Auftragsverarbeitungsvereinbarung

Stand: 12. März 2024

Zwischen Partei 1	und Partei 2
	bardohn GmbH Kleine Johannisstraße 6 20457 Hamburg
(Auftraggeber)	(Auftragnehmer)

Auftraggeber und Auftragnehmer werden nachfolgend gemeinsam als “Parteien“ und jeweils einzeln auch als “Partei” bezeichnet.

Präambel

A. Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Business Intelligence Lösungen auf Cloudbasis gemäß dem Vertrag über die Nutzung des opensubs-BI (im Folgenden: „Hauptvertrag“).

B. Im Rahmen der Durchführung des Hauptvertrags kommt es zur Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung („DSGVO“). Zur Erfüllung der Anforderungen der DSGVO schließen die Parteien diesen Vertrag, dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

1. Gegenstand und Dauer des Auftrags, Zweck der Verarbeitung

1.1. Die Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages bringt es mit sich, dass der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend „Auftraggeberdaten“) erhält und diese ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO verarbeitet.

1.2. Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt ausschließlich in der im Hauptvertrag beschriebenen Art sowie in dem dort spezifizierten Umfang und Zweck. Dem Auftragnehmer ist eine abweichende Verarbeitung von Auftraggeberdaten untersagt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

1.3. Es werden Daten der folgenden betroffenen Personengruppen verarbeitet:

- Kunden/Abonnenten des Auftraggebers

1.4. Es werden Daten der folgenden Kategorien verarbeitet:

- Personenstammdaten (nämlich, jeweils soweit in den Quelldaten erfasst: Kundennummern, Anrede, Vorname, Nachname, Firmenname, Email, Straße, Hausnummer, Postfach, Postleitzahl, Ort, Land, Telefonnummer, Geburtsdatum, Umsatzsteuer-ID, Quelle der Registrierung, Datum der Registrierung, Kundenstatus, Sprache, Validierungsstatus der zugehörigen Adresse)
- Marketing-Optins
- Auftragsdaten (vor allem: Bestellungen inklusive bestellter Produkte und Angebote, Bestellquellen und genutzter Marketingaktionen, Abonnementdaten inklusive Start- und Enddaten sowie Kündigungszeitpunkte und Failed Payments)
- Rechnungsdaten (vor allem: Rechnungsnummern, Rechnungsbeträge, Zahlstatus, Zahlungsart)
- Daten der Kundenkommunikation (vor allem: Informationen zu Reklamationen, Kündigungsgründen, sonstigen Service-Anfragen)
- Daten zur Produktnutzung (nämlich: Login-Zeitpunkte und -häufigkeiten)

1.5. Die Verarbeitung der Auftraggeberdaten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind.

2. Weisungsbefugnisse des Auftraggebers

2.1. Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Beauftragung und ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne des Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber hat insoweit das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch „Weisungsrecht“).

2.2. Weisungen werden vom Auftraggeber grundsätzlich schriftlich oder in Textform erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer wenigstens in Textform zu bestätigen. Die weisungs- und empfangsberechtigten Personen stimmen die Parteien gemeinsam ab.

2.3. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

3. Schutzmaßnahmen des Auftragnehmers

3.1. Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen zum Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

3.2. Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden „Mitarbeiter“ genannt), in Schriftform zur Vertraulichkeit verpflichten.

3.3. Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gemäß Art. 32 DSGVO, insbesondere die in Anlage 1 aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrechtzuerhalten.

3.4. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.5. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der in Anlage 1 bestimmten technischen und organisatorischen Maßnahmen durch geeignete Nachweise nachweisen.

4. Informations- und Unterstützungspflichten des Auftragnehmers

4.1. Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte im Zusammenhang mit der vertragsgegenständlichen Datenverarbeitung wird der Auftragnehmer den Auftraggeber unverzüglich informieren.

4.2. Der Auftragnehmer wird den Auftraggeber in den vorgenannten Fällen bei der Erfüllung seiner diesbezüglichen Aufklärungs-, Abhilfe – und Informationsmaßnahmen im Rahmen des Zumutbaren unterstützen. Der Auftragnehmer wird insbesondere erforderliche Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen durchführen, den Auftraggeber hierüber informieren und diesen um weitere Weisungen ersuchen.

4.3. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle erforderlich sind.

5. Sonstige Verpflichtungen des Auftragnehmers

5.1. Der Auftragnehmer ist verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gemäß Art. 30 Abs. 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

5.2. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Daten-schutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen. Entsprechende Leistungen kann der Auftragnehmer nach Aufwand zu den vereinbarten Vergütungssät-zen berechnen.

5.3. Der Auftragnehmer bestätigt, dass er, soweit eine gesetzliche Verpflichtung hierzu besteht, einen Datenschutzbeauftragten bestellt hat.

5.4. Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder

durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

6. Unterauftragsverarbeiter

6.1. Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 2 genannten Dienstleister (“Unterauftragsverarbeiter”) durchgeführt. Der Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.

6.2. Der Auftragsverarbeiter wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichen Grund Einspruch erheben.

6.3. Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters ist innerhalb von 2 Wochen nach Erhalt der Information über die Änderung zu erheben. Wird kein Einspruch erhoben, gilt die Hinzuziehung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen dem Verantwortlichen und dem Auftragsverarbeiter nicht möglich, steht dem Auftragsverarbeiter ein Sonderkündigungsrecht zum auf den Einspruch folgenden Monatsende zu.

6.4. Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

6.5. Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und

Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

7. Kontrollrechte

7.1. Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen, zu überzeugen. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizie-rungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach vorheriger Ankündigung zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen las-sen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

7.2. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und angemessene Rücksicht auf die Betriebsabläufe des Auftragnehmers nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

7.3. Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

8. Rechte Betroffener

8.1. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung von dessen Pflichten nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO. Er wird dem Auftraggeber die gewünschte Auskunft über Auftraggeberdaten geben, sofern der Auftragnehmer nicht selbst über die entsprechenden Informationen verfügt.

8.2. Macht der Betroffene seine Rechte gemäß Art. 16 bis 18 DSGVO geltend, ist der Auftragnehmer dazu verpflichtet, die Auftraggeberdaten auf Weisung des Auftraggebers zu berichtigen, zu löschen oder einzuschränken. Der Auftragnehmer wird dem Auftraggeber die

Löschung, Berichtigung bzw. Einschränkung der Daten auf Verlangen schriftlich nachweisen.

8.3. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

8.4. Leistungen, die der Auftragnehmer im Rahmen seiner Pflichten gemäß dieser Ziffer 8 erbringt, kann er nach Aufwand zu den vereinbarten Vergütungssätzen berechnen, wenn sie insgesamt ein Volumen von vier Zeitstunden pro Kalenderquartal übersteigen.

9. Laufzeit und Kündigung

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

10. Löschung und Rückgabe nach Vertragsende

10.1. Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen.

10.2. Der Auftragnehmer wird dem Auftraggeber nach Anfrage die Löschung schriftlich bestätigen. Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

10.3. Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen personenbezogenen Daten vertraulich zu behandeln.

11. Haftung

Die Haftung der Parteien im Innenverhältnis richtet sich nach den Regelungen des Hauptvertrags.

12. Schlussbestimmungen

12.1. Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer im Sinne des § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

12.2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Die Schriftform kann durch die Textform eingehalten werden, wenn das Schriftformerfordernis in dieser Vereinbarung nicht ausdrücklich auf § 126 Abs. 1 BGB verweist.

12.3. Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

12.4. Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Hamburg.

Anlagen

Anlage 1: Technische und organisatorische Maßnahmen
Anlage 2: Subunternehmer

Anlage 1

Technische und organisatorische Maßnahmen gemäß Art. 28 Abs. 3 S.2 lit. c i.V.m. Art. 32, Art. 30 Abs. 2 lit. d und g DS-GVO

1. Sicherstellung der Rechtmäßigkeit der Datenverarbeitung

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele Vertraulichkeit, Transparenz, Zweckbindung, Datenminimierung, Nichtverkettbarkeit und Authentizität sicherstellen. Dabei sind auch die Rechte der betroffenen Personen auf Information und nach Art. 7 Abs. 3, 15 ff. DS-GVO sicherzustellen, einschließlich der Schadensminimierungsmaßnahmen und Informationsverpflichtungen gegenüber der Verantwortlichen.

- ☑ Alle Mitarbeitenden sind über eine Dienstanweisung auf die besondere Sensibilität des Umgangs mit datenschutzrechtlich relevanten Kundendaten hingewiesen worden.
- ☑ Es liegt ein fortlaufend aktualisiertes Berechtigungskonzept vor, das sicherstellt, dass nur die Mitarbeitenden und auch nur im jeweils erforderlichen Umfang auf die für ihre Aufgabenerfüllung erforderlichen Daten Zugriff erlangen.

- ☑ Eine über den Auftragsverarbeitungsvertrag hinausgehende Verarbeitung im eigenen Interesse des Auftragnehmers findet derzeit nicht statt, wird den betroffenen Personen in einem solchen Fall aber transparent bekannt gemacht.
- ☑ Eine Übertragung von personenbezogenen Daten auf private Endgeräte oder Systeme ist technisch und / oder organisatorisch unterbunden.

- ☑ Datenschutzfreundliche Voreinstellungen der eingesetzten Systeme zur Datenverarbeitung, insbesondere durch eine umfangreiche Pseudonymisierung von personenbezogenen Daten.
- ☑ Ein Lösch- / Sperrkonzept liegt vor: Nicht mehr erforderliche Daten werden gelöscht oder gesperrt.

---

2. Zutrittskontrolle

Diese Maßnahmen sollen die Einhaltung der Gewährleistungsziele der Vertraulichkeit, Rechtmäßigkeit, Transparenz, Integrität, Intervenierbarkeit sowie der Nichtverkettbarkeit sicherstellen. Sie betreffen vorrangig Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Gebäuden und Räumen, in denen Daten / Datenträger aufbewahrt werden, oder Datenverarbeitungsanlagen, mit denen schützenswerte Daten verarbeitet oder genutzt werden, enthalten sind, zu verwehren bzw. zu detektieren.

Als Maßnahmen zur Zutrittskontrolle können unter anderem automatische Zutrittskontrollsysteme wie Schließsysteme mittels Chipkarten und Transpondern, Kontrolle des Zutritts durch Pförtnerdienste und, ergänzend dazu, Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschlossenen Schränken (Racks) zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit oder auch das Schließen von Fenstern vorsieht) zu stützen.

- ☑ Die Schlüsselvergabe zu Büroräumen erfolgt nur an ausgewählte vertrauenswürdige Personen, Inhaber der Schlüssel sind dokumentiert.
- ☑ Dienstanweisung zum Verschließen von Räumen bei Abwesenheit.

- ☑ Die zugangsberechtigten Personen zur Verfügung gestellten Schlüssel werden personengebunden registriert und die Schlüsselausgabe quittiert.
- ☑ Geordneter Prozess zur Vergabe und zum Entzug von Zutrittsrechten

---

- ☑ Elektronisch gesichertes Zutrittssystem mit der Möglichkeit der Sperrung einzelner Schlüssel.

---

3. Zugangskontrolle

Diese Maßnahmen sollen die Einhaltung der Gewährleistungsziele der Vertraulichkeit, Verfügbarkeit, Authentizität, Rechtmäßigkeit, Transparenz. Integrität, Intervenierbarkeit sowie der Nichtverkettbarkeit sicherstellen. Sie betreffen in Abgrenzung zur Zutrittskontrolle den Zugang zu Daten und Datenträgern direkt. Um

Unbefugten den Zugang zu Daten oder Datenträgern zu verwehren ist mindestens eine Authentifizierung am System vorzusehen.

Möglichkeiten der Zugangskontrolle sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, automatische Sperre des Bildschirms nach einer angemessenen Spanne von Inaktivität, Verpflichtung der Nutzenden, dessen ungeachtet auch manuell den Bildschirm zu sperren, wenn der Arbeitsplatz verlassen wird oder der Einsatz von Chipkarten zur Anmeldung. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern z. B. Dienstanweisungen zur sichtgeschützten Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl von Passwörtern oder dergleichen.

- ☑ Mitarbeiter arbeiten ausschließlich mit personalisiert angelegten Benutzerprofilen.
- ☑ Dienstanweisung zum sicheren Umgang mit mobilen Datenträgern und Geräten sowie der Anlage von und dem Umgang mit Passwörtern.
- ☑ Der Zugang zu IT-Systemen erfolgt mit angemessenem Passwortschutz, der der Sensitivität der verarbeiteten Daten entspricht.
- ☑ Soweit es für den jeweiligen Zweck ausreichend ist, ist der Zugang zu schützenswerten Daten pseudonymisiert.
- ☑ Die Verschlüsselung der Daten erfolgt durch die Services der eingesetzten Subdienstleister (insbesondere Microsoft) nach dem aktuellen Stand der Technik.
- ☑ Schutzsoftware (z. B. Anti-Schadsoftware-Lösungen, Firewalls etc.) wird dem Stand der Technik entsprechend eingesetzt.

4. Zugriffskontrolle

Die Maßnahmen sollen die Einhaltung der Gewährleistungsziele: Vertraulichkeit, Transparenz, Rechtmäßigkeit, Integrität, Authentizität und Intervenierbarkeit gewährleisten.

Sie sollen gewährleisten, 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. Weiterhin sind geeignete Prozesse, Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den

Entzug der Berechtigungen zu dokumentieren und auf dem 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 Benutzerkonten mit erhöhten Berechtigungen (Administratorinnen und Administratoren) zu richten.

- ☑ Der Zugriff auf personenbezogene Daten wird intern abgestuft und nach der jeweiligen Aufgabe eines Mitarbeiters vergeben.
- ☑ Dienstanweisung, die vorsieht, dass Datenanzeigen vor Sichtung durch Unbefugte zu schützen sind, und der Arbeitsplatz durch eine passwortgeschützte Bildschirmsperre für Unbefugte zu sperren ist.

- ☑ Die Daten des Kunden sowie deren Übermittlung werden standardmäßig verschlüsselt. Für die eingesetzten Microsoft-Dienste gilt hierfür der „Datenschutznachtrag zu den Produkten und Services von Microsoft“, für Dropbox das Dokument „Dropbox Business Security“ in seiner jeweiligen Fassung.

---

5. Trennungskontrolle

Die Maßnahmen sollen primär sicherstellen, dass die Gewährleistungsziele der Transparenz, der Rechtmäßigkeit / Erforderlichkeit sowie der Nichtverkettbarkeit von personenbezogenen Daten eingehalten werden.

Schützenswerte Daten anderer Auftraggeber oder die zu eigenen Zwecken verarbeiteten Daten sind von denen, die im Rahmen dieses Auftragsverarbeitungsvertrages verarbeitet werden, zu trennen.

Zu unterschiedlichen Zwecken erhobene Daten sollen getrennt verarbeitet werden. Insbesondere sollen schützenswerte Daten des Auftraggebers nicht nachteilig von Datenschutz- oder Sicherheitsvorfällen betreffend die Daten des Auftragnehmers oder anderer Kunden in Mitleidenschaft gezogen werden. Dieses kann beispielsweise durch logische oder physikalische Trennung der Daten gewährleistet werden. Jeder Versuch einer nicht gerechtfertigten Re-Identifizierung von pseudonymen Daten ist technisch und / oder organisatorisch zu unterbinden. So sollte zum Beispiel kein Kontakt zu betroffenen Personen hergestellt werden.

- [x] Mandantentrennung in den eingesetzten Systemen.
- [x] Trennung von Test- und Produktionsdaten.
- [x] Durch ein Berechtigungskonzept ist organisatorisch und technisch sichergestellt, dass Zugriffe auf Dateien nur durch dazu befugte Personen und nur im jeweils erforderlichen Umfang erfolgt.
- [x] Dienstanweisung zum Verbot der Datenübertragung auf private Endgeräte oder Datenträger.
- [x] Umfangreiche Pseudonymisierung aller personenbezogenen Daten, die nicht im Klartext benötigt werden. Der De-Pseudonymisierungsschlüssel liegt ausschließlich in Systemen des Kunden

6. Weitergabekontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der Verfügbarkeit, der Vertraulichkeit, der Rechtmäßigkeit / Erforderlichkeit, Transparenz, Verfügbarkeit, Intervenierbarkeit sowie der Nichtverkettbarkeit gewährleisten. Personenbezogene Daten dürfen nicht an unbefugte Personen weitergegeben werden.

Bei der Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern dürfen diese nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss überprüft und festgestellt werden können, an welchen Stellen eine Übermittlung personenbezogener Daten erfolgt.

Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken (z. B. Virtual Private Network, VPN) eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

- [x] Der Zugriff auf personenbezogene Daten wird intern abgestuft und nach der jeweiligen Aufgabe eines Mitarbeiters vergeben.
- [x] Mitarbeiter arbeiten ausschließlich mit personalisiert angelegten, passwortgeschützten Benutzerprofilen.

- [x] Die Daten des Kunden sowie deren Übermittlung werden standardmäßig verschlüsselt. Für die eingesetzten Microsoft-Dienste gilt hierfür der „Datenschutznachtrag zu den Produkten und Services von Microsoft“, für Dropbox das Dokument „Dropbox Business Security“ in ihrer jeweils aktuellen Fassung.
- [x] Dienstanweisung zum Verbot der Datenübertragung auf private Endgeräte oder Datenträger.

7. Eingabekontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der, Integrität, Richtigkeit, Rechtmäßigkeit / Transparenz, Authentizität, Verfügbarkeit gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Ereignisse protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass / Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfinden muss.

- [x] Berechtigungskonzept unterscheidet mindestens in Lese- und Schreibrechte.
- [x] Eine Eingabe von nicht berechtigten Personen ist ausgeschlossen:
  - [x] technisch
  - [x] organisatorisch
- [x] Änderungen und Löschungen von Dateien in elektronischen Datenverarbeitungssystemen werden protokolliert.

8. Verfügbarkeitskontrolle

Die Maßnahmen sollen primär die Einhaltung der Gewährleistungsziele der Verfügbarkeit, Transparenz und Intervenierbarkeit gewährleisten. Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust geschützt sein. Dazu gehören Maßnahmen zum Diebstahlschutz, unterbrechungsfreie Stromversorgungsanlagen, Klimaanlagen, Brandschutzmaßnahmen, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

- ☑ Backup- und Wiederherstellungskonzept nach dem Stand der Technik.
- ☑ Regelmäßige stichprobenartige Verfügbarkeitskontrollen für Datenträger.
- ☑ Vorkehrungen zur Wiederherstellung entsprechend „Datenschutznachtrag zu den Produkten und Services von Microsoft“ und „Dropbox Business Security“ in ihrer jeweils aktuellen Fassung.

9. Datenschutz-Management

Die Maßnahmen sollen die angemessene Umsetzung aller datenschutzrechtlichen Gewährleistungsziele bei dem Auftragnehmer sicherstellen. Auf Anfrage ist der Auftraggeber berechtigt, beleghafte Informationen zu den konkreten Maßnahmen zu erhalten, vgl. Haupt-AV-Vertrag.

- ☑ Vorliegen eines datenschutzkonformen Lösch- / Sperrkonzeptes.
- ☑ Testverfahren für neue Verarbeitungstätigkeiten sind implementiert und finden nachvollziehbar statt.
- ☑ Führen eines Verzeichnisses von Verarbeitungstätigkeiten.
- ☑ Administratives Personal für Passwortverwaltung ist benannt und auf das notwendige Maß reduziert.

- ☑ Richtlinien zum Umgang mit der Wahrung der Rechte und Freiheiten betroffener Personen welche berücksichtigen
  - ☑ Eine rechtzeitige Information des Auftraggebers über Datenschutz- oder Informationssicherheitsvorfälle ist sichergestellt. Auch Verdachtsfälle sind unverzüglich zu melden.
  - ☑ Richtlinien / Arbeitsanweisungen zum Umgang mit meldepflichtigen Datenpannen.

10. Auftragskontrolle (Outsourcing an Dritte)

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Daher erfolgt keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch folgende Mindestanforderungen:

- ☑ Eindeutige Vertragsgestaltung.
- ☑ Formalisiertes Auftragsmanagement.
- ☑ Sicherstellung der Datenspeicherung in Europa.

Anlage 2

Subunternehmer

Der Auftraggeber hat der Einbindung der folgenden Subunternehmer/ Unterauftragsverarbeiter zugestimmt:

	Subunternehmer	Leistungsort	Leistung	Weiteres
1	Microsoft Ireland Operations Ltd (verbundenes Unternehmen der Microsoft Corporation, USA)	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Cloudservices	Datenschutz-Nachtrag für Microsoft-Produkte in ihrer jeweils gültigen Form: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14
2	Dropbox International Unlimited Company	One Park Place, Floor 6, Hatch Street Upper Dublin 2	Cloudservices	Datenspeicherung erfolgt auf Servern in der Europäischen Union. Aktuelle Fassung der Dropbox-Datenschutzrichtlinie: https://www.dropbox.com/privacy und ergänzend https://assets.dropbox.com/www/en-us/business/solutions/solutions/dfb_security_whitepaper.pdf
3	Kern.ai	Gerhart-Hauptmann-Allee 71, 15732 Eichwalde	Cloudservices	
4	elbcloud Tech Solutions GmbH	Von-Essen-Straße 76, 22081 Hamburg	IT-Wartung	AVV vom 22.02.2024