Mustervertragsklausel der BKB betr. Cyberrisiken

Die Beschaffungskonferenz des Bundes BKB stellt den Beschaffungsstellen der Bundesverwaltung eine Musterklausel für Beschaffungsvertragsvorlagen betreffend Schutz der Informatik- und Telekommunikationssysteme vor Angriffen verbunden mit einer entsprechenden Meldepflicht zur Verfügung. Die Musterklausel ist als eigenständige Vertragsbestimmung mit mehreren Ziffern ausgestaltet, die in einen Beschaffungsvertrag übernommen werden kann. Die ergänzenden Erläuterungen der Musterklausel dienen dem besseren Verständnis und der konkreten Ausgestaltung für den Anwendungsfall, sie sind jedoch nicht als Vertragsinhalt gedacht. Die Musterklausel ist in erster Linie für Beschaffungen mit hohem Risikopotential für Cyberangriffe im Sinne der nachfolgenden Bestimmungen geeignet. Die Anwendung der Musterklausel ist nach Bedarf zu beurteilen und ihr Inhalt dispositiv in dem Sinne, dass für jeden Vertrag die auf die konkreten Verhältnisse risiko-optimierte Ausgestaltung vereinbart werden soll.

Anschliessend an die Mustervertragsklausel folgen Erläuterungen zu deren Anwendung und Inhalt.

Ziffer X Schutz der Informatik- und Telekommunikationssysteme vor Angriffen und Meldepflicht

1. Der N.N. (Bezeichnung gemäss Vertrag für den Partner der BV)[1] ist verpflichtet, für die und bei der Vertragsabwicklung seine Informatik- und Telekommunikationssysteme (umfassend insbesondere Infrastruktursysteme, Netzwerke, Geräte und Anwendungen sowie Daten[2] und Informationen[3]) - im Folgenden bezeichnet als «Systeme» - in seinem Verantwortungsbereich nach dem jeweils aktuellen Stand der Technik mittels technisch und organisatorisch möglichen sowie wirtschaftlich zumutbaren Vorkehrungen vor Angriffen zu schützen.

2. Als «Angriffe» (äquivalente Begriffe: «Cyberattacken» oder «Cyberangriffe») gelten insbesondere der unbefugte Zugang, die Störung, die Manipulation oder der Missbrauch der Systeme von innen oder aussen. Weiter gehören insbesondere der Diebstahl, die unrechtmässige Verarbeitung oder die Vernichtung von Informationen oder Daten sowie sonstige rechtswidrige Eingriffe in die Systeme dazu (vgl. insbesondere Art. 143, 143bis,144bis, 147,179^{novies}, 272-274 des Strafgesetzbuches (StGB[4])).

3. Der N.N. verpflichtet sich insbesondere, ihm und seinen beigezogenen Dritten[5] (z.B. Subunternehmer und Zulieferer) für die korrekte Vertragserfüllung verfügbar gemachte oder bei ihnen entstandene Daten und Informationen entsprechend den Bestimmungen dieser Ziffer X zu schützen. Das gilt insbesondere, wenn es sich um sicherheitsrelevante Angaben oder um Personendaten handelt. Es sind dabei die Anforderungen und Vorgaben des Bundesgesetzes

---

1 Terminologie anpassen an jeweilige Vertragsvorlage (z.B. Auftragnehmer, Unternehmer)
2 Z.B. Personenangaben zu Mitarbeitenden, Mailadressen, Zugangs- und Zugriffscodes etc.
3 Z.B. Prozessbeschreibungen, Arbeitsabläufe, Pläne, Zutrittsregelungen, Infrastruktur etc.
4 SR 311.0
5 In Frage kommen alle in der Liefer- und Produktionskette eingebundenen Parteien, namentlich auch Rechteinhaber und Hersteller.

Bundesamt für Bauten und Logistik BBL
Fellerstrasse 21, 3003 Bern
Tel. +41 41 58 462 38 50, Fax +41 58 465 50 09
bkb@bbl.admin.ch
www.bbl.admin.ch/bkb

über den Datenschutz (DSG[6]), der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyberRV[7]), der Informationsschutzverordnung (ISchV[8]) und der Bundesinformatikverordnung (BinfV[9]) zu beachten und einzuhalten.

4. Der N.N. meldet dem Leistungsbezüger[10] und/oder der im Vertrag dafür bezeichneten Stelle unaufgefordert jedes erkannte Ereignis, welches die Einhaltung seiner Pflichten beeinträchtigen könnte, unverzüglich nach Auftreten bzw. Kenntnisnahme, spätestens innerhalb einer Frist von X Stunden. Er meldet insbesondere versuchte oder erfolgreiche Angriffe sowie andere befürchtete oder erfolgte technische Kompromittierungen von Systemen, Daten und/oder Informationen und allenfalls entstandene Schäden. Dabei wird auch über die geplanten und getroffenen Massnahmen zu deren Behebung informiert. Zur Vermeidung von Schäden oder weiteren Angriffen gewährt der N.N. dem Leistungsbezüger oder durch ihn beauftragten Dritten auf erstmalige Aufforderung unverzüglich den vollen und umfassenden Zugang zu Analysen, Untersuchungsberichten und anderen Feststellungen (Dokumente, Daten, Log-Daten, Gegenstände etc.), die es erlauben, das Ereignis zu analysieren. Der N.N. stellt sicher, dass mit dem Leistungsbezüger vordefinierte Aktivitäten aufgezeichnet (Logging) und ausgewertet werden, um Angriffe zu erkennen und zu vermeiden. Entdeckte Sicherheitslücken müssen zeitnah behoben werden.

5. Der Leistungsbezüger (oder ein Dritter in seinem Auftrag) kann nach Bedarf - höchstens zwei Mal jährlich - beim N.N. Audits durchführen. Solche werden X Arbeitstage vorangekündigt. Jede Partei trägt ihre Kosten des Audits selbst. Sollten jedoch im Rahmen eines Audits wesentliche Mängel im Sinne dieser Bestimmung festgestellt werden, trägt der N.N. zusätzlich die Kosten zur Behebung dieser Mängel aber auch die Kosten, die dem Leistungsbezüger aus dem Audit entstehen. Der N.N. ist verpflichtet, festgestellte Mängel innert einer Frist von X seit der Meldung zu beheben und dem Leistungsbezüger den Vollzug zu melden.

6. Der N.N. schuldet eine Konventionalstrafe, sofern er die verlangten Vorkehrungen gemäss der vorliegenden Klausel nicht getroffen hat. Diese beträgt je Verletzungsfall 10% der gesamten Vergütung, mindestens jedoch CHF 3'000.-- je Fall. Die Bezahlung der Konventionalstrafe befreit den N.N. nicht von der Einhaltung seiner vertraglichen Pflichten. Die Konventionalstrafe wird auf einen allfälligen Schadenersatz angerechnet.

7. Der N.N. haftet für den Schaden, welcher dem Leistungsbezüger entsteht, sofern er nicht beweist, dass ihn kein Verschulden trifft.

Bei wesentlichen Verletzungen dieser Klausel oder mangelnder Mitwirkung in obengenannten Fällen behält sich der Leistungsbezüger vor, keine weiteren Leistungen zu beziehen und die Vertragsbeziehung zu beenden.

Ev. Ziffer 8 für die Regelung einer Haftpflichtversicherungspflicht einfügen *(s. entsprechende Erläuterungen mit Textvorschlag unten)*

Beschaffungskonferenz des Bundes (BKB)
Ausgabe: 01.09.2020
Stand: 01.09.2020

Erläuterungen s. Folgeseiten

6 SR 235.1
7 SR 120.73
8 SR 510.411
9 SR 172.010.58
10 Terminologie anpassen an jeweilige Vertragsvorlage (z.B. Auftraggeber, Käufer)

Erläuterungen zur Musterklausel:

Hinweis zur Vervollständigung:

Gelb hervorgehobene Platzhalter sind bei der Vertragserstellung durch den gewünschten Inhalt zu ersetzen.

Allgemein:

Ziel ist der Schutz der Daten und Informationen und der Systeme, namentlich vor und bei Cyberangriffen.

Die Mustervorlage soll als allgemeine Bestimmung bei denjenigen Geschäften zur Anwendung gelangen, wo diesbezügliche Risiken erkannt werden, namentlich bei IKT-Beschaffungsverträgen in besonders risikoreichen Situationen. Mit Risiken ist grundsätzlich überall dort zu rechnen, wo ein Vertragspartner im Zuge der Erbringung seiner Leistungen Informatik- und Telekommunikationssysteme einsetzt. Insbesondere geht es darum, eine Schädigung oder einen Verlust von Daten, Informationen und Systemen der Bundesverwaltung durch einen Cyberangriff auf einen ihrer Geschäftspartner zu verhindern oder zu vermindern. Dasselbe gilt, wenn Informationssysteme der Geschäftspartner als Mittel für einen Cyberangriff auf die Bundesverwaltung genutzt werden (sollen). So geht es beispielsweise um den Schutz von Codes und Passwörtern oder von Informationen wie Belegungsplänen, Bauplänen oder Plänen technischer Anlagen (weitere Beispiele s. Fussnote 3 der Musterklausel).

Ist ein Vertrag mit einem Geschäftspartner in Erarbeitung, soll diesen Schutz- und Informationsbedürfnissen mit der Verwendung dieser Musterklausel Rechnung getragen werden.

Wo erforderlich, ist diese Musterklausel anzupassen, die Bestimmungen sind dispositiv. 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 Klausel im Vertrag ausführlicher zu regeln sein werden.

Es ist demgegenüber auch möglich, den weniger risikobehafteten Situationen im Einzelfall durch eine Anpassung einzelner Bestimmungen dieser Klausel angemessen Rechnung zu tragen, etwa durch eine mildere Ausgestaltung der Konventionalstrafe oder des Auditrechts.

Nicht ausgeschlossen ist auch die gegenseitige Vereinbarung der Schutz- und Meldemassnahmen, wenn Geschäftspartner ihrerseits der Bundesverwaltung Geschäftsgeheimnisse, schutzbedürftige Informationen oder Daten anvertrauen. Bei der gegenseitigen Vereinbarung dieser Vertragsbestimmungen oder Teilen davon für beide Vertragsparteien sind allerdings die Verpflichtungen betreffend Zugriffs-, Zugangs- und Auditrechten sowie die Konventionalstrafenregelung seitens der vertragsschliessenden Bundesverwaltungseinheit vor Vertragsabschluss eingehend zu prüfen. Wir empfehlen dafür die Konsultation des zuständigen Rechtsdienstes.

Zu Ziffer 1:

«N.N.» steht als Abkürzung für «nomen nominandum» (lateinisch für „[noch] zu nennender Name“). Dieser Platzhalter wird vorliegend für „Der Name ist hier einzusetzen“ verwendet. Gemeint ist der Name des Vertragspartners, der zum Zweck der Vertragserfüllung Daten oder Informationen der Bundesverwaltung erhalten hat, die es vor Cyberangriffen zu schützen gilt. Bei der Vertragserstellung ist die korrekte Bezeichnung des Vertragspartners einzufügen.

Zu Ziffer 2:

Vgl. dazu ergänzend auch die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» (S. 27) unter folgendem Link:

https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/ncs_strategie-2012.html

Zu Ziffer 3:

Mit «X» gemeint ist die Nummerierung dieser Musterklausel im jeweiligen Vertrag, in welchem sie Anwendung findet. Sie muss derjenigen in der Bezeichnung (Titel) dieser Vertragsklausel entsprechen.

Die Einhaltung der Schweizer Rechtsgrundlagen und –vorgaben mit ausländischen Vertragspartnern kann u.U. auf Schwierigkeiten stossen. Erfahrungsgemäss ergibt sich daraus zusätzlicher Verhandlungsaufwand, was die vertragsschliessende Verwaltungseinheit nicht daran hindert, die Klausel als Verhandlungsgrundlage zu verwenden und allfällige Differenzen im Rahmen der Verhandlungsgespräche zu bereinigen. Für die Geltendmachung Schweizer Rechts ist prinzipiell zu beachten, ob die Leistung in der Schweiz oder im Ausland erbracht wird. Grundsätzlich wird empfohlen, Schweizer Recht und Gerichtsstand Bern zu vereinbaren.

Zu Ziffer 4:

Mit «dem Leistungsbezüger» ist die vertragsschliessende Verwaltungseinheit gemeint.

Die Frist für die Ausübung der Meldepflicht (X Stunden) ist im jeweiligen Vertrag, in welchem sie Anwendung findet, bezogen auf die konkreten Risiken und Bedürfnisse festzulegen. Es gibt keine generelle Vorgabe, die verallgemeinerungsfähig wäre.

Die Meldepflicht bezieht sich insbesondere auf kritische Schwachstellen und Cybervorfälle, die den Schutz der Daten oder die Funktionalität des Systems beeinträchtigen können. Nicht gemeint sind Phishing-Mails, Spam-Mails oder Portscans. Als technisch kompromittiert gilt ein System, eine Datenbank oder auch nur ein einzelner Datensatz, wenn die Integrität der gespeicherten Information nicht mehr gewährleistet werden kann, unabhängig davon, ob der Angriff mit missbräuchlicher Absicht oder die Kompromittierung unbeabsichtigt erfolgt (Begriffserklärung nach Wikipedia[11]). Inhalt und Art dieser Meldung müssen zwischen den Vertragspartnern definiert werden. Dabei ist der Schutzbedarf der Daten und des Systems zu berücksichtigen.

[11] https://de.wikipedia.org/wiki/Technische_Kompromittierung

Zu Ziffer 5:

Die Frist für die Vorankündigung eines Audits (X Arbeitstage) ist im jeweiligen Vertrag, in welchem sie Anwendung findet, bezogen auf die konkreten Risiken und Bedürfnisse festzulegen. Aus der Praxis wird eine Frist von 20 Arbeitstagen vorgeschlagen. Es gibt jedoch keine generelle Vorgabe, die verallgemeinerungsfähig wäre. Sofern vertretbar, können die Modalitäten des Audits im Einzelfall auch davon abweichend ausgestaltet werden.

Anstelle von «X» ist die genaue Frist, bemessen in Tagen einzusetzen. Alternativ kann acuh ein konkretes Datum vereinbart werden, der Satzteil wäre entsprechend anzupassen.

Zu Ziffer 6:

Die Konventionalstrafenregelung orientiert sich an der Standardklausel in den diversen AGB des Bundes. Sie kann im Einzelfall betr. Höhe und Bemessung vertraglich angepasst werden, sofern im konkreten Fall die Risikobeurteilung durch die zuständigen Fachstellen eine andere Regelung für angemessen erachten.

Zu Ziffer 7:

Diese Bestimmung kann weggelassen bzw. muss angepasst werden, wenn die Haftung und Beendigung in anderen Ziffern des jeweiligen Vertrages geregelt sind (vgl. auch Vertragsvorlagen des KBB und die AGB des Bundes) oder die spezifische Risikosituation dies zulässt bzw. erfordert. Grundsätzlich fallen unter die Haftung alle aus Angriffen gemäss Ziffer 2 der Klausel entstandene Schäden.

Zur eventuellen Ziffer 8:

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 Leistungen durch Informatik- und Telekommunikationssystemen liegt, kann es sich optional in Verträgen mit Grossunternehmen (weniger bei KMU) deshalb empfehlen, den Vertragspartner zu verpflichten, sich dem Schadenspotenzial entsprechend zusätzlich zu versichern.

Vorschlag für eine entsprechende Vereinbarung:

«8. Der N.N. verpflichtet sich, eine der vorliegenden Art und dem Schadensrisiko entsprechend angemessene Haftpflichtversicherung abzuschliessen und die ausreichende Versicherungsdeckung zum Zeitpunkt des Vertragsabschlusses nachzuweisen.»