Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DS-GVO

bzgl. der Verarbeitung von Daten durch den DJB für einen Landesverband/Verein

Stand: 09/2024

Was dieser Auftragsverarbeitungsvertrag umfasst

1. Mit der Nutzung der DJB Mitgliederverwaltung by DokuMe ("**Hauptvertrag**") teilen Sie Daten mit uns, die wir in Ihrem Auftrag verarbeiten. Diese Bereitstellung bringt es mit sich, dass wir Zugriff auf personenbezogene Daten im Sinne der DS-GVO[1]erhalten, für die Sie als Verantwortlicher gelten, und wir diese in Ihrem Auftrag und nach Ihrer Weisung im Sinne von Art. 4 Nr. 8 und Art. 28 DS-GVO verarbeiten.
2. Zur Erfüllung der Anforderungen der DS-GVO an derartige Konstellationen schließen Sie mit uns den vorliegenden Auftragsverarbeitungsvertrag ("**AVV**"), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten in Ihrem Auftrag verarbeitet werden, sind in Anhang I aufgeführt.

Pflichten der Parteien

Weisungen

1. Wir verarbeiten personenbezogene Daten nur auf Ihre dokumentierte Weisung, es sei denn, wir sind nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem wir unterliegen, zur Verarbeitung verpflichtet. In einem solchen Fall teilen wir Ihnen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Sie können während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.
2. Wir informieren Sie unverzüglich, wenn wir der Auffassung sind, dass von Ihnen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

Zweckbindung

3. Wir verarbeiten die personenbezogenen Daten nur für den/die in Anhang I genannten spezifischen Zweck(e), sofern wir keine weiteren Weisungen von Ihnen erhalten.

Dauer der Verarbeitung personenbezogener Daten

4. Die Daten werden von uns nur für die in Anhang I angegebene Dauer verarbeitet.

Sicherheit der Verarbeitung

5. Wir ergreifen mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden "**Verletzung des Schutzes personenbezogener Daten**"). Bei der Beurteilung des angemessenen Schutzniveaus tragen Sie und wir dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
6. Wir gewähren unserem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Wir gewährleisten, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Sensible Daten

6. Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden "**sensible Daten**"), wenden wir spezielle Beschränkungen und/oder zusätzlichen Garantien an.

Dokumentation und Einhaltung der Klauseln

7. Sie und wir müssen die Einhaltung dieser Klauseln nachweisen können.
8. Wir bearbeiten Anfragen von Ihnen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
9. Wir stellen Ihnen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DS-GVO und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen von Ihnen gestatten wir ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und tragen zu einer solchen Prüfung bei.
10. Für die Überprüfung der Einhaltung unserer Pflichten können wir auf angemessene Zertifizierungen und andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO, Nachweise nach Art. 42 DSGVO, eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards. Des Weiteren können andere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Internen Revision) zum Nachweis der Einhaltung der Pflichten zur Verfügung gestellt werden.
11. Sie können die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Eine regelmäßige

Prüfung hat zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs und nur nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit zu erfolgen. Sie darf maximal einmal pro Jahr stattfinden. Ad-hoc Prüfungen, die auf einem triftigen Grund basieren, z.B. einem echten oder vermuteten Verstoß unserer Pflichten, dürfen jederzeit anlassbezogen durchgeführt werden. Die Prüfung kann auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen von uns umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

12. Wir stellen einen halben FTE (*full time equivalent*) Tag pro Jahr zur Verfügung, um unsere grundlegenden organisatorischen Aufwände im Zusammenhang mit der Prüfung abzudecken. Alle darüber hinausgehenden Aufwände und Kosten, einschließlich der uns entstehenden Kosten, sind von Ihnen zu tragen, es sei denn, wir haben im Falle einer Ad-hoc Prüfung durch eine tatsächliche Verletzung unserer Pflichten nach diesem AVV den Grund für die Ad-Hoc Prüfung gesetzt.
13. Sie und wir stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Einsatz von Unterauftragsverarbeitern

14. Wir besitzen die allgemeine Genehmigung von Ihnen für die Beauftragung von Unterauftragsverarbeitern, die in der Liste hier in Anhang III aufgeführt sind. Wir unterrichten Sie mindestens zwei (2) Wochen im Voraus ausdrücklich in Textform über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumen Ihnen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Ein Widerspruch ist nur aus wichtigem Grund möglich, z.B. wenn begründeter Anlass zu Zweifel besteht, dass der Unterauftragsverarbeiter die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt. Wir stellen Ihnen die erforderlichen Informationen zur Verfügung, damit Sie Ihr Widerspruchsrecht ausüben können.
15. Beauftragen wir einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (in Ihrem Auftrag), so muss diese Beauftragung im Wege eines Unterauftragsvertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für uns gemäß diesen Klauseln gelten. Wir stellen sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen wir entsprechend diesen Klauseln und gemäß der DS-GVO und/oder der Verordnung (EU) 2018/1725 unterliegen.
16. Wir stellen Ihnen auf Ihr Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, können wir den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
17. Wir haften gegenüber Ihnen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit uns geschlossenen Unterauftragsvertrags nachkommt. Wir benachrichtigen Sie, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.
18. Wir vereinbaren mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach Sie - im Falle, dass wir faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind - das Recht haben, den Unterauftragsvertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Internationale Datenübermittlungen

19. Jede Übermittlung von Daten durch uns an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen von Ihnen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem wir unterliegen, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.
20. Wir erklären uns damit einverstanden, dass in Fällen, in denen wir einen Unterauftragsverarbeiter für die Durchführung bestimmter Verarbeitungstätigkeiten (in Ihrem Auftrag) in Anspruch nehmen und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, wir und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem wir Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

Unterstützung

1. Wir unterrichten Sie unverzüglich über jeden Antrag, den wir von der betroffenen Person erhalten haben. Wir beantworten den Antrag nicht selbst, es sei denn, wir wurden von Ihnen dazu ermächtigt.
2. Unter Berücksichtigung der Art der Verarbeitung unterstützen wir Sie bei der Erfüllung Ihrer Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung unserer Pflichten gemäß den Ziffern 1 und 2 befolgen wir Ihre Weisungen.
3. Abgesehen von unserer Pflicht, Sie gemäß vorgenannter Ziffer zu unterstützen, unterstützen wir Sie unter Berücksichtigung der Art der Datenverarbeitung und der uns zur Verfügung stehenden Informationen zudem bei der Einhaltung der folgenden Pflichten:
    1. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden "**Datenschutz-Folgenabschätzung**"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
    2. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
    3. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem wir Sie unverzüglich unterrichtet, wenn wir feststellen, dass die von uns verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
    4. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679 oder ggf. Artikel 33 und Artikel 36 bis 38 der Verordnung (EU) 2018/1725.

1. Sie und wir legen in Anhang II die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung von Ihnen durch uns bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

Meldung von Verletzungen des Schutzes personenbezogener Daten

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeiten wir mit Ihnen zusammen und unterstützen Sie entsprechend, damit Sie Ihren Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder ggf. den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kannst, wobei wir die Art der Verarbeitung und die uns zur Verfügung stehenden Informationen berücksichtigen.

Verletzung des Schutzes der von Ihnen verarbeiteten Daten

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den von uns verarbeiteten Daten unterstützen wir Sie wie folgt:
    1. bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem Ihnen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
    2. bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 oder ggf. Artikel 34 Absatz 3 der Verordnung (EU) 2018/1725 in Ihrer Meldung anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
        1. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
        2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
        3. die von Ihnen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

    Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt

    3. bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679 oder ggf. Artikel 35 der Verordnung (EU) 2018/1725, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Verletzung des Schutzes der von uns verarbeiteten Daten

1. Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den von uns verarbeiteten Daten melden wir Ihnen diese unverzüglich, nachdem uns die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

1. eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);
2. Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;
3. die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

4. Sie und wir legen in Anhang II alle sonstigen Angaben fest, die wir zur Verfügung zu stellen haben, um Sie bei der Erfüllung von Ihren Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 oder ggf. Artikel 34 und 35 der Verordnung (EU) 2018/1725 zu unterstützen.

Verstöße gegen die Klauseln und Beendigung des AVVs

1. Falls wir unseren Pflichten gemäß diesen Klauseln nicht nachkommen, können Sie - unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 - uns anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis wir diese Klauseln einhalten oder der AVV beendet ist. Wir unterrichten Sie unverzüglich, wenn wir aus welchen Gründen auch immer nicht in der Lage sind, diese Klauseln einzuhalten.
2. Sie sind berechtigt, den AVV zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
    1. Sie die Verarbeitung personenbezogener Daten durch uns gemäß Ziffer 1 ausgesetzt haben und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
    2. wir in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstoßen oder unsere Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllen;
    3. wir einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommen.

1. Wir sind berechtigt, den AVV zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn Sie auf der Erfüllung Ihrer Anweisungen besteht, nachdem Sie von uns darüber in Kenntnis gesetzt wurden, dass Ihre Anweisungen gegen geltende rechtliche Anforderungen verstoßen.
2. Nach Beendigung des AVVs löschen wir nach Ihrer Wahl alle in Ihrem Auftrag verarbeiteten personenbezogenen Daten und bescheinigen Ihnen, dass dies erfolgt ist, oder wir geben alle personenbezogenen Daten an Sie zurück und löschen bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleisten wir weiterhin die Einhaltung dieser Klauseln.

Schlussbestimmungen

Über diesen AVV

1. Die Regelungen dieses AVVs gehen im Zweifel den Regelungen des Hauptvertrags vor.
2. Sollten einzelne Bestimmungen dieses AVVs ganz oder teilweise nichtig oder unwirksam sein oder werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle von nicht einbezogenen oder unwirksamen Bestimmungen dieses AVVs tritt das Gesetzesrecht. Sofern solches Gesetzesrecht im jeweiligen Fall nicht zur Verfügung steht (Regelungslücke) oder zu einem mit dem Willen der Parteien erkennbar nicht vereinbaren Ergebnis führen würde, werden Sie und wir uns bemühen, anstelle der nicht einbezogenen oder unwirksamen Bestimmung eine wirksame Regelung zu vereinbaren, die ihr

wirtschaftlich möglichst nahe kommt.

Aktualisierungen und Änderungen

3. Wir behalten uns vor, diesen AVV für unsere digitalen Inhalte gegebenenfalls zu aktualisieren, um (i) Änderungen unserer Leistungen oder unserer Geschäftsabläufe widerzuspiegeln, beispielsweise, wenn wir neue Dienste, Funktionen, Technologien, Preise oder Vorteile hinzufügen (oder alte entfernen); (ii) aus rechtlichen, regulatorischen oder Sicherheitsgründen oder (ii) um Missbrauch oder Schaden zu verhindern.
4. Wenn wir diesen AVV ändern, informieren wir Sie mindestens 14 Tage vor dem Inkrafttreten der Änderungen. Mit der Information über die Änderungen stellen wir Ihnen die neue Version dieses AVVs zur Verfügung und weisen Sie auf wesentliche Änderungen hin. Wenn Sie nicht vor Inkrafttreten der Änderungen widersprechen, gilt der geänderte AVV als akzeptiert. Sie können die Annahme der Änderungen verweigern - in diesem Fall finden die Änderungen im Verhältnis zu Ihnen keine Anwendung. Wir behalten uns in diesem Fall das Recht vor, diesen AVV fristlos zu beenden.

Geltendes Recht und Gerichtsstand

5. Dieser AVV und jegliche Streitigkeiten aus oder im Zusammenhang mit diesem AVV unterliegen dem Recht des Hauptvertrags.
6. Zum Gerichtsstand für Streitigkeiten oder Meinungsverschiedenheiten aus oder im Zusammenhang mit diesem AVV gelten die Vereinbarungen aus dem Hauptvertrag. Dies gilt nicht, sofern eine anderweitige zwingende ausschließliche gesetzliche Zuständigkeit besteht.

Anhang I

Beschreibung der Verarbeitung

1. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:

- Nutzer;
- Mitglieder;
- Inhaber;
- Beschäftigte;
- Partner;
- Teilnehmer bei Veranstaltungen;
- Ansprechpartner;
- Interessenten.

2. Kategorien personenbezogener Daten, die verarbeitet werden:

- Personenstammdaten (z.B. Vor- und Nachname, Geburtstag, Geschlecht, Nationalität, Adresse, Lichtbild);

- Kommunikationsdaten (z.B. E-Mail-Adressen, Telefon);
- Mitgliedsdaten (z.B. Lizenz-/Mitgliedsnummer, Graduierung, Verein);
- Kundenhistorie (z.B. E-Mails, Dokumente, Rechnungen, Quittungen);
- Vertragsabrechnungs- und Zahlungsdaten;
- Planungs- und Steuerungsdaten (z.B. Bearbeitungsstatus, zu erledigende Aufgaben);
- Digitale Inhalte spezifische Kategorien von personenbezogenen Daten (in der Regel von Ihnen im Rahmen des jeweiligen digitalen Inhalts definierbar).

3. Kategorien sensiblen Daten, die verarbeitet werden:

- Personenbezogene Daten von Kindern mit Einwilligung oder Zustimmung durch den Träger der elterlichen Verantwortung für das jeweilige Kind;
- Besondere Kategorien von personenbezogenen Daten:
  - Biometrische Daten (z.B. Fingerabdruck für Login) als Authentifizierungsmittel bei Nutzung elektronischer Mittel, z.B. Mobiltelefon;
  - Gesundheitsdaten (z.B. Sportverletzungen) als Teil besonderer digitaler Inhalte;

- Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln (z.B. Strafregisterauszug) zur Überprüfung der Geeignetheit einer Person für ein bestimmtes Amt;
- Digitale Inhalte spezifische Kategorien von sensiblen Daten (in der Regel von Ihnen im Rahmen des jeweiligen digitalen Inhalts definierbar).

1. Art der Verarbeitung:

- Ergibt sich aus dem Hauptvertrag und den aktivierten Abonnements über digitale Inhalte.

5. Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden:

- Ergibt sich aus dem Hauptvertrag und den aktivierten Abonnements über digitale Inhalte.

6. Dauer der Verarbeitung:

- Entspricht der Laufzeit des Hauptvertrags bzw. den relevanten Abonnements über digitale Inhalte.

Anhang II

Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten

Vertraulichkeit (Art. 32 Abs. 1 DSGVO)

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen. Diese genannten technischen und organisatorischen Maßnahmen werden aufgrund der Cloud-Infrastruktur von uns im Auftrag und unter Kontrolle durch Unterauftragnehmer durchgeführt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Manuelles Schließsystem	☒ Schlüsselregelung / Liste
☒ Türen mit Knauf Außenseite	☒ Besucherbuch / Protokoll der Besucher
☒ Sicherheitsschlösser	☒ Mitarbeiter- / Besucherausweise
	☒ Besucher ausschließlich in Begleitung durch Mitarbeiter
	☒ Sorgfalt bei Auswahl Reinigungsdienste

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen

☒ Firewall	☒ Erstellen von Benutzerprofilen
☒ Intrusion Detection Systeme	☒ Richtlinie „Sicheres Passwort“
☒ Einsatz VPN bei Remote-Zugriffen	☒ Richtlinie „Löschen / Vernichten“
	☒ Richtlinie „Clean desk“
	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Einsatz Berechtigungskonzepte
☒ Funktion zur Beschränkung von Zugriffsrechten	☒ Minimale Anzahl an Administratoren
	☒ Verwaltung Benutzerrechte durch Administratoren

4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen

☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ Mandantenfähigkeit relevanter Anwendungen	

5. **Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) / Anonymisierung (Erwägungsgrund 26 DSGVO)**

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe zu anonymisieren / pseudonymisieren oder auch nach Ablauf der gesetzlichen Aufbewahrungsfrist zu löschen / anonymisieren

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

1. **Weitergabekontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	

☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

2. **Eingabekontrolle**

Maßnahmen zur Feststellung, ob, wann und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind, sowie die diesbezügliche Dokumentation zum Zwecke der Revertierung.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Eingabe von Daten nur durch authentifizierte Accounts mit definierten Rechten. Rollen und Rechte werden von Ihnen individuellen Accounts zugewiesen	☒ Darstellung des jeweils agierenden Accounts bei Veränderung und Löschung von Daten im Datenverarbeitungssystem inkl. Protokollierung des Datums und Uhrzeit.
☒ Protokollierung und Dokumentation jeglicher Datenverarbeitungssystem Eingaben, Modifikationen und Entfern-Operationen	☒ auf Anfrage kann das Protokoll der Datenverarbeitungssysteme bereitgestellt werden

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b & c DSGVO)

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc. Diese genannten technischen und organisatorischen Maßnahmen werden aufgrund der Cloud-Infrastruktur von uns im Auftrag und unter Kontrolle durch Unterauftragnehmer durchgeführt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Schutzprogrammen (Bspw. Virenscanner, Spamfilter, E-Mail Fraud Prevention)	☒ Datensicherungs- und Wiederherstellungskonzepte
☒ Überwachung und Monitoring relevanter Systeme	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums (anderer Hosting Unterauftragnehmer)
☒ Einsatz unterbrechungsfreier	☒ Getrennte Partitionen für Betriebssysteme

Stromversorgung bei der Serverinfrastruktur	und Daten
☒ Aktiver und dauerhafter DDoS-Schutz	☒ Interne Anweisung, Datensicherungs- und Wiederherstellungskonzepte zu kontrollieren
☒ Vorhaltung von Ersatzhardware	☒ Rasche Wiederherstellbarkeit nach Art. 32 Abs. 1 lit. C DSGVO: Eskalationskette für alle internen Systeme, um im Fehlerfall Informationsfluss und Wiederherstellung zu gewährleisten

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

1. **Datenschutz-Management**

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Privacy by design / Privacy by default Lösung	☒ externer Datenschutzbeauftragter Lisa Hofmann, Pridatect S.L., Av. de Josep Tarradellas 123, Planta 6 08029 Barcelona (Spanien), E-Mail: privacy@dokume.net
	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	☒ Regelmäßige Sensibilisierung der Mitarbeiter (Mindestens jährlich)
	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

	☒ Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet)
	☒ Privacy by design / Privacy by default Richtlinie

2. **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)**

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Privacy by design / Privacy by default Lösung	☒ externer Datenschutzbeauftragter Lisa Hofmann, Pridatect S.L., Av. de Josep Tarradellas 123, Planta 6 08029 Barcelona (Spanien), E-Mail: privacy@dokume.net
	☒ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet

3. **Auftragskontrolle (Outsourcing an Dritte)**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend Ihren Weisungen verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern wir Dienstleister im Sinne einer Auftragsverarbeitung einsetzen, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der von uns getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl durch uns unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung mit den Garantien zu Datenübermittlungen in Drittstaaten, falls

	anwendbar.
	☒ Recht zur Auditierung von Auftragsverarbeitern und Unterauftragnehmer
	☒ Weisungsgebundenheit von uns
	☒ Verpflichtung der Mitarbeiter von uns auf Datengeheimnis
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch uns bei Vorliegen einer Bestellpflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber uns
	☒ Regelung zum und Kontrolle des Einsatzes weiterer Sub-Unternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung von uns und unseres Schutzniveaus

Anhang III

Liste der Unterauftragsverarbeiter

Sie haben uns die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

Name	Anschrift	Beschreibung der Verarbeitung

DokuMe GmbH	Subbelrather Str. 436c, 50825 Köln, Deutschland	Bereitstellung der DJB DokuMe Plattform

[1] **Verordnung (EU) 2016/679** des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), in der jeweils geltenden Fassung.