OpenSlides

Das digitale Antrags- und Versammlungssystem

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen

(Auftraggeber)

– Verantwortlicher, nachstehend AG genannt –

und

Intevation GmbH
Neuer Graben 17
49074 Osnabrück
– Auftragsverarbeiter, nachstehend AN genannt –

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags ist die Bereitstellung von Hosting-Leistungen im Rahmen des vom AN bereitgestellten Produktpakets von OpenSlides.

(2) Die Dauer dieses Auftrags (Laufzeit) richtet sich nach der Dauer der Erbringung von Hosting- Leistungen des AN an den AG. Der Auftrag endet, wenn der AG keine Hosting-Leistungen des AN, entsprechend den Leistungsvereinbarungen/Angeboten der einzelnen Auftragsbestätigungen für Hosting-Leistungen des AN, mehr in Anspruch nimmt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten:

Der Auftragsgegenstandes bezieht sich auf das Hosting von OpenSlides auf einem vom AN administrierten Webserver. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung und / oder Nutzung der Daten ergeben sich aus den Vereinbarungen für die Hosting-Leistungen. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten:
Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten (Vor- und Nachname)

- Kommunikationsdaten (E-Mail-Adresse)
- Gliederungsebene beim AG
- Mitgliedsdaten (vgl. Art. 9 Abs. 1 DS-GVO)
- Politische Meinung (vgl. Art. 9 Abs. 1 DS-GVO)
- Bild und Ton (bei optionaler Nutzung von Audio- oder Videokonferenzdiensten)

(3) Kategorien betroffener Personen:
Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Beschäftigte des AG
- Delegierte bzw. Mitglieder des AG
- Gastteilnehmende

3. Technisch-organisatorische Maßnahmen

(1) Der AN gewährleistet die im Rahmen der ordnungsgemäßen Abwicklung des Auftrags erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 28 und Art. 32 der DS-GVO. Die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen sind passend zum Datensicherheitsrisiko unter Berücksichtigung der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität, Zweckbindung, Transparenz und Intervenierbarkeit detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragsverarbeiter.

(2) Der AN administriert die OpenSlides-Server, welche ausschließlich in zertifizierten Rechenzentren in Deutschland betrieben werden. Die technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO der Rechenzentren können hier abgerufen werden:

- kyberio GmbH:
  `https://www.kyberio.com/wp-content/uploads/Vereinbarung-ueber-Auftragsverarbeitung-kyberio-gmbh.pdf`
- Hetzner Online GmbH:
  `https://www.hetzner.com/AV/TOM.pdf`

(3) Die eingesetzte Software auf den Servern entspricht den aktuellen Sicherheitsanforderungen. Der AN sorgt regelmäßig für die Installation und Dokumentation von Sicherheitsupdates auf den Servern.

(4) Bei optionaler Nutzung des Videostreaming-Angebots, werden die Dienste der nanocosmos Informationstechnologien GmbH eingesetzt. Die technisch-organisatorischen Maßnahmen des Unterauftragnehmers finden sich hier: `https://www.nanocosmos.de/documents/GDPR-DSGVO-DPA-nanocosmos.pdf`.

4. Verarbeitung von Daten

(1) Der AN darf die Daten, die im Auftrag verarbeitet werden, nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach dokumentierter Weisung des AG verarbeiten. Ist der AN durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt der AN die rechtlichen Anforderungen dem AG vor der Verarbeitung mit.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des AGs unmittelbar durch den AN sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der AN gewährleistet, dass alle Personen, die von ihm mit der Bearbeitung und Erfüllung dieses Vertrages betraut werden, in Schriftform zur Vertraulichkeit verpflichtet werden. Der AN darf die aus dem Bereich des AG erlangten Informationen nicht an Dritte offenbaren, sondern ist zur Vertraulichkeit hierüber auch nach Beendigung des Vertragsverhältnisses verpflichtet.

(2) Der AN hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO.

(3) Der AN unterstützt den AG nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des AG nach Art. 12 bis 22 DS-GVO.

6. Unterauftragsverhältnisse

(1) Der AG ist grundsätzlich damit einverstanden, dass der AN an sorgfältig ausgewählte Drittunternehmen Unteraufträge erteilt. Der AN informiert den AG jeweils rechtzeitig vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Drittunternehmer. Der AG kann in diesem Fall gegen die Hinzuziehung oder Ersetzung Einspruch erheben. Wird dem AN dadurch die Erbringung des Vertragsgegenstandes unmöglich, kann er diesen Vertrag und den Vertrag

über die Erbringung von Hosting-Leistungen zum Zeitpunkt der geplanten Hinzuziehung oder Ersetzung außerordentlich kündigen.

(2) Der AN hat bei der Vergabe von Unteraufträgen die Anforderungen des Art. 28 Abs. 2–4 DS-GVO zu beachten und die vertragliche Vereinbarung mit dem Unterauftragnehmer so zu gestalten, dass sie den in dieser Vereinbarung festgelegten Datenschutzanforderung zwischen AN und AG entsprechen.

(3) Als einzige Unterauftragnehmer sind beauftragt:

- kyberio GmbH:
  `https://www.kyberio.com/impressum/`
- nanocosmos Informationstechnologien GmbH:
  `http://www.nanocosmos.de/v6/imprint.html`
- Hetzner Online GmbH:
  `https://www.hetzner.com/de/rechtliches/impressum`

7. Kontrollrechte des Auftraggebers

(1) Der AG hat das Recht, im Benehmen mit dem AN Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den AN in dessen Geschäftsbetrieb zu überzeugen.

(2) Der AN stellt sicher, dass sich der AG von der Einhaltung der Pflichten des ANs nach Art. 28 DS-GVO überzeugen kann. Der AN verpflichtet sich, dem AG auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO bzw. durch Berichte des für den AN zuständigen Datenschutzbeauftragten.

(4) Für die Ermöglichung von Kontrollen durch den AG kann der AN einen Vergütungsanspruch geltend machen. Vorbehaltlich einer anderen Vereinbarung mit dem AG wird der im Hauptvertrag vereinbarte Supportstundensatz für die aufwandsbezogene Abrechnung zugrunde gelegt.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der AN unterstützt den AG bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz- Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den AG zu melden

c) die Verpflichtung, dem AG im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des AGs für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des AGs im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des AN zurückzuführen sind, kann der AN eine Vergütung beanspruchen. Vorbehaltlich einer anderen Vereinbarung mit dem AG wird der im Hauptvertrag vereinbarte Supportstundensatz für die aufwandsbezogene Abrechnung zugrunde gelegt.

9. Weisungsbefugnis des Auftraggebers

(1) Der AG erteilt dem AN Weisungen grundsätzlich in Textform. Mündliche Weisungen bestätigt der AG unverzüglich (mind. Textform). Der AN hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

(2) Der AN hat den AG unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den AG bestätigt oder geändert wird.

10. Qualifizierte Verschwiegenheitsvereinbarung bei nicht-namentlichen bzw. geheimen Wahlen und Abstimmungen

(1) Soweit OpenSlides für die Durchführung von nicht-namentlichen bzw. geheimen Wahlen und Abstimmungen eingesetzt wird, ist der AN verpflichtet, jegliche Maßnahmen zu unterlassen, die das Abstimmungs- bzw. Wahlgeheimnis kompromittieren könnten. Insbesondere dürfen keine auf den Inhalt einzelner Stimmen gerichteten Protokolle angefertigt oder entsprechende Daten ausgelesen werden, wenn dadurch ein Bezug zu der abstimmenden Person hergestellt werden könnte. Soweit doch entsprechende Daten anfallen sollten (z. B. durch einen Programmfehler), ist der AN zur absoluten Verschwiegenheit und umgehenden Vernichtung verpflichtet.

(2) Die Kontroll- und Weisungsrechte des AG nach Nr. 7 und 9 dieses Vertrages sind, soweit die Verpflichtung nach Absatz 1 reicht, eingeschränkt. Insbesondere darf der AG keine auf die Ausforschung des Abstimmungs- bzw. Wahlgeheimnisses gerichteten Weisungen erteilen oder seine Kontrollrechte dergestalt ausüben, dass das Abstimmungs- bzw. Wahlgeheimnisses ausgeforscht würde.

(3) Von der Verpflichtung nach Absatz 1 kann der AN auch nach Vertragsschluss nicht befreit werden, auch nicht durch ausdrückliche Erklärung des AG oder seines gesetzlichen Vertreters oder seiner vertretungsberechtigten Organe. Gleiches gilt für eine abweichende einseitige oder zweiseitige Veränderung der Vereinbarung in Satz 1. Gleiches gilt für eine Aufhebung der Beschränkungen des Absatzes 2.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des AGs nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den AG – spätestens mit Beendigung der Leistungsvereinbarung – hat der AN sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den AN entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem AG übergeben.

12. Datenschutzbeauftragte des Auftragnehmers

(1) Als Datenschutzbeauftragter des Auftragnehmers ist benannt: Dr. Johannes Schröder <datenschutz@intevation.de>.

(2) Ein Wechsel der Datenschutzbeauftragten ist dem AN unverzüglich anzuzeigen.

Osnabrück, 13. September 2024
(Dieser Vertrag wurde elektronisch erstellt und ist ohne Unterschrift gültig.)

A. Anlage 1 – Technisch-organisatorische Maßnahmen

A.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

A.1.1. Zutrittskontrolle

Das Hosting erfolgt in den deutschen Rechenzentren der kyberio GmbH und der Hetzner GmbH. Diese sind nach IT-Grundschutz/ISO 27001 zertifiziert. Der Zugang zur Hardware erfolgt über ein Zugangskontrollsystem, welches unbefugten Zutritt ausschließt.

A.1.2. Zugangskontrolle

OpenSlides wird auf Servern betrieben, die über dedizierte Switche verbunden sind. Die Verbindungen zwischen Rechenzentren (vgl. A.3.1) finden über dedizierte VLANs statt, sodass sämtlicher Datenverkehr zwischen den OpenSlides-Systemen über vertrauenswürdige Verbindungen läuft.

OpenSlides verfügt über ein Zugangskonzept aus verschlüsselter Übertragung und Nutzerauthentifizierung durch Benutzername und Passwort (Login-Verfahren).

Auf Administrationsebene erfolgt der Zugang verschlüsselt per OpenSSH mit Schlüssel-Authentifizierung.

Die OpenSlides-Systeme laufen auf dedizierten Servern mit LUKS-verschlüsselten Datenträgern. Im ausgeschalteten Zustand sind somit sämtliche Kundendaten verschlüsselt. Bei Austausch oder Entsorgung eines Datenträgers ist die Vertraulichkeit der darauf gespeicherten Daten daher von Anfang an gesichert. Datenträger werden durch die Rechenzentrumsbetreiber zusätzlich gelöscht oder zerstört.

A.1.3. Zugriffskontrolle

OpenSlides wird auf Servern betrieben, die über dedizierte Switche verbunden sind. Die Verbindungen zwischen Rechenzentren (vgl. A.3.1) finden über dedizierte VLANs statt, sodass sämtlicher Datenverkehr zwischen den OpenSlides-Systemen über vertrauenswürdige Verbindungen läuft.

OpenSlides verwaltet die Prozesse der einzelnen Kundeninstanzen in jeweils eigenen virtualisierten Netzwerken. Die Datenhaltung findet auf dedizierten Datenbankservern statt, wobei jede Instanz auf eine eigene Datenbank zugreift. Der Zugriff auf die Datenbanken ist nur mit dem jeweils instanzspezifischen Datenbank-Account möglich (Mandantentrennung).

Regelmäßige Sicherheitsupdates (nach dem Stand der Technik) verhindern unberechtigte Zugriffe durch das Ausnutzen von Sicherheitslücken.

Die OpenSlides-Systeme laufen auf dedizierten Servern mit LUKS-verschlüsselten Datenträgern. Im ausgeschalteten Zustand sind somit sämtliche Kundendaten verschlüsselt. Bei Austausch oder Entsorgung eines Datenträgers ist die Vertraulichkeit der darauf gespeicherten Daten daher von Anfang an gesichert. Datenträger werden durch die Rechenzentrumsbetreiber zusätzlich gelöscht oder zerstört.

A.1.4. Trennungskontrolle

Die Daten der Kundeninstanzen werden in separaten Datenbanken gehalten, auf die nur mit den entsprechenden kundeninstanzspezifischen Datenbankusern zugegriffen werden kann.

A.1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Eine OpenSlides-Instanz wird dem Auftraggeber mit einem individuellen Benutzerkonto mit administrativen Rechten übergeben. Alle weiteren Eingaben, inklusive dem Anlegen weiterer Benutzerkonten und ihrer Berechtigungen, erfolgen durch den Auftraggeber.

Es steht dem Auftraggeber frei zu entscheiden, ob die Durchführung der Veranstaltung mit Pseudonymen möglich oder die unmittelbare Identifikation der Teilnehmenden erforderlich ist. OpenSlides erzwingt keine Klarnamen.

Es werden keine personenbezogenen Daten, auch keine IP-Adressen, protokolliert.

A.2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

A.2.1. Weitergabekontrolle

Eine Weitergabe ist innerhalb der Auftragsverarbeitung nicht vorgesehen.

Die Eingabe/Ausgabe der Daten erfolgt im Rahmen der Zugriffskontrolle verschlüsselt über HTTPS.

A.2.2. Eingabekontrolle

Der Zugriff auf OpenSlides und damit auf die Datenverarbeitung erfolgt durch individuelle Benutzerkonten, die durch den Auftragnehmer angelegt werden. Den Benutzerkonten können in OpenSlides detaillierte Zugriffsberechtigungen gegeben oder genommen werden.

Der Zugriff auf die OpenSlides-Server durch Systemadministratoren wird automatisch protokolliert.

A.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

A.3.1. Verfügbarkeitskontrolle

Systemtechnische Maßnahmen Die OpenSlides-Systeme sind redundant ausgelegt. Jedem Datenbank-Cluster stehen zwei Hot-Standby-Systeme bei. Bei Ausfall des primären Clusters übernimmt ein Standby-System automatisch die Rolle des primären Clusters. Durch das dritte System ist selbst nach Ausfall eines Servers weiterhin eine redundante Datenspeicherung gewährleistet.

Darüber hinaus werden regelmäßige Backups angelegt und alle Operationen gespeichert, welche auf den Datenbanken laufen. Dies erlaubt „Point-in-Time-Recovery."

Raumtechnische Maßnahmen Die Rechenzentren verfügen über Brandmeldeanlagen, unterbrechungsfreie Notstromanlagen und Netzersatzanlagen (Notstromdiesel).

Die Server der redundanten OpenSlides-Systeme sind auf zwei Brandschutzabschnitte innerhalb der Rechenzentren verteilt, um eine mögliche physikalische Zerstörung mit einer räumlich getrennten Datensicherung aufzufangen.

Backups werden nicht nur lokal auf den Servern vorgehalten, sondern zusätzlich auf Backup-Speicher der Hetzner GmbH kopiert. Die Datenübertragung zum und die Speicherung in dem Backup-Speicher erfolgt verschlüsselt. Zugriff haben ausschließlich die Administratoren der Intevation GmbH.

A.3.2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Aus den verschiedenen Stufen der Datensicherung können Datenbanken und einzelne Datensätze bei Bedarf wiederhergestellt werden. Die notwendigen Schritte sind im Betriebshandbuch dokumentiert.

A.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

A.4.1. Datenschutz-Management

Die Intevation GmbH hat zusammen mit ihrem externen bestellten Datenschutzbeauftragten ein Datenschutz-Management etabliert, dem ein Vorgehen nach dem PDCA1-Zyklus zugrunde liegt.

A.4.2. Incident-Response-Management

Störungen im Betrieb werden durch das automatische Monitoring der Intevation GmbH erkannt und direkt an die Systemadministration beziehungsweise das IT-Betriebsteam gemeldet. Für persönlich entgegengenommene Vorfallmeldungen (Telefon, E-Mail, Ticketsystem) besteht die Richtlinie, diese umgehend direkt an die Systemadministration beziehungsweise das IT-Betriebsteam weiterzuleiten.

Auf Basis von Ziff. 8 b) dieser Vereinbarung basiert das Incident-Response-Management auf dem in der Luftfahrt verwendeten Ablaufmodell T-DODAR:

1. *Time:* Prüfung, wie schnell eine Entscheidung gefällt und gehandelt werden muss. Mit mehr Zeit lassen sich evtl. bessere Entscheidungen treffen, aber wenn man zu lange wartet, sind manche Aktionen nicht mehr durchführbar oder sinnvoll. Die Entscheidung über das weitere Vorgehen wird innerhalb 15–30 Minuten getroffen. Nur wenn ausgeschlossen werden kann, dass sensitive Daten in die falschen Hände geraten, steht mehr Zeit zur Verfügung.
2. *Diagnose:* Was ist genau das Problem und wie schwerwiegend sind die Folgen?
3. *Options:* Was sind die Handlungsoptionen? Wer kann unterstützen?
4. *Decide:* Was ist die beste Handlungsoption?

5. *Act or Assign:* Die Umsetzung der gewählten Option wird begonnen. Hierbei kann es sinnvoll sein, Aufgaben aufzuteilen oder an jemanden mit mehr Erfahrung in diesem Punkt zu übergeben.

6. *Review:* Bei der Umsetzung muss konstant geprüft werden, ob die gewählte Option noch die richtige ist. Eventuell ist es sinnvoll, den Entscheidungsprozess mit den bei der Umsetzung gewonnenen Informationen neu zu starten.

Sollte bei der Diagnose eine Gefährdung oder Verletzung des Schutzes personenbezogener Daten festgestellt werden, wird der Auftraggeber bei den einzelnen Schritten angemessen informiert und eingebunden. Spätestens nach der Entscheidung (*Decide*) wird eine E-Mail an den Auftraggeber als Zusammenfassung gesendet.

Grundsätzlich gilt: Wenn die Gefahr besteht, dass Daten mit erhöhtem Schutzbedarf in die falschen Hände geraten, müssen die Systeme sofort heruntergefahren oder hart ausgeschaltet werden.

A.4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Zu Beginn der Auftragsverarbeitung legt der Auftragnehmer eine neue OpenSlides-Instanz mit einem individuellen Benutzerkonto für den Auftraggeber an. Das Konto hat administrative Rechte innerhalb der gebuchten OpenSlides-Instanz. Alle weiteren Eingaben, inklusive dem Anlegen weiterer Benutzerkonten und ihrer Berechtigungen, erfolgen durch den Auftraggeber.

Es steht dem Auftraggeber frei zu entscheiden, ob die Durchführung der Veranstaltung mit Pseudonymen möglich oder die unmittelbare Identifikation der Teilnehmenden erforderlich ist. OpenSlides erzwingt keine Klarnamen.

Die OpenSlides-Systeme protokollieren konsequent keine IP-Adressen.

A.4.4. Auftragskontrolle

Grundlage der Datenverarbeitung ist die Beauftragung des Auftraggebers zur Auftragsverarbeitung. Es ist geregelt, dass alle Weisungen in schriftlicher Form oder in einem elektronischen Format (Textform) erfolgen müssen und dass der Auftraggeber vollumfänglich kontrollieren kann.

Die Intevation führt eine Dokumentation des aktuellen Zustands der Server (Hardware, installierte Software), welche vom Auftraggeber jederzeit angefragt werden kann, und überprüft regelmäßig den Hostingdienstleister auf Vorliegen eines gültigen ISO 27001/IT-Grundschutz-Zertifikats.