Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO

zwischen

CNA Insurance Company Limited

Direktion für Deutschland

Im Mediapark 8

D-50670 Köln

- nachstehend **Auftraggeber** genannt -

und der

- nachstehend **Auftragnehmer** genannt –

- gemeinsam auch **die Parteien** genannt –

§ 1 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des als Anlage 1 zu dieser Vereinbarung beigefügten Vertrags (nachfolgend „Hauptvertrag“ genannt). Dabei verarbeitet der Auftragnehmer personenbezogene Daten i.S.d. Art. 4 Nr. 4 DSGVO für den Auftraggeber (nachfolgend „Auftraggeber-Daten“ genannt) ausschließlich im Auftrag und nach Weisung des Auftraggebers. Rahmen und Umfang der Datenverarbeitung ergeben sich aus dem Hauptvertrag.

(2) Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit den Auftraggeber-Daten in Erfüllung des Hauptvertrages.

(3) Die Verarbeitung der Auftraggeber-Daten findet im Gebiet der Bundesrepublik Deutschland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung und Weisung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 2 Laufzeit und Kündigung

(1) Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zu Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieses Vertrages.

(2) Eine isolierte Kündigung dieses Vertrags ist grundsätzlich ausgeschlossen. Der Auftraggeber kann den Vertrag jedoch jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen allgemeine Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann bzw. will oder der Auftragnehmer die Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schwerwiegenden Verstoß dar.

(3) Der Auftragnehmer hat dem Auftraggeber sämtliche Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Vertrages in Folge eines schwerwiegenden Verstoßes i.S.d. Abs. (2) entstehen.

§ 3 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend der in **Anlage 2** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Datenverarbeitung. Sie bezieht sich auf die in **Anlage 2** festgelegte Art der Auftraggeber-Daten und die dort aufgeführten Kategorien betroffener Personen.

(2) Der Auftragnehmer darf die Auftraggeber-Daten nicht für eigene oder sonstige Zwecke - auch nicht in anonymisierter Form - verarbeiten und nutzen, es sei denn, eine solche Verarbeitung dient der Erfüllung des Hauptvertrages oder ist durch diesen Auftragsverarbeitungsvertrag gestattet. Dies gilt auch dann, wenn eine Verarbeitung im Übrigen datenschutzrechtlich zulässig wäre.

§ 4 Weisungen des Auftraggebers

(1) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich im Rahmen des Hauptvertrags und nach Weisung des Auftraggebers gemäß Art. 28 Abs. 3 S. 2 lit. a DSGVO.

(2) Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang, Mittel und Zwecke der Datenverarbeitung vor. Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber in der Folge schriftlich oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Die Weisungsberechtigten und Weisungsempfänger ergeben sich aus **Anlage 3**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(4) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Erteilte Weisungen werden sowohl vom Auftraggeber als auch vom Auftragnehmer dokumentiert. Mündliche Weisungen sind

unverzüglich schriftlich oder in einem dokumentierten elektronischen Format vom Auftragnehmer zu bestätigen.

(5) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen werden schriftlich oder in einem dokumentierten elektronischen Format festgelegt. Erteilt der Auftraggeber Einzelweisungen hinsichtlich des Umgangs mit Auftraggeber-Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, werden diese als Antrag auf Leistungsänderung behandelt.

§ 5 Rechte und Pflichten des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach dokumentierter Weisung des Auftraggebers. Der Auftraggeber bleibt insoweit Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

(2) Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen aus den Art. 12 bis 22 DSGVO ist der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie an den Auftraggeber gerichtet sind, unverzüglich an den Auftraggeber weiterzuleiten und ihn bei der Beantwortung zu unterstützen.

(3) Der Auftraggeber ist berechtigt, sich wie unter § 8 festgelegt, vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer versichert, dass ihm die für die Verarbeitung einschlägigen, geltenden datenschutzrechtlichen Bestimmungen bekannt sind.

(2) Der Auftragnehmer stellt sicher, dass die Verarbeitung der Auftraggeber-Daten im Rahmen der Leistungserbringung nach dem Hauptvertrag in seinem Verantwortungsbereich, der die Unterauftragnehmer nach § 10 dieses Vertrags einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrages erfolgt. Der Auftragnehmer sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Eingang und Ausgang sowie die laufende Verwendung sind zu dokumentieren.

(3) Der Auftragnehmer ist verpflichtet dem Auftraggeber alle erforderlichen Informationen, einschließlich Zertifizierungen sowie Überprüfungs- und Inspektionsergebnisse, die dem Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten dienen, zur Verfügung zu stellen.

(4) Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß der Art. 37, 38 und 39 DSGVO sowie § 5, 35 BDSG-neu ausüben kann, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist bei dem Auftraggeber unverzüglich anzuzeigen. Zusätzlich hat der Auftragnehmer die aktuellen Kontaktdaten des Datenschutzbeauftragten auf der Webseite leicht zugänglich zu hinterlegen (Art. 37 Abs. 7 DSGVO) und sie der Aufsichtsbehörde mitzuteilen. Veröffentlichung und Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(5) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren, insbesondere die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern. Diese Pflicht besteht auch nach Beendigung des Vertrages fort.

(6) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Auftragsverarbeitung beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den maßgebenden Bestimmungen des Datenschutzes vertraut gemacht hat. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden, entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Die Verpflichtungen zur Vertraulichkeit müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

(7) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen aus dem Hauptvertrag (einschließlich der Datensicherung), sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(8) Der Auftragnehmer ist verpflichtet den Auftraggeber bei der Erfüllung seiner gesetzlichen Verpflichtungen aus den Art. 12 bis 22 und 30 bis 36 DSGVO zu unterstützen. Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen sowie nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, insbesondere bei der Beantwortung von Anträgen auf Wahrnehmung der entsprechend in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen (§ 11).

(9) Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis die Weisung vom Auftraggeber bestätigt wird.

(10) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(11) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft

alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in **Anlage 4** aufgeführten Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle.

(2) Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 4** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren und den Auftraggeber entsprechend informieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen Zustimmung des Auftraggebers.

§ 8 Mitteilungspflichten des Auftragnehmers und Verhalten im Falle von Verstößen

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder sonstigen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder bei Dritten wird der Auftragnehmer den Auftraggeber unverzüglich informieren. Dies gilt auch für den Fall, dass Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 58 DSGVO durchgeführt werden, oder soweit eine zuständige Behörde nach Art. 82, 83 DSGVO beim Auftragnehmer ermittelt.

(2) Die Mitteilung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;

b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

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

(5) Soweit den Auftraggeber aufgrund eines Vorkommnisses nach Absatz (1) gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von Auftraggeber-Daten (insbesondere nach Art. 33 und 34 DSGVO) treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen zu unterstützen.

(6) Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers durchführen.

(7) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Beschlagnahme, Pfändung oder aufgrund eines Insolvenz- oder Vergleichsverfahrens oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber

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

(8) Für den Fall, dass der Auftragnehmer nach dem Unionsrecht oder dem Recht eines Mitgliedstaates, dem er unterliegt, zur Verarbeitung entgegen einer Weisung des Auftraggebers verpflichtet ist, teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(9) Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

§ 9 Kontrollrechte des Auftragsgebers

(1) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der technisch organisatorischen Maßnahmen gemäß Anlage 4 und der sonstigen vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten, Datenverarbeitungsanlagen und die Datenverarbeitungsprogramme beim Auftragnehmer vor Ort. Zu diesem Zweck ist der Auftragnehmer auch verpflichtet, dem Auftraggeber Zutritt zu den Räumlichkeiten zu gewähren, in denen die Daten des Auftraggebers physisch oder elektronisch verarbeitet werden.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen i.S.d Art 28 DSGVO i.V.m. der Anlage 4 nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO; 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).

(3) Der Auftraggeber oder ein entsprechend Beauftragter haben das Recht vorgenannte Kontrollen unentgeltlich zu den üblichen Geschäftszeiten vorzunehmen. Diese Kontrollen sind rechtzeitig (in der Regel mindestens zwei Wochen vorher) anzukündigen. Der Auftraggeber stimmt die Durchführung der Kontrollen mit dem Auftragnehmer so ab, dass der Betriebsablauf beim Auftragnehmer so wenig wie möglich beeinträchtigt wird.

(4) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten vorzulegen. Der Auftraggeber wird keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

§ 10 Unterauftragsverhältnisse

Variante 1:

(1) Der Auftraggeber stimmt der Beauftragung der in Anlage 5 aufgeführten Unterauftragnehmer zu Beginn des Auftragsverhältnisses unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 1 bis 4 DSGVO zu. Dem Auftragnehmer ist die Beauftragung weiterer Unterauftragnehmer (weitere Auftragsverarbeiter) nur unter Einhaltung der Anforderungen aus Abs. 3 bis 7 gestattet.

(2) Unterauftragnehmer im Sinne dieser Regelung sind solche Dienstleister, die unmittelbar mit der Erbringung der Hauptleistung betraut sind. Nicht zur Hauptleistung gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie für sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Auftraggeber-Daten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Die Beauftragung weiterer Unterauftragnehmer im Rahmen der vertraglichen Verpflichtungen ist zulässig, soweit:

a. Der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber vorab schriftlich oder in Textform unter Angabe des beabsichtigten Auslagerungsbeginns angezeigt hat, und

b. der Auftraggeber der Beauftragung nicht innerhalb einer Frist von 14 Tagen ab Kenntniserlangung aller relevanten Informationen widersprochen hat.

(4) Der Auftragnehmer hat Sorge dafür zu tragen, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung insbesondere der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(5) Im Fall der Hinzuziehung eines Unterauftragnehmers erlegt der Auftragnehmer diesem, im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats, dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind. Der Vertrag ist so auszugestalten, dass es dem Auftraggeber möglich ist, im Bedarfsfall angemessene Überprüfungen und Inspektionen beim Unterauftragnehmer, auch vor Ort durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(6) Erfüllt ein Unterauftragnehmer die in diesem Vertrag festgelegten Verpflichtungen nicht oder verstößt gegen datenschutzrechtliche Vorschriften, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers.

(7) Sofern eine Einbeziehung von Unterauftragnehmern in einem Drittstaat erfolgen soll, ist dies nur nach vorheriger Zustimmung des Auftraggebers zulässig. Der Auftragnehmer hat sicherzustellen, dass beim jeweiligen Unterauftragsnehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen

den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragnehmern nachweisen.

(8) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit dem Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

Variante 2:

(1) Der Auftraggeber stimmt der Beauftragung der in Anlage 5 aufgeführten Unterauftragnehmer zu Beginn des Auftragsverhältnisses unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 1 bis 4 DSGVO zu. Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(2) Unterauftragnehmer im Sinne dieser Regelung sind solche Dienstleister, die unmittelbar mit der Erbringung der Hauptleistung betraut sind. Nicht zur Hauptleistung gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie für sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Auftraggeber-Daten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(3) Der Auftragnehmer hat Sorge dafür zu tragen, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung insbesondere der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(4) Im Fall der Hinzuziehung eines Unterauftragnehmers erlegt der Auftragnehmer diesem, im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats, dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind. Der Vertrag ist so auszugestalten, dass es dem Auftraggeber möglich ist, im Bedarfsfall angemessene Überprüfungen und Inspektionen beim Unterauftragnehmer, auch vor Ort durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(5) Erfüllt ein Unterauftragnehmer die in diesem Vertrag festgelegten Verpflichtungen nicht oder verstößt gegen datenschutzrechtliche Vorschriften, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Unterauftragnehmers.

(6) Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(7) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit dem Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

§ 11 Rechte der betroffenen Personen

(1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

(2) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zur Wahrnehmung ihrer Rechte gemäß der Art. 12 bis 22 DSGVO der sie betreffenden Daten wenden sollte, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen.

(3) Wenn eine betroffene Person ihre Rechte gemäß der Art. 12 bis 22 DSGVO geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der sich daraus ergebenden Pflichten in angemessenem und für den Auftraggeber erforderlichen Umfang zu unterstützen.

(4) Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Auftraggeber-Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst nicht möglich ist.

§ 12 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer verpflichtet sich, den Auftraggeber im Innenverhältnis von allen Ansprüchen Dritter frei zu stellen, solange und soweit er nicht nachweist, dass der Schaden trotz Einhaltung der Anforderungen des geltenden Datenschutzrechts, der korrekten Umsetzung der Anforderungen aus diesem Vertrag oder einer vom Auftraggeber erteilten Weisung entstanden ist.

(3) Sollte eine Datenschutzbehörde oder ein Gericht gegen den Auftraggeber eine Geldbuße auf Grund einer unzulässigen oder unrichtigen Datenverarbeitung des Auftragnehmers verhängen, hat der Auftragnehmer dem Auftraggeber den entsprechenden Betrag auf schriftliche Mitteilung hin in voller Höhe innerhalb von 30 Tagen ab der schriftlichen Mitteilung zu erstatten.

(4) Der Auftragnehmer hat dem Auftraggeber sämtliche sich aus der von ihm zu vertretenden Rechtsverletzung gemäß Absatz 3 und 4 ergebenden Kosten zu erstatten, einschließlich der Kosten der Rechtsverfolgung.

(5) Unbeschränkte Haftung: Der Auftraggeber haftet unbeschränkt für Vorsatz und grobe Fahrlässigkeit, bei Verletzung einer vertraglich gewährten Garantie sowie nach Maßgabe des Produkthaftungsgesetzes. Für leichte Fahrlässigkeit haftet der Auftraggeber bei Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit von Personen. Im Übrigen gilt folgende beschränkte Haftung: Bei leichter Fahrlässigkeit haftet der Auftraggeber nur im Falle der Verletzung einer wesentlichen Vertragspflicht des Hauptvertrages, deren Erfüllung die ordnungsgemäße Durchführung des Hauptvertrages überhaupt erst ermöglicht und auf deren Einhaltung der Auftragnehmer regelmäßig vertrauen darf (Kardinalpflicht). Die Haftung für leichte Fahrlässigkeit ist der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren Schäden, mit deren Entstehung typischerweise gerechnet werden muss.

§ 13 Rückgabe und Löschung überlassener Auftraggeber-Daten

(1) Der Auftragnehmer ist verpflichtet, sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Vereinbarung – dem Auftraggeber nach Wahl auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.

(2) Über eine Löschung bzw. Vernichtung von Auftraggeber-Daten hat der Auftragnehmer ein Protokoll zu erstellen, das dem Auftraggeber auf Anforderung vorzulegen ist.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 14 Sonstiges

(1) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(2) Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesem Vertrag vor.

(3) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Parteien für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

.....	.....
(Ort, Datum)	(Ort, Datum)
.....	.....
(Unterschrift Auftraggeber)	(Unterschriften Auftragnehmer)

Anlagen:

Anlage 1 Hauptvertrag

Anlage 2 Zwecke und Art der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen

Anlage 3 Weisungsberechtigte und Weisungsempfänger

Anlage 4 Technische und organisatorische Maßnahmen

Anlage 5 Zulässige Unterauftragnehmer

Anlage 2

Zweck und Art der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Der Auftragnehmer erbringt die nach dieser Anlage vereinbarten Leistungen gegenüber dem Auftraggeber ausschließlich nach Weisung des Auftraggebers und auf Grundlage der zwischen den Parteien geschlossenen Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag.

Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers nachfolgende personenbezogene Daten zu den genannten Zwecken:

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Kategorien der betroffenen Personen**

Ort, Datum

Ort, Datum

Auftraggeber

Auftragnehmer

Anlage 3

Weisungsberechtigte und Weisungsempfänger

Weisungsberechtigte Personen des Auftraggebers sind:

xxx

Weisungsempfänger beim Auftragnehmer sind:

xxx

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.

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anlage 4

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

-TEMPLATE-

Beschreibung der getroffenen technischen und organisatorischen Maßnahmen der [XXX GmbH] zur Umsetzung und Einhaltung der Vorgaben der Art. 32 und Art. 25 Abs. 2 S.3 DSGVO.

Alle technischen und organisatorischen Maßnahmen beziehen sich auf [bspw. das Rechenzentrum und den Firmensitz].

Verschlüsselung

Jede Verarbeitungstätigkeit wird daraufhin überprüft, ob sich ihr Zweck auch ohne unmittelbaren Personenbezug realisieren lässt. Ist dies der Fall, werden lesbare Informationen mit Hilfe eines Verfahrens in eine nicht ohne weiteres interpretierbare Zeichenfolge umgewandelt.

Pseudonymisierung

Jede Verarbeitungstätigkeit wird daraufhin überprüft, ob sich ihr Zweck auch ohne unmittelbaren Personenbezug realisieren lässt. Ist dies der Fall, erfolgt eine Verarbeitung personenbezogener Daten in der Weise, dass diese Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen ihrerseits technischen und organisatorischen Maßnahmen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Vertraulichkeit

Folgende Maßnahmen gewährleisten, dass Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen bzw. den Geschäftsräumen der [XXX GmbH] erhalten, mit denen personenbezogene Daten verarbeitet werden:

- ☐ Die Türen zu den betroffenen Bereichen sind mit Sicherheitsschlössern ausgestattet
- ☐ nach außen nur mit starrem Türknopf anstelle einer Klinke ausgestattet
- ☐ mit einem automatischen Zuzieher ausgestattet
- ☐ mit elektronischen Zutritts-Kontrollsystemen mit Chipkarte ausgestattet
- ☐ außer zum Betreten und Verlassen geschlossen
- ☐ Schlüssel bzw. sonstige Zutrittsmittel (persönliche Chipkarten, Transponder etc.) werden ausschließlich an Berechtigte ausgegeben und sofort eingezogen, wenn die Berechtigung erlischt

- ☐ die Berechtigung zum Betreten wird durch geeignete Maßnahmen protokolliert
- ☐ es bestehen schriftliche Zutrittsregelungen
- ☐ bei Verlust eines Zutrittsmittels wird dieses individuell gesperrt
- ☐ ein Generalschlüssel wird sicher verwahrt
- ☐ zentraler Empfangsbereich mit Pförtner
- ☐ Protokollierung der Besucher
- ☐ Sicherung der Grundstücksgrenzen
- ☐ Gebäudesicherung
- ☐ Alarmanlage
- ☐ Einbruchsschutz
- ☐ Verbindung zu einer ständig besetzten Notrufzentrale
- ☐ Videoüberwachung
- ☐ Anwesenheitsaufzeichnungen im Sicherheitsbereich

- ☐ Weitere Maßnahmen:
- ☐ _____
- ☐ _____
- ☐ _____

Integrität

Um zu gewährleisten, dass personenbezogene Daten nicht verfälscht werden können, werden folgende Vorkehrungen getroffen:

- ☐ gemanagte Firewall
- ☐ individuelle Benutzerkennung und persönliches Passwort
- ☐ regelmäßige Kontrolle der bestehenden Berechtigungen
- ☐ Löschung des Passworts, wenn Berechtigung erlischt
- ☐ Passwort muss bestimmte Kriterien erfüllen (Sonderzeichen, Passwortlänge, Groß/Kleinschreibung, Buchstaben, Ziffern)
- ☐ Abmeldung nach 10 minütiger Inaktivität
- ☐ Zugriffe von außen nur durch gesicherte VPN-Verbindung
- ☐ zu übermittelnde Daten werden mit Passwort gesichert und ggfs. verschlüsselt
- ☐ Passwort und Verschlüsselung erfolgen nach Mindestkriterien
- ☐ Datenträger in mobilen Endgeräten (Notebooks) sind verschlüsselt; nicht mehr benötigte Datenträger aus mobilen Endgeräten werden datenschutzgerecht entsorgt
- ☐ keine unerlaubte Einbringung von mobilen Datenträgern durch die Mitarbeiter
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum externen Löschen von Daten)

- ☐ Weitere Maßnahmen:
- ☐ _____
- ☐ _____
- ☐ _____

Verfügbarkeit

Um die jederzeitige Nutzungsmöglichkeit der Systeme sicherzustellen, sind folgende Maßnahmen etabliert:

- ☐ Gewährleistung eines hinreichenden Hardwareschutzes
- ☐ sachkundiger Einsatz von Schutzprogrammen (Firewalls, Verschlüsselungsprogramme, Virenscanner, SPAM-Filter) bei allen Arbeitsplatzrechnern.
- ☐ Unterbrechungsfreie Stromversorgung, USV (Verfügbarkeitslevel 99,99 %)
- ☐ Unabhängig voneinander funktionierende Systeme
- ☐ Automatisierte Meldung von Fehlfunktionen

- ☐ Weitere Maßnahmen:
- ☐ _____
- ☐ _____
- ☐ _____

Belastbarkeit

Um sicherzustellen, dass personenbezogene Daten in den Systemen der [XXX GmbH] auch bei hoher Belastung gegen zufällige Zerstörung oder Verlust geschützt sind, existieren folgende Maßnahmen:

- ☐ Ausführung arbeitsplatzfremder Software wird verhindert durch technische Maßnahmen
- ☐ vertragliche Verbote der Nutzer
- ☐ Spamfilter
- ☐ Updates / Patches
- ☐ Einsatz von Firewalls, Verschlüsselungsprogrammen, Virenscannern, SPAM-Filtern und anderen Schutzprogrammen

- ☐ Weitere Maßnahmen:
- ☐ _____
- ☐ _____
- ☐ _____

Verfügbarkeitssicherung

Die Fähigkeit, personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, wird durch folgende Maßnahmen erreicht:

- ☐ Mehrstufiges Datensicherungskonzept (Backup- & Recoverykonzept)
- ☐ Notfall-Handbuch / Konzept

- ☐ Weitere Maßnahmen:
- ☐ _____
- ☐ _____
- ☐ _____

Maßnahmen zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Um die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs sicherzustellen, werden regelmäßig-Sicherheitsüberprüfungen [durch Dienstleister] durchgeführt.

Dabei werden die Systeme und die ihnen vorgeschalteten Schutzsysteme einem Penetrationstest unterzogen, der aus folgenden Teilschritten besteht:

- ☐ Schwachstellenscan unter Zuhilfenahme von kommerziellen Assessment-Tools und Open Source Programmen
- ☐ ergänzende manuelle Untersuchung auf Sicherheitslücken und Schwachstellen

- ☐ Weitere Maßnahmen:
- ☐ _____
- ☐ _____
- ☐ _____

Anhand einer gegebenenfalls ermittelten Schwachstelle wird ein genaues Abbild der Sicherheitssituation im Unternehmen gezeichnet. Die so gefundenen Risiken/Schwachstellen und Systeme werden im Anschluss an ihre Überprüfung [evtl: nach folgender Maßgabe] bewertet:

[Beispiel:

- Risiko Level 0 (Information)
- Risiko Level 1 (Niedrig)
- Risiko Level 2 (Mittel)
- Risiko Level 3 (Hoch)]

An diese Bewertung schließt sich eine Schwachstellenbeschreibung und eine darauf basierende Maßnahmenempfehlung an.

_____ _____

Datum Unterschrift

-Anlage-

Erläuterungen

Am 25. Mai 2018 wird die DSGVO in allen EU-Mitgliedstaaten unmittelbar wirksam. Sie verlangt unter anderem, dass der für die Verarbeitung personenbezogener Daten Verantwortliche geeignete technische und organisatorische Maßnahmen ergreift, um ein bei der Datenverarbeitung ein angemessenes Schutzniveau sicherzustellen. Diese Maßnahmen sind im Einzelnen nicht festgelegt. Der Verantwortliche ist frei, diese zu bestimmen. Maßgebliche Anforderung an die jeweiligen Vorkehrungen ist nach Art. 32 Abs. 1 Hs. 2 DSGVO aber, dass

„unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, [.....] ein dem Risiko angemessenes Schutzniveau „

gewährleistet wird.

Die Einhaltung der technischen und organisatorischen Maßnahmen nach Art. 25, 32 DSGVO gehört bei Datenschutzverstößen zu den Artikeln, die vom Bußgeldkatalog nach Art. 83 Abs. 4 a) DSGVO, mit einer Geldbuße von bis zu 10 Mio. EUR, bzw. 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bedroht sind. Eine strikte und gut dokumentierte Beachtung dieser Artikel kann bei einer Datenpanne zu deutlichen Vorteilen führen.

A. Mindestmaßnahmen

Mindestens müssen folgende Maßnahmen ergriffen werden:

1. Verschlüsselung

Jede Verarbeitungstätigkeit wird daraufhin überprüft, ob sich ihr Zweck auch ohne unmittelbaren Personenbezug realisieren lässt. Ist dies der Fall, sollen lesbare Informationen mit Hilfe eines Verfahrens in eine nicht ohne weiteres interpretierbare Zeichenfolge umgewandelt werden.

2. Pseudonymisierung

Jede Verarbeitungstätigkeit wird daraufhin überprüft, ob sich ihr Zweck auch ohne unmittelbaren Personenbezug realisieren lässt. Ist dies der Fall, erfolgt eine Verarbeitung personenbezogener Daten in der Weise, dass diese Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen ihrerseits technischen und organisatorischen Maßnahmen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

3. Vertraulichkeit

Bedeutet, dass die Daten für unberechtigte Dritte nicht zugänglich sind.

4. Integrität

Wird so verstanden, dass die Daten nicht verfälscht werden können.

5. Verfügbarkeit

Meint die jederzeitige Nutzungsmöglichkeit der Systeme.

6. Belastbarkeit

Bedeutet, dass Systeme und Dienste einer gewissen Beanspruchung standhalten müssen.

7. Verfügbarkeitssicherung

Meint die Gewährleitung der Fähigkeit, personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

8. Maßnahmen zur Überprüfung Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen

Unternehmen müssen ein Verfahren etablieren, das regelmäßig die Wirksamkeit der Maßnahmen bewertet und evaluiert**.**

B. Stand der Technik

Dabei muss der Stand der Technik berücksichtigt werden. Gemeint sind damit nicht Techniken, die gerade neu entwickelt wurden, sondern solche Maßnahmen, die ihre Geeignetheit und Effektivität in der Praxis bereits bewiesen haben und einen ausreichenden Sicherheitsstandard gewährleisten. Dabei impliziert der Begriff „Stand der Technik", dass es sich um eine gegenwärtige Bewertung handelt und der Stand der Technik immer wieder auf Aktualität übergeprüft werden muss, um die Datensicherheit gewährleisten zu können. Aufgrund des IT-Sicherheitsgesetzes hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) eine Handreichung veröffentlicht, die den Verantwortlichen als Orientierung zur Ermittlung des Standes der Technik in der IT-Sicherheit dienen soll:

https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Darüber hinaus muss stets im Auge behalten werden, was das Bundesamt für Sicherheit und Informationstechnik (BSI), die Aufsichtsbehörden und Fachverbände als „Stand der Technik" ansehen, es handelt sich also um einen dauerhaften Aktualisierungsprozess.

C. Angemessenes Schutzniveau

Art. 32 Abs. 2 DSGVO schreibt für alle Maßnahmen der Datensicherheit ein „angemessenes Schutzniveau" vor. Die Datensicherheit braucht somit nicht „optimal" oder „bestmöglich" zu sein, sondern soll sich an den Risiken orientieren, die mit den jeweiligen Verarbeitungsprozessen verbunden sind. Das Schutzniveau orientiert sich an der Schutzbedürftigkeit der einzelnen gespeicherten personenbezogenen Daten. Es sollte also eine Schutzbedarfsfeststellung vorgenommen werden, indem der jeweilige Schutzbedarf der unterschiedlichen personenbezogenen Daten ermittelt wird. Dabei sollten zunächst typische Schadenszenarien ermittelt und anschließend der Schutzbedarf für die einzelnen personenbezogenen Daten abgeleitet werden. Bisher bewährt hat sich die Einteilung in Schutzbedarfskategorien, wobei eine Orientierung an z.B. den Kategorien des BSI-Standard 100-2 „normal, „hoch" und „sehr hoch" hilfreich sein kann. Der Begriff „angemessen" orientiert sich an dem Stand der Technik, den Implementierungskosten, der Art und dem Umfang der Umstände, dem Zweck der Verarbeitung sowie an den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Dieses Verfahren wird man regelmäßig wiederholen.

Anlage 5

Genehmigte Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer