Anlage 1
Datenschutz

1. Begriffsbestimmungen

In dieser Anlage 1 ("**Auftragsverarbeitung**") haben die folgenden Begriffe die folgende Bedeutung:

„Datenschutzgesetze“ bezeichnet die Datenschutzgesetze des Landes, in dem der Verantwortliche ansässig ist (einschließlich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung - „**DSGVO**“)) und alle weiteren Datenschutzgesetze, die für den Verantwortlichen in Verbindung mit dem Hauptvertrag gelten.

„Personenbezogene Daten“ bezeichnet gemäß der Definition der DSGVO Informationen über eine bestimmte oder bestimmbare natürliche Person, die vom Auftragsverarbeiter im Rahmen der Leistungserbringung für den Verantwortlichen gemäß dieser Auftragsverarbeitung verarbeitet werden.

„Standardklauseln“ bezeichnet die Standardvertragsklauseln für die Übertragung personenbezogener Daten von einem Verantwortlichen im Europäischen Wirtschaftsraum an Auftragsverarbeiter in Drittländern wie im Anhang zur Entscheidung der Europäischen Kommission 2010/87/EU niedergelegt und ergänzt durch die Einbindung der Beschreibung der personenbezogenen Daten und der technischen und organisatorischen Maßnahmen.

„Unterauftragnehmer“ im Sinne dieser Regelung sind vom Auftragsverarbeiter beauftragte Dritte mit solchen Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter 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.

„**Verantwortlicher**“, „**Betroffene Person**“, „**Verletzung des Schutzes personenbezogener Daten**“, „**Auftragsverarbeiter**“ und „**Verarbeiten**“ haben die in der DSGVO festgelegte Bedeutung.

2. Weisungsgebundenheit des Auftragsverarbeiters

2.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nach den Weisungen des Verantwortlichen. Für weitere Weisungen, die zu einer Verarbeitung außerhalb des Geltungsbereichs dieser Auftragsverarbeitung führen würden (z. B. aufgrund der Einführung eines neuen Verarbeitungszwecks), ist eine vorherige schriftliche Vereinbarung zwischen den Parteien erforderlich.

2.2 Der Auftragsverarbeiter legt personenbezogene Daten nur dann gegenüber Dritten (einschließlich Behörden, Gerichten oder Strafverfolgungsbehörden) offen, wenn er die schriftliche Genehmigung des Verantwortlichen eingeholt hat oder laut Gesetz dazu verpflichtet ist. Ist der Auftragsverarbeiter verpflichtet, personenbezogene Daten gegenüber einer Strafverfolgungsbehörde oder sonstigen Dritten offenzulegen, setzt er den Verantwortlichen vor der Offenlegung dieser Daten in Kenntnis (sofern und solange dies nicht gesetzlich verboten ist).

3. Personal des Auftragsverarbeiters

Der Auftragsverarbeiter sorgt dafür, dass seine zur Verarbeitung personenbezogener Daten berechtigten Mitarbeiter sich durch Unterzeichnung eines Vertrags zur Geheimhaltung verpflichtet haben. Eine Verpflichtung zur Geheimhaltung ist nur erforderlich, wenn nicht bereits angemessene gesetzliche Verschwiegenheitspflichten bestehen.

4. Technische und organisatorische Maßnahmen

4.1 Der Auftragsverarbeiter hat angemessene technische und organisatorische Sicherheitsmaßnahmen gemäß Anhang zu treffen und aufrecht zu erhalten, um zu verhindern, dass der Schutz personenbezogener Daten verletzt wird („**TOMs**“) und um die in Abschnitt 5 beschriebene Unterstützung leisten zu können.

4.2 Die TOMs unterliegen dem technischen Fortschritt und der Weiterentwicklung. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten.

5. Umsetzung von Betroffenenrechten

5.1 Erhält der Verantwortliche Anfragen oder Mitteilungen von Betroffenen in Bezug auf die Verarbeitung personenbezogener Daten („**Anfrage**“), unterstützt der Auftragsverarbeiter den Verantwortlichen auf dessen

Anweisung in angemessener Weise und liefert ihm auf Anfrage entsprechende Informationen.

5.2 Auf Weisung des Verantwortlichen hat der Auftragsverarbeiter personenbezogene Daten zu korrigieren, zu löschen oder zu sperren.

6. Unterstützung des Verantwortlichen

6.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen.

6.2 Im Falle einer Verletzung des Schutzes personenbezogener Daten hat der Auftragsverarbeiter:

a) den Verantwortlichen unverzüglich nach Feststellung der Verletzung zu informieren;

b) dem Verantwortlichen erforderliche Informationen, Zusammenarbeit und Unterstützung hinsichtlich der als Reaktion auf eine Verletzung des Schutzes personenbezogener Daten zu ergreifenden Maßnahmen zu bieten.

6.3 Sofern für die Verarbeitung personenbezogener Daten laut Datenschutzgesetzen eine Datenschutzfolgenabschätzung („**DSFA**“) erforderlich ist, stellt der Auftragsverarbeiter dem Verantwortlichen auf Verlangen die für die DSFA nach billigem Ermessen erforderlichen Informationen zur Verfügung und bietet ihm die entsprechend erforderliche Unterstützung.

7. Löschung und Rückgabe personenbezogener Daten

7.1 Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und vorhandene Kopien zu löschen, es sei denn, er ist nach geltendem Recht zur weiteren Speicherung verpflichtet.

7.2 Entstehen zusätzliche Aufwände durch abweichende Vorgaben bei der Rückgabe oder Löschung der personenbezogenen Daten, so trägt diese der Verantwortliche.

8. Auskunftsrechte und Audit

8.1 Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen alle Informationen bzw. Zertifikate zur Verfügung, die nach billigem Ermessen

erforderlich sind, um die Erfüllung der in dieser Auftragsverarbeitung dargelegten Pflichten nachzuweisen.

8.2 Stellt der Auftragsverarbeiter keine ausreichenden Informationen oder Zertifikate zur Verfügung oder sofern dies laut Datenschutzgesetzen erforderlich ist oder von einer zuständigen Behörde gefordert wird, ermöglicht der Auftragsverarbeiter die mit angemessener Frist angekündigte Überprüfung der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter während der normalen Geschäftszeiten vor Ort und wirkt an dieser mit. Diese Überprüfung darf den Geschäftsbetrieb des Auftragsverarbeiters nicht stören.

8.3 Der Auftragsverarbeiter leitet sämtliche Anfragen nationaler Datenschutzbehörden in Bezug auf die von ihm durchgeführte Verarbeitung personenbezogener Daten an den Verantwortlichen weiter. Der Auftragsverarbeiter kooperiert mit dem Verantwortlichen bei dessen Umgang mit nationalen Datenschutzbehörden und von ihnen erhaltenen Auditanfragen.

9. Meldepflicht bei rechtswidriger Weisung des Verantwortlichen

Der Auftragsverarbeiter hat den Verantwortlichen zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen die anwendbaren Datenschutzbestimmungen verstößt. Der Auftragsverarbeiter darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Verantwortlichen bestätigt oder geändert wurde. Die Umsetzung offensichtlich rechtswidriger Weisungen darf der Auftragsverarbeiter ablehnen. Der Auftragsverarbeiter ist nicht verpflichtet, Weisungen des Verantwortlichen rechtlich zu überprüfen.

10. Unterauftragsverhältnisse

10.1 Der Verantwortliche erklärt sich damit einverstanden, dass der Auftragsverarbeiter zur Ausführung bestimmter Verarbeitungstätigkeiten im Hinblick auf personenbezogene Daten Unterauftragnehmer beauftragt.

10.2 Die derzeitigen Unterauftragnehmer sind im Anhang aufgelistet.

10.3 Wenn der Auftragsverarbeiter weitere Unterauftragnehmer beauftragt oder Unterauftragnehmer ersetzt bzw. entfernt, hat er (i) den Verantwortlichen hiervon rechtzeitig vorher in Kenntnis zu setzen und (ii) einen schriftlichen Vertrag mit dem Unterauftragnehmer abzuschließen, der dem Unterauftragnehmer die in Artikel 28 (3) und (4) DSGVO genannten Pflichten auferlegt. Der Verantwortliche kann der Beauftragung von Unterauftragnehmern binnen 30 Tagen schriftlich mit entsprechender Begründung widersprechen, wenn die Beauftragung eines

Unterauftragnehmers gegen diese Auftragsverarbeitung oder Datenschutzgesetze verstößt.

10.4 Der Vertrag des Auftragsverarbeiters mit dem Unterauftragnehmer hat den Anforderungen der Datenschutzgesetze, insb. von Artikel 28 DSGVO zu entsprechen.

10.5 Erfüllt der Unterauftragnehmer seine ihm laut Vertrag oder Datenschutzgesetzen auferlegten Datenschutzverpflichtungen nicht, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Erfüllung von dessen Verpflichtungen gemäß den Bestimmungen dieser Auftragsverarbeitung.

11. Internationale Datenübertragung

11.1 Der Auftragsverarbeiter wird personenbezogene Daten zur Verarbeitung gemäß dieser Auftragsverarbeitung nicht an Länder außerhalb des Europäischen Wirtschaftsraums übertragen („**Drittland**").

12. Vertragslaufzeit und Kündigung

12.1 Diese Auftragsverarbeitung endet automatisch, wenn der Hauptvertrag endet. Der Verantwortliche kann seine Rechte unter dieser Auftragsverarbeitung ausüben, solange der Auftragsverarbeiter personenbezogene Daten verarbeitet.

12.2 Jede der Parteien kann die Auftragsverarbeitung jederzeit mit angemessener Frist aus wichtigem Grund kündigen, wenn die andere Partei eine erhebliche Pflichtverletzung nach dieser Auftragsverarbeitung begeht.

12.3 Im Falle des Einspruchs des Verantwortlichen gegen die Entfernung oder Ersetzung eines Unterauftragnehmers oder gegen die Hinzuziehung eines weiteren Unterauftragnehmers kann der Auftragsverarbeiter die Leistung gegenüber dem Verantwortlichen innerhalb von 4 Wochen nach Zugang des Einspruchs einstellen und die Leistungsvereinbarung fristlos und mit sofortiger Wirkung kündigen, sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragsverarbeiter nicht zumutbar ist.

13. Haftung

13.1 Werden gegenüber einer Partei Schadenersatzansprüche wegen der Verarbeitung personenbezogener Daten geltend gemacht, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren. Für den Verantwortlichen gilt dies nur, wenn der geltend gemachte Anspruch auf einer Pflichtverletzung des Auftragsverarbeiters beruht.

13.2 Der Verantwortliche stellt den Auftragsverarbeiter von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragsverarbeiter aufgrund der vom Verantwortlichen beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer weisungswidrigen Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter beruht. Nichts in dieser Auftragsverarbeitung begrenzt jedoch die Haftung einer Partei für Schäden, die auf vorsätzlichem Fehlverhalten oder grober Fahrlässigkeit der Partei beruhen. Im Übrigen gelten die Regelungen zur Haftung im Hauptvertrag.

14. Verschiedenes

14.1 Im Falle eines Widerspruchs haben die Bestimmungen dieser Auftragsverarbeitung Vorrang vor den Bestimmungen des Hauptvertrages zwischen dem Verantwortlichen und dem Auftragsverarbeiter.

14.2 Keine der Parteien erhält eine Vergütung für die Erfüllung ihrer Pflichten unter dieser Auftragsverarbeitung, es sei denn, dies ist in diesem oder einem anderen Vertrag ausdrücklich festgelegt.

14.3 Für die Unterstützung bei der Durchführung einer Überprüfung beim Auftragsverarbeiter gemäß dieser Anlage darf dieser eine angemessene Vergütung verlangen. Der Aufwand einer Überprüfung ist für den Auftragsverarbeiter grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

14.4 Sofern laut dieser Auftragsverarbeitung eine „schriftliche" Einwilligung oder sonstige Mitwirkung erforderlich ist, kann dies auch in Textform (z.B. per E-Mail) erfolgen.

Anhang zur Anlage 1

Für diesen Anhang gelten die im Vertrag getroffenen Begriffsbestimmungen.

1. Gegenstand der Datenverarbeitung

   Die personenbezogenen Daten sind Gegenstand der folgenden Datenverarbeitung: [**OPTION 1**: [FREITEXT])

   [**OPTION 2**: Die Datenverarbeitung und ihre Zwecke sind im Hauptvertrag beschrieben.]

2. Kategorien betroffener Personen

   Die folgenden Kategorien betroffener Personen sind von der Datenverarbeitung betroffen:

   Ggf. vorgegebene Auswahlfelder:

   ☐ Bestandskunden

   ☐ Interessenten/potentielle Kunden

   ☐ Newsletter-Abonnenten

   ☐ Websitenutzer/-besucher

   ☐ Bewerber

   ☐ Praktikanten/Werkstudenten

   ☐ Mitarbeiter (Stammbelegschaft, Auszubildende, Leiharbeiter, freie Mitarbeiter)

   ☐ Lieferanten/Subunternehmer/Ansprechpartner

   [Freitext]

3. Kategorien personenbezogener Daten

   Die folgenden Kategorien personenbezogener Daten sind von der Datenverarbeitung betroffen:

   ☐ Personalstammdaten (insb. Name, Anschrift, Geburtsdatum, Telefonnummer)

   ☐ Vertragsstammdaten (zum Beispiel Vertragsverhältnis, Name, Anschrift des Personals des Vertragspartners usw.)

   ☐ Adressdaten (z.B. Straße, Postfach, Postleitzahl)

☐ Kommunikationsdaten (z.B. E-Mail-Adresse, Telefonnummer, Mobilfunknummer)

☐ Fotografien von betroffenen Personen

☐ Internet-Protokoll-Adresse (IP-Adresse)

☐ Bankverbindungsdaten (z.B. IBAN, BIC)

☐ Gehalt des Mitarbeiters

☐ Bonitätsauskünfte, Kreditwürdigkeit und Betrugswarnungen

☐ Angaben zum Beschäftigungsverhältnis (Historie)

☐ Bestelldaten (aus Online-Shop)

☐ E-Mail-Nachrichten

[Freitext]

Die folgenden besonderen Arten personenbezogener Daten sind von der Datenverarbeitung betroffen:

☐ Informationen zu physischer und psychischer Gesundheit

☐ Informationen zur medizinischen Betreuung (z. B. Testergebnisse, Medikamente)

☐ Biometrische Identifikatoren (DNA, Finger, Iris und Stimme)

☐ Strafanzeigen, Verurteilungen und Gerichtsakten

☐ Informationen zu Sexualleben oder sexueller Orientierung

☐ Ethnische Herkunft

☐ Religiöse oder weltanschauliche Überzeugungen

☐ Gewerkschaftszugehörigkeit

4. Unterauftragnehmer

Der Auftragsverarbeiter beabsichtigt, folgende Unterauftragnehmer für die Verarbeitung personenbezogener Daten in Anspruch zu nehmen. Der Verantwortliche stimmt der Beauftragung der folgenden Unterauftragnehmer gem. Abschnitt zu:

Name des Unterauftragnehmers	Adresse	Auszuführende Arbeit	Internationale Übermittlung (soweit zutreffend)
[Freitext]	[Freitext]	[Freitext]	[Freitext]
[Freitext]	[Freitext]	[Freitext]	[Freitext]

5. Beschreibung der technischen und organisatorischen Maßnahmen

Um einen angemessenen Schutz der personenbezogenen Daten durch technisch-organisatorische Maßnahmen zu gewährleisten, setzt der Anbieter insbesondere, aber nicht ausschließlich, folgende Maßnahmen um:

5.1 Informationssicherheitsprogramm

Der Auftragsverarbeiter pflegt ein Informationssicherheitsprogramm, das den Einsatz von Personen, Prozessen und Technologien im Umgang mit personenbezogenen Daten regelt. Das beinhaltet:

☐ Der Auftragsverarbeiter muss einen oder mehrere Sicherheitsbeauftragte(n) ernennen, der/die für die Überwachung von Sicherheitsrichtlinien und -verfahren zuständig ist/sind.

☐ Der Auftragsverarbeiter bietet Sicherheitsschulungen an, um sicherzustellen, dass die Mitarbeiter über Sicherheitsrichtlinien und -verfahren und ihre jeweiligen Rollen informiert sind. Der Auftragsverarbeiter informiert das Personal außerdem über mögliche Konsequenzen einer Nichtbefolgung von Sicherheitsrichtlinien und -verfahren.

5.2 Zugangskontrolle

Der Auftragsverarbeiter stellt sicher, dass unbefugte Personen keinen Zugang zu Datenverarbeitungseinrichtungen (insbesondere Telefonsysteme, Datenbanken, Anwendungsserver und angeschlossene Hardware) erlangen, die für die Verarbeitung personenbezogener Daten genutzt werden. Das beinhaltet:

☐ Der Auftragsverarbeiter beschränkt durch den Einsatz einer Ausweiskontrolle den Zugang zu Einrichtungen, in denen sich Informationssysteme für die Verarbeitung personenbezogener Daten befinden, auf die befugten Mitarbeiter.

☐ Das Betriebsgelände des Auftragsverarbeiters wird rund um die Uhr von einem Sicherheitsdienst durch Videoüberwachung oder vergleichbare Methoden an allen Zugangspunkten überwacht.

☐ Der Auftragsverarbeiter macht von angemessenen Sicherheitsmaßnahmen zum Schutz vor Datenverlust durch Störungen wie Stromausfall Gebrauch.

5.3 Systemzugangskontrolle

Der Auftragsverarbeiter ergreift Maßnahmen, um zu verhindern, dass die Datenverarbeitungssysteme von unbefugten Personen genutzt werden können. Dazu gehört:

☐ Der Auftragsverarbeiter führt und aktualisiert eine Liste aller befugten Nutzer, die Zugang zu personenbezogenen Daten haben.

☐ Der Auftragsverarbeiter entfernt den Zugang von Nutzern, die nicht mehr beim Auftragsverarbeiter angestellt sind oder die ihre Rolle gewechselt haben.

5.4 Datenzugangskontrolle

☐ Der Auftragsverarbeiter stellt sicher, dass die zur Datenverarbeitung genutzten IT-Systeme den befugten Nutzern nur den beschränkten Zugang gewähren, den ihre individuellen Zugangsrechte vorgeben. Das beinhaltet:

- Die Rechte von Mitarbeitern auf Zugang zu personenbezogenen Daten sind auf das für ihre Arbeitsaufgaben notwendige Minimum zu beschränken.

- Personenbezogene Daten dürfen nur in vom Auftragsverarbeiter kontrollierten räumlich sicheren Bereichen gedruckt und nur an Mitarbeiter weitergegeben werden, die Kenntnis von ihnen haben müssen.

5.5 Aufgaben-/Auftragskontrolle

Der Auftragsverarbeiter stellt sicher, dass die personenbezogenen Daten nach den Anweisungen des Verantwortlichen verarbeitet werden. Das beinhaltet:

☐ Protokollierung aller Aktivitäten im Bereich der Datenverarbeitung; das beinhaltet auch erfolglose Zugangsversuche oder Berechtigungsänderungen;

☐ Regelmäßige Überprüfung der Systeme auf Informationssicherheitsvorfälle.

5.6 Verfügbarkeit

Der Auftragsverarbeiter stellt sicher, dass personenbezogene Daten nicht unbeabsichtigt verloren gehen oder vernichtet werden können. Das beinhaltet:

☐ Einführung/Bereitstellung von Betriebskontinuitätsplänen und -tests.

☐ Einsatz und regelmäßige Prüfung von Backup-Prozessen und andere Maßnahmen, um bei Bedarf eine schnelle Wiederherstellung von betriebskritischen Systemen und Daten zu ermöglichen.

☐ Nutzung unterbrechungsfreier Stromversorgungen (zum Beispiel: USV, Batterien, Generatoren), um die Stromversorgung von Rechenzentren sicherzustellen.

☐ Bereitstellung ausreichender Datenspeicherkapazitäten.

☐ Regelmäßige Prüfung von Notfallprozessen und -systemen.

5.7 Datentrennung

Der Auftragsverarbeiter stellt sicher, dass Daten, die für unterschiedliche Zwecke erhoben wurden, separat verarbeitet werden. Das beinhaltet die Nutzung technischer Möglichkeiten (zum Beispiel: mandantenfähige oder separate Systemlandschaften) zur Trennung der personenbezogenen Daten der Kunden.

5.8 Arbeitsplatzsicherheit

Der Auftragsverarbeiter ergreift die folgenden Maßnahmen, um die Sicherheit aller Arbeitsplätze zu gewährleisten, die für den Zugriff auf Systeme des Verantwortlichen zur Verarbeitung personenbezogener Daten genutzt werden:

☐ Eine kennwortgeschützte Tastatur-/Bildschirmsperre, die nach einer bestimmten Zeit der Inaktivität (spätestens nach 30 Minuten) automatisch aktiviert wird.

☐ Antiviren- und Desktop-Firewall-Programme werden ausgeführt.

☐ unverzügliche Installation von Sicherheitspatches

☐ Verwenden sicherer Kennwörter