Begriffsdefinitionen

AN Der Auftragnehmer

AG Der Auftraggeber

LV
Leistungsvereinbarung zur Auftragsverarbeitung (DS-GVO-SIMPLE-CLOUD (LV).pdf) mit Stand gemäß Vertrag zur Auftragsverarbeitung (DS-GVO-SIMPLE-CLOUD (**AG**).pdf)

TOM
Technische und organisatorische Maßnahmen zur Auftragsverarbeitung (DS-GVO-SIMPLE-CLOUD (TOM).pdf) mit Stand gemäß Vertrag zur Auftragsverarbeitung (DS-GVO-SIMPLE-CLOUD (**AG**).pdf)

1. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den **AN** für den **AG** sind konkret in der **LV** beschrieben.

(2) Art der Daten

Die Art der verwendeten personenbezogenen Daten sind konkret in der **LV** beschrieben.

(3) Kategorien der Daten

Die Kategorien der durch die Verarbeitung betroffenen Personen sind konkret in der **LV** beschrieben.

2. Technisch-organisatorische Maßnahmen

(1) Der **AN** 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 **AG** zur Prüfung zu übergeben. Bei Akzeptanz durch den **AG** werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des **AG**s einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der **AN** hat die Sicherheit gem. Art. 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 Dokument **TOM**].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem **AN** gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

3. Berichtigung, Einschränkung und Löschung von Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des **AG**s unmittelbar durch den **AN** sicherzustellen.

4. Qualitätssicherung und sonstige Pflichten des AN

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

(1) Der AN ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim AN wird - **Herr Christian Huber, GL, +49 (8642) 597823, chuber@softsimple.de** - benannt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der **AN** 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 **AN** und jede dem AN unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des **AG** verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (Einzelheiten siehe Dokument **TOM**).

(4) Der **AG** und der **AN** arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des **AG** 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 **AN** ermittelt.

(6) Soweit der **AG** 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 **AN** ausgesetzt ist, hat ihn der **AN** nach besten Kräften zu

unterstützen.

(7) Der **AN** kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem **AG** im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

5. Unterauftragsverhältnisse

(1) 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 **AN** 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 **AN** ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des **AG** auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der **AN** darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des **AG** beauftragen.

a) Der **AG** stimmt der Beauftragung des nachfolgenden Unterauftragnehmer – im Folgenden als **UAN** bezeichnet - zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

STRATO AG Pascalstraße 10, 10587 Berlin

Der ***AN*** nimmt für die Verarbeitung von Daten im Auftrag des **AG** Leistungen des **UAN** in Anspruch, die in seinem Auftrag die Basis für die Bereitstellung der per SaaS bereitgestellten Applikation sicherstellen. Durch den ***UAN*** werden jedoch keine personenbezogenen Daten verarbeitet. Es erfolgt ausschließlich eine systemtechnische Bereitstellung eines Servers mit dem Betriebssystem Windows 2008 R2, Windows Server 2012 oder Windows Server 2016.

b) ☐ Die Auslagerung auf Unterauftragnehmer oder

☐ der Wechsel des bestehenden Unterauftragnehmers
sind zulässig, soweit:

- der **AN** eine solche Auslagerung auf Unterauftragnehmer dem **AG** eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der **AG** nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem **AN** 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.

(3) Die Weitergabe von personenbezogenen Daten des **AG** an den **UAN** und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

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

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;
☒ bedarf der ausdrücklichen Zustimmung des **AG** (mind. Textform);
☒ bedarf der ausdrücklichen Zustimmung des **AN** (mind. Textform);

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

6. Kontrollrechte des AGs

(1) Der **AG** hat das Recht, im Benehmen mit dem **AN** 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 **AN** in dessen Geschäftsbetrieb zu überzeugen.
(2) Der **AN** stellt sicher, dass sich der **AG** von der Einhaltung der Pflichten des **AN**s nach Art. 28 DS-GVO überzeugen kann. Der **AN** verpflichtet sich, dem **AG** auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) 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).

(4) Für die Ermöglichung von Kontrollen durch den **AG** kann der **AN** einen Vergütungsanspruch geltend machen.
(5) Der **AN** benennt mindestens eine empfangsberechtigte Person. Diese ist in der LV zu hinterlegen. Für den Fall, dass sich die empfangsberechtigten Personen beim **AN** ändern, wird der **AN** dies dem **AG** schriftlich oder in Textform mitteilen.

7. Mitteilung bei Verstößen des AN

(1) Der **AN** unterstützt den **AG** bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

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 **AG** zu melden
c) die Verpflichtung, dem **AG** 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 **AG**s für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des **AG**s im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des **AN**s zurückzuführen sind, kann der **AN** eine Vergütung beanspruchen.

8. Weisungsbefugnis des AG

(1) Der **AG** hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem **AN** zu erteilen. Weisungen können

☒ schriftlich
☒ per Fax
☒ per E-Mail
☒ mündlich

erfolgen. Der **AG** soll mündliche Weisungen, sofern diese in diesem Vertrag für Weisungen zulässig sind, unverzüglich in Textform (z.B. Fax, E-Mail) gegenüber dem **AN** bestätigen.

(2) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des **AG**s beim **AN** entstehen, bleiben unberührt.

(3) Der **AG** benennt mindestens eine weisungsberechtigte Person sowie einen Vertreter. Für den Fall, dass sich die weisungsberechtigten Personen beim **AG** ändern, wird der **AG** dies dem **AN** schriftlich oder in Textform mitteilen.

(4) Mündliche Weisungen bestätigt der **AG** unverzüglich (mind. Textform).

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

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des **AG**s 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.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den **AG** – spätestens mit Beendigung der Leistungsvereinbarung – hat der **AN** sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem **AG** auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den **AN** entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem **AG** übergeben.

10. Wahrung von Betroffenenrechten

(1) Der **AG** ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Soweit eine Mitwirkung des **AN**s für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den **AG** erforderlich ist, wird der **AN** die jeweils erforderlichen Maßnahmen nach Weisung des **AG**s treffen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem **AG** beim **AN** entstehen, bleiben unberührt.

11. Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12. Vergütung

Die Vergütung des **AN**s wird gesondert vereinbart.

13. Beendigung

(1) Nach Beendigung des Vertrages hat der **AN** sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem **AG** auszuhändigen. Die Datenträger des **AN**s sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim **AN**. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

(2) Der **AG** hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim **AN** zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des **AN**s erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den **AG** angekündigt werden.

14. Zurückbehaltungsrecht

*Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den **AN** i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.*

15. Schlussbestimmungen

(1) Sollte das Eigentum des **AG**s beim **AN** durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der **AN** den **AG** unverzüglich zu informieren. Der **AN** wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.