Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Staatssekretariat für Sicherheitspolitik SEPOS

Leitfaden
für die Verwendung der Standardbestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1])

I. Einführung

Der vorliegende Leitfaden soll es den Bedarfsstellen nach Artikel 2 Buchstabe c Org-VöB[2] erlauben, im Bereich der Informationssicherheit bei allen Beschaffungs- und Dienstleistungsverträgen die Anbieterinnen zielgerichtet mittels standardisierter, vorformulierter Bestimmungen (in der Folge «Standardbestimmung(en)» genannt) zu instruieren, wie mit Informationen oder Informatikmitteln des Bundes bei der Erbringung ihrer vertraglichen Leistung umzugehen ist.

II. Kategorisierung der Beschaffungs- und Dienstleistungsverträge

Beschaffungs- und Dienstleistungsverträge können inhaltlich vielerlei Gestalt haben, weshalb es unmöglich ist – nach dem Motto «One for all» – eine einzige, allgemeingültige Standardbestimmung zu verwenden. Selbst eine schematische Anwendung einer kleinen, geschlossenen Anzahl standardisierter Inhalte erfordert eine vorgängige Kategorisierung der Verträge (nachfolgend Kategorien 1–4).

Innerhalb der Kategorien muss wiederum zwischen verschiedenen **Anwendungsfällen** (a–d) unterschieden werden:

Buchstabe a: Der Beschaffungsvertrag beinhaltet die Bearbeitung von Informationen des Bundes, wobei keine Verwaltung, kein Betrieb, keine Wartung, keine Entwicklung und keine Überprüfung von Informatikmitteln des Bundes im Sinn der nachfolgenden Buchstaben b und c erfolgt.

Buchstabe b: Der Beschaffungsvertrag beinhaltet die Verwaltung, die Wartung, die Entwicklung oder die Überprüfung von Informatikmitteln des Bundes (nicht den Betrieb). Inhaber (Besitzer/Eigentümer) dieser Informatikmittel ist der Bund. Diese Arbeiten werden mit betrieblichen Informatikmitteln (Eigentum/Besitz bei der Anbieterin) oder Bundesgeräten vorgenommen und es können davon auch Informationen des Bundes oder Personendaten betroffen sein. Die unter den genannten Begriffen zu verstehenden Tätigkeiten müssen geeignet sein, so auf eine Hard- oder Software einzuwirken, dass dadurch die Vertraulichkeit, die Verfügbarkeit, die Integrität oder die Nachvollziehbarkeit der Informationen des Bundes beeinträchtigt werden können (z. B. Administratoren). Die einfache Bearbeitung der Informationen mit dem Informatikmittel fällt unter den Buchstaben a.

Buchstabe c: Der Beschaffungsvertrag beinhaltet eine eigentliche Informatik-Leistungserbringung (Betrieb) durch die Anbieterin mit deren betrieblichen Informatikmitteln und es können davon auch Informationen des Bundes oder Personendaten betroffen sein. Das heisst, die Informationen des Bundes werden auf Servern oder in Rechenzentren (Informatikmitteln) gehalten, deren Inhaberin (Besitzerin/Eigentümerin) im Gegensatz zu Buchstabe b die Anbieterin ist und auf die die Auftraggeberin keinen eigenen Zugriff hat (z. B. Cloud-Services).

Buchstabe d: Zur Erfüllung der vertraglichen Leistung werden betriebliche Informatikmittel der Anbieterin oder vom Bund zur Verfügung gestellte Geräte verwendet.

---

1 Informationssicherheitsverordnung (SR **128.1**)

2 Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (SR **172.056.15**)

III. Bestehende AGB des Bundes

Grundsätzlich obligatorischer Bestandteil aller Verträge von Behörden und Organisationen des Bundes sind die Allgemeinen Geschäftsbedingungen des Bundes, welche in verschiedene **Auftragsarten** aufgeteilt sind (vgl. VI. hiernach). Standardbestimmungen zur Informationssicherheit kommen somit stets in Kombination mit diesen AGB und/oder dem Beschaffungsvertrag zur Anwendung.

IV. Klassifizierte Informationen und Datenschutz

Klassifizierte Informationen der Stufe «geheim», «vertraulich» und «intern», Personendaten sowie die Verwaltung, die Wartung, die Entwicklung, der Betrieb oder die Überprüfung von Informatikmitteln des Bundes der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» geniessen besonderen rechtlichen Schutz, den die Standardbestimmungen nicht allein abzudecken vermögen. Für die entsprechenden Vertragsgestaltungen müssen daher vorweg die Informationssicherheitsbeauftragten und/oder die Datenschutzberaterinnen oder Datenschutzberater beigezogen werden.

V. Übersicht Kategorien (1–4) und Anwendungsfälle (a–d)

1	a	Bearbeitung «geheim» klassifizierter Informationen
	b	Verwaltung, Entwicklung, Wartung und Überprüfung von Informatikmitteln[3] der Sicherheitsstufe[4] «sehr hoher Schutz»
	c	Betrieb von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz» (externer Leistungserbringer)
	d	Verwendung betrieblicher Informatikmittel oder von Bundesgeräten zur Erfüllung der vertraglichen Leistung
2	a	Bearbeitung «vertraulich» oder «intern» klassifizierter Informationen oder von Personendaten und besonders schützenswerten Personendaten
	b	Verwaltung, Entwicklung, Wartung und Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz»
	c	Betrieb von Informatikmitteln der Sicherheitsstufe «hoher Schutz» (externer Leistungserbringer)
	d	Verwendung betrieblicher Informatikmittel oder von Bundesgeräten zur Erfüllung der vertraglichen Leistung
3	a	Bearbeitung von Informationen, die dem BGÖ[5] unterliegen
	b	Verwaltung, Entwicklung, Wartung und Überprüfung von Informatikmitteln der Sicherheitsstufe «Grundschutz»
	c	Betrieb von Informatikmitteln der Sicherheitsstufe «Grundschutz» (externer Leistungserbringer)
	d	Verwendung betrieblicher Informatikmittel oder von Bundesgeräten zur Erfüllung der vertraglichen Leistung
4	a	Bearbeitung von Informationen, die dem BGÖ unterliegen
	b	Kein Umgang mit Informatikmitteln des Bundes
	c	Kein Betrieb von Informatikmitteln (externer Leistungserbringer)
	d	Verwendung betrieblicher Informatikmittel oder von Bundesgeräten zur Erfüllung der vertraglichen Leistung

[3] Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen.

[4] Gemäss Schutzbedarfsanalyse

[5] Öffentlichkeitsgesetz (SR **152.3**)

VI. AGB des Bundes (A–G) und Standardbestimmungen zur Informationssicherheit (H–J)

A	Beschaffung von Gütern
B	Dienstleistungsaufträge
C	Forschungsaufträge
D	Informatik: Kauf und Wartung von Hardware
E	Informatik: Beschaffung und Pflege Standardsoftware
F	Informatik: Werkverträge im Informatikbereich und Pflege Individualsoftware
G	Informatik: Informatikdienstleistungen
H1	Standardbestimmung ohne Bezug zu Informatikmitteln des Bundes *mit* Abgabe von Bundesgeräten
H2	Standardbestimmung ohne Bezug zu Informatikmitteln des Bundes *ohne* Abgabe von Bundesgeräten
I1	Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Verwaltung, Wartung, Überprüfung) *mit* Abgabe von Bundesgeräten
I2	Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Verwaltung, Wartung, Überprüfung) *ohne* Abgabe von Bundesgeräten
J	Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Betrieb)

VII. Konkretes Vorgehen

Die Bedarfsstelle kann nun anhand der folgenden Fragen (VIII.–X.) in der nachstehenden Reihenfolge für das fragliche Rechtsgeschäft:

- die **Kategorie** bestimmen (nachfolgend VIII., ergibt eine Ziffer 1–4),
- innerhalb der Kategorie den **Anwendungsfall** festlegen (nachfolgend IX., ergibt zur obigen Ziffer einen Buchstaben a–d),
- die Prüfung **«Klassifizierte Informationen und Personendaten»** durchführen (nachfolgend X., verweist ggf. an die Informationssicherheitsbeauftragten und/oder an die Datenschutzberaterinnen und Datenschutzberater),
- anhand der Matrizen auf den Seiten 5, 6 und 7 mit Hilfe der aus Kategorie und Anwendungsfall ermittelten Ziffern und Buchstaben (horizontal) und der zutreffenden Auftragsart (vertikal) die **passende Kombination** von **AGB** des Bundes und **Standardbestimmung** ermitteln.

VIII. Bestimmung der Kategorie nach Ziffern 1–4

Beinhaltet der zu vergebende Auftrag die Bearbeitung von «geheim» klassifizierten Informationen des Bundes oder die Verwaltung, den Betrieb, die Entwicklung, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz»?

Ja:	Auftrag gehört in Kategorie **1**, weiter zu Ziffer IX	*Nein*:	Weiter zur nächsten Frage

Beinhaltet der zu vergebende Auftrag die Bearbeitung von «vertraulich» oder «intern» klassifizierten Informationen des Bundes, von Personendaten oder besonders schützenswerten Personendaten oder die Verwaltung, den Betrieb, die Entwicklung, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz»?

Ja:	Auftrag gehört in Kategorie **2**, weiter zu Ziffer IX	*Nein*:	Weiter zur nächsten Frage

Beinhaltet der zu vergebende Auftrag die Bearbeitung von Informationen des Bundes, die dem BGÖ unterliegen oder die Verwaltung, den Betrieb, die Entwicklung, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «Grundschutz»?

Ja:	Auftrag gehört in Kategorie **3**, weiter zu Ziffer IX	*Nein*:	Weiter zur nächsten Frage

Beinhaltet der zu vergebende Auftrag die Bearbeitung von Informationen des Bundes, die dem BGÖ unterliegen, ohne Umgang mit Informatikmitteln des Bundes?

Ja:	Auftrag gehört in Kategorie **4**, weiter zu Ziffer IX	*Nein*:	Auftrag benötigt keine Standardbestimmung, Prüfung nach Ziffer IX entfällt.

IX. Bestimmung der Anwendungsfälle nach Buchstaben a–d

Beinhaltet der zu vergebende Auftrag die Bearbeitung von Informationen des Bundes?

Ja:	Weiter zur nächsten Frage	*Nein*:	Weiter zur übernächsten Frage

Werden für die Bearbeitung von Informationen des Bundes betriebliche Informatikmittel oder Bundesgeräte verwendet?

Ja:	Kategorie 1–4: immer Buchstabe **d,** es sei denn, die nächste Frage werde ebenfalls mit «ja» beantwortet.	*Nein*:	Kategorie 1–4: immer Buchstabe **a,** es sei denn, die nächste Frage werde ebenfalls mit «ja» beantwortet.

Beinhaltet der zu vergebende Auftrag die Verwaltung, Entwicklung, Wartung und Überprüfung von Informatikmitteln des Bundes (Bundesinformationen und -daten werden in Rechenzentren oder auf Servern des Bundes gehalten)?

Ja:	Kategorie 1–3: immer Buchstabe **b statt a oder d** gemäss vorheriger Frage	*Nein*:	Weiter zur nächsten Frage

Beinhaltet der zu vergebende Auftrag den Betrieb von Informatikmitteln des Bundes im Sinne einer externen Leistungserbringung (Bundesinformationen und -daten werden in Rechenzentren oder auf Servern der Anbieterin gehalten)?

Ja:	Kategorie 1–3: immer Buchstabe **c**	*Nein*:	Auftrag benötigt keine Standardbestimmung, ausser eine der vorhergehenden Fragen wird mit «ja» beantwortet, dann gilt der dort ermittelte Buchstabe

X. Beurteilung Klassifizierung und Personendaten

Gehört der zu vergebende Auftrag in die Kategorie 1 oder 2[6]?

Ja:	Weiter zur nächsten Frage	*Nein*:	Weiter auf Seite 7

Beinhaltet der zu vergebende Auftrag die Bearbeitung von Informationen, die «geheim», «vertraulich» oder «intern» klassifiziert sind oder die Verwaltung, den Betrieb, die Entwicklung, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz»?

Ja:	Weiter auf Seite 5 und zur nächsten Frage	*Nein*:	Weiter zur nächsten Frage

Beinhaltet der zu vergebende Auftrag die Bearbeitung von Personendaten nach DSG[7]?

Ja:	Weiter auf Seite 6; wenn die vorherige Frage mit «ja» beantwortet wurde, zusätzlich auf Seite 5	*Nein*:	Weiter auf Seite 5, wenn die vorherige Frage mit «ja» beantwortet wurde, sonst auf Seite 7

[6] Zur Klärung dieser Frage ist im Zweifelsfall die oder der zuständige Informationssicherheitsbeauftragte zu konsultieren.

[7] Datenschutzgesetz (SR **235.1**)

Kategorie 1 und 2: Klassifizierte Informationen
Einleitung Betriebssicherheitsverfahren

Zeitpunkt

Der Antrag auf Einleitung des Betriebssicherheitsverfahrens ist möglichst früh bei der Fachstelle Betriebssicherheit einzureichen, wenn ein Auftrag der Kategoire 1 oder 2 zu vergeben ist (vor einer allfälligen Bedarfsmeldung an eine zentrale Beschaffungsstelle bzw. vor der Einladung zur Offertstellung). Zuständig ist die oder der Informationssicherheitsbeauftragte der Verwaltungseinheit, der die Bedarfsstelle angehört. Sind nur «intern» klassifizierte Informationen betroffen, reicht es aus, die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten beratend beizuziehen.

Besondere Sicherheitsvorgaben

Die AGB und Standardbestimmungen (A–J) bilden bezüglich Informationssicherheit **nötige, aber nicht hinreichende Grundlage** des Vertragsverhältnisses. Die spezifischen, auf den Einzelfall zugeschnittenen Sicherheitsvorgaben für die Kategorien 1 und 2 ergeben sich aus dem **betrieblichen Sicherheitskonzept**, welches die Fachstelle Betriebssicherheit im Einvernehmen mit der Auftraggeberin festlegt oder aus den Empfehlungen der oder des Informationssicherheitsbeauftragten.

Teilnahmebedingung bei den Klassifizierungsstufen «geheim» oder «vertraulich» bei der Ausschreibung bzw. der Einladung zur Offertstellung bzw. bei der freihändigen Vergabe

Es ist vorzusehen, dass die Anbieterin:

- bereit ist, ein Betriebssicherheitsverfahren zu durchlaufen, und
- sicherstellen muss, dass sie für die Auftragserfüllung über genügend geeignetes Personal verfügt, welches bereit ist, in eine Personensicherheitsprüfung einzuwilligen.

Auswahl AGB

Der betroffenen Kategorie entsprechend (1a–2d) wird empfohlen, die der Auftragsart entsprechenden Kombinationen der AGB (A–J) zum integralen Bestandteil des Beschaffungsvertrages zu erheben.

Kategorie / Auftragsart	1a	1b	1c	1d	2a	2b	2c	2d
Beschaffung von Gütern	A/H*			A/H*	A/H*			A/H*
Dienstleistungsaufträge	B/H*			B/H*	B/H*			B/H*
Forschungsaufträge	C/H*			C/H*	C/H*			C/H*
IT: Kauf und Wartung Hardware		D/I**	D/J	D/H*		D/I**	D/J	D/H*
IT: Beschaffung und Pflege Standardsoftware		E/I**	E/J	E/H*		E/I**	E/J	E/H*
IT: Werkverträge und Pflege Individualsoftware		F/I**	F/J	F/H*		F/I**	F/J	F/H*
IT: Dienstleistungen		G/I**	G/J	G/H*		G/I**	G/J	G/H*

*Werden Bundesgeräte abgegeben: H1; ohne Abgabe von Bundesgeräten: H2

**Werden Bundesgeräte abgegeben: I1; ohne Abgabe von Bundesgeräten: I2

Kategorie 2: Personendaten
Bearbeitung durch Auftragsbearbeiter

Datenschutzberaterin oder Datenschutzberater / Auftragsdatenbearbeitungsvereinbarung

Die oder der Verantwortliche muss sich vergewissern, dass die Auftragsdatenbearbeiterin oder der Auftragsverarbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Die Datenschutzberaterin oder der Datenschutzberater der zuständigen Verwaltungseinheit muss in jedem Fall für die Ausarbeitung einer **Auftragsdatenbearbeitungsvereinbarung** beigezogen werden.

Besondere Vertragsklauseln bei Bekanntgabe ins Ausland

Die Datenschutzklauseln in einem Vertrag nach dem 2. Kapitel, 3. Abschnitt DSG müssen die Punkte nach dem 1. Kapitel, 3. Abschnitt DSV[8] enthalten.

Auswahl AGB

Der betroffenen Kategorie entsprechend (1a–2d) wird empfohlen, die der Auftragsart entsprechenden Kombinationen der AGB (A–G) und Standardbestimmungen zur Informationssicherheit (H–J) zum integralen Bestandteil des Beschaffungsvertrages zu erheben.

Kategorie / Auftragsart	1a	1b	1c	1d	2a	2b	2c	2d
Beschaffung von Gütern	A/H*			A/H*	A/H*			A/H*
Dienstleistungsaufträge	B/H*			B/H*	B/H*			B/H*
Forschungsaufträge	C/H*			C/H*	C/H*			C/H*
IT: Kauf und Wartung Hardware		D/I**	D/J	D/H*		D/I**	D/J	D/H*
IT: Beschaffung und Pflege Standardsoftware		E/I**	E/J	E/H*		E/I**	E/J	E/H*
IT: Werkverträge und Pflege Individualsoftware		F/I**	F/J	F/H*		F/I**	F/J	F/H*
IT: Dienstleistungen		G/I**	G/J	G/H*		G/I**	G/J	G/H*

*Werden Bundesgeräte abgegeben: H1; ohne Abgabe von Bundesgeräten: H2

**Werden Bundesgeräte abgegeben: I1; ohne Abgabe von Bundesgeräten: I2

[8] Datenschutzverordnung (SR **235.11**)

Kategorie 3 und 4

Auswahl AGB

Der betroffenen Kategorie entsprechend (3a–4d) wird empfohlen, die die der Auftragsart entsprechenden Kombinationen der AGB (A–J) zum integralen Bestandteil des Beschaffungsvertrages zu erheben.

Kategorie / Auftragsart	3a	3b	3c	3d	4a	4b	4c	4d
Beschaffung von Gütern	A/H*			A/H*	A/H*			A/H*
Dienstleistungsaufträge	B/H*			B/H*	B/H*			B/H*
Forschungsaufträge	C/H*			C/H*	C/H*			C/H*
IT: Kauf und Wartung Hardware		D/I**	D/J	D/H*		D/H*	D/H*	D/H*
IT: Beschaffung und Pflege Standardsoftware		E/I**	E/J	E/H*		E/H*	E/H*	E/H*
IT: Werkverträge und Pflege Individualsoftware		F/I**	F/J	F/H*		F/H*	F/H*	F/H*
IT: Dienstleistungen		G/I**	G/J	G/H*		G/H*	G/H*	G/H*

*Werden Bundesgeräte abgegeben: H1; ohne Abgabe von Bundesgeräten: H2

**Werden Bundesgeräte abgegeben: I1; ohne Abgabe von Bundesgeräten: I2

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Staatssekretariat für Sicherheitspolitik SEPOS

Kommentar zu den Standardbestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1])

Inhalt

[1] Informationssicherheitsverordnung (SR **128.1**)

Dokument H1

Der Beschaffungsvertrag beinhaltet keine Verwaltung, keine Entwicklung, keinen Betrieb, keine Wartung und keine Überprüfung von Informatikmitteln des Bundes[2]. Für die Bearbeitung der Informationen des Bundes werden der Anbieterin Bundesgeräte zur Verfügung gestellt.

Ziffer 1: Die Bestimmung nennt die vier Dimensionen der Informationssicherheit: die Vertraulichkeit[3] (Bst. a), die Verfügbarkeit[4] (Bst. b), die Integrität[5] (Bst. c) sowie die nachvollziehbare[6] Bearbeitung (Bst. d). Diese Grundsätze sind auf die Anbieterin zu überbinden und werden in den weiteren Bestimmungen konkretisiert. Neben der Pflicht, diese Grundsätze ständig zu berücksichtigen, ist auch deren Wiederherstellung, wenn sie verletzt werden, teil der Anbieterpflicht (Bst. e). Diese Bestimmungen gelten nicht für von der Auftraggeberin zur Verfügung gestellte Testdaten.

Ziffer 2: Absatz 1 konkretisiert die Geschäftsherrenhaftung, wonach mit der Erfüllung der Vertragsleistung betraute Personen, sorgfältig auszuwählen, einschlägig zu instruieren und angemessen zu überwachen sind. Die Buchstaben a–c geben den Rahmen der nötigen Instruktion vor. Besondere Beachtung verdient hierbei der Hinweis auf das Amtsgeheimnis. Anbieterinnen bzw. die von ihnen mit der Erfüllung der vertraglichen Leistung betrauten Personen unterliegen als Hilfspersonen dem Amtsgeheimnis (Art. 320 Ziff. 1 StGB[7]). Die Auftraggeberin wird hinsichtlich der Grundsatzinstruktion gegenüber der Anbieterin ebenfalls in die Pflicht genommen.

Die Absätze 2 und 3 konkretisieren die Überwachung und die Folgen mangelhaften Verhaltens der beauftragten Personen sowie entsprechende Meldungen an die Auftraggeberin.

Ziffer 3: Absatz 1 statuiert das Recht der Auftraggeberin, Aufsichtsmassnahmen zur Informationssicherheit bei der Anbieterin vorzunehmen. Die Bestimmung setzt somit Artikel 9 Absatz 2 ISG[8] um. Bei der vertraglichen Ausgestaltung von Kontroll- und Überprüfungsrechten muss sichergestellt sein, dass die Anbieterin durch die Offenlegungspflichten nicht ihrerseits gegen Geheimhaltungsverpflichtungen verstösst, die ihr gegenüber Dritten obliegen. Die Beweislast für solch einen Interessenkonflikt liegt bei der Anbieterin.

Absatz 2 gibt der Anbieterin ein Veto-Recht, wenn die Auftraggeberin Dritte mit dieser Überprüfung beauftragt. Damit sollen insbesondere Produktions- und Geschäftsgeheimnisse der Anbieterin geschützt werden. Da die Erbringung eines solchen Beweises nicht ganz einfach ist, soll als Beweismass das Glaubhaftmachen eines wettbewerbsrelevanten oder anderen Nachteils ausreichen.

Strenge Überprüfungsrechte wie vorliegend sind aus Sicht der Informationssicherheit durchaus angezeigt, sollen im Gegenzug kostenmässig grundsätzlich aber nicht der Anbieterin angelastet werden. Die Auftraggeberin soll sich gegebenenfalls über die Schadenersatzregelungen oder Konventionalstrafen schadlos halten (Abs. 3).

Ziffer 4: Bei der Bearbeitung von Informationen des Bundes durch Dritte sind nicht nur die zu Auftragsbeginn übermittelten oder zugänglich gemachten Informationen zu beachten, sondern auch die Tatsache, dass sich diese mit der Fortdauer eines Auftrages oft ungewollt zu einer

---

[2] Unterscheidung «Informatikmittel des Bundes» und «Bundesgeräte»: Bei ersteren handelt es sich um die «behandelten» (verwalteten, gewarteten oder überprüften) Mittel (die z. B. mit dem Penetrationstest angegriffen werden), bei zweiteren um das «behandelnde» Mittel (z. B. Gerät, von dem aus ein Penetrationstest ausgeführt wird).

[3] Sicherstellung, dass nur berechtigte Personen Zugang zur Information erhalten (z. B. durch Verschlüsselung).

[4] Je kleiner die Wahrscheinlichkeit von Systemausfällen gehalten werden kann, desto höhere Verfügbarkeitsanforderungen sind gewährleistet.

[5] Sicherstellung, dass Informationen nicht unbemerkt verändert werden können.

[6] Es muss erkennbar sein, wer zu welchem Zweck und in welchem Rahmen eine Bearbeitung vorgenommen hat. Dies ist entweder technisch sicherzustellen oder durch eine entsprechende Versionierung der einzelnen Informationsträger.

[7] Strafgesetzbuch (SR **311.0**), Bestrafung mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

[8] Informationssicherheitsgesetz (SR **128**)

Gesamtinformation verdichten können, welche unter Umständen höheren Schutzbedarf erhalten (Sammelwerk[9]). Dies kann durch Nachlieferungen oder nachträglich zugänglich gemachte Informationen der Auftraggeberin oder durch Neuerstellung von Informationen bei der Anbieterin erfolgen (Abs. 1). Als Informationsträger gelten Träger von Informationen irgendwelcher Art, namentlich Schriftstücke und Träger von Text-, Bild-, Ton- oder andern Daten; Zwischenmaterial, namentlich Entwürfe, gelten ebenfalls als Informationsträger.

Absatz 2 beschreibt eine für jedermann handhabbare hinreichende Löschung beidseits elektronisch vorhandener Informationen. Sie besteht bspw. aus der Doppellöschung (bspw. auf dem Desktop) und dem Entfernen aus dem Papierkorb.

Um die Löschung im Einzelfall praktikabel zu halten, sollen Anbieterin und Auftraggeberin ein entsprechendes Löschkonzept erstellen. Die Anbieterin hat dann die Gewähr, dass sie mit der konzeptgemässen Löschung die rechtlichen Anforderungen erfüllt (Abs. 3).

Ziffer 5: Absatz 1 enthält die Definition der Bundesgeräte, die zur Erfüllung der vertraglichen Leistung verwendet werden können. Diese bleiben im Eigentum des Bundes und müssen nach Gebrauch zurückgegeben werden.

Absatz 2 verweist auf die nächste Ziffer, in welcher die Voraussetzungen genannt werden, unter denen der Einsatz von Bundesgeräten für die Erfüllung der vertraglichen Leistung erlaubt ist. Soll davon abgewichen werden, ist in jedem Fall das Einverständnis der Auftraggeberin einzuholen.

Ziffer 6: Absatz 1 legt den Grundsatz fest, dass Informationen des Bundes grundsätzlich nur mit Bundesgeräten bearbeitet werden dürfen, wenn deren Software auf dem aktuellen Stand ist. Die vom Leistungserbringer zur Verfügung gestellten Softwareupdates sind sofort zu übernehmen. Deren Übernahme ist der Auftraggeberin laufend zu bestätigen.

Absatz 2 verpflichtet die nutzenden Personen, das Gerät so zu verwenden, dass die Vorteile einer Zweifaktorauthentifizierung stets gewährleistet sind. Die bei der Abgabe der Geräte mitgelieferten Instruktionen sind ebenfalls zu beachten bzw. den mit der Auftragserfüllung betrauten Personen zur Kenntnis zu bringen.

Ziffer 7: Für die Auftraggeberin ist es von grosser Bedeutung, dass sie so schnell wie möglich erfährt, wenn ihre Informationen betreffend Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit gefährdet sind oder möglicherweise manipuliert wurden. Die Wiederherstellungspflicht wird der Anbieterin bereits in Ziffer 1 Absatz 1 Buchstabe e auferlegt. Ziffer 7 regelt die damit verbundenen Meldepflichten. Mit dem Erfüllen der Meldepflicht gegenüber dem Bundesamt für Cybersicherheit profitiert die Anbieterin letztlich auch von der Einschätzung ihres Falles durch eine Fachstelle des Bundes.

Absatz 1 Buchstabe a verlangt von der Anbieterin letzten Endes eine ständige Überwachung der Informationssicherheit bei der Erfüllung ihrer vertraglichen Leistungen. Buchstaben b und c nennen Indizien für ein Hacking oder für Phishing-Attacken, wobei sofort erkannte und gelöschte E-Mails von der Meldepflicht ausgenommen sind. Buchstaben d–f zielen auf den Verdacht, dass unberechtigte Personen auf die Informatikmittel eingewirkt bzw. Informationen des Bundes zur Kenntnis genommen oder entwendet haben könnten. Mit einer Meldung nach Buchstabe g leistet die Anbieterin neben dem auftragsspezifischen Nutzen auch einen generellen Beitrag zur Informationssicherheit des Bundes. Auch in diesem Fall sind sofort behobene Schwachstellen und Sicherheitslücken von der Meldepflicht ausgenommen, wenn nicht zu erwarten ist, dass die Informationen des Bundes gefährdet werden.

Sicherheitsmeldungen nach dieser Bestimmung dulden oft keinen Aufschub, unterliegen aber grundsätzlich dem Amtsgeheimnis. Es ist daher angezeigt, die mit der Erfüllung der vertrag-

[9] Informationen können so aggregiert und verdichtet werden, dass deren Gesamtheit einen neuen Informationsgehalt erhält. Solchermassen aggregierte und verdichtete Gesamtinformationen – oder eben Sammelwerke – können u. U. bei deren missbräuchlichen Verwendung den Landesinteressen einen grösseren Schaden zufügen als die Einzelinformation. Das Sammelwerk muss daher ggf. höher klassifiziert werden als die einzelne Information. Wenn die Anbieterin das feststellt, muss sie entsprechend in die Pflicht genommen werden.

lichen Leistungen betrauten Personen für die Meldungen nach Absatz 1 vorab vom Amtsgeheimnis zu entbinden (Abs. 2). Diese Entbindung muss mit dem Abschluss des Vertrages gewährleistet sein, weshalb die Auftraggeberin zuvor sicherzustellen hat, dass sie entweder hierfür befugt ist oder die zuständige Stelle[10] zugestimmt hat.

Ziffer 8: Absatz 1 verweist für den Fall, dass die Anbieterin die vertragliche Leistung ganz oder teilweise durch eine Dritte juristische oder natürliche Person erbringen lässt, auf die jeweils auf den Auftrag anwendbaren Allgemeinen Geschäftsbedingungen des Bundes.

Die Absätze 2–4 sollen sicherstellen, dass die vorliegenden Standardbestimmungen in der ganzen Lieferkette zum Tragen kommen und für alle Substituentinnen und Subunternehmen klarstellen, dass sie diese mit der Einreichung ihrer Offerte akzeptiert haben. Die Anbieterin wird schliesslich zur Überbindung an alle Subunternehmen verpflichtet.

Absatz 5 stellt einen Auffangtatbestand für den Fall dar, dass marktmächtige Substituentinnen und Subunternehmen die Überbindung der genannten Verpflichtungen ablehnen (Bst. a). Der Verzicht auf das Überbinden soll zwar möglich sein, jedoch nur unter qualifizierten Voraussetzungen, nämlich dem Nachweis, dass keine anderen Anbieterinnen in Frage kommen (Bst. b), dass stattdessen gleichwertige technische und organisatorische Massnahmen getroffen werden (Bst. c) und dass die Auftraggeberin zustimmt (Bst. d). Das voraussetzungslose Veto-Recht der Auftraggeberin (Bst. d) ist im Bereich der Informationssicherheit unabdingbar, da sie für die Sicherheit ihrer Informationen verantwortlich ist und bleibt. Die gewählte Lösung einer risikobasierten Regelung erscheint überdies in diesem Sinne durchaus wettbewerbsverträglich und ermöglicht es der Auftraggeberin, nach erfolgter Risikoanalyse zurückhaltend vom Veto-Recht Gebrauch zu machen.

Ziffer 9: Die Bestimmung verweist hinsichtlich der für die Verletzung von Informationssicherheitsbestimmungen anwendbaren Konventionalstrafen- und Schadenersatzregelungen auf die entsprechende Rubrik der Allgemeinen Geschäftsbedingungen des Bundes.

[10] Die für die Entbindung vom Amtsgeheimnis zuständigen Stellen sind häufig in den Geschäftsordnungen der Departemente und/oder Verwaltungseinheiten aufgeführt.

Dokument H2

Der Beschaffungsvertrag beinhaltet keine Verwaltung, keinen Betrieb, keine Wartung und keine Überwachung von Informatikmitteln des Bundes[11]. Es werden jedoch Informationen des Bundes mit betrieblichen Informatikmitteln bearbeitet.

Ziffer 1: Die Bestimmung nennt die vier Dimensionen der Informationssicherheit: die Vertraulichkeit (Bst. a), die Verfügbarkeit (Bst. b), die Integrität (Bst. c) sowie die nachvollziehbare Bearbeitung (Bst. d). Diese Grundsätze sind auf die Anbieterin zu überbinden und werden in den weiteren Bestimmungen konkretisiert. Neben der Pflicht, diese Grundsätze ständig zu berücksichtigen, ist auch deren Wiederherstellung, wenn sie verletzt werden, teil der Anbieterpflicht (Bst. e).

Ziffer 2: Absatz 1 konkretisiert die Geschäftsherrenhaftung, wonach mit der Erfüllung der Vertragsleistung betraute Personen, sorgfältig auszuwählen, einschlägig zu instruieren und angemessen zu überwachen sind. Die Buchstaben a–c geben den Rahmen der nötigen Instruktion vor. Besondere Beachtung verdient hierbei der Hinweis auf das Amtsgeheimnis. Anbieterinnen bzw. die von ihnen mit der Erfüllung der vertraglichen Leistung betrauten Personen unterliegen als Hilfspersonen dem Amtsgeheimnis (Art. 320 Ziff. 1 StGB[12]). Die Auftraggeberin wird hinsichtlich der Grundsatzinstruktion gegenüber der Anbieterin ebenfalls in die Pflicht genommen.

Die Absätze 2 und 3 konkretisieren die Überwachung und die Folgen mangelhaften Verhaltens der beauftragten Personen sowie entsprechende Meldungen an die Auftraggeberin.

Ziffer 3: Absatz 1 statuiert das Recht der Auftraggeberin, Aufsichtsmassnahmen zur Informationssicherheit bei der Anbieterin vorzunehmen. Die Bestimmung setzt somit Artikel 9 Absatz 2 ISG um. Bei der vertraglichen Ausgestaltung von Kontroll- und Überprüfungsrechten muss sichergestellt sein, dass die Anbieterin durch die Offenlegungspflichten nicht ihrerseits gegen Geheimhaltungsverpflichtungen verstösst, die ihr gegenüber Dritten obliegen. Die Beweislast für solch einen Interessenkonflikt liegt bei der Anbieterin.

Absatz 2 gibt der Anbieterin ein Veto-Recht, wenn die Auftraggeberin Dritte mit dieser Überprüfung beauftragt. Damit sollen insbesondere Produktions- und Geschäftsgeheimnisse der Anbieterin geschützt werden. Da die Erbringung eines solchen Beweises nicht ganz einfach ist, soll als Beweismass das Glaubhaftmachen eines wettbewerbsrelevanten oder anderen Nachteils ausreichen.

Strenge Überprüfungsrechte wie vorliegend sind aus Sicht der Informationssicherheit durchaus angezeigt, sollen im Gegenzug kostenmässig grundsätzlich aber nicht der Anbieterin angelastet werden. Die Auftraggeberin soll sich gegebenenfalls über die Schadenersatzregelungen oder Konventionalstrafen schadlos halten (Abs. 3).

Ziffer 4: Bei der Bearbeitung von Informationen des Bundes durch Dritte sind nicht nur die zu Auftragsbeginn übermittelten oder zugänglich gemachten Informationen zu beachten, sondern auch die Tatsache, dass sich diese mit der Fortdauer eines Auftrages oft ungewollt zu einer Gesamtinformation verdichten können, welche unter Umständen höheren Schutzbedarf erhalten (Sammelwerk[13]). Dies kann durch Nachlieferungen oder nachträglich zugänglich gemachte Informationen der Auftraggeberin oder durch Neuerstellung von Informationen bei der Anbieterin erfolgen (Abs. 1). Als Informationsträger gelten Träger von Informationen irgendwelcher Art, namentlich Schriftstücke und Träger von Text-, Bild-, Ton- oder andern Daten; Zwischenmaterial, namentlich Entwürfe, gelten ebenfalls als Informationsträger.

---

[11] Unterscheidung «Informatikmittel des Bundes» und «Bundesgeräte»: Bei ersteren handelt es sich um die «behandelten» (verwalteten, gewarteten oder überprüften) Mittel (die z. B. mit dem Penetrationstest angegriffen werden), bei zweiteren um das «behandelnde» Mittel (z. B. Gerät, von dem aus ein Penetrationstest ausgeführt wird).

[12] Strafgesetzbuch (SR **311.0**), Bestrafung mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

[13] Informationen können so aggregiert und verdichtet werden, dass deren Gesamtheit einen neuen Informationsgehalt erhält. Solchermassen aggregierte und verdichtete Gesamtinformationen – oder eben Sammelwerke – können u. U. bei deren missbräuchlichen Verwendung den Landesinteressen einen grösseren Schaden zufügen als die Einzelinformation. Das Sammelwerk muss daher ggf. höher klassifiziert werden als die einzelne Information. Wenn die Anbieterin das feststellt, muss sie entsprechend in die Pflicht genommen werden.

Absatz 2 beschreibt eine für jedermann handhabbare hinreichende Löschung beidseits elektronisch vorhandener Informationen. Sie besteht bspw. aus der Doppellöschung (bspw. auf dem Desktop) und dem Entfernen aus dem Papierkorb.

Um die Löschung im Einzelfall praktikabel zu halten, sollen Anbieterin und Auftraggeberin ein entsprechendes Löschkonzept erstellen. Die Anbieterin hat dann die Gewähr, dass sie mit der konzeptgemässen Löschung die rechtlichen Anforderungen erfüllt (Abs. 3).

Ziffer 5: Absatz 1 enthält die Definition der betrieblichen Informatikmittel, die zur Erfüllung der vertraglichen Leistung verwendet werden können. Nicht zu dieser Kategorie gehören Informatikmittel der Anbieterin, die der allgemeinen Funktionsfähigkeit der Unternehmung dienen (Personalverwaltung, Geschäftsplanung, E-Mail, etc.) und keinen Bezug zum Vertragsgegenstand haben.

Absatz 2 verweist auf die nächste Ziffer, in welcher die Voraussetzungen genannt werden, unter denen der Einsatz betrieblicher Informatikmittel für die Erfüllung der vertraglichen Leistung erlaubt ist.

Absatz 3 verlegt die Kosten für die Verwaltung, den Betrieb, die Wartung und die Überprüfung betrieblicher Informatikmittel auf die Anbieterin, welche letztlich auch Eigentümerin dieser Infrastrukturen ist.

Ziffer 6: Absatz 1 legt den Grundsatz fest, dass Informationen des Bundes grundsätzlich nur mit betrieblichen Informatikmitteln bearbeitet werden dürfen, wenn deren Software auf dem aktuellen Stand ist, sowie die entsprechende Nachweispflicht der Anbieterin. Im Bereich der nichtsicherheitsempfindlichen Tätigkeiten reichen dafür die vom Hersteller zur Verfügung gestellten Updates aus, ohne dass von Bundesseite weitere Anforderungen zu stellen wären. Insbesondere wäre es unverhältnismässig[14], für diese Fälle zu verlangen, dass die betrieblichen Informatikmittel den IT-Grundschutz in der Bundesverwaltung umsetzen müssen. Die Wettbewerbseinschränkungen bei der Beschaffung wären viel zu gross, der Sicherheitsgewinn stünde in keinem akzeptablen Verhältnis zum verursachten Aufwand.

Absatz 2 konkretisiert eine Kaskade von Massnahmen (Bst. a–c), die geeignet sind, für die bearbeiteten Informationen des Bundes einen angemessenen Schutz im Sinne von Ziffer 1 sicherzustellen.

Absatz 3 nennt alternative Möglichkeiten für den Fall, dass die Massnahmen nach Absatz 2 Buchstaben b und c nicht umgesetzt werden können. In diesen Fällen sollen die Informationen, mindestens während der Speicherung, vom vernetzten Zugriff abgeschottet werden.

Absatz 4 privilegiert Anbieterinnen, die in der Lage sind, den Zugriff auf die Informationen mittels einer Zwei-Faktor-Authentifizierung sicherzustellen. Die Gleichwertigkeit mit Massnahmen nach Absatz 2 Buchstaben b und c wird vermutet.

Ziffer 7: Für die Auftraggeberin ist es von grosser Bedeutung, dass sie so schnell wie möglich erfährt, wenn ihre Informationen betreffend Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit gefährdet sind oder möglicherweise manipuliert wurden. Die Wiederherstellungspflicht wird der Anbieterin bereits in Ziffer 1 Absatz 1 Buchstabe e auferlegt. Ziffer 7 regelt die damit verbundenen Meldepflichten. Mit dem Erfüllen der Meldepflicht gegenüber dem Bundesamt für Cybersicherheit profitiert die Anbieterin letztlich auch von der Einschätzung ihres Falles durch eine Fachstelle des Bundes.

Absatz 1 Buchstabe a verlangt von der Anbieterin letzten Endes eine ständige Überwachung der Informationssicherheit bei der Erfüllung ihrer vertraglichen Leistungen. Buchstaben b und c nennen Indizien für ein Hacking oder für Phishing-Attacken, wobei sofort erkannte und gelöschte E-Mails von der Meldepflicht ausgenommen sind. Buchstaben d–f zielen auf den Verdacht, dass unberechtigte Personen auf die Informatikmittel eingewirkt bzw. Informationen

[14] Der IT-Grundschutz in der Bundesverwaltung ist in der heutigen Ausprägung auf die Informatikinfrastruktur des Bundes und kaum auf private Unternehmen ausgerichtet und stellt Anforderungen, die insbesondere durch kleinere Unternehmen nur mit grossem Aufwand umgesetzt werden können. Sie wären de facto vom Wettbewerb ausgeschlossen. Im Bereich der nicht sicherheitsempfindlichen Beschaffungen sind die Interessen an einer wirtschaftlich möglichst günstigen Beschaffung höher zu gewichten als Sicherheitsinteressen im niedrigen Risikobereich.

des Bundes zur Kenntnis genommen oder entwendet haben könnten. Mit einer Meldung nach Buchstabe g leistet die Anbieterin neben dem auftragsspezifischen Nutzen auch einen generellen Beitrag zur Informationssicherheit des Bundes. Auch in diesem Fall sind sofort behobene Schwachstellen und Sicherheitslücken von der Meldepflicht ausgenommen, wenn nicht zu erwarten ist, dass die Informationen des Bundes gefährdet werden.

Sicherheitsmeldungen nach dieser Bestimmung dulden oft keinen Aufschub, unterliegen aber grundsätzlich dem Amtsgeheimnis. Es ist daher angezeigt, die mit der Erfüllung der vertraglichen Leistungen betrauten Personen für die Meldungen nach Absatz 1 vorab vom Amtsgeheimnis zu entbinden (Abs. 2). Diese Entbindung muss mit dem Abschluss des Vertrages gewährleistet sein, weshalb die Auftraggeberin zuvor sicherzustellen hat, dass sie entweder hierfür befugt ist oder die zuständige Stelle zugestimmt hat.

Ziffer 8: Absatz 1 verweist für den Fall, dass die Anbieterin die vertragliche Leistung ganz oder teilweise durch eine Dritte juristische oder natürliche Person erbringen lässt, auf die jeweils auf den Auftrag anwendbaren Allgemeinen Geschäftsbedingungen des Bundes.

Die Absätze 2–4 sollen sicherstellen, dass die vorliegenden Standardbestimmungen in der ganzen Lieferkette zum Tragen kommen und für alle Substituentinnen und Subunternehmen klarstellen, dass sie diese mit der Einreichung ihrer Offerte akzeptiert haben. Die Anbieterin wird schliesslich zur Überbindung an alle Subunternehmen verpflichtet.

Absatz 5 stellt einen Auffangtatbestand für den Fall dar, dass marktmächtige Substituentinnen und Subunternehmen die Überbindung der genannten Verpflichtungen ablehnen (Bst. a). Der Verzicht auf das Überbinden soll zwar möglich sein, jedoch nur unter qualifizierten Voraussetzungen, nämlich dem Nachweis, dass keine anderen Anbieterinnen in Frage kommen (Bst. b), dass stattdessen gleichwertige technische und organisatorische Massnahmen getroffen werden (Bst. c) und dass die Auftraggeberin zustimmt (Bst. d). Das voraussetzungslose Veto-Recht der Auftraggeberin (Bst. d) ist im Bereich der Informationssicherheit unabdingbar, da sie für die Sicherheit ihrer Informationen verantwortlich ist und bleibt. Die gewählte Lösung einer risikobasierten Regelung erscheint überdies in diesem Sinne durchaus wettbewerbsverträglich und ermöglicht es der Auftraggeberin, nach erfolgter Risikoanalyse zurückhaltend vom Veto-Recht Gebrauch zu machen.

Ziffer 9: Die Bestimmung verweist hinsichtlich der für die Verletzung von Informationssicherheitsbestimmungen anwendbaren Konventionalstrafen- und Schadenersatzregelungen auf die entsprechende Rubrik der Allgemeinen Geschäftsbedingungen des Bundes.

Dokument I1

Der Beschaffungsvertrag beinhaltet die Verwaltung, die Wartung die Entwicklung oder die Überwachung von Informatikmitteln des Bundes[15] (nicht den Betrieb). Für die Erfüllung der vertraglichen Leistung werden der Anbieterin Bundesgeräte zur Verfügung gestellt und es können auch Informationen des Bundes betroffen sein.

Ziffer 1: Bei der Verwaltung, der Wartung, der Entwicklung und der Überprüfung von Informatikmitteln des Bundes ist die Bearbeitung der darin vorhandenen Informationen in der Regel eher ein Nebenprodukt. Absatz 1 ist daher leicht anders formuliert als in Dokument H. Er nennt drei Dimensionen der Informationssicherheit: die Vertraulichkeit (Bst. a), die Verfügbarkeit (Bst. b) und die Integrität (Bst. c). Diese Grundsätze sind auf die Anbieterin zu überbinden und werden in den weiteren Bestimmungen konkretisiert. Neben der Pflicht, diese Grundsätze ständig zu berücksichtigen, ist auch deren Wiederherstellung, wenn sie verletzt werden, Teil der Anbieterpflicht (Bst. d). Die Nachvollziehbarkeit der Bearbeitung ist nur von Relevanz, wenn letztere auch wirklich Teil der vertraglichen Verpflichtung sind, worauf Absatz 2 Bezug nimmt.

Absatz 2 stellt klar, dass bei der Verwaltung, der Wartung, der Entwicklung und der Überprüfung von Informatikmitteln des Bundes die darin bearbeiteten Informationen für die Anbieterin nur dann zur Bearbeitung freigegeben sind, wenn dies ausdrücklich Vertragsinhalt ist. Solche Arbeiten sollen in der Regel mit Testdaten durchgeführt werden oder der Zugriff auf die Information ist gleich ganz zu unterbinden. Werden trotzdem Echtdaten bearbeitet, hat dies auch nachvollziehbar zu erfolgen.

Ziffer 2: Absatz 1 konkretisiert die Geschäftsherrenhaftung, wonach mit der Erfüllung der Vertragsleistung betraute Personen, sorgfältig auszuwählen, einschlägig zu instruieren und angemessen zu überwachen sind. Die Buchstaben a–c geben den Rahmen der nötigen Instruktion vor. Besondere Beachtung verdient hierbei der Hinweis auf das Amtsgeheimnis. Anbieterinnen bzw. die von ihnen mit der Erfüllung der vertraglichen Leistung betrauten Personen unterliegen als Hilfspersonen dem Amtsgeheimnis. Die Auftraggeberin wird hinsichtlich der Grundsatzinstruktion gegenüber der Anbieterin ebenfalls in die Pflicht genommen.

Die Absätze 2 und 3 konkretisieren die Überwachung und die Folgen mangelhaften Verhaltens der beauftragten Personen sowie entsprechende Meldungen an die Auftraggeberin.

Ziffer 3: Absatz 1 statuiert das Recht der Auftraggeberin, Aufsichtsmassnahmen zur Informationssicherheit bei der Anbieterin vorzunehmen. Die Bestimmung setzt somit Artikel 9 Absatz 2 ISG um. Bei der vertraglichen Ausgestaltung von Kontroll- und Überprüfungsrechten muss sichergestellt sein, dass die Anbieterin durch die Offenlegungspflichten nicht ihrerseits gegen Geheimhaltungsverpflichtungen verstösst, die ihr gegenüber Dritten obliegen. Die Beweislast für solch einen Interessenkonflikt liegt bei der Anbieterin.

Absatz 2 gibt der Anbieterin ein Veto-Recht, wenn die Auftraggeberin Dritte mit dieser Überprüfung beauftragt. Damit sollen insbesondere Produktions- und Geschäftsgeheimnisse der Anbieterin geschützt werden. Da die Erbringung eines solchen Beweises nicht ganz einfach ist, soll als Beweismass das Glaubhaftmachen eines wettbewerbsrelevanten oder anderen Nachteils ausreichen.

Strenge Überprüfungsrechte wie vorliegend sind aus Sicht der Informationssicherheit durchaus angezeigt, sollen im Gegenzug kostenmässig grundsätzlich aber nicht der Anbieterin angelastet werden. Die Auftraggeberin soll sich gegebenenfalls über die Schadenersatzregelungen oder Konventionalstrafen schadlos halten (Abs. 3).

Ziffer 4: Bei der Bearbeitung von Informationen des Bundes durch Dritte sind nicht nur die zu Auftragsbeginn übermittelten oder zugänglich gemachten Informationen zu beachten, sondern

[15] Unterscheidung «Informatikmittel des Bundes» und «Bundesgeräte»: Bei ersteren handelt es sich um die «behandelten» (verwalteten, gewarteten oder überprüften) Mittel (die z. B. mit dem Penetrationstest angegriffen werden), bei zweiteren um das «behandelnde» Mittel (z. B. Gerät, von dem aus ein Penetrationstest ausgeführt wird).

auch die Tatsache, dass sich diese mit der Fortdauer eines Auftrages oft ungewollt zu einer Gesamtinformation verdichten können, welche unter Umständen höheren Schutzbedarf erhalten (Sammelwerk). Dies kann durch Nachlieferungen oder nachträglich zugänglich gemachte Informationen der Auftraggeberin oder Durch Neuerstellung von Informationen bei der Anbieterin erfolgen (Abs. 1). Als Informationsträger gelten Träger von Informationen irgendwelcher Art, namentlich Schriftstücke und Träger von Text-, Bild-, Ton- oder andern Daten; Zwischenmaterial, namentlich Entwürfe, gelten ebenfalls als Informationsträger.

Absatz 2 beschreibt eine für jedermann handhabbare hinreichende Löschung beidseits elektronisch vorhandener Informationen. Sie besteht bspw. aus der Doppellöschung (bspw. auf dem Desktop) und dem Entfernen aus dem Papierkorb.

Um die Löschung im Einzelfall praktikabel zu halten, sollen Anbieterin und Auftraggeberin ein entsprechendes Löschkonzept erstellen. Die Anbieterin hat dann die Gewähr, dass sie mit der konzeptgemässen Löschung die rechtlichen Anforderungen erfüllt (Abs. 3).

Im Ausmass der Beendigung eines Auftrages erlischt hinsichtlich der Informationen des Bundes auch das «Need to Know». Im Bereich der Informatikmittel stellt die technische Einschränkung der Zugangsrechte ein taugliches Mittel des Informationsschutzes dar (Abs. 4).

Ziffer 5 Absatz 1 enthält die Definition der Bundesgeräte, die zur Erfüllung der vertraglichen Leistung verwendet werden können.

Absatz 2 verweist auf die nächste Ziffer, in welcher die Voraussetzungen genannt werden, unter denen der Einsatz von Bundesgeräten für die Erfüllung der vertraglichen Leistung erlaubt ist. Soll davon abgewichen werden, ist in jedem Fall das Einverständnis der Auftraggeberin einzuholen.

Ziffer 6: Absatz 1 legt den Grundsatz fest, dass Informationen des Bundes grundsätzlich nur mit Bundesgeräten bearbeitet werden dürfen, wenn deren Software auf dem aktuellen Stand ist. Die vom Leistungserbringer zur Verfügung gestellten Softwareupdates sind sofort zu übernehmen. Deren Übernahme ist der Auftraggeberin laufend zu bestätigen.

Absatz 2 verpflichtet die nutzenden Personen, das Gerät so zu verwenden, dass die Vorteile einer Zweifaktorauthentifizierung stets gewährleistet sind.

Ziffer 7: Für die Auftraggeberin ist es von grosser Bedeutung, dass sie so schnell wie möglich erfährt, wenn ihre Informationen betreffend Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit gefährdet sind oder möglicherweise manipuliert wurden. Die Wiederherstellungspflicht wird der Anbieterin bereits in Ziffer 1 Absatz 1 Buchstabe d auferlegt. Ziffer 7 regelt die damit verbundenen Meldepflichten. Mit dem Erfüllen der Meldepflicht gegenüber dem Bundesamt für Cybersicherheit profitiert die Anbieterin letztlich auch von der Einschätzung ihres Falles durch eine Fachstelle des Bundes.

Absatz 1 Buchstabe a verlangt von der Anbieterin letzten Endes eine ständige Überwachung der Informationssicherheit bei der Erfüllung ihrer vertraglichen Leistungen. Buchstaben b und c nennen Indizien für ein Hacking oder für Phishing-Attacken, wobei sofort erkannte und gelöschte E-Mails von der Meldepflicht ausgenommen sind. Buchstaben d–f zielen auf den Verdacht, dass unberechtigte Personen auf die Informatikmittel eingewirkt bzw. Informationen des Bundes zur Kenntnis genommen oder entwendet haben könnten. Mit einer Meldung nach Buchstabe g leistet die Anbieterin neben dem auftragsspezifischen Nutzen auch einen generellen Beitrag zur Informationssicherheit des Bundes. Auch in diesem Fall sind sofort behobene Schwachstellen und Sicherheitslücken von der Meldepflicht ausgenommen, wenn nicht zu erwarten ist, dass die Informationen des Bundes gefährdet werden.

Sicherheitsmeldungen nach dieser Bestimmung dulden oft keinen Aufschub, unterliegen aber grundsätzlich dem Amtsgeheimnis. Es ist daher angezeigt, die mit der Erfüllung der vertraglichen Leistungen betrauten Personen für die Meldungen nach Absatz 1 vorab vom Amtsgeheimnis zu entbinden (Abs. 2). Diese Entbindung muss mit dem Abschluss des Vertrages gewährleistet sein, weshalb die Auftraggeberin zuvor sicherzustellen hat, dass sie entweder hierfür befugt ist oder die zuständige Stelle zugestimmt hat.

Ziffer 8: Absatz 1 verweist für den Fall, dass die Anbieterin die vertragliche Leistung ganz oder teilweise durch eine Dritte juristische oder natürliche Person erbringen lässt, auf die jeweils auf den Auftrag anwendbaren Allgemeinen Geschäftsbedingungen des Bundes.

Die Absätze 2–4 sollen sicherstellen, dass die vorliegenden Standardbestimmungen in der ganzen Lieferkette zum Tragen kommen und für alle Subunternehmen klarstellen, dass sie diese mit der Einreichung ihrer Offerte akzeptiert haben. Die Anbieterin wird schliesslich zur Überbindung an alle Subunternehmen verpflichtet.

Absatz 5 stellt einen Auffangtatbestand für den Fall dar, dass marktmächtige Substituentinnen und Subunternehmen die Überbindung der genannten Verpflichtungen ablehnen (Bst. a). Der Verzicht auf das Überbinden soll zwar möglich sein, jedoch nur unter qualifizierten Voraussetzungen, nämlich dem Nachweis, dass keine anderen Anbieterinnen in Frage kommen (Bst. b), dass stattdessen gleichwertige technische und organisatorische Massnahmen getroffen werden (Bst. c) und dass die Auftraggeberin zustimmt (Bst. d). Das voraussetzungslose Veto-Recht der Auftraggeberin (Bst. d) ist im Bereich der Informationssicherheit unabdingbar, da sie für die Sicherheit ihrer Informationen verantwortlich ist und bleibt. Die gewählte Lösung einer risikobasierten Regelung erscheint überdies in diesem Sinne durchaus wettbewerbsverträglich und ermöglicht es der Auftraggeberin, nach erfolgter Risikoanalyse zurückhaltend vom Veto-Recht Gebrauch zu machen.

Ziffer 9: Die Bestimmung verweist hinsichtlich der für die Verletzung von Informationssicherheitsbestimmungen anwendbaren Konventionalstrafen- und Schadenersatzregelungen auf die entsprechende Rubrik der Allgemeinen Geschäftsbedingungen des Bundes.

Dokument I2

Der Beschaffungsvertrag beinhaltet die Verwaltung, die Wartung, die Entwicklung oder die Überwachung von Informatikmitteln des Bundes[16] (nicht den Betrieb). Diese Arbeiten werden mit betrieblichen Informatikmitteln vorgenommen und es können davon auch Informationen des Bundes betroffen sein.

Ziffer 1: Bei der Verwaltung, der Wartung, der Entwicklung und der Überprüfung von Informatikmitteln des Bundes ist die Bearbeitung der darin vorhandenen Informationen in der Regel eher ein Nebenprodukt. Absatz 1 ist daher leicht anders formuliert als in Dokument H. Er nennt drei Dimensionen der Informationssicherheit: die Vertraulichkeit (Bst. a), die Verfügbarkeit (Bst. b) und die Integrität (Bst. c). Diese Grundsätze sind auf die Anbieterin zu überbinden und werden in den weiteren Bestimmungen konkretisiert. Neben der Pflicht, diese Grundsätze ständig zu berücksichtigen, ist auch deren Wiederherstellung, wenn sie verletzt werden, Teil der Anbieterpflicht (Bst. d). Die Nachvollziehbarkeit der Bearbeitung ist nur von Relevanz, wenn letztere auch wirklich Teil der vertraglichen Verpflichtung sind, worauf Absatz 2 Bezug nimmt.

Absatz 2 stellt klar, dass bei der Verwaltung, der Wartung, der Entwicklung und der Überprüfung von Informatikmitteln des Bundes die darin bearbeiteten Informationen für die Anbieterin nur dann zur Bearbeitung freigegeben sind, wenn dies ausdrücklich Vertragsinhalt ist. Solche Arbeiten sollen in der Regel mit Testdaten durchgeführt werden oder der Zugriff auf die Information ist gleich ganz zu unterbinden. Werden trotzdem Echtdaten bearbeitet, hat dies auch nachvollziehbar zu erfolgen.

Ziffer 2: Absatz 1 konkretisiert die Geschäftsherrenhaftung, wonach mit der Erfüllung der Vertragsleistung betraute Personen, sorgfältig auszuwählen, einschlägig zu instruieren und angemessen zu überwachen sind. Die Buchstaben a–c geben den Rahmen der nötigen Instruktion vor. Besondere Beachtung verdient hierbei der Hinweis auf das Amtsgeheimnis. Anbieterinnen bzw. die von ihnen mit der Erfüllung der vertraglichen Leistung betrauten Personen unterliegen als Hilfspersonen dem Amtsgeheimnis. Die Auftraggeberin wird hinsichtlich der Grundsatzinstruktion gegenüber der Anbieterin ebenfalls in die Pflicht genommen.

Die Absätze 2 und 3 konkretisieren die Überwachung und die Folgen mangelhaften Verhaltens der beauftragten Personen sowie entsprechende Meldungen an die Auftraggeberin.

Ziffer 3: Absatz 1 statuiert das Recht der Auftraggeberin, Aufsichtsmassnahmen zur Informationssicherheit bei der Anbieterin vorzunehmen. Die Bestimmung setzt somit Artikel 9 Absatz 2 ISG um. Bei der vertraglichen Ausgestaltung von Kontroll- und Überprüfungsrechten muss sichergestellt sein, dass die Anbieterin durch die Offenlegungspflichten nicht ihrerseits gegen Geheimhaltungsverpflichtungen verstösst, die ihr gegenüber Dritten obliegen. Die Beweislast für solch einen Interessenkonflikt liegt bei der Anbieterin.

Absatz 2 gibt der Anbieterin ein Veto-Recht, wenn die Auftraggeberin Dritte mit dieser Überprüfung beauftragt. Damit sollen insbesondere Produktions- und Geschäftsgeheimnisse der Anbieterin geschützt werden. Da die Erbringung eines solchen Beweises nicht ganz einfach ist, soll als Beweismass das Glaubhaftmachen eines Wettbewerbsnachteils ausreichen.

Strenge Überprüfungsrechte wie vorliegend sind aus Sicht der Informationssicherheit durchaus angezeigt, sollen im Gegenzug kostenmässig grundsätzlich aber nicht der Anbieterin angelastet werden. Die Auftraggeberin soll sich gegebenenfalls über die Schadenersatzregelungen oder Konventionalstrafen schadlos halten (Abs. 3).

Ziffer 4: Bei der Bearbeitung von Informationen des Bundes durch Dritte sind nicht nur die zu Auftragsbeginn übermittelten oder zugänglich gemachten Informationen zu beachten, sondern auch die Tatsache, dass sich diese mit der Fortdauer eines Auftrages oft ungewollt zu einer

[16] Unterscheidung «Informatikmittel des Bundes» und «Bundesgeräte»: Bei ersteren handelt es sich um die «behandelten» (verwalteten, gewarteten oder überprüften) Mittel (die z. B. mit dem Penetrationstest angegriffen werden), bei zweiteren um das «behandelnde» Mittel (z. B. Gerät, von dem aus ein Penetrationstest ausgeführt wird).

Gesamtinformation verdichten können, welche unter Umständen höheren Schutzbedarf erhalten (Sammelwerk). Dies kann durch Nachlieferungen oder nachträglich zugänglich gemachte Informationen der Auftraggeberin oder Durch Neuerstellung von Informationen bei der Anbieterin erfolgen (Abs. 1). Als Informationsträger gelten Träger von Informationen irgendwelcher Art, namentlich Schriftstücke und Träger von Text-, Bild-, Ton- oder andern Daten; Zwischenmaterial, namentlich Entwürfe, gelten ebenfalls als Informationsträger.

Absatz 2 beschreibt eine jedermann handhabbare hinreichende Löschung beidseits elektronisch vorhandener Informationen besteht aus der Doppellöschung (bspw. auf dem Desktop) und dem Entfernen aus dem Papierkorb.

Um die Löschung im Einzelfall praktikabel zu halten, sollen Anbieterin und Auftraggeberin ein entsprechendes Löschkonzept erstellen. Die Anbieterin hat dann die Gewähr, dass sie mit der konzeptgemässen Löschung die rechtlichen Anforderungen erfüllt (Abs. 3).

Im Ausmass der Beendigung eines Auftrages erlischt hinsichtlich der Informationen des Bundes auch das «Need to Know». Im Bereich der Informatikmittel stellt die technische Einschränkung der Zugangsrechte ein taugliches Mittel des Informationsschutzes dar (Abs. 4).

Ziffer 5 Absatz 1 enthält die Definition der betrieblichen Informatikmittel, die zur Erfüllung der vertraglichen Leistung verwendet werden können. Nicht zu dieser Kategorie gehören Informatikmittel der Anbieterin, die der allgemeinen Funktionsfähigkeit der Unternehmung dienen (Personalverwaltung, Geschäftsplanung, E-Mail, etc.) und keinen Bezug zum Vertragsgegenstand haben.

Absatz 2 verweist auf die nächste Ziffer, in welcher die Voraussetzungen genannt werden, unter denen der Einsatz betrieblicher Informatikmittel für die Erfüllung der vertraglichen Leistung erlaubt ist.

Absatz 3 verlegt die Kosten für die Verwaltung, den Betrieb, die Wartung und die Überprüfung betrieblicher Informatikmittel auf die Anbieterin, welche letztlich auch Eigentümerin dieser Infrastrukturen ist.

Ziffer 6: Absatz 1 legt den Grundsatz fest, dass Informatikmittel des Bundes grundsätzlich nur mit betrieblichen Informatikmitteln verwaltet, gewartet und überprüft werden dürfen, wenn deren Software auf dem aktuellen Stand ist, sowie die entsprechende Nachweispflicht der Anbieterin. Im Bereich der nicht-sicherheitsempfindlichen Tätigkeiten reichen dafür die vom Hersteller zur Verfügung gestellten Updates aus, ohne dass von Bundesseite weitere Anforderungen zu stellen wären. Insbesondere wäre es unverhältnismässig, für diese Fälle zu verlangen, dass die betrieblichen Informatikmittel den IT-Grundschutz in der Bundesverwaltung umsetzen müssen. Die Wettbewerbseinschränkungen bei der Beschaffung wären viel zu gross, der Sicherheitsgewinn stünde in keinem akzeptablen Verhältnis zum verursachten Aufwand.

Absatz 2 konkretisiert eine Kaskade von Massnahmen (Bst. a–c), die geeignet sind, für die bearbeiteten Informationen des Bundes einen angemessenen Schutz im Sinne von Ziffer 1 sicherzustellen.

Absatz 3 stellt klar, dass die in Absatz 2 genannten Massnahmen zwingend umzusetzen sind (alternativ). Betriebliche Informatikmittel, bei denen weder das eine noch das andere möglich ist, sind vom Einsatz ausgeschlossen.

Absatz 4 privilegiert Anbieterinnen, die in der Lage sind, den Zugriff auf die Informationen mittels einer Zwei-Faktor-Authentifizierung sicherzustellen. Die Gleichwertigkeit mit Massnahmen nach Absatz 2 Buchstaben b und c wird vermutet.

Ziffer 7: Für die Auftraggeberin ist es von grosser Bedeutung, dass sie so schnell wie möglich erfährt, wenn ihre Informationen betreffend Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit gefährdet sind oder möglicherweise manipuliert wurden. Die Wiederherstellungspflicht wird der Anbieterin bereits in Ziffer 1 Absatz 1 Buchstabe d auferlegt. Ziffer 7 regelt die

damit verbundenen Meldepflichten. Mit dem Erfüllen der Meldepflicht gegenüber dem Bundesamt für Cybersicherheit profitiert die Anbieterin letztlich auch von der Einschätzung ihres Falles durch eine Fachstelle des Bundes.

Absatz 1 Buchstabe a verlangt von der Anbieterin letzten Endes eine ständige Überwachung der Informationssicherheit bei der Erfüllung ihrer vertraglichen Leistungen. Buchstaben b und c nennen Indizien für ein Hacking oder für Phishing-Attacken, wobei sofort erkannte und gelöschte E-Mails von der Meldepflicht ausgenommen sind. Buchstaben d–f zielen auf den Verdacht, dass unberechtigte Personen auf die Informatikmittel eingewirkt bzw. Informationen des Bundes zur Kenntnis genommen oder entwendet haben könnten. Mit einer Meldung nach Buchstabe g leistet die Anbieterin neben dem auftragsspezifischen Nutzen auch einen generellen Beitrag zur Informationssicherheit des Bundes. Auch in diesem Fall sind sofort behobene Schwachstellen und Sicherheitslücken von der Meldepflicht ausgenommen, wenn nicht zu erwarten ist, dass die Informationen des Bundes gefährdet werden.

Sicherheitsmeldungen nach dieser Bestimmung dulden oft keinen Aufschub, unterliegen aber grundsätzlich dem Amtsgeheimnis. Es ist daher angezeigt, die mit der Erfüllung der vertraglichen Leistungen betrauten Personen für die Meldungen nach Absatz 1 vorab vom Amtsgeheimnis zu entbinden (Abs. 2). Diese Entbindung muss mit dem Abschluss des Vertrages gewährleistet sein, weshalb die Auftraggeberin zuvor sicherzustellen hat, dass sie entweder hierfür befugt ist oder die zuständige Stelle zugestimmt hat.

Ziffer 8: Absatz 1 verweist für den Fall, dass die Anbieterin die vertragliche Leistung ganz oder teilweise durch eine Dritte juristische oder natürliche Person erbringen lässt, auf die jeweils auf den Auftrag anwendbaren Allgemeinen Geschäftsbedingungen des Bundes.

Die Absätze 2–4 sollen sicherstellen, dass die vorliegenden Standardbestimmungen in der ganzen Lieferkette zum Tragen kommen und für alle Subunternehmen klarstellen, dass sie diese mit der Einreichung ihrer Offerte akzeptiert haben. Die Anbieterin wird schliesslich zur Überbindung an alle Subunternehmen verpflichtet.

Absatz 5 stellt einen Auffangtatbestand für den Fall dar, dass marktmächtige Substituentinnen und Subunternehmen die Überbindung der genannten Verpflichtungen ablehnen (Bst. a). Der Verzicht auf das Überbinden soll zwar möglich sein, jedoch nur unter qualifizierten Voraussetzungen, nämlich dem Nachweis, dass keine anderen Anbieterinnen in Frage kommen (Bst. b), dass stattdessen gleichwertige technische und organisatorische Massnahmen getroffen werden (Bst. c) und dass die Auftraggeberin zustimmt (Bst. d). Das voraussetzungslose Veto-Recht der Auftraggeberin (Bst. d) ist im Bereich der Informationssicherheit unabdingbar, da sie für die Sicherheit ihrer Informationen verantwortlich ist und bleibt. Die gewählte Lösung einer risikobasierten Regelung erscheint überdies in diesem Sinne durchaus wettbewerbsverträglich und ermöglicht es der Auftraggeberin, nach erfolgter Risikoanalyse zurückhaltend vom Veto-Recht Gebrauch zu machen.

Ziffer 9: Die Bestimmung verweist hinsichtlich der für die Verletzung von Informationssicherheitsbestimmungen anwendbaren Konventionalstrafen- und Schadenersatzregelungen auf die entsprechende Rubrik der Allgemeinen Geschäftsbedingungen des Bundes.

Dokument J

Der Beschaffungsvertrag beinhaltet eine eigentliche Informatik-Leistungserbringung (Betrieb) durch die Anbieterin mit deren betrieblichen Informatikmitteln und es können davon auch Informationen des Bundes betroffen sein.

Ziffer 1: Absatz 1 stellt zunächst klar, dass es sich beim Betrieb von Informatikmitteln durch Dritte um eine Informatik-Leistungserbringung im eigentlichen Sinn handelt, die jedoch mit betrieblichen Informatikmitteln (in Rechenzentren oder auf Servern von Dritten) erfolgt (Bst. a). Diese Informatikmittel sind sicherheitsmässig Schutzobjekten im Sinne von Artikel 7 Absatz 2 ISV gleichzusetzen, was insbesondere auf die zu durchlaufenden Sicherheitsverfahren Auswirkungen hat (Bst. b).

Die Absätze 2 und 3 definieren das «betriebliche Informatikmittel» und treffen eine Kostenregelung zu dessen Verwaltung, Betrieb, Wartung und Überprüfung.

Ziffer 2: Beim Betrieb von Informatikmitteln des Bundes ist die Bearbeitung der darin vorhandenen Informationen in der Regel eher ein Nebenprodukt. Absatz 1 ist daher leicht anders formuliert als in Dokument H. Er nennt drei Dimensionen der Informationssicherheit: die Vertraulichkeit (Bst. a), die Verfügbarkeit (Bst. b) und die Integrität (Bst. c). Diese Grundsätze sind auf die Anbieterin zu überbinden und werden in den weiteren Bestimmungen konkretisiert. Neben der Pflicht, diese Grundsätze ständig zu berücksichtigen, ist auch deren Wiederherstellung, wenn sie verletzt werden, teil der Anbieterpflicht (Bst. d). Die Nachvollziehbarkeit der Bearbeitung ist nur von Relevanz, wenn diese auch wirklich Teil der vertraglichen Verpflichtung ist.

Absatz 2 stellt klar, dass beim Betrieb (Leistungserbringung) von Informatikmitteln des Bundes die darin bearbeiteten Informationen für die Anbieterin nur dann zur Bearbeitung freigegeben sind, wenn dies ausdrücklich Vertragsinhalt ist. Werden trotzdem Echtdaten bearbeitet, hat dies auch nachvollziehbar zu erfolgen.

Ziffer 3: Absatz 1 konkretisiert die Geschäftsherrenhaftung, wonach mit der Erfüllung der Vertragsleistung betraute Personen, sorgfältig auszuwählen, einschlägig zu instruieren und angemessen zu überwachen sind. Die Buchstaben a–c geben den Rahmen der nötigen Instruktion vor. Besondere Beachtung verdient hierbei der Hinweis auf das Amtsgeheimnis. Anbieterinnen bzw. die von ihnen mit der Erfüllung der vertraglichen Leistung betrauten Personen unterliegen als Hilfspersonen dem Amtsgeheimnis. Die Auftraggeberin wird hinsichtlich der Grundsatzinstruktion gegenüber der Anbieterin ebenfalls in die Pflicht genommen.

Die Absätze 2 und 3 konkretisieren die Überwachung und die Folgen mangelhaften Verhaltens der beauftragten Personen sowie entsprechende Meldungen an die Auftraggeberin.

Ziffer 4: Die Absätze 1 und 2 statuieren das Recht der Auftraggeberin, Aufsichtsmassnahmen zur Informationssicherheit bei der Anbieterin vorzunehmen. Die Bestimmung setzt somit Artikel 9 Absatz 2 ISG um. Ziffer 1 Buchstabe a zielt dabei insbesondere auf die Sicherheit der bearbeiteten Informationen, Buchtstabe b zielt auf den sicheren Betrieb des Informatikmittels ab (Einhaltung des IT-Grundschutzes in der Bundesverwaltung). Bei der vertraglichen Ausgestaltung von Kontroll- und Überprüfungsrechten muss sichergestellt sein, dass die Anbieterin durch die Offenlegungspflichten nicht ihrerseits gegen Geheimhaltungsverpflichtungen verstösst, die ihr gegenüber Dritten obliegen. Die Beweislast für solch einen Interessenkonflikt liegt bei der Anbieterin.

Absatz 3 gibt der Anbieterin ein Veto-Recht, wenn die Auftraggeberin Dritte mit dieser Überprüfung beauftragt. Damit sollen Produktions- und Geschäftsgeheimnisse der Anbieterin geschützt werden. Da die Erbringung eines solchen Beweises nicht ganz einfach ist, soll als Beweismass das Glaubhaftmachen eines wettbewerbsrelevanten oder anderen Nachteils ausreichen.

Strenge Überprüfungsrechte wie vorliegend sind aus Sicht der Informationssicherheit durchaus angezeigt, sollen im Gegenzug kostenmässig grundsätzlich aber nicht der Anbieterin

angelastet werden. Die Auftraggeberin soll sich gegebenenfalls über die Schadenersatzregelungen oder Konventionalstrafen schadlos halten (Abs. 3)

Ziffer 5: Bei der Bearbeitung von Informationen des Bundes durch Dritte sind nicht nur die zu Auftragsbeginn übermittelten oder zugänglich gemachten Informationen zu beachten, sondern auch die Tatsache, dass sich diese mit der Fortdauer eines Auftrages oft ungewollt zu einer Gesamtinformation verdichten können, welche unter Umständen höheren Schutzbedarf erhalten (Sammelwerk). Dies kann durch Nachlieferungen oder nachträglich zugänglich gemachte Informationen der Auftraggeberin oder durch Neuerstellung von Informationen bei der Anbieterin erfolgen (Abs. 1 Bst. a). Als Informationsträger gelten Träger von Informationen irgendwelcher Art, namentlich Schriftstücke und Träger von Text-, Bild-, Ton- oder andern Daten; Zwischenmaterial, namentlich Entwürfe, gelten ebenfalls als Informationsträger.

Von besonderer Bedeutung kann eine solche Heraufsetzung der Schutzwürdigkeit auch für die Sicherheitseinstufung des Schutzobjekts sein, allenfalls ist eine neue Schutzbedarfsanalyse vorzunehmen (vgl. Abs. 2).

Der Anbieterin wird in Absatz 2 eine Mitwirkungspflicht bei der Feststellung und Behebung solcher Sachverhalte auferlegt und sie wird instruiert, wie damit umzugehen ist.

Ziffer 6 Erbringt die Anbieterin quantitativ und qualitativ Informatikdienstleistungen in solchem Umfang, dass sie mit einem bundesinternen IKT-Leistungserbringer zu vergleichen ist und dabei insbesondere auf betriebliche Informatikmittel wie eigene Server oder Rechenzentren zurückgreift, müssen für diese auch im nicht-sicherheitsempfindlichen Bereich erhöhte Sicherheitsanforderungen gestellt werden, da in jedem Fall die Gefahr besteht, dass bei Störungen Geschäftsprozesse des Bundes in Mitleidenschaft gezogen werden können. Die Umsetzung des IT-Grundschutzes in der Bundesverwaltung erscheint hier als die minimale und geeignete Voraussetzung, um den nötigen Schutzanforderungen gerecht zu werden (Abs. 1).

Absatz 2 verlangt von der Anbieterin, dass sie diesen Nachweis jährlich selbst erbringt. Faktisch haben solche Anbieterinnen ein professionelles Informationssicherheitsmanagementsystem zu etablieren und aufrecht zu erhalten. Besonderes Augenmerk ist auf risikoerhöhend zu gewichtende Änderungen der Eigentums- und Kontrollrechte an der Anbieterin zu richten.

Ziffer 7: Für die Auftraggeberin ist es von grosser Bedeutung, dass sie so schnell wie möglich erfährt, wenn ihre Informationen betreffend Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit gefährdet sind oder möglicherweise manipuliert wurden. Die Wiederherstellungspflicht wird der Anbieterin bereits in Ziffer 1 Absatz 1 Buchstabe d auferlegt. Ziffer 7 regelt die damit verbundenen Meldepflichten. Mit dem Erfüllen der Meldepflicht gegenüber dem Bundesamt für Cybersicherheit profitiert die Anbieterin letztlich auch von der Einschätzung ihres Falles durch eine Fachstelle des Bundes.

Absatz 1 Buchstabe a verlangt von der Anbieterin letzten Endes eine ständige Überwachung der Informationssicherheit bei der Erfüllung ihrer vertraglichen Leistungen. Buchstaben b und c nennen Indizien für ein Hacking oder für Phishing-Attacken, wobei sofort erkannte und gelöschte E-Mails von der Meldepflicht ausgenommen sind. Buchstaben d–f zielen auf den Verdacht, dass unberechtigte Personen auf die Informatikmittel eingewirkt bzw. Informationen des Bundes zur Kenntnis genommen oder entwendet haben könnten. Mit einer Meldung nach Buchstabe g leistet die Anbieterin neben dem auftragsspezifischen Nutzen auch einen generellen Beitrag zur Informationssicherheit des Bundes. Auch in diesem Fall sind sofort behobene Schwachstellen und Sicherheitslücken von der Meldepflicht ausgenommen, wenn nicht zu erwarten ist, dass die Informationen des Bundes gefährdet werden.

Sicherheitsmeldungen nach dieser Bestimmung dulden oft keinen Aufschub, unterliegen aber grundsätzlich dem Amtsgeheimnis. Es ist daher angezeigt, die mit der Erfüllung der vertraglichen Leistungen betrauten Personen für die Meldungen nach Absatz 1 vorab vom Amtsgeheimnis zu entbinden (Abs. 2). Diese Entbindung muss mit dem Abschluss des Vertrages gewährleistet sein, weshalb die Auftraggeberin zuvor sicherzustellen hat, dass sie entweder hierfür befugt ist oder die zuständige Stelle zugestimmt hat.

Ziffer 8: Absatz 1 verweist für den Fall, dass die Anbieterin die vertragliche Leistung ganz oder teilweise durch eine Dritte juristische oder natürliche Person erbringen lässt, auf die jeweils auf den Auftrag anwendbaren Allgemeinen Geschäftsbedingungen des Bundes.

Die Absätze 2–4 sollen sicherstellen, dass die vorliegenden Standardbestimmungen in der ganzen Lieferkette zum Tragen kommen und für alle Subunternehmen klarstellen, dass sie diese mit der Einreichung ihrer Offerte akzeptiert haben. Die Anbieterin wird schliesslich zur Überbindung an alle Subunternehmen verpflichtet.

Absatz 5 stellt einen Auffangtatbestand für den Fall dar, dass marktmächtige Substituentinnen und Subunternehmen die Überbindung der genannten Verpflichtungen ablehnen (Bst. a). Der Verzicht auf das Überbinden soll zwar möglich sein, jedoch nur unter qualifizierten Voraussetzungen, nämlich dem Nachweis, dass keine anderen Anbieterinnen in Frage kommen (Bst. b), dass stattdessen gleichwertige technische und organisatorische Massnahmen getroffen werden (Bst. c) und dass die Auftraggeberin zustimmt (Bst. d). Das voraussetzungslose Veto-Recht der Auftraggeberin (Bst. d) ist im Bereich der Informationssicherheit unabdingbar, da sie für die Sicherheit ihrer Informationen verantwortlich ist und bleibt. Die gewählte Lösung einer risikobasierten Regelung erscheint überdies in diesem Sinne durchaus wettbewerbsverträglich und ermöglicht es der Auftraggeberin, nach erfolgter Risikoanalyse zurückhaltend vom Veto-Recht Gebrauch zu machen.

Ziffer 9: Die Bestimmung verweist hinsichtlich der für die Verletzung von Informationssicherheitsbestimmungen anwendbaren Konventionalstrafen- und Schadenersatzregelungen auf die entsprechende Rubrik der Allgemeinen Geschäftsbedingungen des Bundes.