Bestimmungen zur Auftragsverarbeitung nach Artikel 28 DS-GVO

für das VAF Cyber Security Center
https://vaf.onmybreev.com

Stand: 17.02.2022

Für die Bereitstellung der Online-Schulungen des Cyber Security Centers des VAF Bundesverband Telekommunikation e.V., Otto Hahn Str. 16, 40721 Hilden (VAF) und der damit verbundenen Verarbeitung der personenbezogenen Daten der Nutzer der Schulung ist der VAF Auftragnehmer i.S. des Art. 28 DSGVO (VAF nachfolgend *Auftragnehmer* genannt). Der Besteller ist Auftraggeber i.S. des Art. 28 DSGVO (nachfolgend *Auftraggeber* genannt).

Für die Verarbeitung gem. Art. 28 DSGVO gelten nachfolgende Bestimmungen, einschließlich der am Dokumentenende enthaltenen **Anhänge 1 bis 3**.

Präambel
Diese Bestimmungen dienen der Vereinbarung zur konkreten Umsetzung der datenschutzrechtlichen Verpflichtungen des *Auftraggebers* und des *Auftragnehmers*, die sich aus den gesetzlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) im Rahmen der Auftragsverarbeitung (Artikel 28 DS-GVO) in Bezug auf den zwischen den Parteien abgeschlossenen und ihrem Verhältnis zugrundeliegenden Vertrag („*Hauptvertrag*“) ergeben. Der Hauptvertrag kommt durch die Buchung von Nutzungslizenzen für das VAF Cyber Security Center durch den Besteller als Auftraggeber beim VAF als Auftragnehmer zustande.

1. Anwendungsbereich

Der Anwendungsbereich dieser Vereinbarung umfasst alle Tätigkeiten, bei denen der *Auftragnehmer*, seine Mitarbeiter oder durch den *Auftragnehmer* beauftragte Dritte mit personenbezogenen Daten des *Auftraggebers,* insbesondere dessen Mitarbeiter oder seinerseitiger Auftraggeber in Berührung kommen und hierbei Weisungen umsetzen sollen („*Auftragsverarbeitung*“). Der konkrete Anwendungsbereich ist hier die Nutzung des VAF Cyber Security Centers durch den Auftraggeber.

Eine „*Weisung*“ im Sinne dieser Vereinbarung ist insbesondere eine auf Grund des zugrundeliegenden Hauptvertrages ergehende Anordnung des *Auftraggebers* an den *Auftragnehmer* im Sinne des Artikel 29 DS-GVO, personenbezogene Daten in Bezug auf den *Auftraggeber* bzw. dessen Auftraggeber oder Mitarbeiter gemäß Artikel 4 Nr. 2 DS-GVO auf datenschutzrelevante Weise zu verarbeiten, insbesondere sie zu erheben, zu erfassen, zu organisieren, zu ordnen, zu speichern, anzupassen oder zu verändern, auszulesen, abzufragen, zu verwenden, durch Offenlegung zu übermitteln, zu verbreiten oder auf andere Weise bereitzustellen, abzugleichen, zu verknüpfen, einzuschränken, zu sperren, zu löschen oder zu vernichten. Unerheblich ist dabei, ob eine Weisung bereits im Hauptvertrag festgelegt ist oder zu einem späteren Zeitpunkt erteilt, ergänzt, geändert oder ersetzt wird.

„*Personenbezogene*“ Daten im Sinne dieser Vereinbarung sind alle Informationen im Sinne des Artikel 4 Nr. 1 DS-GVO, die sich auf eine identifizierte oder identifizierbare natürliche Person („*betroffene*

Person“) beziehen. Hierzu gehören insbesondere Einzelangaben über persönliche oder sachliche Verhältnisse der betroffenen Person.

2. Gegenstand der Auftragsverarbeitung; Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

2.1 Der *Auftragnehmer* verarbeitet personenbezogene Daten im Auftrag des *Auftraggebers*. Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag.

2.2 Der *Auftragnehmer* verarbeitet die personenbezogenen Daten, die ihm im Rahmen der Erfüllung seiner Verpflichtung aus dem zugrundeliegenden Hauptvertrag zugänglich gewordenen sind, ausschließlich nach Weisungen des *Auftraggebers*.

2.3 Der Gegenstand, der Umfang, die Art und der Zweck der Verarbeitung personenbezogener Daten durch den *Auftragnehmer* für den *Auftraggeber*, sowie die Art der personenbezogenen Daten und der Kategorien der betroffenen Personen ergeben sich aus dem Hauptvertrag nebst Anlagen und werden im **Anhang 1** ergänzend aufgeführt.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung vom *Auftraggeber* unmittelbar durch den *Auftragnehmer* sicherzustellen.

2.4 Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist zuvorderst der *Auftraggeber* verantwortlich. Der *Auftraggeber* ist insbesondere für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, so auch für die Rechtmäßigkeit der Datenweitergabe an den *Auftragnehmer* sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich d.h. er ist „*Verantwortlicher*“ im Sinne des Artikel 4 Nr. 7 DS-GVO. Der *Auftraggeber* behält sich insoweit hinsichtlich der Verarbeitung im Auftrag gegenüber dem *Auftragnehmer* ein umfassendes Weisungsrecht vor.

2.5 Die Vergütung für die Auftragsverarbeitung bestimmt sich nach dem Hauptvertrag.

3. Pflichten des Auftragnehmers

3.1 Der *Auftragnehmer* unterstützt den *Auftraggeber* bei der Einhaltung der in den Artikeln 32 – 36 der DS-GVO genannten Pflichten zur Sicherstellung der Sicherheit personenbezogener Daten, in Bezug auf Meldepflichten bei Datenpannen, der Erstellung von Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.

3.2 Der *Auftragnehmer* ist verpflichtet, personenbezogene Daten, die ihm auf der Grundlage des mit dem *Auftraggeber* geschlossenen Hauptvertrages zugänglich werden, ausschließlich im Rahmen der von dem *Auftraggeber* getroffenen Weisungen zu verarbeiten. Der *Auftragnehmer* darf die Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des *Auftraggebers* verarbeiten (Artikel 29 DS-GVO) außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3a) DS-GVO vor.

Der *Auftragnehmer* informiert den *Auftraggeber* unverzüglich, wenn er der Auffassung ist, dass eine Weisung des *Auftraggebers* gegen anwendbare Gesetze verstößt. Der *Auftragnehmer* darf die Umsetzung der Weisung solange aussetzen, bis sie vom *Auftraggeber* bestätigt oder abgeändert wurde.

Kopien von erhobenen oder zur Datenverarbeitung überlassenen Daten werden nicht erstellt. Hiervon ausgenommen sind Sicherungskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung. Der *Auftragnehmer* hat personenbezogene Daten zu berichtigen, zu löschen

oder zu sperren, vorbehaltlich einer anderweitigen Verpflichtung nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland, wenn der *Auftraggeber*, ihn hierzu anweist.

3.3 Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im, bzw. gehen in das Eigentum des *Auftraggeber*s über. Sie werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Ein- und Ausgang werden dokumentiert. Der *Auftragnehmer* wird diese so sorgfältig verwahren, dass sie Dritten nicht zugänglich sind.

3.4 Der *Auftragnehmer* wird gemäß Artikel 32 DS-GVO zur ordnungsgemäßen Erfüllung seiner vertraglichen Verpflichtungen im Rahmen der Auftragsverarbeitung 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 der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, insbesondere seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht und ein angemessenes Schutzniveau erreicht wird. Er wird sich hierbei soweit möglich insbesondere auch der Pseudonymisierung und der Verschlüsselung personenbezogener Daten bedienen.

Er wird ferner **technische und organisatorische Maßnahmen** („*TOMs*“ Anhang 3) zur angemessenen Sicherung der Daten des *Auftraggebers* vor Missbrauch und Verlust treffen, die den Anforderungen der Datenschutz-Grundverordnung (Artikel 28 Abs. 3 lit. c, Artikel 24, Artikel 32 DS-GVO insbesondere i.V.m. Artikel 5 Abs. 2 DS-GVO i.V.m. § 64 BDSG) genügen. Dies beinhaltet insbesondere:

3.4.1 Unbefugten den Zugang zu Verarbeitungsanlagen, mit denen die Verarbeitung personenbezogener Daten durchgeführt wird, zu verwehren (**Zugangskontrolle/Zutrittskontrolle**),

3.4.2 zu verhindern, dass Datenträger von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können (**Datenträgerkontrolle/Weitergabekontrolle**),

3.4.3 zu verhindern, dass personenbezogene Daten unbefugt eingegeben sowie gespeicherte personenbezogene Daten unbefugt zur Kenntnis genommen, verändert oder gelöscht werden (**Speicherkontrolle/Zugangskontrolle**),

3.4.4 zu verhindern, dass automatisierte Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung unbefugt genutzt werden (**Benutzerkontrolle/Zugangskontrolle**),

3.4.5 zu gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. (**Zugriffskontrolle**),

3.4.6 zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogener Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle/Weitergabekontrolle**),

3.4.7 zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle/Zugangskontrolle**),

3.4.8 zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (**Transportkontrolle/Weitergabekontrolle**),

3.4.9 zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellbarkeit/Verfügbarkeitskontrolle**),

3.4.10 zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit/Incident-Response-Management**),

3.4.11 zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität/Verfügbarkeitskontrolle**),

3.4.12 zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen *Auftraggebers* verarbeitet werden können (**Auftragskontrolle**),

3.4.13 zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**)

3.4.14 zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.
(**Trennbarkeit/Trennungsgebot/Trennungskontrolle**).

Näheres ergibt sich aus dem **Anhang 3 (Datensicherheit, TOM)** zu dieser Vereinbarung.

Der *Auftragnehmer* stellt ferner sicher, dass über ein von ihm implementiertes Verfahren (in Bezug auf **Ziffer 3.4.1** – **3.4.7**) die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit sowie die Nachweisbarkeit der vorstehend aufgeführten technischen und organisatorischen Maßnahmen gewährleistet ist.

3.5 Der *Auftragnehmer* setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Er stellt ferner sicher, dass die mit der Verarbeitung der Daten des *Auftraggebers* befassten Mitarbeiter gemäß Artikel 29 DS-GVO diese Daten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland zur Verarbeitung verpflichtet sind, ausschließlich auf Weisung des Verantwortlichen verarbeiten und in die Schutzbestimmungen der Datenschutz-Grundverordnung eingewiesen worden sind sowie ergänzend in die innerbetrieblichen Richtlinien des *Auftragnehmers* eingewiesen und zu deren Einhaltung verpflichtet worden sind.

3.6 Der *Auftragnehmer* benennt dem *Auftraggeber* gegenüber unverzüglich, soweit er zu einer Bestellung gesetzlich verpflichtet ist, den **Datenschutzbeauftragten**, der seine Tätigkeit gem. Artikel 38 und 39 DS-GVO ausübt. Dessen Kontaktdaten werden dem *Auftraggeber* zum Zwecke der Kontaktaufnahme mitgeteilt. Jeder Wechsel des Datenschutzbeauftragten wird dem *Auftraggeber* unverzüglich mitgeteilt.

3.7 Der *Auftragnehmer* übergibt dem *Auftraggeber* auf dessen Anforderung das gemäß Artikel 30 Abs. 2 DS-GVO von ihm hinsichtlich seiner beauftragten Verarbeitungstätigkeiten zu führende **Verarbeitungsverzeichnis** und stellt dieses auf Anfrage der Aufsichtsbehörde zur Verfügung.

3.8 Der *Auftragnehmer* unterrichtet den *Auftraggeber* ferner unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder über andere datenschutzrelevante Unregelmäßigkeiten bei der Verarbeitung der Daten.

3.9 Nach Abschluss der vertraglichen Arbeiten hat der *Auftragnehmer* dem *Auftraggeber* auf dessen schriftliche Anforderung sämtliche in seinen Besitz gelangten Unterlagen des Auftraggebers, die im Zusammenhang mit dem Auftragsverhältnis stehen, auszuhändigen. Datenträger, die Daten des *Auftraggebers* als „*verantwortliche Stelle*“ beinhalten, sind hinsichtlich der betreffenden Daten vorbehaltlich einer anderweitigen Verpflichtung nach dem Unionsrecht oder dem Recht der

Bundesrepublik Deutschland insoweit physisch zu löschen. Die Löschung ist dem *Auftraggeber* schriftlich zu bestätigen.

Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, die auf Einzelanweisungen beruhen, welche über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom *Auftraggeber* zu tragen.

4 Pflichten des *Auftraggebers*

4.1 Der *Auftraggeber* ist für die rechtliche Beurteilung der Zulässigkeit der Datenverarbeitung sowie die Wahrung der Rechte der Betroffenen verantwortlich.

4.2 Der *Auftraggeber* ist verpflichtet Änderungen des zugrundeliegenden Hauptvertrages zur Auftragsverarbeitung soweit sie unter Artikel 28 DS-GVO fallen, schriftlich zu beauftragen. Änderungen von Weisungen über Art, Umfang und Verfahren der Datenverarbeitung, die sich im Rahmen des vertraglich Vereinbarten halten, sollen schriftlich erteilt werden;
Der *Auftragnehmer* ist berechtigt nicht schriftlich erteilte Weisungen zurückzuweisen.

4.3 Der *Auftraggeber* informiert den *Auftragnehmer* unverzüglich und umfassend, wenn es bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt. Entsprechendes gilt für den Fall einer Inanspruchnahme des *Auftraggebers* durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DS-GVO.

4.4 Der *Auftraggeber* behandelt, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen insbesondere im Hinblick auf Datensicherungsmaßnahmen des *Auftragnehmers* vertraulich.

5 Zusammenarbeit des *Auftraggebers* und des *Auftragnehmers*

5.1 Der *Auftragnehmer* und der *Auftraggeber* arbeiten auf entsprechende Anfrage der Aufsichtsbehörde mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der *Auftragnehmer* unterstützt den *Auftraggeber* im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche der betroffenen Personen gem. Kapitel III der DS-GVO (s.h. auch Ziffer 7) sowie bei der Einhaltung der in Artikel 33 – 36 DS-GVO genannten Pflichten.

5.2 Der *Auftragnehmer* verpflichtet sich ferner:

5.2.1 den *Auftraggeber* unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf den dieser Vereinbarung zugrundeliegenden Hauptvertrag beziehen, zu informieren,

5.2.2 den *Auftraggeber*, soweit er seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist, nach besten Kräften zu unterstützen.

5.3 Auch bereits während der Laufzeit dieser Vereinbarung berichtigt, löscht oder schränkt der *Auftragnehmer* die Verarbeitung von personenbezogenen Daten ein, wenn der *Auftraggeber* dies anweist und dies vom Weisungsrahmen umfasst ist.

5.4 Der *Auftraggeber* und der *Auftragnehmer* benennen im Bedarfsfall textlich die weisungsberechtigten Personen.

5.5 Im Falle einer Inanspruchnahme des *Auftraggebers* durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DS-GVO, verpflichtet sich der *Auftragnehmer* den *Auftraggeber* bei der Abwehr einsprechender Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

6 Anfragen Betroffener an den Auftraggeber/den Auftragnehmer

6.1 Ist der *Auftraggeber* auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der *Auftragnehmer den Auftraggeber* dabei unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung stellen.

6.2 Macht der Betroffene sein Recht auf Berichtigung, Löschung oder Sperrung seiner Daten geltend, nimmt der *Auftragnehmer* nur auf Weisung des *Auftraggebers* die Berichtigung, Sperrung oder Löschung vor oder leitet die Anfrage an den *Auftraggeber* weiter, soweit ihm die Vornahme der Anpassungen nicht möglich oder vertraglich nicht erlaubt ist.

6.3 Wendet sich die betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den *Auftragnehmer*, wird der *Auftragnehmer* die betroffene Person an den *Auftraggeber* verweisen, sofern eine Zuordnung nach den Angaben der betroffenen Person möglich ist. Der *Auftragnehmer* leitet den Antrag der betroffenen Person unverzüglich an den *Auftraggeber* weiter und unterstützt diesen nach dessen Weisungen im Rahmen seiner Möglichkeiten.

6.4 Der *Auftraggeber* ist verpflichtet den *Auftragnehmer* die diesem durch Maßnahmen nach **Ziff. 6.1 - 6.3** entstehenden Kosten gemäß der zwischen den Parteien im zugrundeliegenden Hauptvertrag getroffenen generellen Kostenregelungen zu ersetzen.

7 Unterauftragsverhältnisse

7.1 Der *Auftraggeber* erteilt dem *Auftragnehmer* unter den in **Ziffer 7.2** aufgeführten Voraussetzungen hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter hinsichtlich der Verarbeitung von *Auftraggeber*-Daten hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus dem **Anhang 2** zu dieser Vereinbarung. Generell nicht genehmigungspflichtig sind Vertragsverhältnisse mit Dienstleistern, die die Prüfung oder Wartung von Datenverarbeitungsverfahren oder -anlagen durch andere Stellen oder andere Nebenleistungen zum Gegenstand haben, auch wenn dabei ein Zugriff auf *Auftraggeber*-Daten nicht ausgeschlossen werden kann, solange der *Auftragnehmer* angemessene Regelungen zum Schutz der Vertraulichkeit der *Auftraggeber*-Daten trifft.

7.2 Der *Auftragnehmer* wird den *Auftraggeber* über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter informieren. Dem *Auftraggeber* steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potenziellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf von dem *Auftraggeber* nur aus wichtigem, dem *Auftragnehmer* nachzuweisenden Grund erhoben werden. Soweit der *Auftraggeber* nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der *Auftraggeber* Einspruch, ist der *Auftragnehmer* berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

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

8 Kontrollrechte

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

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

8.3 Zur Durchführung von Inspektionen nach Ziffer 8.2 ist der *Auftraggeber* berechtigt, im Rahmen der üblichen Geschäftszeiten (Montag bis Freitag von 09:00 bis 17:00 Uhr) nach rechtzeitiger Vorankündigung gemäß **Ziffer 8.5** auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des *Auftragnehmers,* die Geschäftsräume des *Auftragnehmers* zu betreten, in denen *Auftraggeber*-Daten verarbeitet werden.

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

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

8.6 Beauftragt der *Auftraggeber* einen Dritten mit der Durchführung der Überprüfung, hat der *Auftraggeber* den Dritten schriftlich ebenso zu verpflichten, wie auch der *Auftraggeber* aufgrund von dieser **Ziffer 8** dieses Vertrags gegenüber dem *Auftragnehmer* verpflichtet ist. Zudem hat der *Auftraggeber* den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des *Auftragnehmers* hat der *Auftraggeber* ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der *Auftraggeber* darf keinen Wettbewerber des *Auftragnehmers* mit der Kontrolle beauftragen.

8.7 Nach Wahl des *Auftragnehmers* kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, externer Datenschutzbeauftragter, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit („*Prüfungsbericht*“) erbracht werden, wenn der Prüfungsbericht es dem *Auftraggeber* in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

9. Löschung und Rückgabe von personenbezogenen Daten

9.1 Kopien oder Duplikate der Daten werden ohne Wissen des *Auftraggebers* nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.2 Nach Abschluss der vertraglich vereinbarten Tätigkeiten oder früher nach Aufforderung durch den *Auftraggeber* – spätestens mit Beendigung des Hauptvertrages – hat der *Auftragnehmer* sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem *Auftraggeber* auszuhändigen oder vorbehaltlich einer anderweitigen Verpflichtung nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für den Auftrag betreffendes Test- und Ausschussmaterial. Auf Aufforderung des *Auftraggebers* hat der *Auftragnehmer* ein Protokoll der Löschung vorzulegen.

9.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den *Auftragnehmer* entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende des Hauptvertrages hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende des Hauptvertrages dem *Auftraggeber* übergeben.

10. Haftung

10.1 Der *Auftraggeber* und der *Auftragnehmer* haften gegenüber betroffenen Personen entsprechend der in Artikel 82 DS-GVO getroffenen Regelung.

10.2 Der *Auftragnehmer* haftet im Innenverhältnis ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

10.2.1 er den aus der DS-GVO resultierenden und speziell für den Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder

10.2.2 er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des *Auftraggebers* handelte oder

10.2.3 er gegen die rechtmäßig erteilten Anweisungen des *Auftraggebers* gehandelt hat.

10.3 Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

11. Sonstiges

11.1 Der *Auftragnehmer* und der *Auftraggeber* bestimmen im Bedarfsfall einen fachkundigen Ansprechpartner, der während der Durchführung des Vertrages für die jeweilige Partei verbindliche Entscheidungen treffen kann und bei der Ausübung der bestehenden Kontrollrechte für die jeweils andere Partei zur Verfügung steht.

11.2 Die Einrede des Zurückbehaltungsrechts i.S.d. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger für den *Auftragnehmer* ausgeschlossen.

11.3 Soweit die Daten des *Auftraggebers* bei dem *Auftragnehmer* durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so ist der *Auftragnehmer* verpflichtet, den *Auftraggeber* unverzüglich darüber zu informieren. Der *Auftragnehmer* wird ferner alle in diesem Zusammenhang tätig werdenden Personen oder Organisationen unverzüglich darüber informieren, dass die Hoheit an den Daten ausschließlich bei dem *Auftraggeber* als „*Verantwortlichem*“ i.S.d. Artikels 4 Nr. 7 DS-GVO liegt.

11.4 Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des zugrundeliegenden Hauptvertrages.

11.5 Die Datenverarbeitung unter dieser Vereinbarung soll grundsätzlich nur in Ländern, die Mitglied der Europäischen Union oder ein Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, stattfinden. Entsprechendes gilt für jeglichen Zugriff auf die Daten durch

den *Auftragnehmer*, z.B. im Rahmen interner Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung. Datenverarbeitungen in anderen Ländern (sog. „*Drittstaaten*“) finden nur aufgrund entsprechender Vereinbarungen des zugrundeliegenden Hauptvertrages oder ausdrücklicher schriftlicher Weisung durch den *Auftraggeber* statt. Der *Auftraggeber* trägt dabei dafür Sorge, dass entsprechende Weisungen unter Einhaltung der DS-GVO erfolgen und wird bei einer entsprechenden Weisung den *Auftragnehmer* den zugrundeliegenden Erlaubnistatbestand benennen.

11.6 Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit dieser Vereinbarung ist der Sitz des *Auftragnehmers*.

11.7 Es gilt deutsches Recht.

Anhang 1

Gegenstand, Umfang und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber Onlinetrainings für seine Mitarbeiter zur Nutzung bereit. Der Auftraggeber kann seine Mitarbeiter zur Absolvierung der Schulung per E-Mail einladen. Der Mitarbeiter kann sich dann in dem Online-Schulungsportal anmelden.

Art(en) der personenbezogenen Daten

Name, Vorname, E-Mail-Adresse, ggf. Abteilung, Lernfortschritt.

Kategorien betroffener Person

Mitarbeiter des Auftraggebers

Anhang 2

Unterauftragnehmer

Mybreev GmbH
Bahnhofstr. 1 c
41747 Viersen

Die mybreev GmbH stellt die Plattform für die Onlinetrainings des VAF Cyber Security Centers als Unterauftragnehmer des Auftragnehmers.

Anhang 3

Datensicherheit: Technische und organisatorische Maßnahmen

Die personenbezogenen Daten, die im Rahmen dieses Auftragsverarbeitungsvertrages verarbeitet werden, werden ausschließlich von dem Unterauftragnehmer verarbeitet, so dass nachfolgend die technisch-organisatorischen Maßnahmen des Unterauftragnehmers aufgeführt werden.

Die vom Unterauftragnehmer angebotenen Onlineplattformen werden im Rechenzentrum der Amazon Web Services EMEA SARL (AWS) gehostet. Der Standort des Rechenzentrums ist Frankfurt/Main, Deutschland. Die technisch organisatorischen Maßnahmen können Sie unter https://aws.amazon.com/de/compliance/data-center/controls/ einsehen.

Nachfolgend werden die technisch-organisatorischen Maßnahmen im Unternehmenssitz des Unterauftragnehmers benannt:

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Büroräume der mybreev GmbH befinden sich in einem gemischt genutzten Gebäude in Viersen. Der Eingang des Gebäudekomplexes ist über eine Zutrittstür gesichert, die stets verschlossen und selbstschließend ist. Das Schlüsselmanagement für die Zutrittstür zum Gebäudekomplex liegt beim Vermieter. Die vom Vermieter ausgegebenen Schlüssel sind dem jeweiligen Mieter zugeordnet. Die Verwaltung der einzelnen Schlüssel der mybreev GmbH für die Zutrittstür obliegt der mybreev GmbH selbst.

Für die Türen zu und in den Geschäftsräumen der mybreev GmbH ist ein eigenes Schließsystem der mybreev GmbH im Einsatz.

Diesbezüglich gibt es einen Prozess für die Ausgabe von Schlüsseln auf Basis eines 4-Augen-Prinzips. Die Ausgabe von Schlüsseln wird protokolliert. Mitarbeiter sind verpflichtet, einen Schlüsselverlust unverzüglich zu melden.

Ferner gibt es einen Prozess bei einem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Schlüsseln und sonstigem Eigentum der mybreev GmbH durch den ausscheidenden Mitarbeiter beinhaltet.

Die Büroräume der mybreev GmbH befinden sich im Erdgeschoss des Gebäudes. Die Fenster in den Büroräumen der mybreev GmbH sind gesichert.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Die Büroräume der mybreev GmbH befinden sich im Erdgeschoss. Die Bildschirme der Mitarbeiter sind jedoch stets so ausgerichtet, dass eine Einsichtnahme von außen nicht erfolgen kann.

An jedem IT-System, das bei der mybreev GmbH im Einsatz ist, muss eine vorherige Authentifizierung erfolgen. Dies erfolgt auf Basis eines Benutzernamens und eines Passworts.

Eine Berechtigung zur Nutzung eines IT-Systems oder einer Applikation wird bei der mybreev GmbH nach dem 4-Augen-Prinzip erteilt. Eine Berechtigung muss daher zwingend vom jeweiligen Vorgesetzten für einen Mitarbeiter bei der IT-Administration beantragt werden. Der Vorgesetzte ist verpflichtet, hierbei nur die Berechtigungen zu beantragen, die für den jeweiligen Mitarbeiter unbedingt erforderlich sind, damit dieser die ihm zugewiesenen Aufgaben erfüllen kann. Berechtigungen sind dabei auf das Minimale zu beschränken.

Erteilte Berechtigungen (und der Entzug) werden von der IT-Administration und systemseitig protokolliert. Die IT-Administration prüft regelmäßig in Absprache mit dem Vorgesetzten, ob die erteilten Berechtigungen noch erforderlich sind. Vorgesetzte sind darüber hinaus verpflichtet, im Falle von Aufgabenwechsel von Mitarbeitern eine entsprechende Korrektur von Berechtigungen bei der IT-Administration zu beantragen.

Im Falle des Ausscheidens von Mitarbeiter informieren die Personalverantwortlichen die IT-Administration unverzüglich über anstehende Veränderungen, damit die IT-Administration entsprechende Berechtigungen entziehen kann. Der Entzug von Berechtigungen muss binnen 24 Stunden nach Ausscheiden eines Mitarbeiters durchgeführt worden sein.

Werden Initialpasswörter vergeben, ist bei mybreev stets vorgesehen, dass das Initial-passwort bei der ersten Anmeldung geändert wird. Dies wird technisch erzwungen.

Bei der mybreev GmbH gibt es Richtlinien zur Passwortverwendung, die ebenfalls grundsätzlich technisch erzwungen werden. Die Mindestpasswortlänge beträgt 10 Zeichen. Passwörter sind komplex zu wählen. Dies beinhaltet die Verwendung von Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern, wobei mindestens 3 von 4 dieser Merkmale erfüllt sein müssen.

Ein Passwortwechsel ist spätestens nach 90 Tagen zwingend. Es ist sichergestellt, dass die letzten 10 verwendeten Passwörter eines Nutzers nicht von diesem wiederverwendet werden können. Sollte sich der Stand der Technik bei der Verwendung von Passwörtern ändern, wird die mybreev GmbH die Passwortrichtlinien entsprechend anpassen.

Ein Zugriff auf die externen IT-Systeme findet ausschließlich über verschlüsselte Verbindungen statt. Die dabei verwendeten Verschlüsselungsalgorithmen und Schlüssellängen entsprechen dem Stand der Technik. Für den Fall einer zertifikatsbasierten Zugriffstechnologie ist gewährleistet, dass die Zertifikate durch Mitarbeiter der IT-Administration verwaltet werden.

Alle IT-Systeme, mit denen Daten im Auftrag verarbeitet werden, sind mit Antivirus-Software ausgestattet.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für die Erteilung von Benutzerrechten gilt bei der mybreev GmbH ein Berechtigungskonzept. Dies sieht vor, dass Berechtigungen ausschließlich auf Basis des 4-Augenprinzips und nach dem Minimalprinzip vergeben werden. Dies beinhaltet, dass jeder Mitarbeiter nur die Berechtigungen erhält, die er unmittelbar benötigt, um seine Aufgaben im Unternehmen erfüllen zu können.

Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein.

Die Vergabe und der Entzug von Berechtigungen werden protokolliert. Eine quartalsweise Überprüfung erfolgt durch die IT-Administration in Zusammenarbeit mit den jeweiligen Vorgesetzten der Mitarbeitet.

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten haben, die im Auftrag verarbeitet werden, beschränkt ist. Ein Kopieren von Daten auf externe Datenträger ist systemseitig unterbunden.

Ein Export von Daten wird auf Applikationsebene protokolliert und für einen Zeitraum von 12 Monaten unter Angabe der jeweiligen Benutzerkennung gespeichert.

Jeder Zugriff auf und der Abruf von Daten der Applikation erfolgt verschlüsselt (TLS).

Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch die mybreev GmbH übergeben werden soll, werden die Parteien im Vorweg eine Verschlüsselungsmethode bzw. einen Weg der sicheren Übertragung vereinbaren.

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Jede Eingabe von Daten, die im Auftrag des Auftraggebers von der mybreev GmbH verarbeitet werden, wird systemseitig unter Zuordnung der jeweiligen Benutzerkennung protokolliert. Gleiches gilt für die Änderung und Löschung von Daten. Im Falle einer Änderung von Daten ist aus der Protokollierung erkenntlich, welche Änderungen vorgenommen wurden.

Die Protokolle werden für die Dauer der Vertragslaufzeit von der mybreev GmbH gespeichert. Eine vorherige Löschung kann zwischen den Parteien vereinbart werden.

Durch die Protokollierung ist jederzeit nachvollziehbar, welche Benutzer Daten eingegeben, geändert oder gelöscht hat.

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der mybreev GmbH eine hohe Priorität. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.

Es gibt einen externen Datenschutzbeauftragten, der auch die regelmäßige Schulung der Mitarbeiter plant und durchführt. Alle Mitarbeiter erhalten mindestens eine jährliche Datenschutzschulung bzw. eine „Auffrischung".

Mitarbeiter, die an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, sind im Hinblick auf die Verarbeitung der Daten instruiert. Sofern der Auftraggeber ergänzende Weisungen erteilt, wird die mybreev GmbH alle betroffenen Mitarbeiter unverzüglich über die jeweilige Weisung informieren und Handlungsanweisungen zur Umsetzung geben.

Die Datenschutzvorkehrungen der mybreev GmbH beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Die mybreev GmbH gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Alle personenbezogenen Daten, die für den Auftraggeber verarbeitet werden, befinden sich im Rechenzentrum. Die mybreev GmbH hat Maßnahmen getroffen, die eine Sicherung der Daten und Wiederherstellung von Daten gewährleistet. Die Datenhaltung erfolgt zudem redundant. Es gibt ein Datensicherungs- und Wiederherstellungskonzept, dessen Wirksamkeit regelmäßig getestet wird.

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten getrennt voneinander verarbeitet werden.

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Unternehmensleitung hat sich zum Datenschutz und zur Informationssicherheit bekannt.

Die Mitarbeiter werden regelmäßig zum Datenschutz und zur Informationssicherheit geschult. Die Mitarbeiter werden zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet durch Unterzeichnung einer Vertraulichkeitsvereinbarung.

Eine Datenschutzbeauftragte ist für das Unternehmen benannt.

Es gibt einen Prozess zur Meldung von Datenschutzverletzungen. Es gibt einen Prozess zur Durchführung von Datenschutz Folgeabschätzungen. Es gibt einen Prozess zur Bearbeitung von Betroffenenanfragen. Es ist ein Datenschutzmanagementsystem implementiert worden.