votesUP!

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

Zwischen

Tanzsportverband Nordrhein-Westfalen e.V.
Friedrich-Alfred-Allee 25 · 47055 Duisburg · E-Mail klaus.meng@tnw.de

– Verantwortliche:r (nachfolgend „**Auftraggeber:in**" genannt) –

und

Plattform „votesUP!", vertreten durch Tim Schrock
Postfach 18 01 03 · DE-10205 Berlin · E-Mail support@votesup.eu

– Auftragsverarbeiter:in (nachfolgend „**Auftragnehmer:in**" genannt) –
– zusammen „**Parteien**" genannt –

wird folgende Vereinbarung geschlossen:

1. Gegenstand und Dauer der Vereinbarung

1.1 Gegenstand des Auftrags ist die Datenverarbeitung im Rahmen des von der Auftragnehmer:in betriebenen Dienstes »votesUP! (votesup.eu)«. Die Vereinbarung bezieht sich dabei konkret auf die darüber durchgeführte Veranstaltung mit der Kennung »tnw-vt-2021«, eingerichtet am 07.05.2021.

1.2 Der Vertrag wird auf unbestimmte Zeit geschlossen.

1.3 Er endet durch

- die von dem/der Auftraggeber:in veranlassten manuellen Löschung der Veranstaltung; oder
- die automatische Löschung der Veranstaltung und ihrer Inhalte nach 90 Tagen Inaktivität; oder
- eine Kündigung durch eine der Parteien mit einer Frist von einer Woche; in diesem Fall besteht zum Ende eine unverzügliche Löschpflicht aller verarbeiteten Daten durch die Auftragnehmer:in.

2. Art, Umfang und Zweck der Datenverarbeitung

2.1 Zweck der Datenverarbeitung
Der/die Auftraggeber:in nutzt die Plattform votesup.eu, um bei der Veranstaltung mit dem Titel »65. TNW-Verbandstag« und unter 1. genannter Kennung

- anlassbezogen offene oder geheime Abstimmungen durchzuführen

In diesem Rahmen verarbeitet die Auftragnehmer:in personenbezogene Daten ebenfalls zur Absicherung von Zugängen (Authentifizierung, Nutzer:innen-Verifizierung, Passwort zurücksetzen).

2.2 Folgende personenbezogenen Daten werden verarbeitet

Art der personenbezogenen Daten

- Stamm- und Verkehrsdaten (E-Mail-Adressen, Namen, IP-Adressen)
- Kommunikationsdaten (Benachrichtigungen, Chat-Nachrichten)
- Abstimmungsinhalte

Kategorien betroffener Personen

- Mitarbeitende/Organisationsteam d. Auftraggeber:in
- Teilnehmende an der Veranstaltung d. Auftraggeber:in

2.3 Die zu verarbeitenden personenbezogenen Daten fallen entsprechend der Schutzstufen der Datenschutzbehörden des Bundes und der Länder in die Risiko-Abstufungen „geringfügig" bis „überschaubar" (DSK-Kurzpapier Nr. 18): Betroffene könnten in ihrer gesellschaftlichen Stellung beeinträchtigt werden („Ansehen").

2.4 Aufgrund der technischen Umsetzung ist sichergestellt, dass Einzelstimmen in als „geheim" durchgeführten Abstimmungen nicht konkreten Stimmberechtigten zuzuordnen sind. Dies trifft sowohl für den/die Auftraggeber:in wie auch die Auftragnehmer:in (als Systembetreiber:in) zu. Voraussetzung hierfür sind mindestens zwei abgegebene Stimmzettel in einer Abstimmung.

2.5 Die Auftragnehmer:in verarbeitet personenbezogene Daten für den/die Auftraggeber:in im Sinne von Art. 4 Nr. 2 (Verarbeitung mit Hilfe automatisierter Verfahren) und Art. 28 DS-GVO (als Auftragsverarbeiter:in) auf Grundlage dieser Vereinbarung.

2.6 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.

3. Gewährleistung der technischen und organisatorischen Maßnahmen

3.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Niveau der Sicherheit der Verarbeitung gewährleistet. Dazu werden einerseits mindestens die Schutzziele von Art. 32 Abs. 1 DS-GVO wie Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird (Art. 28 Abs. 3 lit. C DS-GVO).

3.2 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragnehmer:in gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Die Formulierung in Art. 32 Abs. 1 DS-GVO „diese Maßnahmen schließen unter anderem Folgendes ein" verdeutlicht andererseits, dass die dort vorgenommene Aufzählung nicht abschließend ist.

3.3 Der/die Auftraggeber:in hat vor Übermittlung personenbezogener Daten der betroffenen Personen überprüft, dass die von der Auftragnehmer:in aufgestellten technischen und organisatorischen Maßnahmen (TOM) ein angemessenes Schutzniveau sicherstellen. Mit Annahme der beschriebenen TOM wird diese Anlage Bestandteil der Vereinbarung.

4. Rechte und Pflichten sowie Weisungsbefugnisse der/des Verantwortlichen (Auftraggeber:in)

4.1 Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der/die Verantwortliche verantwortlich.

4.2 Der/die Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

4.3 Der/die Verantwortliche ist berechtigt sich vor Beginn der Verarbeitung und danach regelmäßig in angemessener Weise von der Einhaltung der bei der Auftragnehmer:in getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen.

4.4 Der/die Verantwortliche informiert die Auftragnehmer:in unverzüglich, wenn Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse festgestellt wurden.

4.5 Der/die Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragsverarbeiter:in vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrags bestehen.

5. Pflichten der Auftragnehmer:in

5.1 Die Auftragnehmer:in verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen der/des Verantwortlichen, sofern sie nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem die Auftragnehmer:in unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt die Auftragnehmer:in dem/der Verantwortlichen die rechtlichen Anforderungen vor der zusätzlichen Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

5.2 Die Auftragnehmer:in verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen der/des Verantwortlichen nicht erstellt.

5.3. Die Auftragnehmer:in sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Die Einhaltung der Maßnahmen wird durch regelmäßige Kontrollen sichergestellt. Das Ergebnis der Kontrollen ist zu dokumentieren.

5.4 Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den/die Verantwortliche:n, an der Erstellung der Verzeichnissen von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen der/des Verantwortlichen hat die Auftragnehmer:in im

notwendigen Umfang mitzuwirken und den/die Verantwortliche:n soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO).

5.5. Die Auftragnehmer:in wird den/die Verantwortliche:n unverzüglich darauf aufmerksam machen, wenn eine durch den/die Verantwortliche:n erteilte Weisung ihrer Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Die Auftragnehmer:in ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch nach Überprüfung bestätigt oder geändert wird.

5.6 Die Auftragnehmer:in hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der/die Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen der Auftragsverarbeiter:in dem nicht entgegenstehen. Unabhängig davon hat die Auftragnehmer:in personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch einer/eines Betroffenen aus Art. 16, 17 und 18 DS-GVO zugrunde liegt.

5.7 Die Auftragnehmer:in verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten der/des Verantwortlichen die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf die Auftragnehmer:in nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

5.8 Die Auftragnehmer:in sichert zu, dass die bei der Durchführung der Arbeiten beschäftigten Mitarbeitenden vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht worden sind. Alle Mitarbeitenden sind für die Zeit wie auch nach Beendigung ihrer Tätigkeit in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO).

5.9 Beauftragte:r für den Datenschutz bei der Auftragnehmer:in ist Tim Schrock, erreichbar über E-Mail datenschutz@votesup.eu sowie über die o.g. Postanschrift.

5.10 Die Auftragnehmer:in erklärt sich damit einverstanden, dass der/die Verantwortliche grundsätzlich nach Terminvereinbarung berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Verantwortlichen beauftragte Dritte zu kontrollieren (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Die Auftragnehmer:in sichert zu, soweit erforderlich, bei diesen Kontrollen unterstützend mitzuwirken.

5.11 Die Auftragnehmer:in teilt dem/der Verantwortlichen unverzüglich Störungen oder Verstöße bei der Auftragsverarbeitung sowie bei Verletzungen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten der/des Verantwortlichen nach Art. 33 und Art. 34 DS-GVO. Meldungen für den Verantwortlichen darf die Auftragnehmer:in nur nach vorheriger Weisung durchführen.

6. Unterauftragsverarbeitung

Für den grundlegenden Serverbetrieb im Rechenzentrum in Nürnberg wurde beauftragt:

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
Tel.: +49 (0)9831 505-0, Fax: +49 (0)9831 505-3, E-Mail: info@hetzner.com

Der Provider ist zertifiziert nach ISO 27001 (Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems).

Zwischen votesUP und dem Provider besteht eine Vereinbarung zur Auftragsverarbeitung. Die technisch-organisatorischen Maßnahmen des Providers nach Art. 28 DS-GVO können eingesehen werden unter https://www.hetzner.com/AV/TOM.pdf.

7. Haftung und Schadenersatz

Die Vertragsparteien haften entsprechend den einschlägigen gesetzlichen Bestimmungen bzw. gegenüber betroffenen Personen gemäß Art. 82 DS-GVO.

8. Vergütung

Für die zur Erfüllung der in diesem Vertrag vereinbarten Mitwirkungs- und Informationspflichten kann die Auftragnehmer:in eine Aufwandserstattung in Rechnung stellen. Diese beträgt € 25,-- pro angefangener 15 Minuten.

9. Sonstiges

9.1 Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

9.2 Sollten die zu verarbeitenden personenbezogenen Daten der/des Verantwortlichen bei der Auftragnehmer:in durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch Insolvenz oder ein Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat die Auftragnehmer:in den Verantwortlichen unverzüglich zu verständigen.

9.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. Die unwirksame Bestimmung wird durch eine wirksame Regelung ersetzt, die der beabsichtigten Vereinbarung am nächsten kommt. Dies gilt auch für Regelungslücken.

Diese Vereinbarung wurde am 09.05.2021 durch den/die Veranwortliche:n »Klaus Meng« mit dem digitalen votesUP-Assistenten für AV-Vereinbarungen erstellt.

Anlage

Technische und organisatorische Maßnahmen nach DS-GVO

In Art. 32 DS-GVO werden verschiedene Schutzbereiche definiert, für die geeignete technische und organisatorische Maßnahmen (TOM) ergriffen werden sollen. Ziel ist es, unter Berücksichtigung des Stands der Technik, des notwendigen Aufwands und unter Abschätzung von Risiken ein angemessenes Schutzniveau zu gewährleisten. [↗ Rechtstext bei EUR-LEX]

Die folgenden, für votesUP definierten technischen und organisatorischen Maßnahmen stehen nicht für sich allein: Der grundlegende Serverbetrieb wird durch den Provider Hetzner als Auftragsverarbeiter sichergestellt. Die vom Provider aufgestellten TOM sind abrufbar unter ↗ www.hetzner.com/AV/TOM.pdf

Datenschutz ist eine Daueraufgabe. Die IT-Welt entwickelt sich weiter. Organisatorische Maßnahmen sind abhängig von der Größe eines begleitenden Teams und orientieren sich an Risikobewertungen. Daher werden wir die TOM immer wieder an aktuelle Entwicklungen anpassen und auch auf Basis von Erfahrungswerten verbessern.

1. Pseudonymisierung

- Vom System verarbeitete IP-Adressen werden sofort nach Auslieferung der Inhalte gekürzt und reduziert in den Logdateien gespeichert.
- Es werden so wenige personenbezogene Daten wie möglich abgefragt und verarbeitet: Nutzung über anonyme Tokens ist vorgesehen. Nutzer:innen können ihren Anzeigenamen verändern.

2. Verschlüsselung

- Jegliche Verbindungen zu votesUP finden transportverschlüsselt statt.
- Es werden domain-validierte TLS-Zertifikate (früher „SSL-Zertifikate“) nach dem jeweils aktuellen Stand der Technik eingesetzt, die spätestens alle 90 Tage erneuert werden. Wir greifen hierzu auf Zertifikate von Mozillas „Let's Encrypt“-Ausgabestelle zurück.
- Verbindungen werden nur noch nach neueren TLS 1.2/1.3-Standards zugelassen. Damit sind veraltete und nicht mehr abzusichernde Betriebssysteme wie Windows XP allerdings von der votesUP-Nutzung ausgeschlossen.
- Für eine Validierungsüberprüfung der Zertifikate greifen wir auf das verbesserte Online Certificate Status Protocol (OCSP Stapling) zurück, so dass der anfragende Browser den Status des Verschlüsselungszertifikats überprüfen kann.

3. Gewährleistung der Vertraulichkeit

- Vertraulichkeit wird durch das persönliche Verhalten wie auch automatische Zugriffsbeschränkungen gewährleistet. Wir setzen soweit wie möglich auf automatisierte Verfahren, um den Ermessensspielraum von Nutzer:innen nicht unnötig auszuweiten und sie damit unnötiger Verantwortung auszusetzen.
- Der Umfang der möglichen Datenzugriffe ist über die zugewiesenen Nutzer-Rollen und Beschränkungen zum Rollenwechsel festgelegt.
- Der Datenzugriff ist nur über passwortgeschützte Zugänge möglich. Die Passwortanforderungen unterscheiden sich nach Verantwortungsrolle der/des Nutzer:in.
- Passwörter werden nicht direkt gespeichert, sondern nur als Prüfwerte (Hash + Salt).
- Eine zusätzliche Absicherung von Zugängen wird über die optionale Zwei-Faktor-Authentifizierung gewährleistet.
- Administrative Zugänge sind in ihren Datenzugriffsmöglichkeiten auf die zu betreuenden Aufgaben zugeschnitten.
- Betreuende Team-Mitglieder von votesUP sind zu Datenschutz-Anforderungen sensibilisiert und geschult. Sie unterzeichnen eine Vertraulichkeitserklärung.

- Risikobasierte Bewertungen der Datenverarbeitung nehmen wir vorausschauend vor. Die Schwere des möglichen Schadens fällt nach Klassifizierung der Datenschutzbehörden des Bundes und der Länder überwiegend in die Kategorie „überschaubar" (DSK-Kurzpapier Nr. 18): Betroffene könnten in ihrer gesellschaftlichen Stellung beeinträchtigt werden („Ansehen").
- Mittels zentral vermitteltem Stapling des unter 2. genannten OCSP wird die Datenschutzproblematik bei Validierungsanfragen abgewehrt: Der votesUP-Server übermittelt die Validierungsanfrage, so dass die personenbezogene IP-Adressen der Nutzer:innen nicht an die jeweiligen Zertifizierungsstellen weitergegeben werden müssen.

4. Gewährleistung der Integrität

- Die Verarbeitung und insbesondere die Speicherung von Datensätzen erfolgt über mehrere Sicherheitsschleifen (Verfügbarkeit der Anforderung → Berechtigung → Plausibilität).
- Für die Absicherung gegen Manipulation werden in manchen Bereichen (insbesondere Abstimmungen) Prüfmechanismen integriert, für die neben Datenbankzugriff auch der Zugriff auf den Programmcode und Konfigurationsschlüssel notwendig sind. Durch diese Kombination werden Gefahren bei einem Datenbankangriff reduziert und fallen sofort auf. Die Prüfsummen werden mittels standardisierter Hashing-Verfahren erstellt.
- Das Session-Management verwendet erhöhte Standards bei Schlüssellängen, Bit-Tiefe, Anforderungsquellen und Übertragung.
- Durch Fehlerlogging sind Probleme leichter identifizierbar. Das Fehlerlogging wird schrittweise verbessert.

5. Gewährleistung der Verfügbarkeit

- votesUP wird in einem Rechenzentrum bei einem angesehenen deutschen Provider betrieben, der nach ISO 27001 (Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems) zertifiziert ist.
- Die Wartung des grundlegenden Servers (Betriebssystem, Web-Server, Datenbankserver, E-Mail-Server sowie unterstützende Systeme wie Firewalls oder Angriffserkennung) wird von ausgebildeten Techniker:innen des Providers sichergestellt.
- Sowohl die votesUP-Plattform wie auch die nutzergenerierten Daten (Abstimmungen usw.) werden laufend auf redundanten Datenträgern gespeichert. Dadurch ist selbst bei Ausfall einer Festplatte ein ununterbrochener Betrieb sichergestellt.
- Die Systeme werden einmal täglich vollständig und automatisiert gesichert. Diese täglichen Backups reichen 14 Tage zurück.
- Neue Funktionen werden zuerst in einem Testsystem überprüft, bevor sie in das votesUP-Produktivsystem eingespielt werden.
- Größere Wartungsarbeiten und Umbauten an votesUP finden in wenig frequentierten Zeiträumen statt (23 Uhr - 8 Uhr) und werden nach Möglichkeit vorher auf der votesUP-Startseite angekündigt.

6. Gewährleistung der Belastbarkeit der Systeme

- Eine allgemeine Belastbarkeitsprüfung des Systems findet in unregelmäßigen Abständen statt (zuletzt nach Servermigrationen im Dezember 2020 und im Februar 2021).
- Es findet ein durchgehendes Monitoring des Load Average auf dem Server statt.
- Unüblich erhöhte Zugriffsversuche oder Quellen missbräuchlicher Nutzung werden ggf. automatisiert geblockt. Bei nutzerspezifischen Anforderungen werden die Betroffenen über die Limiterreichung informiert.
- Veranstaltungen sind standardmäßig auf eine bestimmte Nutzerzahl beschränkt. Erst auf Antrag und Zeitraum-Angabe wird das Limit vom votesUP-Team erhöht.

- Veranstalter:innen werden in der Verwaltungsoberfläche gebeten, ihre konkreten Veranstaltungszeiträume vorher anzumelden. Der Kalender der zu erwartenden Last wird täglich geprüft.
- Es können anlassbezogen Systemeinstellungen angepasst werden, um die Last pro Nutzer:in zu reduzieren. Dies betrifft insbesondere die Häufigkeit von Statusabfragen (Chat, Session, neue Abstimmungen, Wortmeldungen).
- Ressourcenintensive Datenbankabfragen können gecacht werden.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- Für das gesamte System werden täglich nachts Sicherheitskopien angelegt. Die gespeicherten Daten sind 14 Tage lang wiederherstellbar.
- Die Erstellung und Verwaltung dieser Backups erfolgt automatisiert. Diese Mechanismen werden von uns in unterschiedlichen Abständen auf ihre Funktionstüchtigkeit überprüft.
- Der Programmcode wird versioniert erstellt, d.h. Änderungen sind bei Problemen umkehrbar.
- Für die Evaluierung von Programmcode steht dauerhaft ein Zweitsystem und anlassbezogen ein Drittsystem zur Verfügung.

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Im Rahmen der laufenden Entwicklung wird die Funktionalität und Sicherheit von votesUP ständig einer Überprüfung und Analyse unterzogen.
- Externe Werkzeuge wie das Mozilla Observatory (↗ observatory.mozilla.org/analyze/votesup.eu) und die SSLlabs (↗ www.ssllabs.com/ssltest/analyze.html?d=votesup.eu) stellen ihre Prüfberichte zur jederzeitigen Einsichtnahme öffentlich zur Verfügung.
- Eine öffentlich einsehbare Dokumentation von Veränderungen (votesup.eu/news) wird ergänzt durch den ausführlicheren, entwicklungsinternen Changelog.

Stand der TOM: 04.04.2021