Auftrag gemäß Art. 28 DS-GVO

Vereinbarung[1]

zwischen dem / der

- nachstehend Auftraggeber genannt –

und dem / der

Abendsonne Afrika GmbH
Zur Unteren Mühle 1
89290 Buch

- nachstehend Auftragnehmer genannt –

Kontaktdaten

Auftraggeber	
Firma/Name	
Straße, Nr.	
PLZ, Ort	
Name des fachlichen Ansprechpartners	
- Tel.	
- E-Mail	
Name des Datenschutzbeauftragten	
- Tel.	
- E-Mail	
Name des Informationssicherheitsbeauftragten	
- Tel.	
- E-Mail	
Auftragnehmer	
Firma/Name	Abendsonne Afrika GmbH
Straße, Nr.	Zur Unteren Mühle 1
PLZ, Ort	89290 Buch
Name des fachlichen Ansprechpartners	Michael Merbeck
- Tel.	07343929980
- E-Mail	info@abendsonneafrika.de
Name des Datenschutzbeauftragten	Erwin Feroudj
- Tel.	07318023688
- E-Mail	Erwin.feroudj@data-s.de
Name des Informationssicherheitsbeauftragten	Michael Merbeck
- Tel.	07343 929 980
- E-Mail	info@abendsonneafrika.de

[1] in Anlehnung an: Gesellschaft für Datenschutz und Datensicherheit e. V., Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO, 3/2017.

1) Gegenstand und Dauer des Auftrags

a) **Gegenstand des Auftrags**

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung / SLA /..... vom ....., auf die / das hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

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

.....Beratung und Buchung von Reisen.

b) Dauer des Auftrags

Der Vertragsbeginn des Auftrags wird auf den 25. Mai 2018 festgelegt. Mit Erreichen des Zeitpunkts des Vertragsbeginns wird die zwischen Auftraggeber und Auftragnehmer bereits getroffene Vereinbarung über Auftragsdatenverarbeitung gemäß § 11 BDSG unwirksam.

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet vom …… bis zum .....

☒ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von .....14 Tagen gekündigt werden.
Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2) Konkretisierung des Auftragsinhalts

a) **Art und Zweck der vorgesehenen Verarbeitung von Daten**

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

oder

☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

.....alle erforderlichen personenbezogenen Daten zur Durchführung von Buchungen von Unterkünften, Transport o.ä. werden erhoben und innerhalb der Dauer des Auftrags genutzt.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in: ……

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☒ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

☐ wird hergestellt durch sonstige Maßnahmen: ……
(Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO)

b) **<u>Art der Daten</u>**

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

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

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z. B. Telefon, E-Mail)
- ☐ Vertragsstammdaten
- ☐ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☒ spezielle Kundendaten, die für die komfortable Durchführung der Reisen für den Kunden notwendig sind, z.B. Allergien, Vegetarier, körperliche Einschränkungen

c) **<u>Kategorien betroffener Personen</u>**

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☒ Interessenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ ……

3) Technisch-organisatorische Maßnahmen

a) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und 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.

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

c) 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.

4) Berichtigung, Einschränkung und Löschung von Daten

a) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

b) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, Daten-Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5) Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

- Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau

  Erwin Feroudj, DATA-S, 07318023688, datenschutz@data-s.de

  bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird benannt:

[Eintragen: Name, Organisationseinheit, Telefon, E-Mail]

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union:

[Eintragen: Name, Organisation (falls extern), Organisationseinheit, Telefon, E-Mail]

d) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers

verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

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

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

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

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrags.

6) Unterauftragsverhältnisse

a) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

b) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

i) ☐ Eine Unterbeauftragung ist unzulässig.

ii) ☐ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftrag nehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu:

Firma Unterauftrag-nehmer	Anschrift/Land	Leistung

iii) ☐ Die Auslagerung auf Unterauftragnehmer oder

☒ der Wechsel des bestehenden Unterauftragnehmers

ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

c) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

d) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

e) Eine weitere Auslagerung durch den Unterauftragnehmer

- ☐ ist nicht gestattet;
- ☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7) Kontrollrechte des Auftraggebers

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

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

c) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

8) Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören insbesondere:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

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

9) Weisungsbefugnis des Auftraggebers

a) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

10) Löschung von Daten und Rückgabe von Datenträgern

a) Kopien oder Duplikate der Daten 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.

b) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten 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. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

Wichtiger Hinweis: Nachstehendend sind vom **Auftragnehmer** Angaben in Bezug auf die durch ihn getroffenen technischen und organisatorischen Schutzmaßnahmen zu machen!

Anlage: Technische und organisatorische Schutzmaßnahmen gemäß Art. 32 DS-GVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter nachfolgend dargelegte technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

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

Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische und organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- ☒ Festlegung befugter Personen inklusive Umfang der jeweiligen Befugnisse
- ☐ Ausgabe von Zutrittsberechtigungsausweisen
- ☐ Existenz von Regelungen für Unternehmensexterne
- ☐ Umsetzung einer Schlüsselregelung
- ☐ Protokollierung der ein- und ausgehenden Personen
- ☒ Physische Maßnahmen vorhanden und regelmäßig überprüft:
  - ☒ Gesicherter Eingang (z. B. abschließbare Türen, Ausweisleser)
  - ☐ Einbruchhemmende Fenster
  - ☐ Gerätesicherung gegen Diebstahl, Manipulation oder Beschädigung
  - ☐ Überwachungseinrichtung (z. B. Alarmanlage, Videoüberwachung)
  - ☐ Vereinzelungsanlage (z. B. Drehkreuz, Schleuse)
  - ☐ Wachpersonal, Pförtner
- ☐ Unterteilung in verschiedene Sicherheitszonen

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme und die unbefugte Systemnutzung sind zu verhindern.

Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- ☒ Konzeption und Implementierung eines Berechtigungskonzepts
  - ☒ Berechtigungskonzept für Endgeräte (Rechner)
  - ☒ Berechtigungskonzept für Software/Systeme
- ☒ Identifikation und Berechtigungsprüfung eines Benutzers
- ☐ Implementierung eines Systems zur Verwaltung von Benutzeridentitäten
- ☐ Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle
- ☐ Festlegung und Kontrolle der Zugangsbefugnisse
- ☐ Authentisierungsverfahren dem Schutzbedarf der Informationen entsprechend (Klassifizierung)
- ☐ Verschlüsselung
- ☒ Angemessener Passwortschutz (Verhaltensregeln, verschlüsselte Archive)
- ☒ Spezielle Sicherheitssoftware (z. B. Anti-Malware, VPN oder Firewall)
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Existenz von Regelungen für Unternehmensexterne
- ☐ Zugangsfunktion über Token

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung anhand:

- ☒ Berechtigungs- und Rollenkonzept für Applikationen
- ☐ Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
- ☐ Überprüfung der Berechtigungen
- ☒ Funktionsbegrenzung (funktional/zeitlich)
- ☐ Zugriffsbeschränkungen (gemäß „Need-to-Know“ und „Least Privilege“)
- ☒ Verschlüsselte Speicherung der Daten
- ☒ Protokollierung
  - ☒ Protokollierung des lesenden Zugriffs
  - ☒ Protokollierung des schreibenden Zugriffs
  - ☐ Protokollierung von unberechtigten Zugriffsversuchen
  - ☐ Regelmäßige Auswertung
  - ☒ Anlassbezogene Auswertung
- ☐ Umsetzung von Regelungen zur Löschung von Daten
- ☐ Umsetzung von Regelungen zum Umgang mit elektronischen Speichermedien
- ☐ Umsetzung von Regelungen zur Entsorgung von Speichermedien
- ☐ Integritätskontrolle

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- ☐ Mandantenfähigkeit:
  - ☐ Physische Trennung
  - ☐ Trennung auf Systemebene

☒ Trennung auf Datenebene

☐ Trennung von Produktiv- und Testsystemen

☐ Sandboxing

☐ Dokumentation der Funktionstrennung

☐ Vorhandensein von Richtlinien und Arbeitsanweisungen

☐ Vorhandensein von Verfahrensdokumentationen

☐ Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

Pseudonymisierung und Verschlüsselung

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

☐ Trusted Third Party

☐ Blinde Signatur

☒ Softwarebasierte Verschlüsselung bei Datenspeicherung

☐ Hardwarebasierte Verschlüsselung bei Datenspeicherung

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

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

Weitergabekontrolle

Aspekte der Weitergabe und Übertragung personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle.

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

- ☐ Für elektronische Übertragungen:
  - ☒ Verschlüsselung der Datenübermittlung (z. B. VPN, S/MIME)
  - ☐ Durchführung von Protokollierungen der Datenweitergabe oder Übermittlung
- ☒ Durchführung von Plausibilitäts-, Vollständigkeits- und Richtigkeitsprüfungen
- ☒ Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen (z. B. Deaktivierung der USB-Schnittstellen, regelmäßige Kontrolle der zulässigen Empfänger, technische Beschränkung auf zulässige Empfänger)
- ☐ Vollständige Dokumentation der Formen der Weitergabe von Daten (z. B. Ausdruck, Datenträger, automatisierte Übermittlung)
- ☐ Auflistung der Empfänger der Daten
- ☐ Dokumentationen der Schnittstellen und der Abruf- und Übermittlungsprogramme
- ☐ Für Ausdrucke und Datenträger:
  - ☐ Durchführung von regelmäßigen Bestandskontrollen
  - ☐ Sicherungen des Transports (z. B. Behälter, Verschlüsselung von Speichermedien, Übergabeprotokolle)

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- ☒ Protokollierung der Eingaben und Überprüfung der Protokolle
- ☐ Organisatorisch festgelegte Zuständigkeiten für die Eingabe

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

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

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physisch/logisch):

- ☒ Regelmäßige Kontrolle des Systemzustands (Monitoring)
- ☒ Kurzfristige Wiederherstellbarkeit des normalen Systemzustands
- ☒ Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen):
  - ☐ offline ☒ online ☒ onsite ☒ offsite
- ☒ Datenarchivierungskonzept
- ☐ Vorhandensein eines Notfallkonzepts (Business Continuity, Disaster Recovery)
- ☐ Regelmäßige Tests des Notfallkonzepts
- ☒ Vorhandensein von redundanten IT-Systemen (z. B. Server, Speicher)
- ☐ Replizierbarkeit virtueller Maschinen
- ☒ Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie: USV, Klima)
- ☐ Meldewege und Notfallpläne

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

Belastbarkeitskontrolle

Die Verarbeitung der Daten soll tolerant gegenüber Störungen und Fehlern sein.

- ☒ Virenschutz/Anti-Malware/Anti-Ransomware

☐ großzügig vorhandene Netzwerkkapazität
☐ gehärtete Hardware gegen insbesondere DoS- und DDoS-Angriffe
☐ IDS/IPS
☐ geeignete Systemarchitektur/DMZ
☒ Firewall

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

☒ Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz
☒ Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit
☐ Existenz eines angemessenen Informationssicherheitsmanagements
☐ Existenz eines angemessenen Incident Response Managements
☐ Durchführung einer Informationsklassifizierung
☒ Regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte
☒ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
☒ Auftragskontrolle, um weisungsgemäße Auftragsverarbeitung zu gewährleisten:
  ☒ Strikte Einhaltung der im vorliegenden Auftragsverarbeitungs-Vertrag festgeschriebenen Vereinbarungen und diesbezügliche Überprüfungen
  ☒ Konzept dahingehend, wie die regelmäßige Kontrolle des Auftragsprozesses erfolgt (z. B. Vorlage von Self-Assessments, Vorlage der Verträge mit Unterauftragnehmern, Durchführung von Kontrollen bei Subunternehmern durch den Auftragnehmer)
  ☐ Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B. anhand: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben, oder oben angegebene Maßnahmen spezifizieren wollen, nutzen Sie bitte nachstehendes Freitextfeld:

Ort, Datum Unterschrift Auftraggeber

Ort, Datum Unterschrift Auftragnehmer