Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung (EU-DSGVO) nach Art. 28 - 29 (AV-Vertrag)

Vereinbarung

zwischen der

Auftraggeber: _____

Straße.....: _____

LKZ: ____ PLZ:_____ ORT : _____

- nachstehend Auftraggeber genannt (AG) –

und der

BSD-GmbH - Wandalenweg 26 D-20097 Hamburg

- nachstehend Auftragnehmer genannt (AN) -

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.
Der vorliegende Auftragsverarbeitungsvertrag einschließlich seiner Anhänge (im Folgenden „AV-Vertrag“) konkretisiert die ab Mai 2018 neu geltenden datenschutzrechtlichen Verpflichtungen der Vertragsparteien unter Berücksichtigung der Anforderungen nach Art. 28 der EU-Datenschutz-Grundverordnung (im Folgenden „DS-GVO“). Er ersetzt die bis dahin geltenden Vereinbarungen zur Auftragsdatenverarbeitung und findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen, und bei denen durch den Auftragnehmer eingesetzte Personen personenbezogene Daten für den Auftraggeber und/oder dessen Kunden verarbeiten. Begriffsbestimmungen: Die in diesem AV-Vertrag verwendeten Begriffe wie z.B. „personenbezogene Daten“, „Verarbeitung“, „Verantwortlicher“, „Auftragsverarbeiter“ oder „betroffene Person“ entsprechen den Begriffsbestimmungen der DS-GVO, soweit in diesem AV-Vertrag keine anderweitigen Definitionen enthalten sind. Mit „Daten des Auftraggebers“ sind im Folgenden ausschließlich solche personenbezogenen Daten des Auftraggebers sowie auch seiner Kunden gemeint, die im Zusammenhang mit dem Hauptvertrag überlassen oder erhoben wurden bzw. werden. „Rechtliche Rahmenbedingungen“ sind alle einschlägigen (i) Gesetze und Verordnungen, (ii) rechtskräftigen Entscheidungen von Gerichten der Bundesrepublik Deutschlands und des Europäischen Gerichtshofs sowie (iii) behördliche Vorschriften, Anordnungen, Bekanntmachungen, Richtlinien, Leitlinien, Orientierungshilfen und sonstige aufsichtsrechtliche Anforderungen, einschließlich solche der Artikel 29 Datenschutzgruppe bzw. des Europäischen Datenschutzausschusses.

Inhalt:

1.1 Gegenstand des Auftrags

Gegenstand des Auftrags

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

☐ Dokumenten - Scanning im Onlineverfahren
☐ Dokumenten - Scanning im Offlineverfahren

☐ Automatische - Erkennung von gescannten Dokumenten
☐ Automatische - Datenerfassung – von gescannten Dokumenten

☐ Manuelle-Datenerfassung im Onlineverfahren
☐ Manuelle-Datenerfassung im Offlineverfahren
☐ Manuelle-Prüfdatenerfassung im Onlineverfahren
☐ Manuelle-Prüfdatenerfassung im Offlineverfahren

☐ Call Center Dienstleistungen Inbound
☐ Call Center Dienstleistungen Outbound
☐ Call Center Dienstleistungen im Onlineverfahren
☐ Call Center Dienstleistungen im Offlineverfahren

☐ Servicerufnummern Dienstleistung

☐ Versand: von Briefen / Lettershop Dienstleistungen
☐ Druck: Farbe / Lettershop Dienstleistungen
☐ Druck: S/W / Lettershop Dienstleistungen
☐ Empfang: Ver-/Bearbeitung von Briefen / Lettershop Dienstleistungen

☐ Versand: von Faxen / Lettershop Dienstleistungen
☐ Empfang: Ver-/Bearbeitung von Faxen / Lettershop Dienstleistungen

☐ Versand: von Emails / Lettershop Dienstleistungen
☐ Empfang: Ver-/Bearbeitung von Emails / Lettershop Dienstleistungen

☐ Versand: von SMS oder MMS / Lettershop Dienstleistungen
☐ Empfang: Ver-/Bearbeitung von SMS oder MMS/ Lettershop Dienstleistungen

☐ Belegarchivierung im Onlineverfahren
☐ Belegarchivierung im Offlineverfahren

☐ Hardcopy Originalbelegarchivierung im BSD Archivlager

☐ Manuelle-Qualitätsprüfung im Offlineverfahren
☐ Manuelle-Qualitätsprüfung im Onlineverfahren

☐ Originalbelegvernichtung nach ____ Monaten mit der

Firma: _____ Zertifikatsnummer: _____

☐ Programmierdienstleistungen im Offlineverfahren
☐ Programmierdienstleistungen im Onlineverfahren
☐ Hardware/Software Erstellung-Verkauf
☐ Sonst bitte beschreiben wenn hier nicht aufgeführt!

Art: Die BSD-GmbH erfasst und speichert Kundendaten im Auftrag des Auftraggebers

*Onlineverfahren (System des Auftraggebers)
*Offlineverfahren (System des Auftragnehmers)

1.2 Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung/ des Vertrages. Die Verarbeitung beginnt am ___.___.20___ und endet am ___.___.20___ .

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt. oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum _____ und verlängert sich automatisch um jeweils 12 Monate, sofern nicht eine der beiden Parteien mit einer Frist von ___ Monaten den Vertrag aufkündigt.

2. Konkretisierung des Auftragsinhalts

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.
Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der EU-DSGVO erfüllt sind.

Die Verarbeitung dient folgendem Zweck: _____

Die Daten werden von der BSD-GmbH zur Arbeitserleichterung für den Auftraggeber in eine Datenbank - mittels einer Software eingespeist, damit der Auftraggeber effizient das Alltagsgeschäft mit den Kunden und Interessenten abwickeln kann. - Die Dokumente, werden nach der Bearbeitung entweder zur Archivierung an den Auftraggeber zurück geliefert, oder von der Mammut GmbH vernichteten.

Hierbei gilt mindestens Schutzklasse: _____

Stufe	**Personenbezogene Daten,**	**zum Beispiel**
A:	die frei zugänglich sind. Der Einsichtnehmende muss dabei kein berechtigtes Interesse geltend machen.	Telefonbücher, Adressbücher, Wahlvorschlagsverzeichnisse
B:	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse der Einsichtnehmenden gebunden ist.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen
C:	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen").	Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten
D:	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträch-tigen könnte („Existenz").	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Gesundheitsdaten, Schulden, Pfändungen
E:	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können

zu 2. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien)

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten **(Zutreffendes bitte Unterstreichen)**

☐ Firmen-Stammdaten

☐ Privatpersonen-Stammdaten

☐ Bank bezogene Stammdaten

☐ Kommunikationsdaten (z.B. Telefon, E-Mail, Sozialnetwork) / Call Center

☐ Kundendaten zur Aufnahme und dem Versand von Briefen / Lettershop

☐ Kundendaten zum Empfang von Briefen über BSD Postfächer / Lettershop

☐ _____

zu 2. Kreis der Betroffenen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung / Beschreibung der betroffenen Personenkategorien):

☐ Endkunden B2B

☐ Endkunden C2B

☐ Vereinsmitglieder / Förderer

☐ Clubmitglieder

☐ Sonst: _____

2.1 Weisungsgebundenheit des Auftragnehmers

(1) Der Auftragnehmer darf die Daten des Auftraggebers nur im Rahmen der Regelungen des Hauptvertrags (einschließlich dieses AV-Vertrags) sowie sonstiger dokumentierter Weisungen des Auftraggebers verarbeiten. Dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland ebenso wie für eine Weiterverarbeitung der Daten des Auftraggebers zu anderen Zwecken, selbst in lediglich anonymisierter Weise. Sollte der Auftragnehmer abseits erteilter Weisungen auch zu Verarbeitungen aufgrund gesetzlicher Bestimmungen von EU-Mitgliedstaaten oder aus dem EU Recht verpflichtet sein, teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen in Textform vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) „Weisungen“ sind die auf eine bestimmte Verarbeitung der Daten des Auftraggebers durch den Auftragnehmer gerichteten, dokumentierten Anordnungen des Auftraggebers. Sie werden anfänglich durch den Hauptvertrag (einschließlich dieses AV-Vertrags) festgelegt und können vom Auftraggeber danach jederzeit durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung).

(3) Die Weisungen des Auftraggebers sind grundsätzlich in Textform zu erteilen.
Im Ausnahmefall erteilte mündliche Weisungen sind vom Auftragnehmer unverzüglich in Textform zu bestätigen, soweit dies nicht der Auftraggeber übernommen hat. Weisungsberechtigte Personen auf Seiten des Auftraggebers und empfangsberechtigte Personen auf Seiten des Auftragnehmers werden der jeweils anderen Partei mitgeteilt. Die bei In-Kraft-Treten dieses AV-Vertrages entsprechend befugten Personen sind in (Nr. 9 und 10) aufgeführt. Die jeweilige Partei wird die andere Partei unverzüglich über einen Wechsel dieser Person in Textform informieren.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung des Auftraggebers gegen die DS-GVO oder andere Datenschutzbestimmungen der EU oder der EU-Mitgliedstaaten verstößt, ist er verpflichtet, den Auftraggeber unverzüglich in Textform zu informieren. Der Auftragnehmer ist insoweit berechtigt, die Durchführung der vereinbarten Tätigkeit solange auszusetzen, bis der Auftraggeber über das weitere Vorgehen entschieden und den Auftragnehmer hierüber in Textform informiert hat. Die in Ziffer 5 Abs. 5 Satz 1 dieses AV- Vertrages geregelte Vertraulichkeit bleibt unberührt bestehen.

2.2 Pflichten des Auftragnehmers

(1) Der Auftragnehmer wird geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen und während der Laufzeit des AV-Vertrages aufrechterhalten. Diese Maßnahmen (Anhang 2) müssen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit dieser Auftragsverarbeitung auf Dauer sicherstellen. Sie müssen ferner die Fähigkeit haben, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

(2) Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind in Anhang 1 niedergelegt (im Folgenden „TOMs“). Der Auftragnehmer trägt die Verantwortung dafür, dass die TOMs für die Risiken der im Rahmen dieses AV-Vertrages zu verarbeitenden personenbezogenen Daten ein angemessenes Schutzniveau bieten. Bei der Beurteilung des angemessenen Schutzniveaus wird der Auftragnehmer insbesondere die Risiken berücksichtigen, die mit der Verarbeitung verbunden sind. Hierzu zählen Risiken durch unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. Zugang zu Daten des Auftraggebers. Der Auftragnehmer wird den Auftraggeber vollumfänglich von allen erhobenen Ansprüchen freistellen, die daraus resultieren oder damit zusammenhängen, dass diese TOMs nicht ausreichend sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(3) Eine Änderung der getroffenen TOMs bleibt dem Auftragnehmer vorbehalten, soweit das in Nr. 2 niedergelegte Schutzniveau damit nicht unterschritten wird. Der Auftragnehmer ist zu einer Änderung der getroffenen TOMs verpflichtet, wenn ihm während der Dauer dieses AV-Vertrages Anhaltspunkte vorliegen, die mindestens tatsächliche Zweifel an einem dem Risiko angemessenen Schutzniveau begründen, oder der technologische Fortschritt eine Anpassung erforderlich macht, um mindestens die Einhaltung des festgelegten Schutzniveaus sicherzustellen. Zu diesem Zweck überwacht der Auftragnehmer die hierauf anwendbaren Rechtlichen Rahmenbedingungen und teilt dem Auftraggeber jede Änderung unverzüglich nach deren Ankündigung unter Angabe eventueller kundenseitiger Auswirkungen auf die Verarbeitung unter diesem AV-Vertrag schriftlich mit.

zu (3) Der Auftragnehmer wird Änderungen der getroffenen TOMs dokumentieren und dem Auftraggeber diese Dokumentation unaufgefordert zusenden. Bei wesentlichen Änderungen ist der Auftraggeber vorab, unter Angabe der Gründe für diese Änderungen und die Auswirkungen auf den AV-Vertrag, in Textform zu informieren. Der Auftraggeber ist ebenso wie dessen Kunde berechtigt, einer vom Auftragnehmer vorgeschlagenen Änderung der TOMs zu widersprechen, oder von dem Auftragnehmer die Umsetzung weiterer Maßnahmen zu verlangen, wenn dies aus Sicht des Auftraggebers bzw. des Kunden zur Her-stellung eines angemessenen Schutzniveaus geboten ist.

(4) Der Auftragnehmer stellt eine hohe Verarbeitungsqualität sicher und wird die Wirksamkeit der TOMs regelmäßig überprüfen, bewerten und evaluieren, um sicherzustellen, dass die Verarbeitung im Einklang mit den Anforderungen des Datenschutzrechts erfolgt und die Sicherheit der Verarbeitung sowie der Schutz der Rechte der betroffenen Personen stets gewährleistet ist. Der Auftragnehmer hat hierzu ein geeignetes Verfahren etabliert. Der Auftragnehmer wird die Ergebnisse der jeweiligen Überprüfung schriftlich dokumentieren und dem Auftraggeber diese Dokumentation unverzüglich nach Abschluss dieser Über-prüfung zur Verfügung stellen. Soweit Mängel festgestellt werden, wird der Auftragnehmer diese unverzüglich abstellen und den Auftraggeber unaufgefordert in Textform informieren, wenn diese abgestellt sind.

(5) Der Auftragnehmer sichert zu, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen, diese Daten nur gemäß den Weisungen des Auftraggebers verarbeiten, sofern sie nicht gesetzlich zur Verarbeitung verpflichtet sind. Die Regelungen über eine vorherige Mitteilung an den Auftraggeber gemäß Ziffer 4.1 3. Satz dieses AV-Vertrages gelten entsprechend.

(6) Der Auftragnehmer sichert ferner zu, dass sich die von ihm zur Verarbeitung der Daten des Auftraggebers eingesetzten Personen zur Vertraulichkeit verpflichtet haben oder einer vergleichbaren angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Diese Verpflichtung besteht auch nach Beendigung des AV-Vertrages fort. Ebenfalls wird der Auftragnehmer bei den von ihm eingesetzten Personen regelmäßige Datenschutzschulungen durchführen und dies entsprechend dokumentieren. Die Doku-mentation zu den Schulungen und den Verschwiegenheitspflichten wird der Auftragnehmer dem Auftraggeber auf dessen Verlangen zur Verfügung stellen.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, spätestens jedoch binnen 24 Stunden, nachdem ihm Verletzungen des Schutzes der Daten des Auftraggebers be-kannt werden (wie z.B. bei unbefugter Offenlegung von oder unbefugten Zugang zu per-sonenbezogenen Daten). Die Unterrichtung hat in Textform zu erfolgen und enthält zu-mindest folgende Informationen:

- eine Beschreibung der Art der Verletzung
- Angabe der Kategorie und der ungefähren Zahl der betroffenen Personen
- Angabe der betroffenen Kategorie und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- ggf. neben den in Ziffer 5 Abs. 8 dieses AV-Vertrages benannten Ansprechpart-nern, weitere Ansprechpartner für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Da-ten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit die Informationen zum Zeitpunkt der Unterrichtung nicht oder nicht voll-ständig dem Auftraggeber zur Verfügung gestellt werden können, kann der Auftragnehmer diese Informationen ohne unangemessene weitere Verzögerung schrittweise dem Auftraggeber zur Verfügung stellen. Der Auftraggeber ist über die Gründe dieser Verzögerung unverzüglich in Textform zu informieren.
Der Auftraggeber weist den Auftragnehmer hiermit bereits jetzt an, bei Bekanntwerden der Verletzung unverzüglich in seinem Verantwortungsbereich sämtliche Maßnahmen einzuleiten, die erforderlich sind, um entstandene Gefährdungen für die Integrität, Vertraulichkeit und Sicherheit der Daten auszuschließen (z.B. durch das Trennen von Netz-werkverbindungen ein unbefugtes Verbreiten der Daten zu verhindern), den Schutz der personenbezogenen Daten wiederherzustellen und mögliche nachteilige Auswirkungen für die betroffenen Personen zu mindern. Der Auftraggeber kann vom Auftragnehmer weitere Maßnahmen verlangen, wenn die von dem Auftragnehmer bereits ergriffenen Maßnahmen aus seiner Sicht nicht ausreichend sind.

(8) Der Ansprechpartner beim Auftragnehmer für im Rahmen des AV-Vertrags anfallende Datenschutzfragen ist in Nr. 12 benannt. In Zweifelsfällen kann sich der Auftraggeber direkt an diesen wenden. Der Auftragnehmer wird den Auftraggeber über einen Wechsel des Ansprechpartners unverzüglich in Textform informieren.

(9) Sofern der Auftragnehmer ausweislich (Nr. 13) ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO führt, ist er befugt, das diesen AV-Vertrag betreffende Verzeichnis einer Aufsichtsbehörde auf deren Anfrage zur Verfügung zu stellen. Der Auftragnehmer ist ferner verpflichtet, dem Auftraggeber oder dessen Kunde auf Anfrage unverzüglich das diesen AV-Vertrag betreffende Verzeichnis zur Verfügung zu stellen, etwa im Rahmen von Anfragen der Aufsichtsbehörden oder auch im Rahmen von Audits und Zertifizierungen. Der Auftragnehmer wird den Auftraggeber sowie dessen Kunden ihn im Rahmen seiner Möglichkeiten bei der Erstellung des eigenen, diesen AV-Vertrag betreffenden Verzeichnis von Verarbeitungstätigkeiten zu unterstützen.

(10) Der Auftragnehmer unterstützt den Auftraggeber bzw. dessen Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO geregelten Pflichten.

(11) Sollten die Daten des Auftraggebers 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 das jeweils geltende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragnehmer wird den Dritten unverzüglich darüber informieren, dass die Hoheit und das "Eigentum an den Daten" allein beim Auftraggeber liegen.

2.3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist alleiniger Herr der Daten und entsprechend Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO, soweit er nicht seinerseits als Auftragsverarbeiter für seine Kunden tätig wird, die dann (auch) entsprechend Verantwortliche sind. Der Auftraggeber ist dann jedoch gegenüber seinem Kunden dafür verantwortlich, dass er dem Auftragnehmer dieselben Datenschutzpflichten auferlegt, die zwischen ihm und dem Kunden festgelegt sind. Der Auftragnehmer ist insoweit berechtigt, entsprechende Weisungen zu erteilen.

(2) Der Auftraggeber wird den Auftragnehmer unverzüglich informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt oder von seinem Kunden einen entsprechenden Hinweis erhält.

(3) Der Ansprechpartner beim Auftraggeber für im Rahmen des AV-Vertrags anfallende Datenschutzfragen ist in Nr. 5 benannt. Der Auftraggeber wird den Auftragnehmer über einen Wechsel des Ansprechpartners unverzüglich in Textform informieren.

2.4 Wahrung von Betroffenenrechten

(1) Hinsichtlich dieses AV-Vertrags ist der Auftraggeber bzw. dessen Kunden für die Wahrung der nach Kapitel III der DS-GVO vorgesehenen Betroffenenrechte verantwortlich, insbesondere im Hinblick auf Auskunfts-, Löschungs- und Berichtigungs-Ansprüche sowie das Recht auf Daten-Portabilität. Der Auftragnehmer wird den Auftraggeber und dessen Kunden im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisa-torischen Maßnahmen bei der Erfüllung seiner diesbezüglichen Verpflichtungen auf Wei-sung des Auftraggebers und innerhalb der vom Auftraggeber gesetzten, angemessenen Fristen unterstützen. Eine gesonderte Vergütung kann hierfür nicht verlangt werden.

(2) Wendet sich ein Betroffener mit der Geltendmachung von in der DS-GVO geregelten datenschutzrechtlichen Betroffenenrechten (beispielsweise Forderungen zur Datenporta-bilität, Berichtigung, Löschung oder Auskunft) an den Auftragnehmer, wird der Auftrag-nehmer diese Anfrage unverzüglich an den Auftraggeber weiterleiten, soweit nicht der Auftraggeber eine Weiterleitung direkt an den Kunden angewiesen hat. Im Hinblick auf Löschungen, Sperrungen und Änderungen wird Auftragnehmer erst nach einer in Textform gefassten Weisung des Auftraggebers der Aufforderung des Betroffenen nachkommen. Im Hinblick auf angefragte Auskünfte und Daten-Portabilität hat der Auftragnehmer dem Auftraggeber zusammen mit der Anfrage des Betroffenen den Entwurf einer Antwort an den Betroffenen einschließlich einer Aufstellung bzw. Zusammenstellung der bei ihm vorhandenen personenbezogenen Daten übermitteln. Den Parteien bleibt unbenommen, im Einzelfall abweichende Änderungen zu vereinbaren.

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung dem Auftraggeber zur Prüfung zu übergeben.
Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots (vgl. Anlage ...), sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs / Bereitstellung von Daten, Art / Umstände der Verarbeitung / der Datenhaltung sowie Art / Umstände beim Output / Datenversand, die – soweit sie sich nicht aus der zugrundeliegenden Leistungsvereinbarung ergeben - wie folgt gesondert beschrieben werden:

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach EU-DSGVO dem Auftraggeber zur Verfügung zu stellen.

Die technischen und organisatorischen Maßnahmen (TOM´s) sind als Anlage 1 beigefügt.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu sperren oder unter Beachtung gesetzlicher Aufbewahrungsfristen zu löschen.
Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich dem Betroffenem schriftlich beantworten und dieses Ersuchen unter Beachtung gesetzlicher Aufbewahrungsfristen umsetzen.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach EU-DSGVO folgende Pflichten:

- Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß EU-DSGVO ausüben kann.

  Kontaktdaten Datenschutzbeauftragter:
  Patrick Peters, Telefon: 040-23520-0
  Mail: p.peters@bsd-cc.de

  Kontaktdaten Qualitätssicherung / Produktionsleitung:
  Sylvia Bliebenich, Telefon: 040-23520-407
  Mail: produktionsleitung@bsd-cc.de

  Kontaktdaten Teamleitung:
  Telefon: 040-23520-/ACD: _____
  Mail: _____@bsd-cc.de

- Die Wahrung des Datengeheimnisses entsprechend EU-DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend EU-DSGVO und Anlage.

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach EU-DSGVO. Dies gilt auch, soweit eine zuständige Behörde nach EU-DSGVO beim Auftragnehmer ermittelt.

6. Sicherung und Aufbewahrung

Der Auftraggeber wird dem AN Belegdokumente liefern. Der AN erhält die Belegdokumente, um logistische Leistungen durchzuführen. Angesichts der erheblichen Werte die in / anbei der Belege/Sendungen seien könnten,

☐ Bargeld

☐ Schecks

☐ Gutscheine

☐ Spendenbescheinigungen

☐ Bank Einzugsermächtigungen

☐ _____

☐ _____

sind die Parteien darüber einig, dass an die Aufbewahrung und Lagerung der Belege besonders hohe Anforderungen zu stellen sind. Vor diesem Hintergrund setzen die Parteien nachfolgende Bedingungen auf.

Mit der Übergabe durch den Auftraggeber an einen BSD-Kurier (AN),
geht die Gefahr auf den AN über.

Bei fremden Kurieren übernimmt die Gefahr der AG.

Übergebene Materialien und Unterlagen bleiben im Eigentum des Auftraggebers. Der AN kann hieran kein Pfand- oder Zurückbehaltungsrecht geltend machen.

Der AN verpflichtet sich, dem Auftraggeber bei der Vertragsausführung entstandene Einwände oder Unregelmäßigkeiten unverzüglich anzuzeigen und diese zu dokumentieren.

Der AN verpflichtet sich, für eine sichere und schadenfreie Abwicklung der Aufträge zu sorgen. Dies gilt insbesondere für das Einlagern, Versenden und Befördern. Die Lagerung hat in Lagerräumen des AN zu erfolgen. Die Lagerräume sind nach dem aktuellen Stand der Sicherheitstechnik zu überwachen und zu sichern. der Auftraggeber steht es frei, Lagerräume zu besichtigen oder besichtigen zu lassen. Unterlässt der Auftraggeber die Besichtigung, kann AN hieraus keine Rechte herleiten.

7. Unterauftragsverhältnisse

Der Auftragnehmer darf sich - nach vorheriger schriftlicher Zustimmung seitens der Auftraggeber - auf eigene Kosten und Gefahr für die Durchführung seiner Leistungen erfahrener Dritter bedienen.

Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des EU-DSGVOi.V.m. Nr. 6 der Anlage zu EU-DSGVO einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Versanddienstleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Der Auftraggeber erteilt seine Zustimmung, dass die nachfolgend beschriebenen Teilleistungen unter Einschaltung folgender Subunternehmer durchgeführt werden. **Die Verarbeitung findet nur in Deutschland/EU statt.**

a) 1. Subunternehmer: Wurde hiermit vom Auftraggerber akzeptiert : ☑
Name: GreenDataProtection Akten- und Datenträgervernichtung GmbH & Co.KG
Anschrift: Im Hegen 13 - D- 22113 Oststeinbek
Beschreibung der Teilleistung: **Akten- und Datenträgervernichtung DIN 66399, Stellung von Sicherheitsbehältern inkl. Einwurfschlitz**
Name/Kontakt: https://www.green-dp.de/

b) 2. Subunternehmer: Wurde hiermit vom Auftraggerber akzeptiert : ☑
Name: trigonon GmbH
Anschrift: Griegstrasse 75 - Haus 26a, D-22763 Hamburg
Beschreibung der Teilleistung: **Externe Unterstützung der BSD IT-Abteilung**
Name/Kontakt Datenschutzbeauftragter:
B³ Unternehmensgruppe - Andreas Bethke - Papenbergallee 34 - D-25548 Kellinghusen - http://www.b3-unternehmensgruppe.de/kontakt/

8. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu EU-DSGVO vorgesehene Auftragskontrolle im Beisein mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach EU-DSGVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß EU-DSGVO und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

9. Mitteilung bei Verstößen des Auftragnehmers
Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach EU-DSGVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.

Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach EU-DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

10. Weisungsbefugnis des Auftraggebers
Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl.EU-DSGVO). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers 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.

Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend EU-DSGVO zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

Auftraggeber und Auftragnehmer vereinbaren als Weisungsberechtigte und für die Annahme von Weisungen Berechtigte für die laufende Abwicklung folgende Ansprechpartner:

Beim Auftragnehmer _____
(Sylvia Bliebenich, 040-23520-0, Produktionsleitung)

Beim Auftragnehmer _____
(Olaf Schmidt, 040-23520-0, GF & Technische Leitung)

Beim Auftragnehmer _____
(Patrick Peters, 040-23520-0, Datenschutzbeauftragter)

Beim Auftraggeber _____

(_____, _____,

_____)

Beim Auftraggeber _____

(_____, _____,

_____)

Beim Auftraggeber _____

(_____, _____,

_____)

11. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Gesetzliche Aufbewahrungspflichten sind hierbei zu achten.
Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen (HGB, AO) über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12. Etwaige Mitteilung des Auftragnehmers in Bezug auf Art. 28 Abs. 3 Nr. a DS-GVO

Keine bekannten Verpflichtungen zur Herausgabe an andere Staaten oder UN Organisationen bzw. sonstige internationale Organisationen im Sinne von Art. 4 Abs. 1 Nr. 26 DS-GVO. Im Übrigen unterliegt der Auftragnehmer - je nach Fallkonstellation - gegebenenfalls den in Deutschland geltenden Verpflichtungen zur Aufbewahrung bzw. Bereitstellung von personenbezogenen Daten für und an staatliche Stellen, wie beispielsweise dem Fiskus, den Strafverfolgungsbehörden oder dem Verfassungsschutz. Diese können im Einzelfall auch einer Mitteilung wegen eines wichtigen öffentlichen Interesses verbieten.

13 Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO

Der Auftragnehmer ist verpflichtet, ein Verarbeitungsverzeichnis zu führen: **Ja!**

14. Drittlandtransfer

Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Verarbeitung der personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers, die zumindest in Textform (z.B. E-Mail) erfolgen muss. Eine Zustimmung des Auftraggebers kommt nur dann in Betracht, wenn gewährleistet ist, dass die jeweils nach den Art. 44 – 49 DSGVO einzuhaltenden Rechtsvorschriften eingehalten werden, um ein angemessenes Schutzniveau für den Schutz der personenbezogenen Daten zu gewährleisten.

Handelt es sich bei der Garantie um EU-Standardvertragsklauseln Controller to Processor, sind die Angaben um das Datum des jeweiligen Vertragsabschlusses zu ergänzen. Soweit die Datenverarbeitung außerhalb der EU bzw. des EWR auf Grundlage eines Angemessenheitsbeschlusses gemäß Art. 45 DS-GVO stattfindet oder ein Ausnahmetatbestand nach Art. 49 DS-GVO Anwendung findet, gilt entsprechendes.

BSD und deren Subunternehmer Arbeitet und Verarbeitet nur in Deutschland/EU!

15. Nachweise des Auftragnehmers

https://www.bsd-cc.de/css/BSD-Organisatorische_Massnahmen_WEB.pdf

Zum Nachweis der Einhaltung der in diesem AV-Vertrag niedergelegten Pflichten bietet der Auftragnehmer an, den Auftraggeber mit folgenden Informationen zu unterstützen:

(X) Durchführung eines Selbstaudits oder Self-Assessments über die Einhaltung der in diesem AV-Vertrag niedergelegten Pflichten in regelmäßigen Abständen, mindestens einmal pro Kalenderjahr

( ) Vorlage und Aufrechterhaltung eines Zertifikats zu Datenschutz und/oder Informationssicherheit (z.B. ISO 27001)

( ) Vorlage und Aufrechterhaltung von Zertifikaten nach Art. 42 DS-GVO

16. Schlussbestimmungen

(1) Im Fall eines Widerspruchs zwischen dem Hauptvertrag und dem AV-Vertrag gehen die Regelungen dieses AV-Vertrags vor. Sollten einzelne Teile dieses AV-Vertrags unwirksam sein, so berührt dies die Wirksamkeit des AV Vertrag im Übrigen nicht.

(2) Änderungen und Ergänzungen dieses AV-Vertrags und seiner Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Die Parteien vereinbaren für diesen AV-Vertrag die Geltung deutschen Rechts unter Ausschluss der Regelungen des internationalen Privatrechts. Der ausschließliche Gerichtstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem AV-Vertrag ist Hamburg.

_____ _____

Ort, Datum **Auftraggeber**
Vor-/Nachname:_____
Position :_____

_____ _____

Ort, Datum **Auftraggeber**
Vor-/Nachname:_____
Position :_____

_____ _____

Ort, Datum **Auftragnehmer**
Vor-/Nachname: Olaf Schmidt
Position : Geschäftsführer

_____ _____

Ort, Datum **Auftragnehmer**
Vor-/Nachname: Sylvia Bliebenich
Position : Produktionsleitung

TOM-Technische und organisatorische Maßnahmen nach EU-DSGVO

BSD-GmbH - Wandalenweg 26 D-20097 Hamburg
Anhang 1

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☒ Alarmanlage
- ☒ Automatisches Zugangskontrollsystem
- ☒ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☒ Lichtschranken / Bewegungsmelder
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Absicherung von Gebäudeschächten
- ☐ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Videoüberwachung der Zugänge
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Pförtner / Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Gehäuseverriegelungen
- ☒ Sperren von externen Schnittstellen (USB etc.)
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☒ Einsatz von Intrustion-Detection-Systemen
- ☒ Erstellen von Benutzerprofilen
- ☒ Authentifikation mit biometrischen Verfahren
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Einsatz von VPN-Technologie
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle beim Pförtner / Empfang
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Tragepflicht von Berechtigungsausweisen
- ☒ Verschlüsselung von mobilen Datenträgern

☐ Verschlüsselung von Smartphone-Inhalten

☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

☒ Einsatz von Anti-Viren-Software

☒ Verschlüsselung von Datenträgern in Laptops / Notebooks

☒ Einsatz einer Hardware-Firewall

☒ Einsatz einer Software-Firewall

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.

☒ Erstellen eines Berechtigungskonzepts

☒ Verwaltung der Rechte durch Systemadministrator

☒ Anzahl der Administratoren auf das „Notwendigste" reduziert

☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☒ Sichere Aufbewahrung von Datenträgern

☒ physische Löschung von Datenträgern vor Wiederverwendung

☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☒ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☒ Protokollierung der Vernichtung

☒ Verschlüsselung von Datenträgern

4. Weitergabe Kontrolle

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.

☒ Einrichtungen von Standleitungen bzw. VPN-Tunneln

☒ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

☒ E-Mail-Verschlüsselung

☒ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen

☒ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☒ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☒ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☒ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. EU-DSGVO
- ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (EU-DSGVO)
- ☒ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☒ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- ☒ Vertragsstrafen bei Verstößen

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☒ Unterbrechungsfreie Stromversorgung (USV)
- ☒ Klimaanlage in Serverräumen
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts

☒ Testen von Datenwiederherstellung

☒ Erstellen eines Notfallplans

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☒ Serverräume nicht unter sanitären Anlagen

☒ In Hochwassergebieten: Serverräume über der Wassergrenze

8. Trennungsgebot

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

☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☒ Logische Mandantentrennung (softwareseitig)

☒ Erstellung eines Berechtigungskonzepts

☒ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☒ Versehen der Datensätze mit Zweckattributen/Datenfeldern

☒ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

☒ Festlegung von Datenbankrechten

☒ Trennung von Produktiv- und Testsystem

Hamburg,

BSD-GmbH

Verantwortlicher Datenschutzbeauftragter,
Patrick Peters

Unterschrift des Verantwortlichen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO) Anhang 2

1.1 Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

		Ja	Nein
a)	Für alle relevanten Standorte sind Sicherheitszonen und deren physischer Schutz in einem Sicherheitszonenkonzept definiert, dokumentiert und kann auf Anfrage vorgelegt werden.	☒	☐
b)	Das definierte Sicherheitszonenkonzept ist für alle relevanten Standorte umgesetzt.	☒	☐
c)	Das Sicherheitszonenkonzept wird min. 1x pro Jahr überprüft.	☒	☐
d)	Die Sicherheitszonen sind für alle relevanten Standorte durch physische Barrieren (Zaun, feste Wände, Türen, Zutrittskontrollanlage, Einbruchmeldeanlage etc.) geschützt, um nur autorisierten Personen Zutritt zu gewährleisten. Besucher in Sicherheitszonen werden durch autorisiertes Personal begleitet.	☒	☐
e)	Es existiert ein dokumentiertes und wirksames Verfahren zur Vergabe, Änderung und Entzug von Zutrittsrechten inkl. Rückgabe der Zutrittsmittel.	☒	☐

Etwaige Abweichungen oder Erläuterungen:

https://www.bsd-cc.de/css/BSD-Organisatorische_Massnahmen_WEB.pdf

1.2 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

		Ja	Nein
a)	Es existiert ein dokumentiertes und wirksames Zugangskontrollkonzept inkl. Netzwerksicherheitszonen und Netzsegmentierung.	☒	☐
b)	Das Zugangskontrollkonzept definiert die Vergabe, Änderungen und den Entzug von Zugangsrechten sowie deren Freigabe für interne und externe Mitarbeiter.	☒	☐
c)	Die Vorgänge für die Vergabe, Änderungen und den Entzug von Zugangsrechten sowie deren Freigabe werden nachvollziehbar protokolliert.	☒	☐
d)	Das Zugangskontrollkonzept wird mindestens 1x pro Jahr überprüft.	☒	☐
e)	Jede Benutzerkennung ist zu jedem Zeitpunkt eindeutig einer natürlichen Person zugeordnet.	☒	☐
f)	Es werden sichere Passworte verwendet. Aufbau und Handhabung erfolgt gemäß einer dokumentierten Passwortrichtlinie.	☒	☐
g)	Default Passwörter von Systemen und Applikationen (z.B. Oracle, SAP) werden grundsätzlich geändert.	☒	☐
h)	Es wird sichergestellt das Initialkennwörter für Benutzer nach einer kurzen Frist wieder ungültig werden, sofern sie nicht unverzüglich geändert wurden.	☒	☐
i)	Passwörter dürfen nur von dafür berechtigten Personen gemäß definiertem Prozess zurückgesetzt oder geändert werden.	☒	☐
j)	Administratoren nutzen separate Zugänge für das Management von Systemen und deren privilegierte Aktivitäten werden protokolliert.	☒	☐
k)	Die Delegation von Rechten (Vertretungsregelung) erfolgt ausschließlich gemäß definierter Vorgaben.	☒	☐

		Ja	Nein
l)	Alle Mitarbeiter sind angewiesen, ihre Arbeitsplätze zu sperren, wenn sie diese verlassen. Standardmäßig werden Arbeitsplätze mit automatischer Sperre konfiguriert.	☒	☐
m)	Alle Zugänge zu Systemen (Applikationen, Betriebssystemen, BIOS, Boot-Devices etc.) sind mit Passwort gesichert oder gesperrt.	☒	☐
n)	Der externe Zugriff (Remote Access) wird über eine Firewall, mittels starker Verschlüsselung und 2-Faktor Authentisierung gesichert.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

1.3 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.

		Ja	Nein
a)	Es wird sichergestellt, dass nur die Zugriffsrechte vergeben werden, die zur Erfüllung der jeweiligen Aufgabenstellung erforderlich sind.	☒	☐
b)	Die Vergabe und Freigabe von Zugriffsrechten ist nachvollziehbar dokumentiert, sodass festgestellt werden kann, wer auf die Daten Zugriff hat.	☒	☐
c)	Das Vergabeverfahren und die Zugriffrechte werden regelmäßig geprüft und bestätigt. Zugriffsrechte werden unverzüglich entzogen, sofern sie nicht mehr erforderlich sind.	☒	☐
d)	Für alle Daten ist jeweils ein Verantwortlicher festgelegt, der entscheidet, wer welchen Zugriff erhalten darf.	☒	☐
e)	Zugriffsrechte werden angepasst, wenn sich die Aufgabenstellungen in den Geschäftsabläufen ändern.	☒	☐
f)	In den Applikationen ist sichergestellt, dass die zugeteilten Zugriffsrechte technisch umgesetzt sind.	☒	☐
g)	In allen Umgebungen, die Produktionsdaten enthalten (auch Entwicklung, Test etc.), wird der unbefugte Zugriff ausgeschlossen.	☒	☐
Etwaige Abweichungen oder Erläuterungen: https://www.bsd-cc.de/css/BSD-Organisatorische_Massnahmen_WEB.pdf			

1.4 Trennungskontrolle

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

		Ja	Nein
a)	Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden so separiert (physisch oder logisch), dass diese dem Zweck entsprechend getrennt verarbeitet, gespeichert und gelöscht werden (Rollen und Berechtigungskonzept).	☒	☐
b)	Entwicklungs-, Test- und Produktivumgebungen sind getrennt.	☒	☐

	Ja	Nein
Etwaige Abweichungen oder Erläuterungen:		

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

	Ja	Nein
Sofern möglich, erfolgt die Verarbeitung mit pseudonymisierten Daten. Die Verarbeitung personenbezogener Daten erfolgt dann in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.	☒	☒
Etwaige Abweichungen oder Erläuterungen: Wenn der Auftragsverarbeiter auf Online-Systemen des Auftraggebers arbeitet, muss dieser dafür Sorge tragen. Beim Auftragsverarbeiter sind die Datenbanken verschlüsselt.		

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

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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.

	Ja	Nein
a) Die Daten werden bei Transport, Speicherung, Übertragung und Verarbeitung außerhalb des geschützten Bereiches des Unternehmens mit Verfahren wie starker Verschlüsselung, Zwei-Faktor-Authentifizierung gesichert (z. B. Festplattenverschlüsselung).	☒	☐
b) Es sind Anweisungen für die Handhabung von Informationen festgelegt und die Mitarbeiter werden geschult, um den Missbrauch der Daten zu verhindern (z.B. zertifizierte Entsorgung von Papier und Datenträger, Auswahl der Übermittlungsverfahren).	☒	☐
c) Kryptografische Schlüssel zum Schutz der Daten werden sicher in einem entsprechenden Managementsystem verwaltet.	☒	☐
Etwaige Abweichungen oder Erläuterungen:		

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

		Ja	Nein
a)	Die folgenden Ereignisse werden protokolliert (systemseitig oder anderweitig): • An- und abmelden • Konfigurationsänderungen • Passwortänderungen • Erstellen, Ändern und Löschen von Konten und Gruppen • Änderungen in der Protokollkonfiguration • Aktivierung und Deaktivierung von Sicherheitssoftware wie Virenscanner oder lokaler Firewall • Änderungen von personenbezogenen Daten in Applikationen	☒	☐
b)	Die Nutzung und die Administration von System- und Netzwerkressourcen wird überwacht und die Überwachungsergebnisse werden regelmäßig überprüft.	☒	☐
c)	Log-Systeme und Logging-Informationen werden vor unbefugtem Zugriff, Änderung und Löschung geschützt und regelmäßig ausgewertet.	☒	☐
d)	Die Uhren aller kritischen Systeme werden mit einem zuverlässigen und vereinbarten Zeitserver synchronisiert.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b+c DS-GVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

		Ja	Nein
a)	Es sind Schutzmaßnahmen (USV, Netzersatzanlage, Feuerlöscher, Branderkennung etc.) gegen elementare Gefährdungen - insb. Feuer, Wasser, Ausfall von Versorgungsnetzen, Denial of Service - vorhanden.	☒	☐
b)	Die Daten werden in physisch geschützten Bereichen verarbeitet, die Maßnahmen zur Absicherung des Bereiches sind dokumentiert und werden regelmäßig geprüft.	☒	☐
c)	Anlagen zur Versorgung der Datenverarbeitungssysteme werden regelmäßig gewartet.	☒	☐
d)	Die Nutzung von (System-) Ressourcen wird überwacht und ggf. angepasst, um eine ausreichende Systemkapazität sicherzustellen.	☒	☐
e)	Auf allen Informationssystemen ist ein aktueller Schutz vor Malware, Zero-Day-Exploits oder böswilligem Verhalten von Software installiert, wird zentral verwaltet und auf dem aktuellen Stand gehalten.	☒	☐
f)	Serversysteme werden in sicheren Umgebungen betrieben (z.B. Serverräume oder Rechenzentren) und die Installation in Büros wird unterbunden.	☒	☐
g)	Daten werden so gesichert, dass sie dem Zweck entsprechend separiert in einer definierten Zeit wiederhergestellt werden können.	☒	☐

		Ja	Nein
h)	Bei der Datensicherung werden der Umfang, die Häufigkeit, die Art (voll, differentiell, inkrementell), der Zeitrahmen, eine Verschlüsselung und physisch getrennte Aufbewahrung berücksichtigt und nachvollziehbar dokumentiert.	☒	☐
i)	Bei jeder Änderung des Datensicherungsverfahrens wird die Wiederherstellbarkeit der Daten aus der Datensicherung geprüft.	☒	☐
j)	Eingerichtete Redundanzen (z.B. RAID, Cluster, Load-Balancer) werden, sofern diese nicht kontinuierlich in Betrieb sind, regelmäßig auf Funktion überprüft. Durchgeführte Prüfungen werden dokumentiert.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

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

4 Datenschutz-Management

Maßnahmen, die gewährleisten, dass die Datenschutzanforderungen umgesetzt werden und diese auch nachweisbar sind.

		Ja	Nein
a)	Relevante interne und externe Mitarbeiter werden in den Datenschutz eingewiesen und auf diesen verpflichtet.	☒	☐
b)	Interne und externe Mitarbeiter werden für Verarbeitungstätigkeiten/Anwendungen geschult und auf die Folgen von Verletzungen des Datenschutzes hingewiesen.	☒	☐
c)	Die Austrittsverfahren für Mitarbeiter gewährleisten, dass Sicherheitsverletzungen vermieden werden und zur Verfügung gestellte Ausstattung zurückgegeben wird.	☒	☐
d)	Geräte werden so entsorgt, dass keine Daten rekonstruiert werden können.	☒	☐
e)	Die IT-Betriebsverfahren (z. B. User Management, Backup, Netzwerkmanagement) sind nachvollziehbar dokumentiert, werden regelmäßig geprüft und bei Bedarf angepasst.	☒	☐
f)	Alle Änderungen werden im Rahmen eines nachvollziehbar dokumentierten Change-Management Prozesses abgewickelt.	☒	☐
g)	Das Risiko von Datenpannen wird durch Trennung von Verantwortlichkeiten (z. B. System- getrennt von Datenadministration) reduziert.	☒	☐
h)	Identifizierung, Bereitstellung und Test von Updates sind Bestandteil des Regelbetriebes.	☒	☐
i)	Sicherheitsfunktionen von Systemen und Anwendungen sind konfiguriert und aktiviert.	☒	☐
j)	Es existiert ein Regelwerk für Informationssicherheit und Datenschutz.	☒	☐
k)	Das Regelwerk für Informationssicherheit und Datenschutz sowie die Sicherheitsmaßnahmen werden regelmäßig auf Einhaltung und Wirksamkeit geprüft.	☒	☐
l)	Es gibt eine System- und Softwareentwicklungsrichtlinie, die die Aspekte des Datenschutzes beinhaltet.	☒	☐
Etwaige Abweichungen oder Erläuterungen: https://www.bsd-cc.de/css/BSD-Organisatorische_Massnahmen_WEB.pdf			

5 Incident-Response-Management

Maßnahmen, die gewährleisten, dass Datenpannen schnell erkannt und gemeldet werden.

		Ja	Nein
a)	Es ist ein an „best practices“ ausgerichteter Prozess (ITIL) eingerichtet, der sicherstellt, dass Sicherheitsvorfälle identifiziert, bewertet und angemessen behandelt werden.	☒	☐
b)	Mit allen relevanten Parteien sind Eskalationsverfahren und organisatorische Schnittstellen definiert und der Datenschutzbeauftragte wird unverzüglich involviert.	☒	☐
c)	Alle Informationssicherheitsvorfälle, die über eine typische geringfügige Störung im Tagesgeschäft hinausgehen, werden unverzüglich ohne weitere Prüfung an festgelegte Stellen gemeldet.	☒	☐
d)	Mitarbeiter, die für die Verwaltung von IT-Systemen / Anwendungen zuständig sind, werden geschult, um Sicherheitsvorfälle zu erkennen, zu klassifizieren und zu melden.	☒	☐
e)	Es ist ein Prozess etabliert, der auch während einer Krise oder eines Desasters für alle kritischen Geschäftsprozesse die Informationssicherheit gewährleistet.	☒	☐
f)	Für einen Notfall / eine Krise sind Prozesse und Verantwortlichkeiten definiert und es finden entsprechende Übungen statt.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

6 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Maßnahmen, die gewährleisten, dass Privacy by Default und Privacy by Design berücksichtigt sind.

		Ja	Nein
a)	Bestandteil eines neuen oder zu ändernden Datenverarbeitungsvorgangs ist eine Bewertung der Risiken der Betroffenen und davon abhängig die Identifikation und Realisierung technischer und organisatorischer Sicherheitsmaßnahmen.	☒	☐
b)	Vor Produktionsaufnahme eines neuen oder geänderten Datenverarbeitungsvorgangs wird im Rahmen einer Abnahme geprüft, ob der Datenschutz durch entsprechende Voreinstellungen gegeben ist.	☒	☐
Etwaige Abweichungen oder Erläuterungen:			

7 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

		Ja	Nein
a)	Es existieren formelle Vereinbarungen über den Informationsaustausch zwischen den o.g. Vertragsparteien, die die Sicherheit der Daten berücksichtigen.	☒	☐

		Ja	Nein
b)	Vor Aufnahme einer Auftragsverarbeitung wird mit jedem Dienstleister rechtsverbindlich im Rahmen einer AV festgelegt, wie Informationen/Daten zu handhaben sind.	☒	☐
c)	Vor der Beauftragung externer Dienstleister erfolgt eine Bewertung hinsichtlich ihrer Reputation, Qualifikation, Software, Hardware, personellen und finanziellen Ressourcen und Sicherheitsaspekten in Bezug auf ihre zukünftigen Aufgaben.	☒	☐
d)	Die Einhaltung der Verträge wird durch regelmäßige Kontrolle der Vertragsausführung überwacht. Bei Abweichungen werden die definierten Ansprechpartner für Informationssicherheit / Datenschutz involviert und ggf. der Vertrag oder die Vertragsausführung angepasst.	☒	☐
e)	Im Falle einer fristlosen Kündigung werden zusätzliche Maßnahmen ergriffen, die den vorsätzlichen Missbrauch von Infrastruktur oder Daten durch den externen Dienstleister verhindern (z. B. durch Sperren von Zugängen).	☒	☐
f)	Weisungsgeber auf Seiten des Auftraggebers bzw. Weisungsempfänger auf Seiten des Auftragnehmers sind namentlich (oder als Rolle) bekannt.	☒	☐
Etwaige Abweichungen oder Erläuterungen: https://www.bsd-cc.de/css/BSD-Organisatorische_Massnahmen_WEB.pdf			