Auftragsverarbeitungsvertrag bezüglich der Nutzung der Centify-Plattform zur Provisionsabrechnung

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag zwischen der **Centify GmbH („Auftragnehmer")** und dem im Hauptvertrag genannten Vertragspartner **(„Auftraggeber")**

1. Vertragsgegenstand

Im Rahmen der Bereitstellung der SaaS-Plattform zur Provisionsabrechnung von Centify nach Maßgabe der Centify AGB **(„Hauptvertrag")** ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber entweder als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften oder seinerseits als Auftragsverarbeiter für andere Verantwortliche (z.B. verbundene Gruppenunternehmen) fungiert (nachfolgend „**Auftraggeber-Daten**" genannt). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten zur Durchführung des Hauptvertrages.

2. Umfang und Gegenstand der Auftragsverarbeitung

2.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag (bzw., soweit der Auftraggeber selbst Auftragsverarbeiter ist, im Unterauftrag) und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung).

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt in der Art, dem Umfang und zu dem Zweck wie nachfolgend spezifiziert; die Verarbeitung betrifft die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen:

Zweck der Datenverarbeitung	Bereitstellung und Betrieb der vom Auftraggeber bezogenen Centify Services, insbesondere Bereitstellung und Betrieb der SaaS-Plattform für Provisionsbe- und abrechnung sowie damit verbundener Dienstleistungen.
Art und Umfang der Datenverarbeitung	– Verarbeitung von Informationen im Zuge der Bereitstellung des in Anspruch genommenen Service; Art und Umfang der Datenverarbeitung richten sich hierbei nach den in Anspruch genommenen Services. Hierbei kommen insbesondere das Erheben, das Erfassen, die Speicherung, das Auslesen, das Abfragen, das Verwenden und das Löschen von Daten im Zusammenhang mit Provisionsabrechnungen in Frage. – Anonymisierung von Nutzungsdaten zur Ermöglichung technischer Analysen.
Art der Daten	– Vom Auftraggeber zur Verfügung gestellte Daten; hierbei kann es sich prinzipiell um alle Arten personenbezogener Daten handeln, die in Dokumenten und anderen elektronischen Formaten enthalten sind, die unter Nutzung der Centify Services verarbeitet werden; also insbesondere alle personenbezogenen Daten jeglicher Art, die der Auftraggeber auf der Cenbtify-Plattform eingibt; bestimmungsgemäß ist die Art der Daten nicht beschränkt.

	– Insbesondere fallen darunter: Stammdaten (z.B. Anrede, Name, Personalnummer, Steueridentifikationsnummer, Anschrift), Provisionsdaten (z. B. Daten im Zusammenhang mit Verkaufstransaktionen, Provisionsstrukturen, Provisionssätzen und Zahlungen), Finanzdaten (z. B. gestellte Rechnungen, Zahlungsinformationen für Provisionsauszahlungen) sowie Transaktionsdaten (z. B. Daten im Zusammenhang mit Verkaufstransaktionen, die über die Centify-Plattform abgewickelt werden).
Kategorien betroffener Personen	Alle Personen, für die Provisionen berechnet werden; insbesondere Geschäftskunden und deren Mitarbeiter und/ oder sonstige mit dem Geschäftskunden in einer Beziehung stehende Dritte.

2.3 Außerdem erfasst der Auftragnehmer die Nutzung des Services durch den Auftraggeber (nachfolgend „Nutzungsdaten“ genannt, die ebenfalls Auftraggeber-Daten im Sinne dieses Vertrages darstellen) und verarbeitet diese Nutzungsdaten im Auftrag des Auftraggebers zum Zwecke der Erfüllung des Vertrags, der bedarfsgerechten Gestaltung der Plattform, der Bereitstellung von Nutzungsübersichten und -analysen, der Gewährleistung von IT- und Datensicherheit und der Fehlerdiagnose und -behebung. Zu diesem Zweck wird der Auftragnehmer die Nutzungsdaten ebenfalls anonymisieren und in dieser Form verarbeiten. Dem Auftragnehmer bleibt es vorbehalten, anonymisierte Nutzungsdaten für eigene Zwecke zu verarbeiten, z.B. um seine Leistungen zu verbessern und weiterzuentwickeln. Die Parteien stimmen darin überein, dass dieser Vertrag nicht auf die Verarbeitung von anonymisierten Nutzungsdaten Anwendung findet. Eine Verarbeitung von Nutzungsdaten in nicht anonymisierter Form für eigene Zwecke des Auftragnehmers bleibt im Rahmen des datenschutzrechtlich Zulässigen (insbesondere etwa zur Erfüllung von gesetzlichen Pflichten) hiervon unberührt.

2.4 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.5 Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44–48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt. Für den Fall einer Verarbeitung in einem Drittland durch einen weiteren Auftragsverarbeiter gelten die Regelungen in Ziff. 7.4.

3. Weisungsbefugnisse des Auftraggebers

3.1 Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Die Weisungen des Auftraggebers sind grundsätzlich abschließend in diesem Vertrag und seinen Anlagen festgelegt und dokumentiert. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, sind nur im Einklang mit dem Mechanismus zur Leistungsänderung zulässig, wie er im Hauptvertrag geregelt ist.

3.3 Der Auftragnehmer gewährleistet, dass er die Auftraggeber-Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt aber nicht verpflichtet, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die Rechtskonformität der Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt.

4. Verantwortlichkeit des Auftraggebers

4.1 Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer wegen einer vermeintlich unzulässigen Verarbeitung von Auftraggeber-Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach Maßgabe des Hauptvertrages zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

4.3 Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4.4 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

5. Verpflichtung zur Vertraulichkeit

Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung dieser Daten zur Vertraulichkeit zu verpflichten.

6. Sicherheit der Verarbeitung

6.1 Der Auftragnehmer wird gemäß Art. 32 DSGVO erforderliche, geeignete technische und organisatorische Maßnahmen ergreifen, die im Hinblick auf die vom Auftraggeber in Anspruch genommenen Leistungen unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der

Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten. Der Auftragnehmer verpflichtet sich, die in **Anhang 1** benannten technischen und organisatorischen Maßnahmen umzusetzen und während der Vertragslaufzeit aufrecht zu erhalten.

6.2 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

6.3 Der Auftraggeber ist verpflichtet, dem Auftragnehmer einen möglichen Missbrauch seiner Accounts oder Authentifizierungsdaten oder sicherheitsrelevante Vorfälle im Zusammenhang mit der Nutzung seiner Systemzugänge unverzüglich mitzuteilen.

7. Inanspruchnahme weiterer Auftragsverarbeiter

7.1 Der Auftraggeber erteilt dem Auftragnehmer hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von Auftraggeber-Daten in Anspruch zu nehmen. Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen weiteren Auftragsverarbeiter sind:

Firma, Anschrift	**Ort der Daten-verarbeitung**	**Art der Dienstleistung**
Google Ireland Limited, Europe HQ, Google Building Gordon House, 4 Barrow St, Dublin, D04 E5W5, Irland	Europäische Union	Google Cloud Platform und Services
MailerSend, Inc., 228 Park Ave S, PMB 54955, New York, New York 10003-1502, USA	USA	E-Mail-Benachrichtigungsdienst für den E-Mail-Versand

Generell nicht genehmigungspflichtig ist die Inanspruchnahme von Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen oder andere Nebenleistungen ausführen, die keine Verarbeitung von Auftraggeber-Daten mit sich bringen, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann, solange der Auftragnehmer angemessene Regelungen zum Schutz der Vertraulichkeit der Auftraggeber-Daten trifft.

7.2 Der Auftragnehmer wird den Auftraggeber über beabsichtigte Änderungen in Bezug auf die Inanspruchnahme oder die Ersetzung weiterer Auftragsverarbeiter in geeigneter Form informieren; z.B. per E-Mail an die hinterlegte E-Mail Adresse. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Inanspruchnahme eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung per Textform Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Inanspruchnahme. Erhebt der

Auftraggeber Einspruch, kann der Auftragnehmer die Testphase-AGB nach dortiger Maßgabe kündigen.

7.3 Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

7.4 Unter Einhaltung der Anforderungen der Ziffer 2.5 dieses Vertrags gelten die Regelungen in dieser Ziffer 7 auch, wenn ein weiterer Auftragsverarbeiter in einem Drittstaat eingeschaltet wird. In einem solchen Fall ist der Auftragnehmer berechtigt und – soweit die Anforderungen der Ziff. 2.4 nicht anderweitig erfüllt werden – verpflichtet, mit dem weiteren Auftragsverarbeiter einen Vertrag unter Einbeziehung der Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates nach Maßgabe des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 unter Einbeziehung des Moduls 3 (Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter) zu schließen. Die Parteien sind sich einig, dass auch ein solcher Vertrag die Anforderungen gemäß Ziff. 7.3 erfüllt. Der Auftraggeber erklärt sich bereit, an der Erfüllung der Voraussetzungen nach Art. 49 DSGVO im erforderlichen Maße mitzuwirken.

8. Rechte der betroffenen Personen

8.1 Der Auftragnehmer wird den Auftraggeber mit technischen und organisatorischen Maßnahmen im Rahmen des Zumutbaren dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

8.2 Soweit eine betroffene Person einen Antrag auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten, sofern ihm eine hinreichend sichere Identifikation des Antragstellers und eine Zuordnung zum Auftraggeber möglich und zumutbar ist.

8.3 Der Auftragnehmer wird es dem Auftraggeber ermöglichen, im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Auftraggeber-Daten zu berichtigen, zu löschen oder ihre weitere Verarbeitung einzuschränken oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

8.4 Soweit die betroffene Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten nach Art. 20 DSGVO besitzt, wird der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Bereitstellung der Auftraggeber-Daten in einem gängigen und maschinenlesbaren Format unterstützen.

9. Mitteilungs- und Unterstützungspflichten des Auftragnehmers

9.1 Soweit den Auftraggeber eine gesetzliche Melde- oder Benachrichtigungspflicht wegen einer Verletzung des Schutzes von Auftraggeber-Daten (insbesondere nach Art. 33, 34 DSGVO) trifft, wird der Auftragnehmer den Auftraggeber unverzüglich über etwaige meldepflichtige Ereignisse in seinem Verantwortungsbereich informieren. Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten unterstützen.

9.2 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

10. Datenlöschung

10.1 Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages gemäß der Weisung des Auftraggebers entweder löschen oder an ihn herausgeben (und dann im Anschluss eine etwa beim Auftragnehmer verbliebene Kopie löschen), sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Daten besteht.

10.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

11. Nachweise und Überprüfungen

11.1 Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

11.2 Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

11.3 Zur Durchführung von Inspektionen nach Ziffer 11.2 ist der Auftraggeber berechtigt, im Rahmen der üblichen Geschäftszeiten (montags bis freitags von 10 bis 18 Uhr) nach rechtzeitiger Vorankündigung gemäß Ziffer 11.5 auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers zu betreten, in denen Auftraggeber-Daten verarbeitet werden.

11.4 Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des

Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Überprüfungszwecke sind, zu erhalten.

11.5 Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens zwei Wochen vorher) über alle mit der Durchführung der Überprüfung zusammenhängenden Umstände zu informieren. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

11.6 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund von dieser Ziffer 11 dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf mit der Kontrolle ausschließlich unabhängige Dritte wie insbesondere Beratungsgesellschaften, Wirtschaftsprüfer o.ä. beauftragen. Das Unternehmen, das mit der Kontrolle beauftragt werden soll, wird dem Auftragnehmer vor Beauftragung mitgeteilt. Der Auftragnehmer erhält das Recht, ungeeigneten Dritten zu widersprechen.

11.7 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrag anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. eines Wirtschaftsprüfers, oder eines Datenschutz- oder Qualitätsauditors) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach ISO 27001 oder BSI-Grundschutz – („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

11.8 Eine Überprüfung der Sicherheit der Verarbeitung bei etwaigen Unterauftragsverarbeitern des Auftragnehmers obliegt allein dem Auftragnehmer.

12. Schlussbestimmungen

12.1 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

12.2 Soweit dieser Vertrag keine Regelungen enthält, gelten die Regelung des Hauptvertrages sowie die darin in Bezug genommenen Regelungen. Im Fall von Widersprüchen zwischen diesem Auftragsverarbeitungsvertrags und sonstigen Vereinbarungen zwischen den Parteien gehen die Regelungen dieses Vertrags vor.

Anhang 1 – Technische und Organisatorische Maßnahmen

Kontrollziele bezüglich des Umgangs mit personenbezogenen Daten	**Maßnahmen**
1. Vertraulichkeit 1.1 Zutrittskontrolle (Räume und Gebäude) Zielbeschreibung: Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.	Die Geschäftsräume sind stets verschlossen. Der Zutritt zu den Geschäftsräumen wird durch eine Büroschließanlage geschützt. Die Ausgabe von Schlüsseln und Zugangsmitteln zur Büroschließanlage erfolgt ausschließlich personalisiert; geteilte Zugangsmittel werden nicht ausgegeben.
1.2 Zugangskontrolle (IT-Systeme, Anwendungen) Zielbeschreibung: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Die Datenverarbeitungssysteme werden insbesondere durch Firewall-Systeme (Software) geschützt. Die Verwaltung der Sicherheitssoftware wird regelmäßig sichergestellt und erfolgt nur durch autorisiertes Personal. Die Autorisierung des Personals wird durch zugeordnete Benutzerrechte bzw. Benutzerprofile sichergestellt. Über diese Profile kann eine Anmeldung an den jeweiligen IT-Systemen mittels E-Mail-Adresse und Passwort und, soweit möglich, unter Einbindung einer Zwei-Faktor-Authentifizierung erfolgen. Zugriffe auf Datenverarbeitungssysteme erfolgen über gesicherte Verbindungen. Zur Verringerung des Risikos des Ablesens von Daten während des Transports zwischen IT-Systemen werden Netzwerksegmente gebildet. Der Zugang für Entwicklungsteams zu Entwicklungs- und Testumgebungen sowie der operative Zugang zu Produktivumgebungen ist ausschließlich über eine Authentifizierung möglich und erfolgt nicht ungeschützt über das Netzwerk. Zugangsdaten werden durch Verschlüsselungs- und Authentifizierungsverfahren (SSL/TLS, HTTPS, SSH, SFTP) gegen unbefugtes Abfangen geschützt.
1.3 Zugriffskontrolle auf Daten Zielbeschreibung: Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass	Zugriffsberechtigungen werden ausschließlich für diejenigen IT-Systeme und Verarbeitungsvorgänge erteilt, die für die jeweilige Aufgabenwahrnehmung erforderlich sind („Prinzip der geringsten Privilegien“). Die Rechtevergabe wird gemäß Berechtigungskonzept umgesetzt und die Verwaltung obliegt den Systemadministratoren. Grundsätzlich ist die Anzahl der Administratoren

personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	nur auf das „Notwendigste“ beschränkt. Um den Zugriff auf Daten nur autorisiertem Personal zu ermöglichen, werden Datenträger und Daten verschlüsselt und der Zugriff über die Nutzerrechte reguliert. Zugriffe auf Daten erfolgen stets über verschlüsselte Protokolle wie SSH oder TLS (z. B. HTTPS). Die Authentifizierung gegenüber dem Kernsystem der Centify GmbH erfolgt über das OAuth-2-Protokoll. Die Authentifizierung gegenüber den die Daten enthaltenden Managementsystemen erfolgt mittels E-Mail-Adresse und Passwort und, soweit möglich, unter Einbindung einer Zwei-Faktor-Authentifizierung - jeder Mitarbeiter kann im Rahmen seines Tätigkeitsbereiches nur auf die notwendigen Funktionen zur Verrichtung seiner Tätigkeiten zugreifen. Die Mitarbeitenden der Centify GmbH unterliegen strikten Beschränkungen hinsichtlich der Weitergabe von Passwörtern sowie der Nutzung gemeinsamer Benutzerkonten („Shared Accounts“) für den Zugriff auf Kunden- und Administrationssysteme. Der unrechtmäßige Zugriff auf Systeme oder auf die Datenintegrität über Sicherheitslücken in Programmen wird durch regelmäßiges Monitoring der Infrastruktur und umgehende Behebung gefundener Probleme verhindert. Sowohl externe als auch interne Zugriffe werden dadurch erkannt und deren Auswirkungen minimiert. Kundendaten auf den Servern des Hosting-Dienstleisters werden verschlüsselt gespeichert. Die Datenspeicherung erfolgt nach dem Stand der Technik und unter Beachtung anerkannter Standards der Informationssicherheit. Mitarbeitende der Centify GmbH sind verpflichtet, Kundendaten nicht auszudrucken oder lokal (z. B. auf Arbeitsplatzrechnern oder mobilen Endgeräten) zu speichern, es sei denn, dies ist für die Aufgabenerfüllung zwingend erforderlich. Mitarbeitende beenden aktive Computersitzungen oder melden sich aus sämtlichen Anwendungen/Systemen ab, wenn sie ihre Arbeit beenden. Sensible physische Dokumente werden bei Nichtnutzung weggeschlossen und sind, wenn sie nicht mehr benötigt werden und keiner Aufbewahrungspflicht unterliegen, in Übereinstimmung mit datenschutzrechtlichen Vorgaben sicher zu vernichten. Schlüsselverwaltung: Die Schlüssel für den Zugang zu den Datenbanken der Centify GmbH

	werden durch ein zentrales System verwaltet, das ausschließlich über ein Master-Passwort zugänglich ist, das nur bestimmten, dazu autorisierten Mitarbeitenden zur Verfügung steht.
1.4 Eingabekontrolle in Datenverarbeitungs-systeme Zielbeschreibung: Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.	Durch die restriktive Vergabe von Rechten durch individuelle Benutzer wird die Eingabe, Änderung oder Entfernung von personenbezogenen Daten in Datenverarbeitungssystemen eingeschränkt. Es wird jede Eingabe, Änderung und Entfernung von Daten protokolliert. Kontrolle des Zugriffs durch Dritte: Soweit Dritte Zugriff auf personenbezogene Daten erhalten, wird dieser Zugriff auf einer „Need-to-know"-Basis auf das zur Aufgabenerfüllung erforderliche Maß beschränkt. Zur Aufdeckung von Missbrauch werden regelmäßige Auswertungen stichprobenartig durchgeführt.
1.5. Datentrennungskontrolle (zweckbezogen) Zielbeschreibung: Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Die Centify GmbH stellt durch eine logische Mandantentrennung sicher, dass Daten verschiedener Kunden getrennt verarbeitet und gespeichert werden. Die Zuordnung und Identifizierung der Daten erfolgt durch die Vergabe eines eindeutigen Identifikators an jeden Kunden (z.B. Kundennummer/Organisations-ID).
2. Integrität (Art. 32 Abs. 1 lit. b DSGVO) 2.1 Weitergabekontrolle von Daten Zielbeschreibung: Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen 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 Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Alle Mitarbeitenden sowie sonstige Personen, die auf Weisung des Verantwortlichen handeln, sind nachweislich auf den Datenschutz und die Wahrung der Vertraulichkeit im Sinne von Art. 32 Abs. 1 lit. b DSGVO zu verpflichten. Personenbezogene Daten dürfen im Auftrag des Kunden nur im Rahmen der Weisungen und nur insoweit weitergegeben werden, wie dies für die Erbringung der vertraglich geschuldeten Leistungen für den Verantwortlichen erforderlich ist. Der elektronische Datenaustausch wird durch Sicherungssysteme überwacht, sämtliche ein- und ausgehenden Datenströme des Kernsystems werden durch eine Transportverschlüsselung (z. B. TLS/HTTPS) geschützt. Soweit eine Übermittlung von Daten an Server erforderlich ist, bei denen keine Übertragung über TLS-verschlüsselte HTTPS-Uploads möglich ist, erfolgt die Übertragung mittels Secure File Transfer Protocol (SFTP) oder eines sonstigen dem Stand der Technik entsprechenden, verschlüsselten Verfahrens.

	Grundsätzlich werden alle von Mitarbeitenden versandten E-Mails mit TLS 1.2 oder höher verschlüsselt.
3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs.1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO) 3.1 Auftragskontrolle Zielbeschreibung: Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Mitarbeiterverpflichtung & Schulung: Alle Mitarbeiter sind schriftlich auf das Datengeheimnis und die Weisungsgebundenheit verpflichtet. Strikte Datentrennung (Mandantentrennung): Technische Gewährleistung, dass Daten verschiedener Kunden logisch getrennt verarbeitet werden. Ein Zugriff oder eine Vermischung von Daten unterschiedlicher Auftraggeber ist systemseitig ausgeschlossen. Rollen- und Berechtigungskonzept: Zugriff auf Kundendaten haben nur autorisierte Mitarbeiter im Rahmen ihrer Aufgabenerfüllung (Need-to-Know-Prinzip). Administrative Zugriffe werden protokolliert. Lieferantenauswahl: Die Centify GmbH wählt Dienstleister, Lieferanten und sonstige Geschäftspartner sorgfältig aus. Die datenschutzrechtlichen Regelungen und Vorkehrungen der Geschäftspartner werden im Vorfeld geprüft, um einen insgesamt datenschutzkonformen Prozess zu gewährleisten.
4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs.1 lit. b DSGVO) 4.1 Verfügbarkeitskontrolle von Daten Zielbeschreibung: Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Um zufällige Zerstörung oder Verlust im Rahmen der auftragsbezogenen Verarbeitung von Daten einzuschränken, wurde ein Backup- & Recoverykonzept mit stündlichen inkrementellen Backups und wöchentlichen Vollbackups aller relevanten Daten erstellt und implementiert. Backups von Datenbanksystemen werden ausschließlich in verschlüsselter Form vorgehalten. Die Centify GmbH setzt Point-in-Time-Recovery ein, um Datenbanken zu einem bestimmten Zeitpunkt wiederherstellen zu können, und verhindert unbefugte Zugriffe auf Daten in Backups, lokal gespeicherten Caches oder Datenbanken sowohl organisatorisch als auch technisch. Die Verfügbarkeit und der Status der Serversysteme werden durch ein Warnsystem überwacht; im Falle eines Ausfalls wird das Incident-Response-Team automatisch

	benachrichtigt, um unverzüglich Gegenmaßnahmen einzuleiten. Die Centify GmbH verfügt über ein internes Konzept zum Umgang mit Informationssicherheitsvorfällen. Dieses regelt insbesondere die Erkennung, Bewertung und Behebung sicherheitsrelevanter Ereignisse sowie die internen und externen Kommunikationswege im Falle eines Sicherheitsvorfalls.
5. Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) Zielbeschreibung: Es ist zu gewährleisten, dass zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, frühzeitig getroffen werden.	Die Centify GmbH berücksichtigt die Anforderungen des Artikels 25 DSGVO bereits in der Konzeptionierungs- und Entwicklungsphase ihrer Produkte. Prozesse und Funktionalitäten werden so ausgestaltet, dass datenschutzrechtliche Grundsätze wie Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung sowie die Sicherheit der Verarbeitung frühzeitig berücksichtigt werden.