

Besondere Vertragsbedingungen zur Auftragsverarbeitung -Regelungsteil (nach Art. 28 Abs. 3 DS-GVO)

Version: 2.2	Stand: 02/2023
---------------------	-----------------------

1. Gegenstand und Dauer der Vereinbarung

Der Auftragnehmer (AN)* verarbeitet im Rahmen seiner Leistungserbringung personenbezogene Daten für den Auftraggeber (AG)* im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieser Vertragsbedingungen.

Die vertraglich vereinbarte Dienstleistung ist ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum zu erbringen. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des AG und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der AG kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des AN gegen Datenschutzvorschriften oder die Bestimmungen dieser Vertragsbedingungen vorliegt, der AN eine Weisung des AG nicht ausführen kann oder will oder der AN Kontrollrechte des AG vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesen Vertragsbedingungen vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

* Hinweis: AN bzw. AG kann bei atypischen Verträgen auf individuelle Vertragsparteienbezeichnung abgeändert werden.

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

- 2.1. Sofern nicht durch die Leistungsbeschreibung definiert, ist Anlage zu Ziffer 2 auszufüllen. Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO) **siehe Anlage zu Ziffer 2.1** ausfüllen. (vom AG auszufüllen)
- 2.2. Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14, 15 DS-GVO) Anlage zu Ziffer 2.2 ausfüllen. (vom AG auszufüllen)
- 2.3. Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO) Anlage zu Ziffer 2.3 ausfüllen. (vom AG auszufüllen)

3. Rechte und Pflichten sowie Weisungsbefugnisse des AG

- 3.1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der AG verantwortlich. Gleichwohl ist der AN verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den AG gerichtet sind, unverzüglich an diesen weiterzuleiten.
- 3.2. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen AG und AN abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- 3.3. Der AG erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- 3.4. Der AG ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen sowie der in diesen Vertragsbedingungen festgelegten Verpflichtungen zu überzeugen.
- 3.5. Der AG informiert den AN unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
- 3.6. Der AG ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des AN vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertragsverhältnisses bestehen.

4. Weisungsberechtigte des AG, Weisungsempfänger des AN

4.1. Weisungsberechtigte Personen

Weisungsberechtigte Personen des AG s. **Anlage zu Ziffer 4.1a auszufüllen**, Weisungsempfänger beim AN s. **Anlage zu Ziffer 4.1b auszufüllen**.

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

4.2. Für die Weisung zu nutzende Kommunikationskanäle

Weisungen über E-Mail oder Internet dürfen nur erfolgen, wenn das Schriftstück verschlüsselt übertragen wurde und mit einer digitalen Signatur versehen worden ist. Der Postweg kann ebenfalls für Weisungen gewählt werden.

5. Pflichten des AN

- 5.1. Der AN verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des AG, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
- 5.2. Der AN verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des AG nicht erstellt.
- 5.3. Der AN sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den AG verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- 5.4. Die Datenträger, die vom AG stammen bzw. für den AG genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
- 5.5. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den AG, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des AG hat der

AN im notwendigen Umfang mitzuwirken und den AG soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat die dazu erforderlichen Angaben dem AG unverzüglich weiterzuleiten.

- 5.6. Der AN wird den AG unverzüglich darauf aufmerksam machen, wenn eine vom AG erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der AN ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim AG nach Überprüfung bestätigt oder geändert wird.
- 5.7. Der AN hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der AG dies mittels einer Weisung verlangt und berechtigte Interessen des AN dem nicht entgegenstehen.
- 5.8. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der AN nur nach vorheriger Weisung oder Zustimmung durch den AG erteilen.
- 5.9. Der AN erklärt sich damit einverstanden, dass der AG - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie dieser Vertragsbedingungen im angemessenen und erforderlichen Umfang selbst oder durch vom AG beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Der AN kann hierfür keine Vergütung verlangen.

Der AN sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

- 5.10. Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des AN) ist nur mit Zustimmung des AG gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.
- 5.11. Der AN bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem AG obliegen, die **Anlage zu Ziffer 5.11 ist auszufüllen:**

<< z. B. *Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis nach § 35 Abs. 1 SGB I, Berufgeheimnisse nach § 203 StGB etc.*) <<

- 5.12. Der AN verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des AG die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
- 5.13. Der AN sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO). Der AN überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
- 5.14. Der AN hat eine(n) Beauftragte(n) für den Datenschutz bestellt. Ein Wechsel des/der Datenschutzbeauftragten ist dem AG unverzüglich mitzuteilen.
- 5.15. Siehe **Anlage zu Ziffer 5.15** Datenschutzbeauftragte/r ist auszufüllen, es sei denn ein betrieblicher Datenschutzbeauftragter ist beim AN nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.
Ein Wechsel der/s Datenschutzbeauftragten ist dem AG unverzüglich mitzuteilen.
- 5.16. Der AN verpflichtet sich den AG über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des AN bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der AN teilt dem AG unverzüglich Störungen, Verstöße des AN oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des AG nach Art. 33 und Art. 34 DS-GVO. Der AN sichert zu, den AG erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den AG darf der AN nur nach vorheriger Weisung gem. Ziff. 4 dieser Vertragsbedingungen durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des AG ist dem AN gestattet, sofern es sich nicht um eine kritische Aufgabe im Sinne des § 47 Abs. 5 VgV handelt. (**Siehe Anlage 7.1 zu Ziffer 7**). Der Auftragnehmer ist verpflichtet im Rahmen seiner vertraglichen Vereinbarung mit seinem Subunternehmer die Inhalte dieser Besonderen Vertragsbedingungen durch seinen Subunternehmer sicherzustellen.

Im Falle der gestatteten Subunternehmerbeauftragung hat die Benennung der vom Subunternehmer zu erbringenden Leistung sowie seiner Daten gemäß Formblatt VHB 235 zu erfolgen.

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

- 8.1 Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden mindestens die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität der Systeme und Dienste, sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
- 8.2 Das in **Anlage 8.2** beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim AN dar.
- 8.3 Das in **Anlage 8.3** beschriebene wird als verbindlich festgelegt.
- 8.4 Der AN hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Das Ergebnis samt vollständigem Auditbericht ist dem AG mitzuteilen.
- 8.5 Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen AN und AG abzustimmen.
- 8.6 Soweit die beim AN getroffenen Maßnahmen den Anforderungen des AG nicht genügen, benachrichtigt er den AG unverzüglich.

- 8.7 Die Maßnahmen beim AN können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
- 8.8 Wesentliche Änderungen muss der AN mit dem AG in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer des Vertrages aufzubewahren.

9. Verpflichtungen des AN nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

- 9.1 Nach Abschluss der vertraglichen Arbeiten hat der AN sämtliche in seinen Besitz gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen.

10. Haftung

- 10.1. AG und AN haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.
- 10.2. Der AN haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der
 - er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
 - er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des AG handelte oder
 - er gegen die rechtmäßig erteilten Anweisungen des AG gehandelt hat.
- 10.3. Soweit der AG zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den AN vorbehalten.
- 10.4. Im Innenverhältnis zwischen AG und AN haftet der AN für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er
 - seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
 - unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des AG oder gegen diese Anweisungen gehandelt hat.
- 10.5. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

11. Vertragsstrafe

Bei Verstoß des AN gegen die Regelungen dieser Vertragsbedingungen wird eine Vertragsstrafe verwirkt. Die Höhe der Vertragsstrafe ist der **Anlage zu Ziffer 11** zu entnehmen.

12. Sonstiges

- 12.1 Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Gelungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
- 12.2 Änderungen und Ergänzungen zu diesen Vertragsbedingungen, einschließlich dieser Regelung, bedürfen zu ihrer Wirksamkeit der Schriftform. Die Schriftform wird nur durch eigenhändige Unterzeichnung durch beide Parteien gewahrt.
- 12.3 Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des AG beim AN durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der AN den AG unverzüglich zu verständigen.
- 12.4 Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den AG verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- 12.5 Sollten einzelne Bestimmungen dieser Vertragsbedingungen unwirksam sein oder werden, so wird die Wirksamkeit dieser Vertragsbedingungen im Übrigen nicht berührt. Die Parteien werden anstelle der unwirksamen Bestimmung eine wirksame Regelung treffen, die der unwirksamen Bestimmung inhaltlich und wirtschaftlich möglichst nahekommt. Im Falle von Regelungslücken werden die Parteien eine Regelung treffen, die sie getroffen hätten, wenn sie den betreffenden Punkt bei Abschluss des Vertrages bedacht hätten.