

**VEREINBARUNG ÜBER AUFTRAGS-
VERARBEITUNG**

zwischen

Bundesdruckerei GmbH

Kommandantenstraße 18

10969 Berlin

– nachstehend Bundesdruckerei genannt –

und

[Vollständiger Name, inkl. jur. Form und Adresse des Partners]

dem im Zuschlagsschreiben namentlich bezeichneten Unternehmen

– nachstehend "**AUFTRAGNEHMER**" genannt –

(die Bundesdruckerei und der Auftragnehmer werden nachfolgend auch als die "**Parteien**" bezeichnet, einzeln jeweils als "**Partei**")

Inhaltsverzeichnis

PRÄAMBEL	3
§ 1 Vertragsgegenstand	3
§ 2 Begriffsbestimmungen	3
§ 3 Rechte und Pflichten sowie Weisungsbefugnisse Bundesdruckerei	3
§ 4 Weisungsberechtigt bei Bundesdruckerei, Weisungsempfänger beim Auftragnehmer	4
§ 5 Pflichten des Auftragnehmers	4
§ 6 Weitere datenschutzrechtliche Maßnahmen beim Auftragnehmer	5
§ 7 Datenverarbeitung in der Europäischen Union	6
§ 8 Unterauftragsverhältnisse	7
§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO	8
§ 10 Haftung des Auftragnehmers	8
§ 11 Dauer und Beendigung dieses Vertrags	8
§ 12 Ausschluss des Zurückbehaltungsrechts	9
§ 13 Schlussbestimmungen	9

PRÄAMBEL

Die Parteien haben eine Vereinbarung über die Erbringung von Leistungen durch den Auftragnehmer abgeschlossen. Bei der Erbringung seiner Leistungen verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag der Bundesdruckerei; zumindest kann dies nicht ausgeschlossen werden. Mit diesem Vertrag über die Auftragsverarbeitung wollen die Parteien die rechtliche Grundlage für die Datenverarbeitung durch den Auftragnehmer schaffen und insbesondere die Pflichten des Auftragnehmers in diesem Zusammenhang konkretisieren.

§ 1 Vertragsgegenstand

- 1.1 Zwischen den Parteien besteht ein Vertrag über „Lizenzen und Implementierung einer Cloud-Lösung für das Lieferantenmanagement“ ("**Leistungsvereinbarung**"). Der Gegenstand der Beauftragung des Auftragnehmers ergibt sich aus der Leistungsvereinbarung.
- 1.2 Im Rahmen der Durchführung der Leistungsvereinbarung verarbeitet der Auftragnehmer personenbezogene Daten für die Bundesdruckerei. Dabei handelt es sich um eine Datenverarbeitung im Auftrag gemäß Art. 28 DSGVO.
- 1.3 Die Art der Verarbeitung von Daten, die Art der betroffenen personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus dem **Anhang A**. Dort finden sich auch Informationen zum Gegenstand des Auftrags sowie zum Zweck der Verarbeitung.
- 1.4 Die weiteren Einzelheiten der Rechte und Pflichten beider Parteien im Rahmen einer Auftragsverarbeitung regelt dieser Vertrag.

§ 2 Begriffsbestimmungen

- 2.1 Datenschutz-Grundverordnung ("**DSGVO**") bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG unter Einbeziehung der am 19. April 2018 von der EU veröffentlichten Korrekturen zur Datenschutz-Grundverordnung. Für verwendete Begriffe, für die Art. 4 DSGVO eine Begriffsbestimmung vorsieht, gilt diese gesetzliche Definition in der im Zeitpunkt des Vertragsschlusses geltenden Fassung.
- 2.2 **Besonders schutzwürdige personenbezogene Daten** sind einerseits besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, genetische Daten gemäß Art. 4 Abs. 13 DSGVO, biometrische Daten gemäß Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gemäß Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Umfasst sind ebenfalls personenbezogene Daten gemäß Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse der Bundesdruckerei

- 3.1 Für die Beurteilung der Zulässigkeit der Verarbeitung, insbesondere gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist der Verantwortliche für die Datenverarbeitung zuständig. Gleichwohl ist der Auf-

tragnehmer verpflichtet, alle Anfragen, sofern sie erkennbar ausschließlich an die Bundesdruckerei gerichtet sind oder eine datenschutzrechtliche Verpflichtung der Bundesdruckerei betreffen, unverzüglich an diese weiterzuleiten.

- 3.2 Änderungen des Verarbeitungsgegenstands und Änderungen der Verfahren der Verarbeitung sind gemeinsam zwischen Bundesdruckerei und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format (beispielsweise E-Mail), unter Berücksichtigung der Leistungsvereinbarung, festzulegen.
- 3.3 Die Bundesdruckerei erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind gültig; die Bundesdruckerei wird sich bemühen, diese innerhalb angemessener Frist schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- 3.4 Die Bundesdruckerei ist berechtigt, sich vor Beginn der Tätigkeit des Auftragnehmers und dann in regelmäßigen Abständen in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftragnehmer wird bei Überprüfungen (Audits) in dem erforderlichen Umfang mitwirken; Kosten für die Mitwirkung des Auftragnehmers entstehen für die Bundesdruckerei nicht. Der Auftragnehmer ist auch damit einverstanden, dass die Bundesdruckerei Dritte mit der Überprüfung (Audits) beauftragt. Es gilt Art. 28 Abs. 3 Satz 2 lit. h DSGVO. Die Auftragnehmer stellt der Bundesdruckerei alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.
- 3.5 Die Bundesdruckerei wird sich bemühen, den Auftragnehmer in angemessener Zeit zu informieren, wenn sie Fehler oder Unregelmäßigkeiten bei einer etwaigen Überprüfung der Auftragsergebnisse erkennt.

§ 4 Weisungsberechtigt bei der Bundesdruckerei, Weisungsempfänger beim Auftragnehmer, Verstoß von Weisungen gegen gesetzliche Vorschriften

4.1 Weisungsberechtigt ist/sind bei der Bundesdruckerei:

Patrick Raatz, patrick.raatz@bdr.de, M + 49 151 - 16925482

4.2 Weisungsempfänger ist/sind beim Auftragnehmer:

[...] (Vorname, Name, ggf. Organisationseinheit, Telefon und Erreichbarkeit per E-Mail)

- 4.3 Bei einem Wechsel oder einer längerfristigen Verhinderung der Weisungsberechtigten sind der anderen Partei unverzüglich und schriftlich oder in einem dokumentierten elektronischen Format die Nachfolger bzw. Vertreter mitzuteilen.
- 4.4 Der Auftragnehmer wird die Bundesdruckerei unverzüglich darauf aufmerksam machen, wenn eine von der Bundesdruckerei erteilte Weisung nach seiner Ansicht gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis durch die Bundesdruckerei die Gültigkeit der Weisung bestätigt oder die Weisung geändert wird.

§ 5 Pflichten des Auftragnehmers

- 5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen vertraglichen Vereinbarungen und nach den Weisungen der Bundesdruckerei, sofern

er nicht durch das Recht der Europäischen Union oder durch sein Heimatrecht zu einer anderen Verarbeitung verpflichtet ist (beispielsweise bei Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer der Bundesdruckerei 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 DSGVO).

- 5.2 Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen der Bundesdruckerei nicht erstellt, sofern dies nicht zur Erbringung der Leistungen des Auftragnehmers nach der Leistungsvereinbarung erforderlich ist.
- 5.3 Der Auftragnehmer sichert zu, dass die für die Bundesdruckerei verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Dies gilt auch für den Eingang und Ausgang von Daten, auch auf Datenträgern.
- 5.4 Bei der Erfüllung der Rechte von betroffenen Personen nach den Art. 12 bis 22 DSGVO durch die Bundesdruckerei, bei der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO sowie bei ggf. erforderlichen Datenschutz-Folgeabschätzungen der Bundesdruckerei gemäß Art. 35 DSGVO und der Einhaltung der in den Artikeln 32 und 36 DSGVO genannten Pflichten der Bundesdruckerei hat der Auftragnehmer im erforderlichen Umfang mitzuwirken und die Bundesdruckerei so weit wie möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO). Der Auftragnehmer hat die hierzu erforderlichen Angaben jeweils auf Anforderung unverzüglich an den Weisungsberechtigten der Bundesdruckerei gemäß § 4.1 dieses Vertrags weiterzuleiten; die Überlassung dieser Informationen und die Erbringung der Mitwirkungsleistungen ist mit der Leistungsvereinbarung abgegolten, zusätzliche Kosten entstehen für die Bundesdruckerei nicht.
- 5.5 Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch die Bundesdruckerei gegenüber Dritten oder dem Betroffenen gegenüber erteilen. Dies gilt entsprechend für jegliche Wahrnehmung von Rechten betroffener Personen, beispielsweise die Berichtigung und Löschung von Daten, beim Auftragnehmer.
- 5.6 Der Auftragnehmer teilt der Bundesdruckerei unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen der einschlägigen Gesetze, nach diesem Vertrag oder der Leistungsvereinbarung sowie bereits den Verdacht auf solche Verstöße schriftlich oder in elektronisch dokumentierter Form mit. Dies gilt insbesondere im Hinblick auf evtl. Melde- und Benachrichtigungspflichten der Bundesdruckerei nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, die Bundesdruckerei erforderlichenfalls bei der Erfüllung ihrer Pflichten gemäß Art. 33 und Art. 34 DSGVO unverzüglich und in zumutbarem Umfang zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder Art. 34 DSGVO für die Bundesdruckerei darf der Auftragnehmer nur nach vorheriger Weisung von einem Weisungsberechtigten gemäß § 4.1 dieses Vertrags durchführen. Die Erfüllung dieser Verpflichtungen durch den Auftragnehmer erfolgt für die Bundesdruckerei kostenfrei. Die Erfüllung eigener gesetzlicher Pflichten des Auftragnehmers bleibt hiervon unberührt; insbesondere ersetzt eine Meldung durch die Bundesdruckerei nicht eine eigene Meldung des Auftragnehmers, wenn er eine solche absetzen muss.

§ 6 Weitere datenschutzrechtliche Maßnahmen beim Auftragnehmer, Homeoffice

- 6.1 Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau

[...]

bestellt. Einen Wechsel des Datenschutzbeauftragten ist der Bundesdruckerei unverzüglich mitzuteilen.

- 6.2 Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO.
- 6.3 Einer Verarbeitung personenbezogener Daten außerhalb der Betriebsräume des Auftragnehmers (Standard-Mobilarbeitsplätze, z.B. Telearbeit, Heimarbeit, Homeoffice, mobiles Arbeiten) wird unter folgenden Bedingungen zugestimmt:
- Die Standard-Mobilarbeitsplätze werden im Rahmen eines vom Auftragnehmer intern freigegebenen Datenschutzkonzeptes betrieben. Die Mitarbeitenden des Auftragnehmers sind sowohl mit technischem Equipment als auch mit entsprechenden Handlungsanweisungen ausgestattet.
 - Es findet außerhalb der Betriebsräume keine lokale Verarbeitung von Daten auf dem Arbeitsplatz-PC statt.
 - Der Zugriff auf die Administrationsumgebung des Auftragnehmers erfolgt gesichert über VPN u. ä. Der Zugriff und die Verarbeitung personenbezogener Daten erfolgt im Rahmen und unter Weisungslage der Bundesdruckerei bzw. des Verantwortlichen.

Bei der Verarbeitung personenbezogener Daten, deren Schutzbedarf in Anlehnung an das Standard-Datenschutzmodell oder BSI IT-Grundschutz entsprechend hoch eingestuft ist, sind Telearbeit und mobiles Arbeiten nicht zulässig.

Die Auftragsverarbeitung erfolgt gemäß § 7 dieser Vereinbarung im Grundsatz in der Europäischen Union bzw. innerhalb des Europäischen Wirtschaftsraums. Dies schließt (Fern-)Wartung und sonstige Fernzugriffe im Rahmen der Auftragsverarbeitung mit ein.

- 6.4 Der Auftragnehmer sichert zu, dass er die bei der Durchführung von Datenverarbeitungen nach der Leistungsvereinbarung und nach diesem Vertrag beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut gemacht und für die Zeit ihrer Tätigkeit wie auch nach der Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet hat (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Verantwortungsbereich.
- 6.5 Der Auftragnehmer sichert zu, jederzeit mit der Aufsichtsbehörde, soweit dies zur Durchführung der Leistungsvereinbarung oder dieses Vertrags gehört, zu kooperieren.

§ 7 Datenverarbeitung in und außerhalb der Europäischen Union/des Europäischen Wirtschaftsraums

- 7.1 Die Datenverarbeitung nach Maßgabe der Leistungsvereinbarung und dieses Vertrags wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht.
- 7.2 Im Falle einer Datenverarbeitung mit einem Auftragnehmer mit Sitz in einem Drittstaat, darf diese nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind beispielsweise Angemessenheitsbeschluss der Europäischen Kommission, Standardvertragsklauseln oder genehmigte Verhaltensregeln etc.). Bei der Verwendung von Standardvertragsklauseln der EU-Kommission – vgl. den Durchführungsbeschluss (EU) 2021/914 der Kommis-

sion vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittstaaten gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Text von Bedeutung für den EWR) gilt **Anhang D** dieses Vertrages zwischen den Parteien.

- 7.3 Jede Verlagerung von Verarbeitungsvorgängen oder von Teilarbeiten durch den Auftragnehmer in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum in einen Drittstaat oder eine weitere Unterbeauftragung eines Auftragnehmers in einem Drittstaat darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (beispielsweise Angemessenheitsbeschluss der Europäischen Kommission, Standardvertragsklauseln oder genehmigte Verhaltensregeln etc.) und die schriftliche oder elektronisch dokumentierte vorherige Zustimmung der Bundesdruckerei vorliegt.
- 7.4 Sind im Falle von § 7.3 dieses Vertrages die aktuellen Standardvertragsklauseln – als Transferinstrument für die Übermittlung personenbezogener Daten an einen unsicheren Drittstaat vorgesehen, sind diese vom Auftragnehmer als weiteren **Anhang D** zu dieses Vertrages anzufügen, wenn er die personenbezogenen Daten exportiert. Der Auftragnehmer bestimmt das jeweilige Modul sowie ggf. weitere zusätzliche Maßnahmen, die ein angemessenes Datenschutzniveau sicherstellen sollen und stimmt diese mit der Bundesdruckerei ab.
- 7.5 Der Auftragnehmer stellt der Bundesdruckerei unverzüglich alle notwendigen Informationen bereit, damit die Bundesdruckerei bzw. der Verantwortliche für die Verarbeitung personenbezogener Daten die Rechtmäßigkeit der Übermittlung personenbezogener Daten an einen unsicheren Drittstaat überprüfen kann.

§ 8 Unterauftragsverhältnisse

- 8.1 Die Beauftragung von Subunternehmern zur Verarbeitung von Daten der Bundesdruckerei ist dem Auftragnehmer nur mit vorheriger schriftlicher oder zumindest elektronisch dokumentierter Genehmigung der Bundesdruckerei gestattet, vgl. Art. 28 Abs. 2 DSGVO. Die vorherige Genehmigung wird nur erteilt, wenn der Auftragnehmer der Bundesdruckerei Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt und zusichert, dass er den Subunternehmer unter besonderer Berücksichtigung von dessen Eignung und der bei diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig ausgewählt hat. Auf Anforderung sind der Bundesdruckerei alle für die Überprüfung relevanten Unterlagen und Informationen zur Verfügung zu stellen.
- 8.2 Eine Beauftragung von Subunternehmern in Drittstaaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums darf nur erfolgen, wenn die Voraussetzungen von § 7 dieses Vertrages erfüllt sind.
- 8.3 Der Auftragnehmer hat vertraglich sicherzustellen, dass die aufgrund dieses Vertrages ihm gegenüber geltenden Regeln auch in seinem Verhältnis zum Subunternehmer gelten.
- 8.4 Der Vertrag mit dem Subunternehmer muss schriftlich oder in elektronisch dokumentierter Form abgeschlossen werden (Art. 28 Abs. 4 und Abs. 9 DSGVO).
- 8.5 Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers in regelmäßigen Abständen in angemessenem Umfang zu überprüfen und auf Anforderung der Bundesdruckerei die Ergebnisse der Überprüfung mitzuteilen.
- 8.6 Zurzeit sind für den Auftragnehmer die in **Anhang B** bezeichneten Subunternehmer beschäftigt. Mit deren Beauftragung ist die Bundesdruckerei einverstanden. Sofern diesem Vertrag kein ausgefüllter **Anhang B** beigelegt ist, bestätigt der Auftragnehmer damit verbindlich, dass

er derzeit keine Subunternehmer für die Datenverarbeitung im Rahmen der Leistungsvereinbarung dieses Vertrags einsetzt.

Der Auftragnehmer stellt der Bundesdruckerei mit Angebotsabgabe alle notwendigen Informationen (**Anhang C**) aller nach **Anhang B** benannten Subunternehmer mit Angebotsabgabe bereit, damit die Bundesdruckerei bzw. der Verantwortliche für die Verarbeitung personenbezogener Daten die Rechtmäßigkeit überprüfen kann.

- 8.7 Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

- 9.1 Der Auftragnehmer gewährleistet ein für die Datenverarbeitung nach Maßnahme der Leistungsvereinbarung angemessenes Schutzniveau nach Maßgabe von Art. 32 Abs. 1 DSGVO, vgl. Art. 28 Abs. 3 Satz 2 lit. c DSGVO. Die konkreten technischen und organisatorischen Maßnahmen ergeben sich aus dem **Anhang C** zu diesem Vertrag.
- 9.2 Der Auftragnehmer sichert zu, dass die in **Anhang C** aufgezeichneten Maßnahmen angemessen und wirksam sind und jederzeit aufrechterhalten werden. Änderungen dieser Maßnahmen stellen eine Änderung dieses Vertrages dar und sind nur unter Einhaltung der entsprechenden Anforderungen zulässig.
- 9.3 Die Maßnahmen sind während der Dauer dieses Vertrags an die geltenden rechtlichen Vorgaben und den Stand der Technik anzupassen. Der Auftragnehmer aktualisiert den Anhang C entsprechend und teilt der Bundesdruckerei auf diese Weise die Änderungen mit.

§ 10 Haftung des Auftragnehmers

- 10.1 Für die Haftung des Auftragnehmers gilt Art. 82 DSGVO.
- 10.2 In Anlehnung an Art. 82 Abs. 4 DSGVO haften Bundesdruckerei und Auftragnehmer gesamtschuldnerisch, wenn beide an der streitgegenständlichen Verarbeitung beteiligt sind.
- 10.3 Im Innenverhältnis treffen die Parteien die Regelung, dass der Auftragnehmer die Bundesdruckerei von Ansprüchen natürlicher Personen (Dritte) freistellt. Dies gilt nicht, wenn der Auftragnehmer nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden der natürlichen Person eingetreten ist, verantwortlich ist. Weist der Auftragnehmer nach, dass er nur für einen Teil des Schadens der natürlichen Person verantwortlich ist, beschränkt sich seine Freistellungsverpflichtung auf diesen Teil.

§ 11 Dauer und Beendigung dieses Vertrags

- 11.1 Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit der Leistungsvereinbarung.
- 11.2 Das Recht der Bundesdruckerei, diesen Vertrag aus wichtigem Grund zu kündigen, bleibt unberührt. Ein wichtiger Grund ist insbesondere die Nichterfüllung gesetzlicher oder vertraglicher

datenschutzrechtlicher Pflichten des Auftragnehmers. Die Bundesdruckerei hat vor einer Kündigung aus wichtigem Grund wegen einer Pflichtverletzung des Auftragnehmers grundsätzlich eine angemessene Frist zur Abhilfe zu setzen, sofern dies nicht aus gesetzlichen Gründen entbehrlich ist.

- 11.3 Der Auftragnehmer wird dann der Bundesdruckerei nach deren Wahl entweder Unterlagen, Daten und/oder Datenträger zurückgeben oder diese auf Wunsch der Bundesdruckerei datenschutzgerecht löschen bzw. entsorgen. Der Auftragnehmer wird die Löschung oder Vernichtung in geeigneter Form auf Anforderung der Bundesdruckerei nachweisen. Die Bundesdruckerei ist berechtigt, die Einhaltung dieser Vorgaben beim Auftragnehmer zu kontrollieren.

§ 12 Ausschluss des Zurückbehaltungsrechts

Ein Zurückbehaltungsrecht des Auftragnehmers an personenbezogenen Daten gemäß § 273 BGB wird ausgeschlossen. Dies gilt auch für alle diesbezüglichen Datenträger, Unterlagen oder sonstigen Medien.

§ 13 Schlussbestimmungen

- 13.1 Änderungen und Ergänzungen dieses Vertrags und seiner Anhänge bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.
- 13.2 Gerichtsstand für sämtliche Streitigkeiten zwischen den Parteien aus oder im Zusammenhang mit diesem Vertrag ist Berlin. Die Bundesdruckerei ist berechtigt, den Auftragnehmer auch an anderen gesetzlich eröffneten Gerichtsständen in Anspruch zu nehmen.
- 13.3 Sollten einzelne Regelungen dieses Vertrags unwirksam oder undurchführbar sein oder werden, wird die Wirksamkeit der übrigen Regelungen davon nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, die dem mit dieser Vereinbarung verfolgten datenschutzrechtlichen und wirtschaftlichen Zweck am nächsten kommt. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich dieser Vertrag als lückenhaft erweist.

Anlagenverzeichnis

- Anhang A** Kategorien von Daten und Betroffene etc.
- Anhang B** Liste von beauftragten Subunternehmern
- Anhang C** Auflistung technisch-organisatorischer Maßnahmen

Diese Vereinbarung über die Auftragsverarbeitung wird als Anlage zum Vertrag mit Zuschlagerteilung verbindlich vereinbart.

Anhang A

Kategorien von Daten und Betroffene etc.

1. Gegenstand des Auftrags

„Lizenzen und Implementierung einer Cloudlösung für das Lieferantenmanagement“

2. Art und Zweck der Verarbeitung

Speicherung von Lieferantendaten

3. Betroffene Personen

Mitarbeiter, Lieferanten

4. Art der verarbeiteten Daten

Lieferantenstammdaten

- Firmenname, Rechtsform
- Anschrift(en)
- Handelsregisterdaten
- Steuerinformationen (z. B. USt-ID, Steuernummern)

Onboarding- und Qualifizierungsdaten

- Selbstauskünfte und Fragebögen
- Zertifikate und Nachweise (z. B. ISO, Nachhaltigkeit, Compliance)
- Risikoeinstufungen

Vertragsmanagement (CLM)

- Vertragsstammdaten
- Vertragstypen (Rahmenvertrag, Einzelvertrag etc.)
- Vertragsparteien
- Vertragslaufzeiten, Start- und Enddaten
- Kündigungsfristen
- Vertragsstatus (Entwurf, aktiv, beendet)

Fristen- & Ereignisdaten

- Kündigungs- und Verlängerungsfristen

Ausschreibungsmodul

Ausschreibungsstammdaten

- Vergabe- und Projektnummern
- Vergabearten (z. B. offene Ausschreibung, Verhandlungsverfahren)

- Zeitpläne und Fristen

- Warengruppen

Vergabeunterlagen

- Preisblätter
- Vertragsentwürfe
- Fragen- & Antwortkataloge

Bieter- & Angebotsdaten

ggf Teilnahmeanträge

- Angebote (kaufmännisch und technisch)
- Preis- und Kalkulationsdaten

Kommunikations- & Interaktionsdaten

- Bieterfragen und Antworten

Bewertungs- & Entscheidungsdaten

- Bewertungsmatrizen
- Punktzahlen und Gewichtungen
- Zuschlagsentscheidungen

Daten mit mittlerem Risiko bezüglich Integrität und Vertraulichkeit:

Lieferantenstammdaten

- Bankverbindungen (IBAN, BIC)
- Klassifikationen (Warengruppen, Kategorien, Regionen)
- Statusinformationen (z. B. aktiv, gesperrt, in Prüfung)

Kaufmännische & fachliche Vertragsdaten

- Vertragswerte und Volumina
- Vertragsbezogene Warengruppe

Daten zu Lieferantenbewertung und Maßnahmen mit keinem bis zu sehr hohem Risiko je nach Klassifizierung der Leistungen

(Klassifizierung können sein: intern, vertraulich, streng-vertraulich, normal/secure/high secure information ISO14298, VS-NfD, VSVertraulich...):

Performance- und Bewertungsdaten

Lieferantenbewertungen

- KPIs (z. B. Qualität, Termintreue, Nachhaltigkeit)
- Historische Bewertungsverläufe
- Maßnahmenpläne

Vertragsmanagement (CLM)

Vertragsinhalte & Dokumente

- Vertragsdokumente (z. B. PDF, Word)
- Anhänge und Anlagen
- Versionen und Änderungshistorien

Kaufmännische & fachliche Vertragsdaten

- Preise, Preisstaffeln
- Leistungsbeschreibungen
- Service Levels (SLAs)

Ausschreibungsmodul

Vergabeunterlagen

- Leistungsbeschreibungen

5. Verarbeitung besonders schutzwürdiger personenbezogener Daten

(#Bitte Angaben zu Charakter der Daten. Vgl. die Begriffsdefinition unter § 2. Sofern besonders schutzwürdige personenbezogene Daten Verarbeitungsgegenstand sind, bestehen ggf. erhöhte Anforderungen für die TOMs.#)

keine

5. Verarbeitung besonders schutzwürdiger personenbezogener Daten

(#Bitte Angaben zu Charakter der Daten#)

Anhang B**Liste von beauftragten Subunternehmern**

Mit den folgenden Subunternehmern hat der Auftragnehmer Verträge abgeschlossen, wonach die mit der Bundesdruckerei vereinbarten Regeln und Pflichten zum Datenschutz auch gegenüber den Subunternehmern gelten.

Im Rahmen des Vertrags über die Auftragsverarbeitung setzt der Auftragnehmer folgende Subunternehmer/ Unterauftragnehmer zur Erfüllung seiner Pflichten ein. Ebenso sind die Subunternehmer der Subunternehmer aufzulisten:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen	Ort der Leistungserbringung

Der Auftragnehmer bestätigt Folgendes:

Mit den im Nicht-EU-Ausland ansässigen Subunternehmern hat der Auftragnehmer in folgender Weise sichergestellt, dass ein dem EU-Datenschutz vergleichbares Datenschutzniveau gegeben ist:

(#Hier müsste der Auftragnehmer einfügen, ob Standardvertragsklauseln abgeschlossen wurden etc.#)

Anhang C

Technische und organisatorische Maßnahmen gem. Art. 32, 28 Abs. 3 Satz 2 lit. c DSGVO

Anhang C ist ausgefüllt für jeden Subunternehmer (Anhang B) einzureichen, der mit der Verarbeitung personenbezogener Daten betraut ist.

Der Auftragnehmer trifft folgende technische und organisatorische Maßnahmen zur Datensicherheit im Sinne von Art. 32, 28 Abs. 3 Satz 2 lit. c DSGVO:

§ 1 Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1 Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

(#Hier sind Maßnahmen wie Schließanlage, Alarmanlage etc. aufzuführen.#)

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen benutzen:

- Benutzerrollen über IDM
- Rollentrennung in der Software
- Benutzerauthentifizierung über OKTA
- automatische Sperrung
- Inhaltsverschlüsselung nach dem neustestens Stand der Technik

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsanlagen Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

(#Hier sind beispielsweise eine differenzierte Berechtigung, Auswertungen, die Behandlung nicht mehr benötigter Datenträger etc. aufzuführen.#)

- Benutzerrollen über IDM
- Rollentrennung in der Software
- Benutzerauthentifizierung über OKTA
- automatische Sperrung
- Inhaltsverschlüsselung nach dem neustestens Stand der Technik

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden:

(#Hier sind Maßnahmen wie Mandantenfähigkeit, Trennung zwischen Test- und Produktionssystem etc. aufzuführen.)

- Mandantentrennung
- Rollenbasierter Zugriff auf Daten
- Rollen werden über das Berechtigungsmanagement gesteuert

§ 2 Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und die gewährleisten, dass Weitergaben kontrolliert und ggf. protokolliert werden können:

(#Hier sind beispielsweise Identifizierung und Authentifizierung, die Benutzung von VPNs, elektronische Signaturen, Transportsicherungen, Verschlüsselungen etc. aufzuführen.)

- Benutzerrollen über IDM
- Rollentrennung in der Software
- Benutzerauthentifizierung über OKTA

2.2 Eingabekontrolle

Maßnahmen zur Feststellung, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind:

(#Hier sind beispielsweise Protokollierungssysteme, Protokollauswertungen etc. aufzuführen.)

§ 3 Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b und c DSGVO; Datenschutzmanagement

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust gesichert sind:

(#Hier sind Maßnahmen wie Backup-Verfahren, unterrechnungsfreie Stromversorgung, Virenschutz, Firewall oder Notfallpläne aufzuführen.#)

- In der LB sind diverse SLAs definiert
- Als Systembetriebszeit wird eine Zeit Mo-Fr jeweils 9 bis 17 Uhr MEZ festgelegt. Es wird eine Systemverfügbarkeit von mindestens 95% pro Jahr während der Systembetriebszeit gewährleistet
- Backup-/Recovery-Rechenzentrum wird zur Verfügung gestellt

3.2 Verfahren zur Überprüfung Bewertung und Evaluierung der Wirksamkeit gem. Art. 32 Abs. 1 lit. d DSGVO i.V.m. Art. 25 Abs. 1 DSGVO

(#Hier sind Maßnahmen des Datenschutzmanagements, also etwa Bestellung eines Datenschutzbeauftragten, Verpflichtungserklärungen der Mitarbeiter, ggf. Zertifizierungen, externe Prüfungen etc. aufzuführen.#)

- ISO9001 und 27001 Zertifizierungen müssen vorgelegt werden
- Es werden ggf. weitere Prüfungen im Software-Einführungsprozess der bdr vorgenommen

§ 4 Auftragskontrolle

Maßnahmen, die sicherstellen, dass keine weitere Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne vorherige Zustimmung der Bundesdruckerei stattfindet:

(#Hier sind Maßnahmen wie eindeutige Vertragsgestaltung, Konzentration von Zeichnungsberechtigungen etc. aufzuführen.#)

- Klar geregelte EU-Vergabeunterlagen