Zusätzliche Vertragsbedingungen über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO
Ausgabe Februar 2021

1 Dauer der Verarbeitung

Die Auftragsdatenverarbeitung beginnt mit Vertragsschluss und erfolgt für die gesamte Dauer des Vertrages. Nachvertragliche Pflichten bleiben hiervon unberührt.

2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

2.1 Der Auftragnehmer übernimmt die folgende Verarbeitung personenbezogener Daten i.S. des Art. 4 Nr. 2 DSGVO:

- ☐ Erheben
- ☐ Erfassen
- ☒ Organisation
- ☐ Ordnen,
- ☒ Speicherung
- ☐ Anpassung oder Veränderung
- ☐ Auslesen
- ☐ Abfragen
- ☒ Verwendung
- ☐ Offenlegung durch Übermittlung
- ☐ Verbreitung oder eine andere Form der Bereitstellung
- ☐ Abgleich oder die Verknüpfung
- ☐ Einschränkung
- ☐ Löschen oder die Vernichtung

Die Verarbeitung erfolgt zu folgendem Zweck:

Auftragsabwicklung

2.2 Gegenstand der Verarbeitung sind folgende personenbezogene Daten i.S. des Art. 4 Abs. 1 DSGVO:

Name, Anschrift, Mailadrese, Telefon- und Fax

2.3 Von der Verarbeitung sind folgende Kategorien betroffener Personen umfasst:

Leitungsebene

2.4 Dem Auftragnehmer ist eine abweichende oder über die Festlegungen in den Ziffern 2.1 bis 2.3 hinausgehende Verarbeitung von Auftraggeberdaten untersagt. Dies gilt auch für die Verwendung anonymisierter Daten.

2.5 Die Verarbeitung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine Verlagerung der Verarbeitung personenbezogener Daten oder von Teilarbeiten dazu in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere ein angemessenes Schutzniveau für die betroffene Person gewährleistet ist (z. B. durch Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

3 Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Auftraggeberdaten nur im Rahmen der Regelungen dieser Vertragsbedingungen und ausschließlich im Auftrag und auf dokumentierte Weisung des Auftraggebers iSv Art. 28 Abs. 3 lit. a) DSGVO. Dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation.

3.2 Die Dokumentation kann in Textform erfolgen. Der Auftraggeber hat das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch "Weisungsrecht"). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

3.3 Weisungen werden vom Auftraggeber grundsätzlich zumindest in Textform erteilt. Mündlich erteilte Weisungen sind vom Auftragnehmer in Textform zu bestätigen. Die Parteien vereinbaren und dokumentieren die weisungs- und empfangsberechtigten Personen. Bei einem Wechsel oder einer längerfristigen Ver-

hinderung der darin benannten Personen ist der anderen Partei unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen. Der Auftragnehmer wird dem Auftraggeber einen Wechsel der Person des Empfangsberechtigten frühzeitig anzeigen. Bis zum Zugang einer solchen Mitteilung beim Auftraggeber gelten die benannten Personen weiter als empfangsberechtigt.

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

4 Schutzmaßnahmen des Auftragnehmers

4.1 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 Bestandteil des Vertrages. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

4.2 Der Auftragnehmer hat die Datensicherheit gem. Art. 32 DS-GVO und eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme zu gewährleisten. Er hat die nach Art. 28 Abs. 3 S. 2 Buchst. c in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO angemessenen technischen und organisatorischen Schutzmaßnahmen zu treffen. Insbesondere folgende besonderen technischen und organisatorischen Maßnahmen sind durch den Auftragnehmer bei der Verarbeitung einzuhalten:

4.2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren.
- Zugangskontrolle: Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
- 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.
- Trennungskontrolle: Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
- Pseudonymisierung: Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer konkreten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

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

- Weitergabekontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten bei elektronischer 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.
- 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

4.2.3 Verfügbarkeit und Belastbarkeit

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

- Belastbarkeit: Mindestmaßnahmen, die sicherstellen, dass im Falle eines Ausfalls der Datenverarbeitungssysteme diese rasch wiederhergestellt werden können.

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

- Datenschutz-Management
- Incident-Response-Management: Maßnahmen zur Unterstützung bei der Reaktion auf Sicherheitsverletzungen
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
- Auftragskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten, im Rahmen der Auftragsverarbeitung nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

4.3 Die technischen und organisatorischen Maßnahmen unterliegen dem Stand der Technik, 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.

4.4 Der Auftragnehmer hat den Auftraggeber unverzüglich in Textform zu informieren, wenn er Grund zu der Annahme hat, dass die Maßnahmen gemäß Absatz 2 nicht mehr ausreichend sind und wird sich mit ihm hinsichtlich weiterer technischer und organisatorischer Maßnahmen abstimmen.

4.5 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen. Das Sicherheitsniveau der festgelegten Maßnahmen ist fortlaufend zu gewährleisten und zu dokumentieren und dem Auftraggeber bei Verlangen nachzuweisen.

4.6 Ferner gewährleistet der Auftragnehmer, dass die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betrauten Personen (im Folgenden "Mitarbeiter") schriftlich gemäß Art. 28 Abs. 3 lit. b DSGVO zur Vertraulichkeit verpflichtet werden bzw. einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Einhaltung dieser Verpflichtung ist mit der gebotenen Sorgfalt sicherzustellen. Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

5 Informationspflichten des Auftragnehmers

5.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Insbesondere informiert er unverzüglich den Auftraggeber bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Datenverarbeitung der personenbezogenen Daten durch den Auftragnehmer, seiner Mitarbeiter oder durch Dritte.

5.2 Der Auftragnehmer informiert den Auftraggeber ebenfalls unverzüglich 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.

5.3 Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

5.4 Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses

Ersuchen unverzüglich an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

5.5 Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

5.6 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 ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als "Verantwortlichem" im Sinne der DSGVO liegen.

5.7 Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragen/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

5.8 Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen. An der Erstellung des Verzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

6 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieser Vertragsbedingungen die gesetzlichen Pflichten gemäß Art. 28 ff. DSGVO einzuhalten.
Insbesondere benennt er einen Datenschutzbeauftragten, sofern er nach den Vorschriften der Art. 37 ff. DSGVO dazu verpflichtet ist. Hat der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er schriftlich einen Vertreter in der Union nach Art. 27 Abs. 1 DSGVO.
Ein Wechsel des Datenschutzbeauftragten oder des Vertreters ist dem Auftraggeber unverzüglich mitzuteilen.

7 Unterauftragsverhältnisse

7.1 Der Auftragnehmer hat dafür Sorge zu tragen, dass die in diesen Vertragsbedingungen vereinbarten Regelungen auch gegenüber den von ihm beauftragten Unterauftragnehmer gelten, wobei dem Auftraggeber gegenüber dem Unterauftragnehmer sämtliche Kontrollrechte entsprechend diesen Vertragsbedingungen einzuräumen sind. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

7.2 Hat der Unterauftragnehmer seinen Sitz außerhalb der EU stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen im Sinne der Nr. 4.4 dieser Vertragsbedingungen sicher.

8 Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber ist berechtigt, sich regelmäßig von der Einhaltung der Regelungen dieser Vertragsbedingungen, insbesondere der Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß § 4 dieser Vereinbarung, zu überzeugen. Hierfür kann er Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers zu den üblichen Geschäftszeiten selbst persönlich bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

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

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

9 Berichtigung, Veränderung, Löschung und Rückgabe von personenbezogenen Daten

9.1 Der Auftragnehmer berichtigt, verändert oder löscht die zu verarbeitenden Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9.2 Nach Beendigung des Vertrages oder jederzeit auf Verlangen des Auftraggebers wird der Auftragnehmer diesem alle ihm mit im Rahmen des Vertragsverhältnisses überlassenen Dokumente, Unterlagen, Daten und Datenträger zurückgeben oder nach vorheriger Zustimmung des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragsnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren und auf Verlangen an den Auftragsgeber herauszugeben.

9.3 Die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ist ausgeschlossen.

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

9.5 Der Auftragnehmer ist verpflichtet, auch über das Ende des Vertrags hinaus die ihm im Zusammenhang mit dem Vertragsverhältnis bekannt gewordenen Daten vertraulich zu behandeln.

10 Haftung

10.1 Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag einschließlich dieser Vertragsbedingungen bleibt hiervon unberührt.

10.2 Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist Satz 1 gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.