**Mustervertragsklausel der BKB betreffend Cyberangriffen**

Die Beschaffungskonferenz des Bundes BKB stellt den öffentlichen Auftraggeberinnen[[1]](#footnote-1) der Bundesverwaltung eine Mustervertragsklausel betreffend Vorgehen im Falle von Cyberangriffen zur Verfügung.

Mit der Vereinbarung dieser Bestimmungen im Vertrag tragen die Vertragspartner zum Schutz der Daten und Informationen des Bundes und der Systeme bei Cyberangriffen bei, namentlich bei sicherheitsempfindlichen Tätigkeiten[[2]](#footnote-2).

Die Bundesverwaltung ist verpflichtet, bei der Zusammenarbeit mit Dritten für die Einhaltung der datenschutzrechtlichen und informationssicherheitsrechtlichen Vorgaben zu sorgen[[3]](#footnote-3). Die Verwaltungseinheiten sind in ihrem Zuständigkeitsbereich für die Informatiksicherheit verantwortlich.

Die Mustervertragsklausel dient den öffentlichen Auftraggeberinnen der Bundesverwaltung als Vorlage zur Vereinbarung von Massnahmen zum Schutz vor Cyberangriffen und des Vorgehens nach[[4]](#footnote-4) einem Cyberangriff auf einen Lieferanten bzw. Dienstleister[[5]](#footnote-5), der Informatikmittel der Bundesverwaltung betreibt oder schutzwürdigen Daten und Informationen des Bundes auf seinen Systemen bearbeitet. Sie unterstützt damit die Umsetzung der Verpflichtungen der Verwaltungseinheiten aus Artikel 9 Absatz 1 und 10 Absatz 1 ISG, Artikel 13 ISV sowie Artikel 24 DSG (zu den zitierten Rechtsgrundlagen s. die Verweise in den FN 8 und 9).

Die Mustervertragsklausel ist als eigenständige Vertragsbestimmung mit mehreren Ziffern ausgestaltet und kann typischerweise bei Informatikleistungen, aber auch in anderen Bereichen[[6]](#footnote-6) als Vertragsbestandteil zur Anwendung kommen[[7]](#footnote-7).

Die an die Mustervertragsklausel anschliessenden Erläuterungen dienen dem besseren Verständnis und der konkreten Ausgestaltung für den Anwendungsfall, sie sind jedoch nicht als Vertragsinhalt gedacht.

Massgebend für die Einschätzung, ob die Vereinbarung der Mustervertragsbestimmungen angezeigt ist, sind namentlich die Schutzbedarfs- und Risikoanalysen der zuständigen Fachstellen, die Klassifizierung von Informationen und die Sicherheitsstufen von Informatikmitteln. Sie dienen im Anwendungsfall als Grundlage für die Beurteilung, ob und welche der Ziffern der Mustervertragsklausel in den Vertrag integriert werden sollen. Dem Zweck der Mustervertragsklausel entsprechend sollten mindestens die Bestimmungen der Ziffern X1 – X3 zusammen im Vertrag integriert werden, zudem - soweit im Vertragswerk nicht anderweitig geregelt - die Haftung für Pflichtverletzungen. Für die Förderung der Einhaltung der Verpflichtungen steht die vorgeschlagene Konventionalstrafen-Regelung zur Verfügung sowie insbesondere bei festgestelltem erhöhtem Schutzbedarf, Risiko- oder Schadenspotenzial die Nachweis- und Audit-Massnahmen. Werden im Vertrag weitere Regelungen zur Informations- und Datensicherheit getroffen, sind die Inhalte der Mustervertragsklausel auf diese abzustimmen.

**Übersicht über die Regelungsinhalte** der Mustervertragsklausel:

Ziffer **X1** regelt die Verpflichtungen des Leistungserbringers zum *Schutz* der Informatikmittel vor Cyberangriffen sowie zu *Massnahmen* zur Verhinderung und Behebung von Gefahren und Schwachstellen und definiert den «*Cyberangriff*».

Ziffer **X2** verpflichtet den Leistungserbringer zur Einhaltung der einschlägigen *Rechtsgrundlagen* und *Vorgaben* sowie die Übertragung dieser Verpflichtungen auf von ihm beigezogene Dritte.

Ziffer **X3** regelt die *Meldepflicht* von Cyberangriffen.

Ziffer **X4** verpflichtet den Leistungserbringer zum *Nachweis* über seine Cybersicherheit und berechtigt den Leistungsbezüger, *Audits* beim Leistungserbringer durchzuführen.

Ziffer **X5** enthält eine *Konventionalstrafen*-Regelung.

Ziffer **X6** ist eine *Haftungsklausel*.

Ziffer **X7** dient der Vereinbarung einer *Haftpflichtversicherungspflicht*.

Die Ziffern werden anschliessend an die Mustervertragsklausel erläutert.

**Ziffer X Schutz der Informatikmittel vor Cyberangriffen und Meldepflicht**

**X1**. Der Leistungserbringer verpflichtet sich, seine Informatikmittel (d.h. Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen) mit potenzieller Berührung zum vorliegenden Vertragsgegenstand nach dem jeweils aktuellen Stand der Technik vor Cyberangriffen dem Risiko angemessen zu schützen.

Der Leistungserbringer stellt sicher, dass die vom Leistungsbezüger vordefinierten Aktivitäten aufgezeichnet und diese Aufzeichnungen laufend ausgewertet werden, um Cyberangriffe frühzeitig erkennen und abwehren zu können.

Der Leistungserbringer ist verpflichtet, die Verwirklichung einer erkannten Gefahr wirksam zu verhindern, deren Behebung umgehend einzuleiten und den Leistungsbezüger unverzüglich darüber zu informieren.

Der Leistungserbringer behebt vor, während oder nach einem Cyberangriff entdeckte Schwachstellen (d.h. Schwächen oder Fehler in Informatikmitteln mit dem Potenzial, einen Cyberangriff zu ermöglichen) umgehend und auf eigene Kosten.

Als «Cyberangriff» gilt jedes absichtlich ausgelöste Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist.

**X2**. Der Leistungserbringer verpflichtet sich, bei der Bearbeitung von Daten und Informationen des Bundes die Anforderungen und Vorgaben des Datenschutzgesetzes (DSG[[8]](#footnote-8)) und des Informationssicherheitsgesetzes (ISG[[9]](#footnote-9)) unter Einschluss der jeweiligen Ausführungsverordnungen sowie zum IKT-Grundschutz des Bundes zu beachten und einzuhalten. Er überträgt diese Verpflichtungen auf von ihm beigezogene Dritte (z.B. Zu- und Unterlieferanten, Substituten, Subunternehmer).

**X3**. Der Leistungserbringer meldet potenziell erfolgreiche Cyberangriffe, wenn also die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von Informationen des Bundes direkt oder indirekt gestört oder gefährdet sind oder solches beabsichtigt wurde. Dies gilt insbesondere, wenn die angegriffenen Informatikmittel Zugang zu Informatikmitteln des Bundes haben oder wenn Anzeichen dafür bestehen, dass diese Angriffe zur Vorbereitung weiterer Cyberangriffe ausgeführt wurden oder mit Erpressung, Drohung oder Nötigung verbunden sind. Der Leistungserbringer meldet Art und Ausführung einen solchen Cyberangriff spätestens innert 24 Stunden nach Entdeckung. Die Parteien tauschen sich dann laufend über Art und Ausführung, mögliche und tatsächliche Auswirkungen, geplante und getroffene Massnahmen aus.

Die Meldungen sind an folgende Stellen zu richten:

* Leistungsbezüger (Ansprechstellen mit Kontaktangaben bezeichnen), und
* Bundesamt für Cybersicherheit (BACS, ex NCSC) via online-Formular[[10]](#footnote-10)

Sofern der Leistungsbezüger oder das BACS es zum Schutz der Daten und Informationen des Bundes für notwendig erachten, gewährt der Leistungserbringer ihnen und von ihnen für die Vorfallbearbeitung beigezogenen Dritten unverzüglich Zugang zu Analysen, Untersuchungsberichten und anderen Feststellungen und Informationen (Dokumente, Daten, Log-Daten, Gegenstände etc.), die es erlauben, den Cyberangriff und dessen Auswirkungen zu analysieren und abzuwehren.

**X4**. Der Leistungserbringer erbringt dem Leistungsbezüger halbjährlich unaufgefordert und ohne separate Verrechnung Nachweise zu seiner Cybersicherheit in Form von (Form konkretisieren und einfügen). Sofern diese Nachweise als ungenügend erachtet werden oder wenn Hinweise auf Lücken in der Cybersicherheit bestehen, kann der Leistungsbezüger (oder ein Dritter in seinem Auftrag) beim Leistungserbringer und von ihm beigezogenen Dritten Audits zur Cybersicherheit durchführen. Solche Audits werden X Arbeitstage zum Voraus angekündigt. Jede Partei trägt ihre Kosten des Audits selbst. Sollten jedoch im Rahmen eines Audits wesentliche Mängel der Cybersicherheit festgestellt werden, trägt der Leistungserbringer neben den eigenen Kosten und den Aufwänden zur Behebung zusätzlich die Audit-Kosten des Leistungsbezügers.

**X5**. Der Leistungserbringer schuldet eine Konventionalstrafe, sofern er seinen Meldepflichten aus den Ziffern X1 – X4 gegenüber dem Leistungsbezüger nicht oder nicht fristgerecht nachkommt oder entdeckte Schwachstellen bzw. festgestellte Mängel nicht umgehend behebt. Diese beträgt je Verletzungsfall 10% der gesamten Vergütung, mindestens jedoch CHF 10'000.-- je Fall. Die Bezahlung der Konventionalstrafe befreit den Leistungserbringer nicht von der Einhaltung seiner vertraglichen Pflichten. Die Konventionalstrafe wird auf einen allfälligen Schadenersatz angerechnet.

**X6**. Der Leistungserbringer haftet für den Schaden, welcher dem Leistungsbezüger durch Cyberangriffe und die Nichteinhaltung der Bestimmungen in Ziff. X1 - X4 entsteht, sofern er nicht beweist, dass ihn kein Verschulden trifft.

Ev. Ziffer **X7** für die Regelung einer Haftpflichtversicherungspflicht einfügen *(s. entsprechende Erläuterungen mit Textvorschlag unten)*

Beschaffungskonferenz des Bundes (BKB)

Ausgabe: 01.01.2024[[11]](#footnote-11)

Stand: 01.03.2024[[12]](#footnote-12)

Erläuterungen s. Folgeseiten

**Erläuterungen zur Mustervertragsklausel:**

 **Hinweis zur Vervollständigung:**

Gelb hervorgehobene Platzhalter sind bei der Vertragserstellung durch den gewünschten Inhalt zu ersetzen. Mit «X» gemeint ist die Nummerierung dieser Musterklausel im jeweiligen Vertrag, in welchem sie Anwendung findet; sie wird daran anzupassen sein.

**Zu Ziffer X1:**

Mit «Leistungserbringer» ist der Vertragspartner gemeint, der zum Zweck der Vertragserfüllung Daten und / oder Informationen der Bundesverwaltung erhalten oder Zugriff darauf erhalten hat, die es vor Cyberangriffen zu schützen gilt. Bei der Vertragserstellung ist die Bezeichnung des Vertragspartners einzufügen, wie sie im gesamten Vertragswerk verwendet wird.

Mit «Leistungsbezüger» ist die vertragsschliessende Verwaltungseinheit gemeint. Massgebend ist die Organisationseinheit, die den Vertrag mit dem Leistungserbringer unterzeichnet. Das können die Beschaffungsstelle oder die Bedarfsstelle oder beide sein.

Mit der Verpflichtung des Leistungserbringers zu Schutzmassnahmen soll ein direkt oder indirekt erfolgreicher Cyberangriff verhindert oder mindestens dessen Auswirkungen vermindert werden. So geht es beispielsweise um den Schutz von Codes und Passwörtern, von klassifizierten Informationen und Systemen, oder von nicht öffentlichen Informationen wie Belegungsplänen, Bauplänen oder Plänen technischer Anlagen, Personendaten, Prozessbeschreibungen und Arbeitsabläufen oder Zutrittsregelungen.

Der Schutz ist nach dem aktuellen Stand der Technik dem Risiko angemessen vorzukehren, was im konkreten Fall die Berücksichtigung der technischen und organisatorischen Möglichkeiten, allenfalls auch die der wirtschaftlichen Zumutbarkeit ermöglicht. Die Kosten, die dem Leistungserbringer für den Schutz und dessen Aufrechterhaltung entstehen, trägt er selbst. Infolgedessen auch die Kosten für die Behebung von Schwachstellen, die vor, während oder nach einem Cyberangriff entdeckt werden.

Die Verpflichtung ist in der Textvorlage nicht an eine bestimmte Dauer gebunden. Sie besteht mindestens für die Dauer der Gültigkeit des Vertragsverhältnisses. Wenn im konkreten Fall aufgrund der Risiken die Informatikmittel bereits vor Vertragsabschluss und/oder nach Vertragsabschluss geschützt werden sollen, sind entsprechende Verpflichtungen bereits im Vorfeld (z.B. bei der Ausschreibung, bei der Vertragsverhandlung etc.) zu definieren und mit dem Leistungserbringer zu vereinbaren. Das betrifft namentlich auch Systeme, auf denen nach der Leistungserbringung Daten oder Informationen des Leistungsbezügers verbleiben, z.B. bis zu deren Rückgabe, Löschung oder Vernichtung (diesbezüglich empfiehlt sich die Festlegung einer Frist, soweit diese nicht in den Allgemeinen Geschäftsbedingungen des Bundes, die für das Vertragsverhältnis vereinbart werden, bereits festgelegt ist).

Der Anwendungsbereich dieser Ziffer kann – soweit angezeigt – auf Systeme des Leistungserbringers beschränkt werden, die für die Sicherheit der Bundesverwaltung relevant sind.

Gemäss Artikel 5 des revidierten ISG sind Cyberangriffe absichtlich ausgelöste Cybervorfälle, also Ereignisse bei der Nutzung von Informatikmitteln, die dazu führen, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt sind.

Beispiele sind etwa der unbefugte Zugang, die Störung, die Manipulation oder der Missbrauch der Systeme und Daten von innen oder aussen, oder der Diebstahl, die unrechtmässige Verarbeitung oder die Vernichtung von Informationen oder Daten sowie sonstige rechtswidrige Eingriffe in die Systeme und damit verbundene Handlungen (vgl. insbesondere Art. 143, 143bis,144bis, 147,179novies, 272 - 274 des Strafgesetzbuches (StGB[[13]](#footnote-13)))

Vgl. dazu ergänzend auch die Erläuterungen zu Art. 5 in der Botschaft zum revidierten ISG sowie die Informationen des BACS zur «Nationalen Cyberstrategie NCS» (unter folgendem Link: [Nationale Cyberstrategie NCS (admin.ch)](https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html)).

**Zu Ziffer X2:**

Die Verpflichtung gilt für den Leistungserbringer und seine beigezogenen Dritten (z.B. Subunternehmer, Substituten und Zulieferer). Er garantiert, für die korrekte Vertragserfüllung verfügbar gemachte oder bei ihm und/oder bei den von ihm zugezogenen Dritten entstandene und/oder bearbeitete Daten und Informationen entsprechend den Vorgaben zu schützen. Das gilt insbesondere für sicherheitsrelevante Angaben oder Personendaten.

**Zu Ziffer X3:**

Im Vertrag ist sicherzustellen, dass die Parteien für die Meldung eines Cyberangriffs und den darauffolgenden Austausch und die Zusammenarbeit vom Amtsgeheimnis entbunden sind, um Verzögerungen nach einem Cyberangriffs zu vermeiden.

Im Vertrag sind die Ansprechstellen beim Leistungsbezüger konkret zu bezeichnen, an die der Leistungserbringer seine Meldung über den Cyberangriff zu richten hat (i.d.R. ist das die bzw. der Informationssicherheitsverantwortliche des Leistungsbezügers). Zusätzlich ist das BACS Meldungsempfängerin. Gegebenenfalls sind auch weitere Meldungsempfängerinnen im Vertrag zu bezeichnen.

Die in dieser Ziffer aufgeführten Konstellationen lösen je einzeln die Meldepflicht aus und müssen bei einem Cyberangriff nicht kumulativ vorliegen.

Die Meldepflicht bezieht sich auf Cyberangriffe, die den Schutz der Daten oder die Funktionalität der Informatikmittel beeinträchtigen können. Keiner Meldepflicht unterliegen nicht erfolgreiche und ungefährliche Cyberangriffe, wie massenhaft versandte Spam-Mails oder Portscans. Ein Cyberangriff ist erfolgreich, wenn die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von Informationen des Bundes nicht mehr gewährleistet werden kann, unabhängig davon, ob dies unbeabsichtigt oder mit missbräuchlicher Absicht erfolgt. Inhalt und Art dieser Meldung müssen zwischen den Vertragspartnern im Vertrag definiert werden. Dabei ist der Schutzbedarf der Daten und der Informatikmittel zu berücksichtigen.

Die Meldung muss innert 24 Stunden nach der Entdeckung des Cyberangriffs erfolgen[[14]](#footnote-14). Wenn im Einzelfall eine andere Frist angemessen und angezeigt ist[[15]](#footnote-15), kann von der Vorlage abgewichen werden, sofern die organisatorischen Voraussetzungen für die Entgegennahme und Bearbeitung der Meldung(en) beim Leistungsbezüger gegeben sind. Innerhalb der vereinbarten Frist müssen nur die bis zum Meldezeitpunkt bekannten Informationen gemeldet werden; die Meldung kann später ergänzt werden.

Die Meldung und der weitere Austausch unter den Parteien bezwecken die schnelle Vermittlung der Informationen zur Art und Ausführung des Cyberangriffs, zu seinen möglichen Auswirkungen, zu ergriffenen Massnahmen und zum geplanten weiteren Vorgehen. Eine Orientierung zu Struktur und Inhalt einer Meldung bietet die Vorlage des BACS für die Meldung von Cybervorfällen: [Meldung (admin.ch)](https://www.report.ncsc.admin.ch/de/)

Weitere Informationen des BACS zum Vorgehen bei Cyberangriffen finden sich hier:

[Cyberattacke – was tun? Informationen und Checklisten (admin.ch)](https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden/vorfall-was-nun/checkliste-ciso.html)

**Zu Ziffer X4:**

Der Nachweis kann beispielsweise in Form bestimmter Zertifizierungen oder von Auditberichten erfolgen, in Frage kommen übliche oder anerkannte Nachweisarten. Zwecks Rechtssicherheit und Durchsetzbarkeit ist die Form der Nachweise in der Bestimmung X4 bzw. im Vertragswerk (z.B. als Anhang) festzulegen.

Der Rhythmus der halbjährlichen Erbringung der Nachweise kann den Umständen im Anwendungsfall angepasst oder mit einem zusätzlichen Recht des Leistungsbezügers, Nachweise jederzeit anfordern zu dürfen, verbunden werden. Aus der Erbringung eines Nachweises entsteht dem Leistungserbringer kein Anspruch auf zusätzliche, separate Entschädigung der damit verbundenen Kosten und Aufwände.

Der Leistungsbezüger schafft die Voraussetzungen für die Durchführung von Audits. Es empfiehlt sich, die Modalitäten des Audits im Vertrag zu konkretisieren. In dieser Mustervertragsvorlage ist Voraussetzung für ein Audit, dass die Nachweise als ungenügend erachtet werden oder dass Hinweise auf Lücken in der Cybersicherheit bestehen. Dies ist praxisgerecht und rechtfertigt zudem, dass jede Partei ihre aus dem Audit entstehenden jeweiligen Aufwände und Kosten selber trägt. Als Variante zu dieser Regelung denkbar ist auch ein generelles Recht des Leistungsbezügers, ein Audit anzuordnen und durchzuführen. In der Praxis werden ein voraussetzungsloses, jederzeitiges Auditrecht mit Kostenteilung jedoch schwer mit dem Leistungserbringer zu vereinbaren sein.

Die Frist («X» Arbeitstage) für die Vorankündigung eines Audits ist im jeweiligen Vertrag, in welchem sie Anwendung findet, bezogen auf die konkreten Risiken und Bedürfnisse festzulegen. Anstelle von «X» ist die genaue Frist, bemessen in Tagen einzusetzen. Alternativ kann auch ein konkretes Datum vereinbart werden, der Satzteil wäre entsprechend anzupassen. Aus der Praxis wird eine Frist von 20 Arbeitstagen vorgeschlagen. Es gibt jedoch keine generelle Vorgabe, die verallgemeinerungsfähig wäre.

Die Kostenübertragung an den Leistungserbringer im Falle von wesentlichen Mängeln ist sachgerecht. Die Mängel wie deren Wesentlichkeit hängen von den konkreten Umständen im Einzelfall ab und sind im Vertrag soweit möglich zu konkretisieren.

Im Grundsatz und gemäss Ziffer X1 gilt die Verpflichtung zur umgehenden Behebung festgestellter Schwachstellen. Bei Bedarf kann im Vertrag eine separate Frist für die Behebung von Mängeln, die während eines Audits entdeckt werden, abhängig von der Art oder der Kategorie des Mangels und den Umständen, praxisgerecht festgelegt werden.

**Zu Ziffer X5:**

Die Konventionalstrafen-Regelung deckt sich nicht mit der Standard-Konventionalstrafen-Klausel in den diversen AGB des Bundes. Die Mindestsumme ist höher und liegt bei 10'000.- Franken. Sie kann im Einzelfall entsprechend der Risikobeurteilung der zuständigen Fachstellen in Höhe und Bemessung vertraglich angepasst werden. Alternativ kann auch auf eine generelle Konventionalstrafen-Regelung im Vertragswerk abgestellt werden, sofern deren Ausgestaltung die hier geregelten Verletzungsfälle mitumfasst. Zwecks Nachvollziehbarkeit empfiehlt es sich, die Motive für eine Anpassung, insbesondere bei einer Herabsetzung der Mindesthöhe, zu dokumentieren (verbunden mit einer nachvollziehbaren Begründung, weshalb im konkreten Fall von einem geringen Risiko ausgegangen wird).

**Zu Ziffer X6:**

Grundsätzlich fallen unter die Haftung alle aus Angriffen gemäss Ziffer X1 und sonstigen Nichteinhaltungen der Mustervertragsbestimmungen entstandene Schäden. Damit erfasst die Haftungsklausel die Schäden aufgrund des Cyberangriffs und weitere, die durch die Missachtung der Bestimmungen aus dieser Musterklausel beim Leistungsbezüger entstehen.

Ob diese Haftungsregelung für die konkreten Verhältnisse angemessen ist, muss jeweils vom Leistungsbezüger geprüft und gegebenenfalls adaptiert werden.

Diese Bestimmung kann weggelassen bzw. muss angepasst werden, wenn die Haftung an anderer Stelle im Vertrag geregelt ist und dort die Haftungsfälle aus dieser Mustervertragsklausel umfasst (vgl. auch Vertragsvorlagen des Bundesamtes für Bauten und Logistik BBL, des Kompetenzzentrums Beschaffungswesen Bund KBB und die AGB des Bundes), oder wenn die spezifische Risikosituation dies zulässt bzw. erfordert.

Im Vertrag ist bei den Kündigungsvoraussetzungen darauf zu achten, dass die Nichteinhaltung der Bestimmungen betreffend Cyberangriffen als Kündigungsgrund für den Leistungsbezüger festgelegt wird (als ausserordentlicher Kündigungsgrund oder als Kündigung aus wichtigem Grund).

**Zur eventuellen Ziffer X7:**

Gewisse Versicherungsunternehmen bieten die Möglichkeit, Risiken im Zusammenhang mit Cyberangriffen zu versichern. Im Einzelfall und bei Verträgen, in welchen der Kernpunkt bei der Erbringung von Informatikleistungen liegt, kann es sich optional empfehlen, den Vertragspartner zu verpflichten, sich dem Schadenspotenzial entsprechend zusätzlich zu versichern. In der Praxis werden sehr unterschiedliche Versicherungslösungen angeboten. Es empfiehlt sich mit Blick auf die Angemessenheit der Versicherungsdeckung, vor deren Abschluss die darauf anwendbaren Versicherungsbedingungen dem Leistungsbezüger zur Kontrolle vorlegen zu lassen. Die Modalitäten dazu sind im Vertrag festzulegen.

Vorschlag für eine entsprechende Vereinbarung:

*«X7. Der Leistungserbringer verpflichtet sich, eine der vorliegenden Art und dem Schadensrisiko entsprechend angemessene Haftpflichtversicherung abzuschliessen und die ausreichende Versicherungsdeckung zum Zeitpunkt des Vertragsabschlusses nachzuweisen. Die auf das Versicherungsverhältnis anwendbaren Versicherungsbedingungen sind vor Abschluss der Versicherung dem Leistungsbezüger zur Kontrolle vorzulegen.»*

Im Vergabeverfahren ist diesfalls als Eignungskriterium festzulegen, dass die Anbieterin im Falle des Zuschlages auf Verlangen des Auftraggebers zur Erbringung des entsprechenden Nachweises verpflichtet wird.

\*\*\*\*\*

1. Diese Mustervertragsklausel steht allen Leistungsbezügern der Bundesverwaltung zur Verfügung, namentlich den öffentlichen Auftraggeberinnen, die für die Beschaffung von IKT-Leistungen zuständig sind. Die Beschaffungskompetenzordnung ist in der Verordnung vom 24. Oktober 2012 über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB, SR 172.056.15) geregelt. [↑](#footnote-ref-1)
2. Nicht Zweck und Inhalt dieser Musterbestimmungen sind die vertragliche Festlegung der Mindestanforderungen an die Informatikmittel und die Gewährleistung für deren Sicherheit und Schutz durch den Leistungserbringer. [↑](#footnote-ref-2)
3. Die Allgemeinen Geschäftsbedingungen des Bundes (AGB) enthalten Standardklauseln zur Geheimhaltung, zum Datenschutz und zur Datensicherheit (inkl. Datenrückgabe, -löschung und -vernichtung). Die AGB sind verfügbar auf der Webseite der BKB ([www.bkb.admin.ch](http://www.bkb.admin.ch)). [↑](#footnote-ref-3)
4. Die Vereinbarung der Mustervertragsklausel im Vertrag entbindet nicht von der Verantwortung, die Sicherheitsverfahren, Vorschriften, Vorgaben und Anforderungen mit Bezug auf die Daten- und Informationssicherheit (inklusive dem IKT-Grundschutz) in allen öff. Aufträgen über Informatikleistungen zu berücksichtigen und wo nötig über diese Mustervertragsklausel hinaus Massnahmen (z.B. Penetrationstests) mit dem Leistungserbringer (s. FN 5) vertraglich zu vereinbaren. [↑](#footnote-ref-4)
5. In der Mustervertragsklausel als «Leistungserbringer» bezeichnet. [↑](#footnote-ref-5)
6. Dort, wo Vertragspartner Informationen oder Daten des Bundes verarbeiten, ohne dabei Informatikleistungen an den Bund zu erbringen, wie etwa bei Druckereien, Advokaturen, Beratungsunternehmen, Übersetzungs-, Architektur- oder Planerbüros etc. [↑](#footnote-ref-6)
7. Insbesondere sofern vom Vertragspartner Daten und / oder Informationen bearbeitet werden, die namentlich entweder dem Amtsgeheimnis oder anderen Geheimhaltungsbestimmungen unterstehen, oder gemäss den geltenden Informationsschutzbestimmungen des Bundes als klassifiziert gelten, ist im Einzelfall zusätzlich zu prüfen, ob die Bestimmungen dieser Mustervertragsklausel im Vertrag zu konkretisieren, ausführlicher zu regeln oder durch weitere Bestimmungen zu ergänzen sein werden. [↑](#footnote-ref-7)
8. Bundesgesetz vom 25. September 2020 über den Datenschutz, SR 235.1 [↑](#footnote-ref-8)
9. Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund, SR 128 [↑](#footnote-ref-9)
10. Verfügbar auf <https://www.report.ncsc.admin.ch/de/> [↑](#footnote-ref-10)
11. Diese Musterklausel ersetzt die Vorlage der BKB betreffend Cyberrisiken vom 01.09.2020 (Stand 09.11.2022). [↑](#footnote-ref-11)
12. Im Vergleich zum Stand vom 01.01.2024 (verfügbar nur auf Deutsch) wurden die Bezeichnung des BACS angepasst, Links aktualisiert und ein fehlerhafter Verweis auf zwei Fussnoten korrigiert. [↑](#footnote-ref-12)
13. SR 311.0 [↑](#footnote-ref-13)
14. Analog zur Regelung in Artikel 74e revISG. [↑](#footnote-ref-14)
15. Eine Klärung und Absprache mit dem BACS ist empfehlenswert, da die Meldung auch an das BACS geht. [↑](#footnote-ref-15)