Vertrag zur gemeinsamen Verantwortlichkeit für die Verarbeitung personenbezogener Daten (Art. 26 DSGVO)

zwischen

CNA Insurance Company Limited

Direktion für Deutschland

Im Mediapark 8

D-50670 Köln

– nachfolgend „CNA Germany“ genannt –

und

– nachfolgend „A/B/C“ genannt –

§ 1. Vertragsgegenstand

(1) CNA Germany ist die deutsche Direktion der CNA Hardy Insurance Company Limited, einem führenden Spezialisten für Industrieversicherungen auf dem Lloyd’s Versicherungsmarkt und verschiedenen Unternehmensmärkten.

A (B, C …) sind (Beschreibung der jeweiligen Unternehmen).

Zur Optimierung der Verarbeitungsschritte und Schaffung von Synergien verarbeiten diese Unternehmen gemeinsam Daten von Kunden, Dienstleistern und Mitarbeitern in einem gemeinsamen System mit Berechtigung und Mandatstrennung.

(2) Das gemeinsame System liegt auf den Servern der Vertragsparteien. Beschreibung des gemeinsamen Systems. Über ein festgelegtes Berechtigungs- und Zugriffskonzept haben die

berechtigten Mitarbeiter der Vertragsparteien je nach Auftrag und Abteilung Zugriff auf das gemeinsame System. Das Berechtigungs- und Zugriffskonzept **(Anlage 1)** unterscheidet sich nach den (z.B. bestehenden Abteilungen)

- Marketing,
- Vertrieb,
- Schadensmanagement.

(3) Das vertragsgegenständliche System und die darin enthaltenen Daten stehen – unabhängig von der Herkunft einzelner Daten – datenschutzrechtlich in der gemeinsamen Verantwortung der Vertragsparteien nach Art. 26 Datenschutz-Grundverordnung (DSGVO).

(4) Dieser Vertrag konkretisiert die gemeinsame datenschutzrechtliche Verantwortlichkeit der Vertragsparteien als Joint Controllers nach Art. 26 DSGVO, insbesondere die Wahrung der Datenschutzrechte der Betroffenen und die Erfüllung der datenschutzrechtlichen Informationspflichten.

(5) Ungeachtet der nachfolgenden Vertragsbestimmungen können alle Kunden und sonstigen betroffenen Personen im Sinne des Art. 4 Abs. 1 DSGVO ihre Rechte bei und gegenüber jeder der Vertragsparteien geltend machen.

§ 2. Art, Umfang, Zweck und Laufzeit des Vertrags

(1) Die Verarbeitung der vertragsgegenständlichen Daten im Rahmen der gemeinsamen datenschutzrechtlichen Verantwortlichkeit 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) Dieser Vertrag tritt am 25. Mai 2018 in Kraft und endet am 31. Dezember 2019. Danach verlängert sich der Vertrag automatisch und stillschweigend um jeweils ein Kalenderjahr (1. Januar bis 31. Dezember), sofern er nicht durch eine Partei gekündigt wird. Zur Gültigkeit einer Kündigung muss diese der anderen Partei sechs (6) Monate vor Ablauf des Vertrages mitgeteilt werden. Das Recht auf außerordentliche Kündigung des Vertrages aus wichtigem Grund bleibt unberührt.

§ 3. Aufgabenbeschreibungen und -abgrenzung

(1) Im Kundenservicecenter haben Kunden die Möglichkeit sich über die Produkte und Leistungen zu erfahren, sowie Verträge anzubahnen. Hierbei wird über das Berechtigungs- und Zugriffskonzept sichergestellt, dass die Mitarbeiter des Kundenservicecenters die entsprechenden Auskünfte geben und Verträge anbahnen können.

(2) Die Kommunikation via Call Center oder E-Mail wird je nach beteiligtem Unternehmen in das gemeinsame System eingetragen. Die personenbezogenen Daten bei Vertragsanbahnung und –

erfüllung werden für die Dauer der gesetzlichen Aufbewahrungspflichten nach Gewerbeordnung, Handelsgesetzbuch und Abgabenordnung gespeichert.

§ 4. Weitere Beteiligte

Die **XY** verarbeitet im Rahmen des Marketings Daten potentieller Kunden. Die Kundendaten werden digitalisiert und in das gemeinsame System der Vertragsparteien übertragen. Zwischen den Vertragsparteien und XY besteht ein Auftragsverarbeitungsvertrag **(Anlage).**

§ 5. Verantwortlichkeiten der Parteien

(1) CNA Hardy Germany ist für die Rechtmäßigkeit der Erhebung aller personenbezogenen Daten verantwortlich, die im Bereich Vertrieb und Schadensmanagement erhoben werden.

(2) A ist für die Rechtmäßigkeit der Erhebung aller personenbezogenen Daten verantwortlich, die in dem Bereich Marketing erhoben werden.

(3) Für die Einholung von Werbeeinwilligungen im Sinne des § 7 Abs. 2 Nr. 3 UWG ist jeweils die Partei verantwortlich, die die Einwilligungen einholt.

(4) CNA Hardy Germany ist für die Verwaltung des gemeinsamen Systems allein verantwortlich. Die Verantwortlichkeit erstreckt sich auf die datenschutzrechtliche Zulässigkeit der Speicherung und Nutzung von personenbezogenen Daten.

(5) Für den Fall, dass eine betroffene Person Rechte auf Berichtigung, Löschung oder Sperrung von personenbezogenen Daten oder auf Auskunft über die gespeicherten personenbezogenen Daten geltend macht, ist diejenige Partei für die Erfüllung der Ansprüche der betroffenen Personen verantwortlich, gegenüber welcher die Geltendmachung der Rechte erfolgt.

(6) Wenn Betroffenenrechte nach Maßgabe des vorstehenden Absatzes 5 geltend gemacht werden, werden sich die Parteien wechselseitig unterstützen, soweit dies zur Wahrung der Betroffenenrechte erforderlich oder zweckmäßig ist. Soweit erforderlich werden die Vertragsparteien auch Weisungsrechte aus den zugrundeliegenden Auftragsverarbeitungsverträgen ausüben.

(7) Die Parteien sind verpflichtet, sich gegenseitig unverzüglich zu benachrichtigen, wenn eine betroffene Person Rechte gemäß Absatz 5 geltend macht, soweit sich nicht ausschließen lässt, dass die Unterstützung der anderen Partei nach Maßgabe des vorstehenden Absatzes 6 erforderlich wird.

(8) Die Vertragsparteien versichern sich gegenseitig, dass ihnen die für die Verarbeitung einschlägigen, geltenden datenschutzrechtlichen Bestimmungen bekannt sind.

(9) Die Vertragsparteien sind jeweils 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. Die Vertragsparteien teilen sich die

Kontaktdaten des jeweiligen Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten ist allen Vertragsparteien unverzüglich anzuzeigen. Zusätzlich hat jede Vertragspartei die aktuellen Kontaktdaten ihres Datenschutzbeauftragten auf ihrer Webseite leicht zugänglich zu hinterlegen (Art. 37 Abs. 7 DSGVO) und sie der Aufsichtsbehörde mitzuteilen.

§ 6. Mitteilungspflichten der Vertragsparteien und Verhalten im Falle von Verstößen

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen, Verdacht auf sicherheitsrelevante Vorfälle oder sonstigen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten haben sich die Vertragsparteien unverzüglich zu 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 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 der Vertragspartei ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(3) Die unmittelbar betroffene Vertragspartei trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen.

(4) Soweit eine Vertragspartei aufgrund eines Vorkommnisses nach Absatz (1) gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung (insbesondere nach Art. 33 und 34 DSGVO) treffen, haben sich die Vertragsparteien bei der Erfüllung der Informationspflichten auf Ersuchen einer Partei im Rahmen des Zumutbaren und Erforderlichen zu unterstützen.

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

(6) Sollten die Daten bei einem Vertragspartner durch Beschlagnahme, Pfändung oder aufgrund eines Insolvenz- oder Vergleichsverfahrens oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so sind die anderen Vertragspartner unverzüglich darüber zu informieren, sofern dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist.

§ 7 Technische und Organisatorische Anforderungen

(1) Jede Vertragspartei wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie 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 jeder Vertragspartei 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. Verantwortlichkeit für die Datenschutzerklärung

(1) Die Parteien haben jeweils eine Datenschutzerklärung für die Unternehmenswebsites formuliert. Für die Rechtmäßigkeit und Vollständigkeit der Datenschutzerklärungen sind die Parteien jeweils selbst verantwortlich.

(2) Die Parteien werden die Datenschutzerklärung für die Unternehmenswebsites eigenständig abändern und ergänzen, soweit dies wegen geänderter Abläufe der Datenverarbeitung oder aus rechtlichen Gründen erforderlich oder zweckmäßig ist.

§ 9. Haftung

(1) Soweit einer Vertragspartei (Geschädigter) ein Schaden entsteht, weil die andere Vertragspartei (Verletzer) Verpflichtungen aus diesem Vertrag verletzt hat, ist der Verletzer verpflichtet, dem Geschädigten den entstandenen Schaden zu ersetzen.

(2) Liegt der Schaden gemäß vorstehendem Absatz 1 darin, dass Dritte Ansprüche gegen den Geschädigten geltend machen, ist der Verletzer zur Freistellung des Geschädigten auf erstes Anfordern verpflichtet.

(3) Der Schadensersatz bzw. die Freistellung umfasst auch gerichtliche und außergerichtliche Rechtsverteidigungskosten. Soweit rechtlich zulässig, umfasst der Schadensersatz bzw. die Freistellung auch Bußgelder, die eine Aufsichtsbehörde gegen den Geschädigten verhängt.

§ 10. Schlussbestimmungen

(1) Ergänzungen und Änderungen dieses Vertrages bedürfen zu ihrer Rechtswirksamkeit der Schriftform. Mündliche Nebenabreden haben die Parteien nicht getroffen.

(2) Das Vertragsverhältnis unterliegt dem deutschen Recht. Als Gerichtsstand wird für beide Vertragsparteien Köln vereinbart.

(3) Die etwaige Unwirksamkeit einzelner Bestimmungen dieses Vertrages lässt die Wirksamkeit der übrigen Vertragsbestimmungen unberührt.

.....	.....	.....
(Ort, Datum)	(Ort, Datum)	(Ort, Datum)
.....	.....	.....
(Unterschrift CNA Hardy Germany)	(Unterschrift A)	(Unterschrift B)

Beispiele für Anlagen:

Anlage 1: Berechtigungs- und Löschkonzepte

Anlage 2: Zweck und Art der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Anlage 3: Auftragsverarbeitungsvertrag 1

Anlage 4: Technische und Organisatorische Anforderungen

Anlage 2

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

Die Vertragsparteien verarbeiten in gemeinsamer Verantwortlichkeit die nach dieser Anlage konkretisierten Daten auf Grundlage des zwischen den Parteien geschlossenen Vertrages zur gemeinsame Verantwortlichkeit für die Verarbeitung personenbezogener Daten.

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 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.