm ggf. über die einzelnen Stimmabgaben bekannt geworden sind (qualifizierte Verschwiegenheitsklausel). Es muss vertraglich ausgeschlossen sein, dass die Organisation den Dienstleister von dieser Verschwiegenheitsberechtigung und –verpflichtung entbindet. Ferner muss ausgeschlossen sein, dass der Dienstleister Weisungen mit Blick auf den Betrieb der Software und des Hostings unterliegt, nach denen er Zugriff auf die einzelnen Stimmabgaben erlangen könnte. Maßgeblich für diese zusätzliche Anforderung ist, dass bei einem Betrieb des Wahlsystems durch Organe der Organisation selbst (z. B. Hosting der Software durch den Vorstand eines Vereins bei Vorstandswahlen) die Vertraulichkeit und Integrität der Stimmabgaben und die Richtigkeit des Wahlergebnisses nicht sichergestellt sind.

Nicht erforderlich ist unseres Erachtens, dass das System das Verzeichnis der stimmberechtigten Teilnehmenden einerseits und die abgegebenen und anonymisierten Stimmen andererseits auf physisch getrennten Server speichert. Eine solche Anforderung bietet keinen zusätzlichen Schutz gegen die bestehenden Missbrauchsgefahren. Risiken hinsichtlich der Verfügbarkeit der Daten hingegen kann mit den in der Dokumentation genannten Standby- und Backup-Systemen begegnet werden.

Nicht erforderlich ist unseres Erachtens ferner, dass das System die Stimmen verschlüsselt speichert. Ausreichend ist, wenn die Stimmen vom Dienstleister in einer unter seiner alleinigen Kontrolle stehenden Umgebung gespeichert werden. Eine zusätzliche Verschlüsselung in der elektronischen Wahlurne bietet keinen beachtlichen zusätzlichen Vorteil, weil der Schlüssel zur Auswertung des Wahlergebnisses sich ebenfalls in der Hand des Dienstleisters befinden müsste.

Die oben genannten Anforderungen sind gesetzlich nicht geregelt, sondern ergeben sich aus einer Zusammenschau der Erfordernisse eines demokratischen Willensbildungsprozesses, dem ein gewisses Vertrauen in die Integrität der das Wahlsystem betreibenden Personen innewohnt.

Einschlägige Rechtsprechung zu diesem Anforderungskatalog gibt es derzeit nicht.

In der rechtswissenschaftlichen Literatur (wie beispielsweise oben zitiert) werden die Anforderungen nicht im Detail erörtert. In aktuellen Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (vgl. Ansätze zur Risikoabwägung bei digitalen geheimen Abstimmungen im Rahmen von Versammlungen, Virtuelle Versammlungen und Abstimmungen (ViVA), Version 0.5 als Aufruf zur Kommentierung, Stand 2.11.2020; Anforderungen an Produkte für virtuelle Versammlungen und Abstimmungen Virtuelle Versammlungen und Abstimmungen (ViVA), Version 0.5 als Aufruf zur Kommentierung, Stand 20.11.2020) werden in erster Linie Fragen zu möglichen Gestaltungen aufgeworfen. Konkrete Anforderungen sind dort nicht formuliert.

Es kann daher im Ergebnis nicht ausgeschlossen werden, dass Gerichte künftig noch weitergehende Anforderungen aufstellen. Gleichwohl spricht viel dafür, dass die oben

genannten Anforderungen für nicht-politischen Wahlen mit geringem Angriffspotential ausreichend sind.

Diese Anforderungen bleiben gleichwohl hinter den verfassungsrechtlichen Wahlgrundsätzen der allgemeinen, freien, gleichen, unmittelbaren, geheimen und öffentlichen Wahl zurück, welche direkt nur für politische Wahlen zu Volksvertretungen gelten (vgl. BVerfG, Urteil vom 3.3.2009 – 2 BvC 3, 4/07). Wesentlicher Unterschied ist, dass durch geheime elektronische Wahlen die Öffentlichkeit der Wahl nicht gewährleistet ist.

Die ausschließliche elektronische Stimmabgabe bietet – jedenfalls nach dem Stand der Technik – keine Möglichkeit, dass der Vorgang der Speicherung der Stimmabgabe und der Auszählung des Wahlergebnisses von außen nachvollzogen werden kann. Dieser Vorgang vollzieht sich auf einem oder mehreren Servern, die sich in der Verfügungsbefugnis des Dienstanbieters befinden. Ein offen gelegtes schlüssiges Konzept einer vollständigen geheimen und zugleich öffentlich nachvollziehbaren Stimmabgabe ist uns bisher nicht bekannt, auch nicht auf Basis der Blockchain-Technologie (a. A. Lukan, EuR 2019, 222, der jedoch kein solches Konzept beschreibt, sondern lediglich die Machbarkeit behauptet; vgl. Edge, Jake, *Cryptography and elections*, <https://lwn.net/Articles/810465/> (Abruf am 23.3.2021), der über eine Keynote speech der Professorin Vanessa Teague berichtet: Untersuchungen aktueller eVoting-Systeme habe gezeigt, dass keines der Systeme bisher insoweit einen vollständigen Schutz bietet).

2. Zulassung von geheimen elektronischen Abstimmungen und Wahlen durch die für die Organisation einschlägigen Rechtsvorschriften

Allerdings kann das für die jeweilige Organisation einschlägige Recht geheime elektronische Abstimmungen und Wahlen mit den oben genannten Einschränkungen zulassen. Beispielsweise ist für einen Verein eine einfache Satzungsermächtigung ausreichend (vgl. *Schindler/Schaffner*, a. a. O.; *Roßnagel, Gitter, Opitz-Talidou*: Telemedienwahlen in Vereinen MMR 2009, 383; vgl. auch *Noack*, NJW 2018, 1345; *D. U. Otto* in: *Herberger/Martinek/Rüßmann/Weth/Würdinger*, jurisPK-BGB, 9. Aufl., § 32 BGB (Stand: 22.10.2020) Rn. 18).

Hingegen bestimmt § 52 Abs. 4 S. 3 Nr. 3 BWG, dass eine mögliche Rechtsverordnung nach Satz 1 dieser Vorschrift elektronische Abstimmungen und Wahlen nur mit Ausnahme der Schlussabstimmung vorsehen kann. Daraus kann man entnehmen, dass der Gesetzgeber elektronische Wahlen für Parteien im Übrigen für unzulässig hält.

Es ist Sache der jeweiligen Organisation und nicht Gegenstand dieses Berichts, zu prüfen, ob die für die Organisation geltenden Rechtsvorschriften geheime elektronische Wahlen allgemein bzw. mit den oben genannten Kriterien zulassen.

3. Zusammenfassung

OpenSlides 3, wie es in der vorstehenden Dokumentation beschrieben ist, hält die oben genannten Anforderungen ein und kann daher für geheime elektronische Abstimmungen und Wahlen eingesetzt werden.

Dies gilt, soweit die Rechtsvorschriften der jeweiligen Organisation solche digitalen Willensbildungsprozesse zulassen. Dies kann insbesondere bei nicht-politischen Wahlen mit geringem Angriffspotential der Fall sein. Außerdem muss mit der Intevation GmbH als Dienstleisterin die oben genannte qualifizierte Verschwiegenheitsvereinbarung getroffen werden.

Wir weisen darauf hin, dass wir keine vollständige Prüfung des Quellcodes oder der Hosting-Konfiguration durchgeführt haben. Wir haben auch nicht die o. g. BSI-CC-PP-0037-2008 oder andere Zertifizierungsrichtlinien im Einzelnen geprüft. Es handelt sich bei unserer Prüfung nicht um eine Zertifizierung in diesem Sinne. Wir haben schließlich auch nicht geprüft, ob die in der in Anlage 1 genannten Dokumentation gemachten Angaben im tatsächlichen Betrieb zutreffen. Es ist Sache der jeweiligen Organisation, durch wirksame vertragliche Verpflichtung sicherzustellen, dass die Intevation GmbH die Angaben einhält.

An der Erstellung des Berichts hat außer dem Unterzeichner Herr Rechtsanwalt Norman Jäckel mitgewirkt.

Ende des Berichts