Open Administration UG (haftungsbeschränkt)

Besondere Bedingungen zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Stand: 3. August 2022

Inhaltsverzeichnis

Besondere Bedingungen zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem Verantwortlichen,

– nachstehend Auftraggeber:in oder Kund:in genannt –

und der

Open Administration UG (haftungsbeschränkt)

– Auftragsverarbeiterin –

wird vereinbart:

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Der Gegenstand des Auftrags bestimmt sich nach den zugrundeliegenden Angaben gemäß dem Angebot und den AGB, auf welche hier verwiesen wird (im Folgenden Leistungsvereinbarung).

Wesentliche Softwarekomponenten seien im folgenden genannt. Darüber hinaus kann individuell auch weitere Software genutzt werden.

Die “Mitgliederverwaltung“ ist eine Accountverwaltung zur Erstellung eines Profils mit Kontaktdaten und Organisationszugehörigkeiten von natürlichen Personen. Dazu gehört insbesondere die Verwaltung der E-Mail-Adresse und des Passwortes.

Die “Finanzverwaltung“ ist eine vollumfassende Verwaltung der kameralen Buchhaltung mit inbegriffenem Antrags- und Abrechnungssystem. Im Kern werden Belege wie z.B. Rechnungen im System hochgeladen, erfasst und können darüber verbucht werden. Das Auslösen von Überweisungen, der Abgleich von Zahlungsvorgängen mit einem online angebundenen Bankkonto ist ebenso möglich. Hierbei werden Mitglieder-, Kund:innen- und Lieferantendaten verwaltet. Die Einsicht, der Zugriff und die Erstellung von Belegen und Anträgen ist über die Mitgliederverwaltung steuerbar. Die Verantwortung für die hochgeladenen Belege und Dokumente sowie erstellten Anträge und Abrechnungen obliegt dem/der Verantwortlichen, da deren Inhalt nicht von der Auftragsverarbeiterin geprüft wird.

Die Nextcloud ist eine Software über welche Dateien, Dokumente und weitere Inhalte wie z.B. Kalendereinträge und Aufgaben angelegt, hochgeladen, gespeichert und geteilt werden können. Das Teilen ist an Dritte möglich. Die Verantwortung für die hochgeladenen Dokumente sowie weitere Inhalte obliegt dem/der Verantwortlichen, da deren Inhalt nicht von der Auftragsverarbeiterin geprüft wird.

Der RocketChat ist eine Instant-Messaging-Plattform, über welche Chats, Gruppen und Threads automatisch erstellt werden können. Die Namen der Nutzer:innen sind hierbei für alle anderen innerhalb des Systems sichtbar.

1.2 Dauer des Auftrags

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien gemäß der Leistungsvereinbarung gekündigt werden.

2 Geltungsbereich und Konkretisierung des Auftragsinhalts

1. Der Zweck ist es, Organisationen wie Studierendenvertretungen bei der Durchführung ihrer Geschäftstätigkeit optimal zu unterstützen und zu entlasten. Hierbei erbringt Open Administration insbesondere Leistungen der Datenverarbeitung und der Telekommunikation sowie andere Dienstleistungen und Nebenleistungen. Die Auftragsverarbeiterin erhält dabei Zugriff auf die bei der Benutzung der in der Leistungsvereinbarung genannten Softwarekomponenten gespeicherten personenbezogenen Daten. Folgende Datenkategorien können von dem/der Verantwortlichen durch direkte Eingabe oder durch Hochladen in allen zur Verfügung gestellten Softwarekomponenten verarbeitet werden:
    - Angabe zu Mitbenutzenden (Mitglied/Nutzer:in): Name, Vorname, E-Mail-Adresse
    - Angaben zur Organisation/dem Unternehmen: u.a. Name, Adresse, vollständiger Name von Verantwortlichen, Telefonnummer, E-Mail-Adresse, IBAN/BIC
2. Diese Besonderen Bedingungen zur Auftragsverarbeitung sind nur dann in das o.a. Vertragsverhältnis einbezogen, wenn die Vereinbarung zur Auftragsverarbeitung zwischen den o.a. Parteien von beiden Seiten geschlossen wurde.
3. Eine Konkretisierung des Auftragsinhalts ist dort individuell vereinbart.
4. Unabhängig vom Abschluss dieser Vereinbarung gewährleistet Open Administration generell die Einhaltung der hier in der aufgeführten technisch-organisatorischen Maßnahmen gemäß der Leistungsvereinbarung.

3 Technisch-organisatorische Maßnahmen

1. Die Auftragsverarbeiterin hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und die Auftraggeber:in zur Prüfung zu übergeben. Bei Akzeptanz durch die Auftraggeber:in werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit der Auftraggeber:in einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2. Die Auftragsverarbeiterin hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten siehe Anlage).

3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragsverarbeiterin gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4 Berichtigung, Einschränkung und Löschung von Daten

1. Die Auftragsverarbeiterin darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggeber:in berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die Auftragsverarbeiterin wendet, wird die Auftragsverarbeiterin dieses Ersuchen unverzüglich an die Auftraggeber:in weiterleiten.

2. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung der Auftraggeber:in unmittelbar durch die Auftragsverarbeiterin sicherzustellen.

5 Qualitätssicherung und sonstige Pflichten der Auftragsverarbeiterin

Die Auftragsverarbeiterin hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Die Auftragsverarbeiterin setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Auftragsverarbeiterin und jede der Auftragsverarbeiterin unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung der Auftraggeber:in verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

2. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S.2 lit. c, 32 DS-GVO (Einzelheiten in der Anlage).

3. Die Auftraggeber:in und die Auftragsverarbeiterin arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

4. Die unverzügliche Information der Auftraggeber:in über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei der Auftragsverarbeiterin ermittelt.

5. Soweit die Auftraggeber:in seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei der Auftragsverarbeiterin ausgesetzt ist, hat ihn die Auftragsverarbeiterin nach besten Kräften zu unterstützen.

6. Die Auftragsverarbeiterin kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

7. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber der Auftraggeber:in im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6 Unterauftragsverhältnisse

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die die Auftragsverarbeiterin z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Die Auftragsverarbeiterin ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten der Auftraggeber:in auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
   Die Auftragsverarbeiterin verpflichtet externe Rechenzentren sowie sonstige Unterauftragsverarbeiterinnen, die innerbetriebliche Organisation so zu gestalten, dass es den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere findet die Datenverarbeitung auf Datenverarbeitungsanlagen statt, für die das Rechenzentrum oder der sonstige Unterauftragsverarbeiterinnen alle technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

2. Der Auftragsverarbeiterin hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten in Anlage 1).

3. Die Weitergabe von personenbezogenen Daten der Auftraggeber:in an der Unterauftragsverarbeiterinnen und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

4. Die Auftragsverarbeiterin führt jegliche Verarbeitung in Rechenzentren innerhalb der Bundesrepublik durch. Dies gilt auch für etwaige Unterauftragsverarbeiterinnen.

5. Beim Einsatz von UnterAuftragsverarbeiterinnen stellt die Auftragsverarbeiterin die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragsverarbeiterin

gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

7 Kontrollrechte der Auftraggeber:in

1. Die Auftraggeber:in hat das Recht, im Benehmen mit der Auftragsverarbeiterin Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Sie hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch die Auftragsverarbeiterin in dessen Geschäftsbetrieb zu überzeugen.

2. Die Auftragsverarbeiterin stellt sicher, dass sich die Auftraggeber:in von der Einhaltung der Pflichten der Auftragsverarbeiterin nach Art. 28 DS-GVO überzeugen kann. Die Auftragsverarbeiterin verpflichtet sich, der Auftraggeber:in 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 aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).

4. Für die Ermöglichung von Kontrollen durch der Auftraggeber:in kann die Auftragsverarbeiterin einen Vergütungsanspruch geltend machen.

8 Mitteilung bei Verstößen der Auftragsverarbeiterin

1. Die Auftragsverarbeiterin unterstützt die Auftraggeber:in bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz- Folgeabschätzungen und vorherigen 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 Auftraggeber:in zu melden;

c) die Verpflichtung, der Auftraggeber:in im Rahmen ihrer Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung der Auftraggeber:in für ihre Datenschutz-Folgenabschätzung;

e) die Unterstützung der Auftraggeber:in im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

2. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten der Auftragsverarbeiterin zurückzuführen sind, kann die Auftragsverarbeiterin eine Vergütung beanspruchen.

9 Weisungsbefugnis der Auftraggeber:in

1. Mündliche Weisungen bestätigt die Auftraggeber:in unverzüglich (mind. Textform).

2. Die Auftragsverarbeiterin hat die Auftraggeber:in unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Die Auftragsverarbeiterin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeber:in bestätigt oder geändert wird.

10 Berichtigung, Einschränkung und Löschung von personenbezogenen Daten

1. Kopien oder Duplikate der Daten werden ohne Wissen der Auftraggeber:in 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. Die Auftragsverarbeiterin darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die Auftragsverarbeiterin wendet, wird die Auftragsverarbeiterin dieses Ersuchen unverzüglich an den Verantwortlicher weiterleiten.

3. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch der Auftraggeber:in
– spätestens mit Beendigung der Leistungsvereinbarung –
hat die Auftragsverarbeiterin sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeber:in auszuhändi-

gen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

4. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragsverarbeiterin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende der Auftraggeber:in übergeben.

11 Sozialgeheimnis und Daten von Berufsgeheimnisträgern

Als vorsorgliche organisatorische Maßnahme hat Open Administration ihre Mitarbeiter:innen generell auf die Wahrung des Sozialgeheimnisses, § 35 SGB I, sowie auf die Geheimnisse von Berufsgeheimnisträgern bei der Mitwirkung an deren Verarbeitung, § 203 StGB, verpflichtet.

12 Fernmeldegeheimnis

Als weitere organisatorische Maßnahme hat Open Administration ihre Mitarbeiter:innen generell auf die Wahrung des Fernmeldegeheimnisses, jetzt § 3 TTDG, verpflichtet.

13 Zusatzvereinbarungen

1. Soweit die Auftraggeber:in nach Ziffer 7 Kontrollrechte ausüben wird, orientiert sich die vorab zu vereinbarende Höhe des Entgelts an einem festzulegenden Stundensatz des für die Betreuung von der Auftragsverarbeiterin abgestellten Mitarbeiter:innen.

2. Erteilt die Auftraggeber:in der Auftragsverarbeiterin Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten.

3. Soweit die Auftraggeber:in Unterstützung nach Ziffer 8 für die Beantwortung von Anfragen Betroffener benötigt, hat er die hierdurch entstehenden Kosten zu erstatten.

4. Die Vertragsdauer dieser Vereinbarung ist abhängig vom Bestand eines Hauptvertragsverhältnisses gemäß Ziffer 1. Die Kündigung oder anderweitige Beendigung des Hauptvertragsverhältnisses gemäß Ziffer 1 beendet gleichzeitig die vorliegende Vereinbarung. Das Recht zur außerordentlichen Kündigung dieser Vereinbarung sowie die Ausübung gesetzlicher Rücktrittsrechte für diese Vereinbarung bleiben hierdurch unberührt.

5. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich. Als Gerichtsstand wird das für die Auftraggeber:in örtlich zuständige Gericht vereinbart.

6. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

14 Anhang - technisch-organisatorische Maßnahmen

14.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

14.1.1 Zutrittskontrolle

Zutrittskontrolle dient dem Schutz der Datenverarbeitungsanlagen vor unberechtigtem, physischem Zutritt. Open Odministration realisiert die Zutrittskontrolle über folgende, mehrstufige Absicherung:

- Die Kund:innendaten werden ich Rechenzentren von Hostsharing eG, Flughafenstraße 52a, 22335 Hamburg und Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen gespeichert und verarbeitet.

- Die technisch-organisatorischen Maßnahmen von Hostsharing sind hier einsehbar.

- Die technisch-organisatorischen Maßnahmen von Hetzner sind hier einsehbar.

14.1.2 Zugangskontrolle

Zugangskontrolle dient dem Schutz der Datenverarbeitungsanlagen vor unberechtigtem, logischem Zugriff. Open Administration realisiert die Zugangskontrolle über folgende, mehrstufige Absicherung:

- Die Nutzer:innen und der Administratorzugriff auf die Open Administration Systeme beruhen auf einem rollenbasierten Zugriffsberechtigungsmodell. Jede Nutzer:in erhält eine eindeutige Kennung, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Nutzer:innen und Administratoren genutzt werden können.

- Open Administration stellt dem Kund:inn eine Benutzerverwaltung bereit, um ihn bei der Implementation der Zugangskontrolle in seinem Verantwortungsbereich zu unterstützen.

- Bei Open Administration gilt das Prinzip der Minimalberechtigung. Jede Nutzer:in erhält nur die Zugriffsrechte, die erforderlich sind, um ihre vertraglichen Tätigkeiten durchzuführen. Nutzer:innenkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.

- Einsatz von Firewallsystemen, Virenscanner und Intrusion Detection Systemen auf Open Administration Serversystemen.
- Der Zugang über von Open Administration bereitgestellte Verfahren zur Administration der Server erfolgt ausschließlich über eine geschützte Verbindung.
- Der Zugang über von Open Administration bereitgestellte Verfahren ist per Passwort geschützt.
- Der Zugang über von Open Administration bereitgestellte Verfahren wird protokolliert.
- Die Verantwortung der Zugangskontrolle in Bezug auf Sicherheit und Updates der betriebsbereit vorgehaltenen Software obliegt Open Administration.

14.1.3 Zugriffskontrolle

Zugriffskontrolle dient dem Schutz der Daten von unbefugtem Lesen, Kopieren, Verändern oder Löschen personenbezogener Daten innerhalb des Systems. Open Administration realisiert die Zugriffskontrolle über folgende, mehrstufige Absicherung:

- Zugriffsberechtigung auf Open Administration Produktivsysteme ist auf einen kleinen Kreis von Mitarbeiter:innen beschränkt.
- Open Administration hat ein verbindliches Berechtigungsvergabeverfahren für die Mitarbeiter:innen festgelegt.
- Open Administration soll im Falle des Bekanntwerdens von Sicherheitslücken unverzüglich Sicherheitsupdates installieren.
- Für Admin-Zugriffe durch Dienstleister:innen siehe die technisch-organisatorischen Maßnahmen von Hostsharing und Hetzner.

14.1.4 Datenminimierung

Der Auftragsverarbeiterin verwendet für den Betrieb seiner Dienstleistungen persönliche Daten nur in dem für die Gewährleistung des Betriebes erforderlichen Umfang. Open Administration gestaltet die Software für die Nutzung mölichst datensparsam.

14.1.5 Trennungskontrolle

Trennungskontrolle dient der Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden. Open Administration realisiert die Trennungskontrolle über folgende, mehrstufige Absicherung:

- Open Administration nutzt festgelegte Strategien und Maßnahmen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) entsprechen.

- Open Administration verarbeitet oder speichert Daten unterschiedlicher Kund:inn auf den Datenverarbeitungsanlagen in getrennten Datenbanken oder Benutzerverzeichnissen.
- Open Administration stellt dem Kund:inn eine Benutzerverwaltung bereit, um ihn bei der Implementation der Trennungskontrolle in seinem Verantwortungsbereich zu unterstützten.
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) obliegt der Kund:in.
- Die Verantwortung der Trennungskontrolle in Bezug auf Sicherheit und Updates der betriebsbereit vorgehaltenen Software obliegt Open Administration.

14.1.6 Aufzeichnung und Löschen von Videokonferenzen mit Bigbluebutton

Bei der Nutzung von Bigbluebutton sind die technisch-organisatorischen Maßnahmen von Hostsharing relevant.

14.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

14.2.1 Weitergabekontrolle

Weitergabekontrolle dient dem Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen von personenbezogenen Daten bei elektronischer Übertragung oder Transport. Open Administration realisiert die Weitergabekontrolle über folgende, mehrstufige Absicherung:

- Open Administration unterweist alle Mitarbeiter:innen, die in Kontakt mit personenbezogenen Daten kommen, nach Art. 32 Abs. 4 DS-GVO und verpflichtet sie zur Verschwiegenheit und Sicherstellung des datenschutzkonformen Umgangs mit personenbezogenen Daten.
- Open Administration stellt der Kund:inn im Umfang der Leistungsbeschreibung des Hauptauftrages Möglichkeiten zur verschlüsselten Datenübertragung zur Verfügung.
- Open Administration gewährleistet die datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

14.2.2 Eingabekontrolle

Eingabekontrolle dient der Nachvollziehbarkeit des Lesens, Kopierens, Veränderns oder Löschens von personenbezogenen Daten. Open Administration realisiert die Eingabekontrolle über folgende, mehrstufige Absicherung:

- Open Administration realisiert die Eingabekontrolle durch Aufzeichnung der durch die Open Administration-Mitarbeiter:innen beim administrativen Zugriff getätigten Eingaben.
- Die Verantwortung der Eingabekontrolle beim Zugriff mit der Auftraggeber:in überlassenen Benutzerkonten obliegt der Auftraggeber:in.

14.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

14.3.1 Verfügbarkeitskontrolle

Verfügbarkeitskontrolle dient dem Schutz personenbezogener Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust sowie der rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO). Open Administration realisiert die Verfügbarkeitskontrolle über folgende, mehrstufige Absicherung:

- Open Administration führt regelmäßig Datensicherungen der Konfigurations- und Serverdaten durch, welche auf separaten Servern in einem gesonderten Rechenzentrum an einem anderen Standort aufbewahrt werden.
- Open Administration verfügt über ein partielles (einzelne Dateien) und vollständiges (virtuelle Maschinen) Datensicherungs- und Wiederherstellungskonzept.
- Open Administration alarmiert die Mitarbeiter:innen der technische Rufbereitschaft im Fehlerfall auf zwei unabhängigen Wegen.
- Zur Ausstattung der Rechenzentren siehe die technisch-organisatorischen Maßnahmen von Hostsharing und Hetzner.

14.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Verfahren hat Open Administration folgende Konzepte implementiert:

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen werden bei der Softwareentwicklung berücksichtigt (Art. 25 Abs. 2 DS-GVO)

14.4.1 Auftragskontrolle

Verfügbarkeitskontrolle dient dem Schutz personenbezogener Daten gegen nicht weisungsgemäße, unbefugte Verarbeitung.

Die verordnungsgemäße Umsetzung der Auftragsverarbeitung gemäß Art. 28 DS-GVO, wird bei Open Administration realisiert durch eindeutige Vertragsgestaltungen, sorgfältige Auswahl der Auftragsverarbeiterin, Vorabüberzeugung und Nachkontrollen, insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen.

- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung der Verantwortlichen
- Klare, eindeutige Weisungen
- Verhinderung von Zugriffen unbefugter Dritter auf die Daten
- Verbot, Daten in unzulässiger Weise zu kopieren
- Vereinbarungen über Art des Datentransfers und deren Dokumentation
- Kontrollrechte durch den Auftraggeber
- Vereinbarung von Vertragsstrafen
- strenge Auswahl der Dienstleister
- Nachkontrollen