



ISG 2.0 : Avanti – Arbeitspaket 01 «Lieferantensicherheit»

Aufsicht bei der Zusammenarbeit mit Lieferanten des Bundes mit Blick auf die Informationssicherheit

Grundlagen – Handlungsformen – Instrumente – Lösungsvorschläge

Berichterstattung gemäss
Bundesratsbeschluss vom 1. Mai 2024

Verfasserin: Staatssekretariat für Sicherheitspolitik
Fachstelle des Bundes für Informationssicherheit
Monbijoustrasse 51A
3003 Bern

Mitarbeit: Bundesamt für Bauten und Logistik
Beschaffungskonferenz des Bundes
Bundesamt für Rüstung
Bundesamt für Cybersicherheit
Bundesamt für Sozialversicherungen
Generalsekretariat VBS
Bundesamt für Justiz

Bern, 25. April 2025



Inhalt

Zusammenfassung	4
1. Einleitung	5
1.1. Anlass und Ausgangslage	5
1.2. Ziel des Berichts	5
1.3. Abgrenzungen	5
1.4. Das «Österreichische Modell»	5
2. Grundlagen	7
2.1. Begriffe	7
2.2. Rechtlicher Rahmen	7
2.2.1. Verfassung	7
2.2.1.1. Grundsätze staatlichen Handelns	7
2.2.1.2. Grundrechte	7
2.2.2. ISG und Verordnungen	7
2.2.3. Verträge	8
2.2.4. Gesetzliche Zuständigkeitsordnungen	8
2.3. Weitere Prinzipien von rechtlicher Bedeutung	9
2.3.1. Wirkungsorientierung, Wirtschaftlichkeit, Verhältnismässigkeit	9
2.3.2. Risikomanagement	9
2.3.3. Best Practices und internationale Standards	9
2.3.4. Sorgfaltspflicht der Auftraggeberin	10
2.4. Zwischenfazit	10
3. Staatliches Handeln	11
3.1. Organisatorisches	11
3.1.1. Vorbemerkung	11
3.1.2. Bedarfsstellen	11
3.1.3. Beschaffungsstellen	11
3.1.4. Fachstelle Betriebssicherheit	12
3.1.5. De lege ferenda: Verwaltungsinterne Auditoren-Pools	12
3.2. Im Besonderen: Beschaffungsprozess	12
3.2.1. Teilnahmebedingungen, Eignungs- und Zuschlagskriterien	12
3.2.2. Lenkungsfunction des Beschaffungsprozesses	13
3.3. Zwischenfazit	13
4. Aufsichtsinstrumente	14
4.1. Vorbehalt der umfassenden rechtlichen Grundlage	14
4.2. Ansätze und Prozesse	14
4.3. Instrumente der direkten Aufsicht	14
4.3.1. Im weiteren Sinne: Betriebssicherheitsverfahren	14
4.3.2. Im engeren Sinne: Kontrollen	15
4.3.2.1. Definition	15
4.3.2.2. Leistungsprofil	15
4.3.2.3. Aufwand	15
4.3.3. Im engeren Sinne: Besuche	15

4.3.3.1.	Definition	15
4.3.3.2.	Leistungsprofil	15
4.3.3.3.	Aufwand	15
4.3.4.	Im engeren Sinne: Audits.....	16
4.3.4.1.	Definition	16
4.3.4.2.	Leistungsprofil	16
4.3.4.3.	Aufwand	16
4.4.	Instrumente der indirekten Aufsicht.....	16
4.4.1.	Selbstdeklarationen.....	16
4.4.1.1.	Definition	16
4.4.1.2.	Leistungsprofil	16
4.4.1.3.	Aufwand	16
4.4.2.	Externe Audits und Zertifikate.....	17
4.4.2.1.	Definition	17
4.4.2.2.	Leistungsprofil	17
4.4.2.3.	Aufwand	17
4.4.3.	Betriebliche Informationssicherheitsmanagementsysteme (ISMS)	17
4.4.3.1.	Definition	17
4.4.3.2.	Leistungsprofil	17
4.4.3.3.	Aufwand	17
4.5.	Sonderfall: Aufsicht in der Lieferkette	17
4.5.1.	Ausgangslage	17
4.5.2.	Problematik.....	18
4.5.3.	Lösung	18
4.6.	Exkurs: Auslagerung der Aufsicht.....	19
4.7.	Zwischenfazit.....	19
5.	Lösungsvorschläge	20
5.1.	Vorbereitungshandlungen	20
5.1.1.	Konsequente Rollenteilung und -zuweisung.....	20
5.1.2.	Konsequente Anwendung des risikobasierten Ansatzes	20
5.1.3.	Nutzung des Beschaffungsprozesses, Vertragsgestaltung.....	20
5.1.4.	Bildung von Risikokategorien	20
5.2.	Einsatz des risikoangemessenen Aufsichtsinstruments.....	21
5.2.1.	Sehr hohe Risiken	21
5.2.2.	Hohe Risiken	22
5.2.3.	Mittlere Risiken	22
5.2.4.	Geringe Risiken	23
5.3.	Überprüfung des Mitteleinsatzes.....	23
5.4.	Retrospektive auf das «Österreichischer Modell».....	23
Anhang 1: Begriffe	I	I
I. Informationssicherheit.....	I	I
II. Informatikmittel.....	I	I
III. Öffentlicher Auftrag	I	I
IV. Sicherheitsempfindlicher öffentlicher Auftrag.....	II	II
V. Auftraggeberin	II	II

a. Vorbemerkung.....	II
b. Bedarfsstelle	II
c. Zentrale Beschaffungsstelle.....	II
d. Delegationsempfängerin.....	II
e. Dezentrale Beschaffungsstelle.....	III
VI. Lieferant.....	III
VII. Sublieferant und Substituent.....	III
VIII. Geheimnis/Geheimnisherr	III
IX. Aufsicht	III
Anhang 2: Formen staatlichen Handelns	V
I. Informelles Verwaltungshandeln: Realakt	V
II. Rechtliches Verwaltungshandeln: Verfügung	V
III. Rechtliches Verwaltungshandeln: Verwaltungsrechtlicher Vertrag	V
IV. Rechtliches Verwaltungshandeln: Privatrechtlicher Vertrag	V

Zusammenfassung

Gegenstand der Aufsicht über Lieferanten im Bereich der Informationssicherheit können sein: *Informationen* des Bundes, *Informatikmittel* des Bundes und *betriebliche Informatikmittel* des Lieferanten. Informationen des Bundes können, jeweils in Abhängigkeit vom Schadenpotenzial bei Missbrauch, *unterschiedlichen Schutzbedarf* und Informatikmittel des Bundes eine *unterschiedliche Sicherheitsstufe* aufweisen.

Die Umsetzung bzw. Durchsetzung von Massnahmen zur Informationssicherheit bei Lieferanten bedeutet stets einen Eingriff in deren Grundrechte. Das heisst, diese Eingriffe müssen eine rechtliche Grundlage haben und im öffentlichen Interesse liegen. Vor allem müssen sie *verhältnismässig* sein, das heisst, sie müssen *erforderlich* und *geeignet* sein und es dürfen *keine milderen Mittel* zur Verfügung stehen. Mit den knappen, für die Aufsicht zur Verfügung stehenden Mitteln ist *grösstmögliche Wirkung* zu erzielen. Das heisst, sie sind dort einzusetzen, wo die Risiken am höchsten sind. Wo die Risiken klein sind, ist der Aufsichtsaufwand zu minimieren oder gar darauf zu verzichten.

Entscheidende Weichen einer wirksamen und wirtschaftlichen Informationssicherheit bei Lieferanten können bereits bei der Bedarfsstelle und noch *vor Einleitung des Beschaffungsverfahrens* gestellt werden. Das Beschaffungsrecht bietet den Bedarfsstellen insbesondere im frühen Stadium der Bedarfserhebung und der Ausschreibung (oder Einladung zur Offertstellung) geeigneten Raum, um die Vorgaben der Informationssicherheit zum *Inhalt des Rechtsgeschäftes* mit dem Lieferanten zu machen.

Die verschiedenen Aufsichtsinstrumente haben unterschiedliche Leistungs- und Aufwandprofile. Bei deren Einsatz sind Kosten-/Nutzenüberlegungen nach den Kriterien der Verhältnismässigkeit, Wirksamkeit und Wirtschaftlichkeit zu tätigen. Der vorliegende Bericht betrachtet die folgenden, praxiserprobten Aufsichtsinstrumente:

- Kontrollen
- Besuche
- Audits
- Selbstdeklarationen
- Externe Auditierungen mit Zertifizierung durch zugelassene Organisationen
- Informationssicherheitsmanagementsysteme

Als Lösung für eine wirksame, wirtschaftliche und verhältnismässige Aufsicht über die Lieferanten des Bundes wird folgendes Vorgehen vorgeschlagen:

- Konsequente Rollenteilung und -zuweisung
- Konsequente Anwendung des risikobasierten Ansatzes
- Nutzung des Beschaffungsprozesses, Vertragsgestaltung
- Bildung von Kategorien
- Einsatz der risikoangemessenen Aufsichtsinstrumente

Informationssicherheit bei Dritten darf sich nicht auf «Erstlieferanten» beschränken, sondern hat überdies zu beachten, dass hinter einer vertraglichen Leistungserfüllung häufig ganze Lieferketten mit zahlreichen Lieferanten stehen, die zu verwalten und zu beaufsichtigen sind.

1. Einleitung

1.1. Anlass und Ausgangslage

Im Zuge des Vorfalles Xplain 2023 hat der damals durch die Bundesverwaltung einberufene *Politisch-Strategische Krisenstab Datenabfluss* diverse Massnahmen getroffen und die Fachstelle des Bundes für Informationssicherheit im Staatssekretariat für Sicherheitspolitik (SEPOS) beauftragt, eine *Auslegeordnung zur Supply Chain Security im Lichte des Informationssicherheitsgesetzes unter Berücksichtigung weiterer Modelle und der getroffenen Massnahmen* zu erstellen. Anfang 2024 hat das SEPOS entsprechend Bericht erstattet.

Das Thema der Lieferantensicherheit war aufgrund der damals gegebenen Zeitverhältnisse zu umfangreich und zu komplex, um zuverlässige Analysen und Ergebnisse liefern zu können. Stattdessen wurde das SEPOS mit Bundesratsbeschluss vom 1. Mai 2024 beauftragt, bis Ende 2024 einen entsprechenden, mit den betroffenen Bundesstellen bereinigten Bericht vorzulegen. Diesem Auftrag wird hiermit nachgekommen.

1.2. Ziel des Berichts

Der Bericht soll den mit der Vergabe öffentlicher Aufträge befassten Behörden und Organisationen des Bundes im Sinne eines Leitfadens Möglichkeiten aufzeigen, wie sie unter Berücksichtigung rechtsstaatlicher Prinzipien, unter Ausnützung von Ermessensspielräumen und mit Blick auf die für die Aufsicht zur Verfügung stehenden Mittel eine wirksame, wirtschaftliche und risikobasierte Aufsicht über ihre Lieferanten verwirklichen können.

1.3. Abgrenzungen

Im Fokus der vorliegenden Betrachtungen steht die Informationssicherheit bei Lieferanten unter dem Regime des ISG¹. Lieferantensicherheit kann nicht losgelöst von den bundesrechtlich vorgeschriebenen Beschaffungsprozessen betrachtet werden. Letztere werden für den vorliegenden Bericht jedoch als Konstanten betrachtet und daher nicht näher daraufhin beleuchtet, ob sie im Sinne der Informationssicherheit geeignet oder angemessen sind.

Das DSG² kennt eigene Sicherheitsvorgaben für den sicheren Umgang mit Personendaten. Auf diese Sicherheitsvorgaben wird im vorliegenden Bericht nur eingegangen, soweit sich hierbei für die Lieferantensicherheit wesentliche, von den Massnahmen des ISG abweichende Punkte ergeben.

1.4. Das «Österreichischer Modell»

Der vorliegende Bericht soll auch das sog. «Österreichischer Modell» diskutieren. Dieses setzt zusammengefasst darauf, dass einerseits ein Katalog an einzuhaltenden Vorgaben existiert und dass andererseits Anbieterinnen per Selbstdeklaration (Self-Assessment) erklären, diese einzuhalten. Die Vorgaben sollen dabei durch eine vom Staat finanzierte Non-Profit-Organisation definiert werden. Ab einem gewissen Auftragsvolumen oder einer gewissen Anzahl von Auf-

¹ Informationssicherheitsgesetz (SR 128)

² Datenschutzgesetz (SR 235.1)

trägen wird ein Audit durch die Non-Profit-Organisation notwendig. Auch werden die Compliance-Anforderungen gestuft, so dass Firmen mit weniger Volumen oder kritischen Projekten weniger Anforderungen erfüllen müssen. Die Eckpfeiler des Modells sind somit:

- ein Katalog von Vorgaben,
- eine Selbstdeklaration der Anbieterin (Self-assessment),
- eine Auslagerung der Aufsicht (Non-Profit-Organisation),
- eine Auditpflicht,
- eine Abstufung der Anforderungen.

Bei Lichte betrachtet handelt es sich um Punkte, die allesamt unabhängig von einem besonderen Modell im vorliegenden Bericht diskutiert werden. Das «Österreichische Modell» weist im Vergleich zu den unter schweizerischem Recht möglichen Aufsichtsinstrumenten keine Besonderheiten auf, welche als Alleinstellungsmerkmal angesehen werden könnten. Es wird daher auf eine vertiefte Analyse des «Österreichischen Modells» verzichtet. Stattdessen wird ganz am Schluss des Berichtes (Ziff. 5.4) eine kurze Retrospektive auf das Modell gehalten.

2. Grundlagen

2.1. Begriffe

Die für das Verständnis des vorliegenden Berichtes notwendigen Begriffsbestimmungen sind in Anhang 1 aufgeführt.

2.2. Rechtlicher Rahmen

2.2.1. Verfassung

2.2.1.1. Grundsätze staatlichen Handelns

Der im Titel des vorliegenden Berichts verwendete Begriff «Aufsicht» impliziert staatliches Handeln. Artikel 5 BV³ hält fest, dass Grundlage und Schranke staatlichen Handelns stets das Recht ist. Es muss im öffentlichen Interesse liegen und verhältnismässig sein. Staatliche Organe (...) haben nach Treu und Glauben zu handeln (Abs. 1–3).

Die nachfolgend genannten Vorgaben (Ziff. 2.2.1.2–2.2.4) bilden in diesem Sinne im Bereich der Informationssicherheit des Bundes die Grundlagen und Schranken für die Aufsicht über dessen Lieferanten.

2.2.1.2. Grundrechte

Wer staatliche Aufgaben wahrnimmt, ist gemäss Artikel 35 Absatz 2 BV an die Grundrechte gebunden. Diese dürfen gemäss Artikel 36 Absatz 2 BV nur eingeschränkt werden, wenn dafür ein öffentliches Interesse besteht und der Eingriff verhältnismässig ist. Das heisst, dass die staatlichen Massnahmen für die Zielerreichung erforderlich und geeignet sein müssen und keine milderen Mittel vorhanden sein dürfen. Bei der Umsetzung von Massnahmen der Informationssicherheit werden mindestens folgende Grundrechte tangiert:

- *Schutz der Privatsphäre* (Art. 13 BV): Die Ermittlungen der Fachstellen für Personensicherheitsprüfungen stellen staatliches Handeln dar und greifen je nach Prüfstufe relativ gravierend in den privaten bis höchstpersönlichen Bereich einer Person ein⁴.
- *Wirtschaftsfreiheit* (Art. 27 BV): Namentlich bei der Festsetzung von Sicherheitsvorgaben, die durch die Anbieterinnen umzusetzen sind, liegt ein Eingriff in die Wirtschaftsfreiheit vor, welcher die Frage der Wettbewerbsneutralität aufwirft. Je nach zu vergebendem öffentlichem Auftrag (insb. im sicherheitsempfindlichen Bereich) sind die Vorgaben und Anforderungen auch bezüglich Sicherheitsvorgaben nach Möglichkeit quantitativ wie qualitativ so auszugestalten, dass der öffentliche Auftrag im Wettbewerb vergeben werden kann.

2.2.2. ISG und Verordnungen

Mit dem ISG und entsprechender Verordnungsgebung hat der Gesetzgeber für die Informationssicherheit eine einheitliche formelle Rechtsgrundlage für den ganzen Bund geschaffen. Mit seinen relativ ausführlichen Regelungen zur Personensicherheitsprüfung (Art. 27–48) sowie zum Betriebssicherheitsverfahren (Art. 49–73) hat er einerseits die obengenannten Eingriffe in Grundrechte hoch legitimiert und gleichzeitig begrenzt sowie andererseits durch risikobasierte

³ Bundesverfassung (SR 101)

⁴ Vgl. Anhang 7 der Verordnung über die Personensicherheitsprüfungen (SR 128.3)

Rechtsetzung⁵ einen für die Belange der Informationssicherheit praktikablen Ansatz statuiert, welcher die Informationen, für deren Schutz der Bund zuständig ist, vollumfänglich umfasst.

Das ISG und seine Verordnungen sind nicht automatisch auf Lieferanten anwendbar (Art. 9 Abs. 1 ISG *e contrario*, wonach die Behörden und Organisationen des Bundes die gesetzlichen Anforderungen und Massnahmen auf Dritte zu überbinden haben).

In den Artikeln 11–19 zeigt das ISG auf, dass einerseits nicht alle Informationen des Bundes den gleichen Schutzbedarf aufweisen und dass andererseits auch bei den Informatikmitteln des Bundes dem Schutzbedarf entsprechend verschiedene Sicherheitsstufen bestehen.

Auf die für den vorliegenden Bericht relevanten rechtlichen Instrumente wird anschliessend in Ziffer 4 näher eingegangen.

2.2.3. Verträge

Mit Artikel 9 ISG hat die Vertragsform für staatliches Handeln – mindestens im Bereich der Informationssicherheit – neben Artikel 8 Absatz 1 BöB⁶ quasi eine zusätzliche positivrechtliche Grundlage erhalten. Für die Zwecke des vorliegenden Berichtes soll ansonsten der Verweis auf die bundesgerichtliche Rechtsprechung⁷ ausreichen, wonach der Staat sich für sein Handeln überall dort der Vertragsform bedienen darf, wo das Gesetz für ihn Raum lässt und er im Einzelfall die geeignetere Handlungsform darstellt als die Verfügung. Benötigt der Staat Güter oder Dienstleistungen, die am Markt erhältlich sind, schliesst er privatrechtliche Verträge ab und tritt damit gleichermassen von seiner hoheitlichen Einwirkungsmöglichkeit auf das Vertragsverhältnis zurück.

Jeder Vertragsschluss stellt auf Seiten des Staates natürlich immer noch staatliches Handeln dar, weshalb die Prinzipien von Artikel 5 BV volle Gültigkeit behalten.

2.2.4. Gesetzliche Zuständigkeitsordnungen

Staatliches Handeln wird durch entsprechende Verfahrenserlasse⁸ gesteuert. Ihnen gemein ist, dass gesetzlich festgelegte Zuständigkeitsordnungen nicht durch Vereinbarung oder Delegation abgeändert werden können⁹. Aufsichts- und gegebenenfalls Vollstreckungsmassnahmen sind Teil des staatlichen Gewaltmonopols und häufig mit Grundrechtseingriffen verbunden (vgl. Ziff. 2.2.1.2), weshalb diese den dafür vorgesehenen, gesetzlich bestimmten Behörden und Organisationen vorbehalten sind.

Für die in diesem Bericht interessierenden Aufsichtsmassnahmen gegenüber Lieferanten heisst dies, dass der Auslagerung solcher Aufgaben enge Grenzen gesetzt sind. Der Kerngehalt der Aufsicht (Veranlassung, Überprüfung und Korrektur von Massnahmen) verbleibt unabänderlich bei der durch Rechtssatz zuständig erklärten Behörde oder Organisation. Auf diesen Punkt wird zurückzukommen sein, wenn über den Beizug Dritter für Vollzugsaufgaben die Rede ist (Ziff. 4.5.).

⁵ Zum Begriff der risikobasierten Rechtsetzung vgl. Ziffer 2.3.2.

⁶ Vgl. auch Ziffer III. Anhang 1

⁷ BGE 136 II 415 E. 2.6.2 S. 425–426

⁸ Grunderlass: Verwaltungsverfahrensgesetz (VwVG, SR 172.021); für die Beschaffung im Speziellen: Org-VöB und ISG.

⁹ Vgl. Artikel 7 Absatz 2 VwVG.

2.3. Weitere Prinzipien von rechtlicher Bedeutung

2.3.1. Wirkungsorientierung, Wirtschaftlichkeit, Verhältnismässigkeit

Unter der – wohl unbestrittenen – Annahme, dass die Mittel für die Erfüllung staatlicher Aufgaben stets knapp sind, ist dafür zu sorgen, dass mit den vorhandenen Mitteln die grösstmögliche Wirkung erzielt wird.

Wirksamkeit und Wirtschaftlichkeit sind nicht zuletzt auch massgebende Aufsichtskriterien (vgl. Ziff. IX Anhang 1). Ebenso gehört die Verhältnismässigkeit zu den Grundlagen und Schranken staatlichen Handelns (vgl. Art. 5 Abs. 2 BV sowie Ziff. 2.2.1.1 hiervor). Aus dieser Konstellation ergibt sich der folgende Rahmen für die Umsetzung der Informationssicherheitsvorgaben in der Zusammenarbeit mit Dritten:

- *Wirkungsorientierung*: Die vorgegebenen Wirkungen sind mit kleinstmöglichem Leistungsvolumen zu erreichen.
- *Wirtschaftlichkeit*: Die benötigten Leistungen sind mit kleinstmöglichem Mitteleinsatz zu erreichen.

2.3.2. Risikomanagement

Artikel 8 ISG verpflichtet die Behörden und Organisationen des Bundes zur laufenden Beurteilung der Risiken der Informationssicherheit (Abs. 1) und zum Treffen von Massnahmen zu deren Vermeidung oder deren Reduktion auf ein tragbares Mass (Abs. 2). Risiken, die getragen werden sollen, müssen nachweislich akzeptiert werden (Abs. 3).¹⁰

Das ISG setzt somit konsequent auf den Ansatz risikobasierter Regulierungen¹¹. Das heisst zusammengefasst:

- Es schreibt nicht einzelne zu treffende Massnahmen vor, sondern das Modell eines maximal zulässigen Risikos. Die Adressaten haben grundsätzlich grossen Ermessensspielraum in der Wahl der Mittel zur Zieleinhaltung.
- Es geht davon aus, dass Risiken nie völlig eliminiert aber optimiert werden können. Der Adressat darf Risiken bewusst in Kauf nehmen, muss aber versuchen, diese soweit wie möglich zu begrenzen.

2.3.3. Best Practices und internationale Standards

Insbesondere der Standard ISO 27001¹² hat eine Relevanz für die Lieferantensicherheit und stützt sich auf das im vorliegenden Bericht vertretene Modell des risikobasierten Ansatzes. Die Vorteile der Nutzung von ISO 27001 sind, dass dieser international anerkannte Standard die Beurteilung ausländischer Lieferanten erleichtert und damit der Aufwand für individuelle Sicherheitsüberprüfungen reduziert wird.

¹⁰ Vgl. hierzu auch die Botschaft zum ISG, BBL 2017 3019

¹¹ Vgl. hierzu: SEILER, Hansjörg (2000), *Risikobasiertes Recht – Wieviel Sicherheit wollen wir? Risk Based Regulation – ein taugliches Konzept für das Sicherheitsrecht*, S. 1, Bern: Stampfli Verlag AG.

¹² [ISO/IEC 27001:2022 - Information security management systems](https://www.iso.org/standard/54539.html)

2.3.4. Sorgfaltspflicht der Auftraggeberin

Das Prinzip «Cura in eligendo, instruendo et custodiendo», welches teilweise explizit in Artikel 20 Absatz 1 ISG abgebildet ist, bedeutet für die Weitergabe von schutzwürdigen Informationen bzw. die Gewährung des Zugangs zu solchen, dass künftige Geheimnisträger¹³ von den Geheimnisherren¹⁴ sorgfältig ausgewählt (eligendo), angewiesen und ausgebildet (instruendo) sowie überwacht (custodiendo) werden müssen. Artikel 20 Absatz 1 ISG auferlegt den verpflichteten Behörden und Organisationen des Bundes (Geheimnisherren) explizit die Pflicht zur Einhaltung dieses Grundsatzes.

2.4. Zwischenfazit

Zur Gewährleistung einer rechtskonformen Aufsicht über Lieferanten ergeben sich vorerst folgende Erkenntnisse:

- Gegenstand der Aufsicht über Lieferanten im Bereich der Informationssicherheit können sein: *Informationen* des Bundes, *Informatikmittel* des Bundes und *betriebliche Informatikmittel* des Lieferanten.
- Im Informatikbereich gibt es Lieferanten, die mit einem *Leistungserbringer* nach Artikel 9 VDTI¹⁵ vergleichbar sind und mit betrieblichen Informatikmitteln Geschäftsprozesse des Bundes mindestens beeinflussen können.
- Informationen des Bundes können, jeweils in Abhängigkeit vom Schadenpotenzial bei Missbrauch, *unterschiedlichen Schutzbedarf* und Informatikmittel des Bundes eine *unterschiedliche Sicherheitsstufe* aufweisen.
- Staatliches Handeln hat neben den Grundsätzen der Recht- und Ordnungsmässigkeit auch diejenigen der *Wirkungsorientierung*, der *Zweckmässigkeit* und der *Wirtschaftlichkeit* zu beachten.
- Die Umsetzung bzw. Durchsetzung von Massnahmen zur Informationssicherheit bei Lieferanten bedeutet stets einen Eingriff in deren Grundrechte. Das heisst, diese Eingriffe müssen eine rechtliche Grundlage haben und im öffentlichen Interesse liegen. Vor allem müssen sie *verhältnismässig* sein, das heisst, sie müssen *erforderlich* und *geeignet* sein und es dürfen *keine milderen Mittel* zur Verfügung stehen. Gesetzliche Zuständigkeitsordnungen sind zwingend.
- Mit den knappen, für die Aufsicht zur Verfügung stehenden Mitteln ist *grösstmögliche Wirkung* zu erzielen. Das heisst, sie sind dort einzusetzen, wo die Risiken am höchsten sind. Wo die Risiken klein sind, ist der Aufsichtsaufwand zu minimieren, ganz sicher aber tiefer zu priorisieren.
- Den Bund als Auftraggeber trifft eine gesetzliche Verpflichtung zur sorgfältigen *Auswahl*, *Instruktion* und *Überwachung* seiner Lieferanten.

¹³ Person, die Kenntnis von einer schutzwürdigen Information hat oder erhält.

¹⁴ Person oder Bundesorgan, die oder das ein objektiv schutzwürdiges Interesse an der Geheimhaltung und damit am Schutz einer Information hat.

¹⁵ Verordnung über die digitale Transformation und die Informatik (SR 172.010.58)

3. Staatliches Handeln

3.1. Organisatorisches

3.1.1. Vorbemerkung

Staatliches Handeln geht von staatlichen Organen aus, denen durch Rechtssatz in einem bestimmten Gebiet bestimmte Aufgaben, Kompetenzen und Verantwortungen auferlegt werden. Im Bereich des Umgangs mit Lieferanten stehen insbesondere die am Beschaffungsverfahren beteiligten Behörden und Organisationen des Bundes im Zentrum des Interesses, weshalb nachfolgend kurz auf diese eingegangen wird.

Ausführungen allgemeiner Art zu den möglichen Formen staatlichen Handelns werden in Anhang 2 kurz beleuchtet.

3.1.2. Bedarfsstellen

Die Bedarfsstellen (Begriff in Ziff. V./b. Anhang 1) ermitteln den Bedarf und teilen diesen der zuständigen zentralen Beschaffungsstelle mit (Art. 13–14 Org-VöB).

Im Bereich der sicherheitsempfindlichen öffentlichen Aufträge prüfen sie gemäss Artikel 16 Org-VöB mit der Fachstelle Betriebssicherheit, ob die beabsichtigte Beschaffung eine sicherheitsempfindliche Tätigkeit beinhaltet und beantragen gegebenenfalls die Einleitung des Betriebssicherheitsverfahrens (Abs. 1). Sie teilen der zentralen Beschaffungsstelle mit, wenn ein Betriebssicherheitsverfahren eingeleitet wird und informieren über die Anforderungen an die Informationssicherheit für das Vergabeverfahren und die Auftrags Erfüllung (Abs. 2).

Handelt die Bedarfsstelle bei einer sicherheitsempfindlichen Beschaffung als dezentrale Beschaffungsstelle (Begriff in Ziff. V./e. Anhang 1), gilt sie gemäss Artikel 26 Org-VöB als Auftraggeberin nach den Artikeln 49–69 ISG und ist damit allein für die Abstimmung der Beschaffung und des Betriebssicherheitsverfahrens zuständig.

In der Informationssicherheit gelten stets die Bedarfsstellen als Geheimnisherren (Begriff in Ziff. VIII Anhang 1). Das heisst, sie bestimmen bei der Beschaffung im Wesentlichen über alle Teilnahmebedingungen, Eignungs- und Zuschlagskriterien, die einen Bezug zur Informationssicherheit haben. Das gilt auch dann, wenn sie Delegationsempfängerinnen sind (Begriff in Ziff. V./d. Anhang 1).

3.1.3. Beschaffungsstellen

Den Beschaffungsstellen (Begriff in Ziff. V./c. Anhang 1) obliegt die zentrale Beschaffung von Waren und Dienstleistungen nach Massgabe der von den Bedarfsstellen übermittelten Bedarfsmeldungen. Weitere Einzelheiten aus den Aufgaben, Kompetenzen und Verantwortlichkeiten im Beschaffungsverfahren sind für das Verständnis des vorliegenden Berichts entbehrlich und werden daher nur dort aufgegriffen, wo sie berichtsrelevant sein können.

Im Bereich der sicherheitsempfindlichen öffentlichen Aufträge übernehmen sie im Einvernehmen mit den Bedarfsstellen die Aufgaben einer Auftraggeberin nach den Artikeln 55–67 ISG. Das sind die Fälle, in denen das Betriebssicherheitsverfahren mit den Prozessschritten des Beschaffungsverfahrens koordiniert werden muss (Art. 12 Org-VöB).

In der Informationssicherheit gelten die Beschaffungsstellen nur als Geheimnisherren (Begriff in Ziff. VIII. Anhang 1), wenn sie eigenen Bedarf decken. In ihrer Rolle als zentrale Beschafferin für andere Bedarfsstellen sind sie nie Geheimnisherr. Das heisst sie bestimmen bei der Beschaffung nur in Absprache mit der Bedarfsstelle über Teilnahmebedingungen, Eignungs- und Zuschlagskriterien, die einen Bezug zur Informationssicherheit haben.

3.1.4. Fachstelle Betriebssicherheit

Wird ein sicherheitsempfindlicher öffentlicher Auftrag (Begriff in Ziff. IV. Anhang 1) vergeben, so obliegt der Fachstelle Betriebssicherheit die Durchführung des Betriebssicherheitsverfahrens, welches der Gewährleistung der Informationssicherheit bei der Erfüllung von öffentlichen Aufträgen durch Lieferanten dient (Art. 49 ISG).

Das Betriebssicherheitsverfahren ist in den Artikel 49–73 ISG geregelt und ist ein Instrument des rechtlichen Verwaltungshandelns (Vgl. Ziff. II.–IV. Anhang 2), mit anderen Worten, es ist an strikte Verfahrensvorschriften gebunden.

Das Betriebssicherheitsverfahren ist dem Beschaffungsverfahren vorgelagert (vgl. Art. 52 ISG) und greift teilweise in letzteres über (vgl. Art. 58 ISG). Die Fachstelle Betriebssicherheit setzt damit jeweils zu einem sehr frühen Zeitpunkt mit der Bedarfsstelle (Geheimnisherr) die Sicherheitsvorgaben für das Vergabeverfahren und die Auftrags Erfüllung fest (vgl. Art. 54 ISG), so dass diese bereits in die Bedarfsmeldung an die Beschaffungsstelle einfließen.

3.1.5. De lege ferenda: Verwaltungsinterne Auditoren-Pools

Aus Gründen der Wirtschaftlichkeit wäre allenfalls die Einrichtung eines «Auditoren Pools» zu prüfen, in welchem verwaltungsinterne Sicherheitsspezialisten mit entsprechender Ausbildung und Erfahrung zusammengefasst und für Aufsichtshandlungen bei Lieferanten eingesetzt werden könnten. Aus Wirtschaftlichkeitsgründen sollte er dem ganzen Bund zur Verfügung stehen.

3.2. Im Besonderen: Beschaffungsprozess

3.2.1. Teilnahmebedingungen, Eignungs- und Zuschlagskriterien

Anforderungen der Informationssicherheit können je nach Risikolage beträchtliche organisatorische und finanzielle Folgen für einen Lieferanten haben. In einigen Fällen werden diese aus sachlichen oder finanziellen Gründen gar nicht umgesetzt werden können. Mit der öffentlichen Ausschreibung (oder Einladung zur Offertstellung) müssen Lieferanten diesbezüglich Gewissheit haben. Um Leerläufe zu vermeiden (Abbruch von Beschaffungsverfahren) sollen Teilnahmebedingungen, Eignungs- und Zuschlagskriterien mit Bezug zur Informationssicherheit von der Bedarfsstelle so früh wie möglich festgelegt und in die Bedarfsmeldung eingebracht werden. Mit der Publikation der Ausschreibung müssen Lieferanten diesbezüglich Gewissheit haben.

Nur bedingt anwendbar ist dieses Vorgehen bei Rahmenverträgen nach Artikel 25 BöB. Im Zeitpunkt, da diese ausgeschrieben werden, können häufig noch keine hinreichend genauen sicherheitsmässigen Spezifikationen festgelegt werden. Zum Zeitpunkt der Einzelabrufe werden sie zwar bekannt sein, jedoch gelten dann gemäss Artikel 25 Absatz 4 BöB immer noch die Bedingungen (auch die sicherheitsmässigen) des Rahmenvertrages. Somit muss bereits die Ausschreibung des Rahmenvertrages die grundlegenden Anforderungen sowie ein Verfahren zur Berücksichtigung der Informationssicherheit für die Abrufe enthalten.

3.2.2. Lenkungsfunktion des Beschaffungsprozesses

Die Behörden und Organisationen des Bundes haben hinsichtlich Auswahl, Instruktion und Überwachung der Lieferanten eine explizite gesetzliche Verpflichtung (vgl. Ziff. 2.3.4).

Durch das Erstellen eines möglichst exakten, der Risikosituation angemessenen Katalogs von Anforderungen an die Informationssicherheit können bereits die ersten Weichen für eine sorgfältige *Auswahl* eines Lieferanten gestellt werden. Potenzielle Anbieter werden entweder bereits auf das Einreichen eines Angebotes verzichten, wenn sie merken, dass sie den Anforderungen nicht gewachsen sind, oder ihre Angebote kommen relativ schnell z. B. wegen objektiv nicht erfüllter Eignungskriterien für einen Zuschlag nicht mehr in Frage.

Werden die Anforderungen der Informationssicherheit bereits in die Ausschreibungsunterlagen (oder in die Einladung zur Offertstellung) aufgenommen, so können potenzielle Lieferanten bereits als *instruiert* gelten. Umgekehrt gilt sogar, dass nachträglich keine Anforderungen mehr gestellt werden dürfen, die nicht publiziert wurden.

Anforderungen, die sich aus dem Beschaffungsverfahren ergeben, müssen dann schliesslich in Vertragsform gegossen und dem Lieferanten in geeigneter Form überbunden werden.

3.3. Zwischenfazit

Zur Gewährleistung einer rechtskonformen Aufsicht über Lieferanten ergeben sich weiter folgende Erkenntnisse:

- Die Formen rechtsstaatlichen Handelns sind auf *wenige, meist durchregulierte Formen* begrenzt. Selbst dort, wo Raum für alternative Formen (z. B. Verträge) bleibt, gilt das Prinzip, dass Grundlage und Grenze staatlichen Handelns das Recht ist.
- Entscheidende Weichen einer wirksamen und wirtschaftlichen Informationssicherheit bei Lieferanten können bereits bei der Bedarfsstelle und noch *vor Einleitung des Beschaffungsverfahrens* gestellt werden.
- Das Beschaffungsrecht bietet insbesondere im frühen Stadium der Bedarfserhebung und der Ausschreibung (oder Einladung zur Offertstellung) den Bedarfsstellen geeigneten Raum, um die Vorgaben der Informationssicherheit zum *Inhalt des Rechtsgeschäftes* mit dem Lieferanten zu machen. Das trägt zur sorgfältigen Auswahl und zur Instruktion des Lieferanten bei.
- Sicherheitsanforderungen, die nicht publiziert wurden (oder nicht Gegenstand der Einladung zur Offertstellung waren) können nachträglich nicht mehr einseitig auf den Lieferanten überbunden werden.

4. Aufsichtsinstrumente

4.1. Vorbehalt der umfassenden rechtlichen Grundlage

Wie in Ziffer 2.2.1.2 erkannt, bedeutet die Umsetzung bzw. Durchsetzung von Massnahmen zur Informationssicherheit bei Lieferanten stets einen Eingriff in deren Grundrechte. Das heisst, diese Eingriffe müssen rechtlich verankert sein und im öffentlichen Interesse liegen. Vor allem müssen sie *verhältnismässig* sein, das heisst, sie müssen *erforderlich* und *geeignet* sein und es dürfen *keine mildereren Mittel* zur Verfügung stehen.

Bevor also über Aufsichtsmassnahmen gegenüber Lieferanten diskutiert wird, ist sicherzustellen, dass die angewendeten Instrumente vorweg rechtlich verankert sind. Hierbei kann auf Grundlage des ISG in zwei Arten unterschieden werden, wie Sicherheitsanforderungen auf Lieferanten übertragen werden (einzeln oder in Kombination):

- Sicherheitskonzept im Betriebssicherheitsverfahren (Art. 59 ISG),
- Vereinbarungen und Verträge (Art. 9 Abs. 1 ISG).

Es ist zu bedenken, dass nicht nur die Sicherheitsanforderungen zum Vertragsinhalt zu machen sind, sondern auch das entsprechende Recht, beim Lieferanten Prüfungen vornehmen zu dürfen (Art. 9 Abs. 2 ISG).

4.2. Ansätze und Prozesse

Die nachfolgend beschriebenen Aufsichtsinstrumente können einerseits zur Prüfung eingesetzt werden, ob bestimmte Normwerte vorhanden sind, mit der Hypothese, dass ein Lieferant sicher ist, solange er diese erfüllt (verifizierender Ansatz). Andererseits kann nach Sicherheitslücken oder Fehlern gesucht werden mit der Hypothese, dass ein Lieferant sicher ist, solange keine solchen gefunden werden (falsifizierender Ansatz).

Der vorliegende Bericht verzichtet bewusst darauf, Prozesse und Organisation der Prüfungshandlungen vorzuschlagen. Dies soll Sache der mit der Aufsicht betrauten Stellen sein.

4.3. Instrumente der direkten Aufsicht

4.3.1. Im weiteren Sinne: Betriebssicherheitsverfahren

Das Betriebssicherheitsverfahren dient gemäss Artikel 49 ISG zur Gewährleistung der Informationssicherheit bei der Erfüllung von öffentlichen Aufträgen durch Unternehmen und Subunternehmen oder Teile davon (Betriebe), sofern die Aufträge die Ausübung einer *sicherheitsempfindlichen Tätigkeit* einschliessen (sicherheitsempfindliche Aufträge).

Es handelt sich hierbei um ein Verwaltungsverfahren, in welchem die Sicherheitsaufsicht im sicherheitsempfindlichen Bereich vollumfänglich in den Händen der zuständigen Fachstelle Betriebssicherheit liegt. Steht einmal fest, dass der zu vergebende öffentliche Auftrag die Kriterien der Sicherheitsempfindlichkeit erfüllt (Ziff. IV. Anhang 1), so besteht auf Seiten der Auftraggeberin (Ziff. V. Anhang 1.), hinsichtlich der Beantragung auf Einleitung des Betriebssicherheitsverfahrens kein Ermessensspielraum (Art. 52 Abs. 1 ISG).

Auf die Einleitung des Betriebssicherheitsverfahrens kann nur verzichtet werden, wenn sich die Auftraggeberin und die Fachstelle Betriebssicherheit darüber einig sind, dass das Risiko mit

anderen Massnahmen auf ein tragbares Mass reduziert werden kann (Art. 53 Abs. 2 ISG) und keine sonstigen Gründe entgegenstehen (Art. 5 Abs. 2 VBSV¹⁶).

Die Auftraggeberin hat im Betriebssicherheitsverfahren in der Regel einen relativ kleinen Prüfungsaufwand zu tragen. Die Fachstelle Betriebssicherheit legt fest, welches der nachfolgend beschriebenen Aufsichtsinstrumente – auch indirekte – zur Anwendung kommt.

4.3.2. Im engeren Sinne: Kontrollen

4.3.2.1. *Definition*

Die Kontrolle, als punktuelle Überprüfung der Einhaltung der Sicherheitsvorgaben beim Lieferanten (Ziff. VI. Anhang 1), ist geeignet, einen Zustand auf seine Übereinstimmung mit den Sicherheitsanforderungen zu prüfen und ist daher relativ statisch. Entsprechende Anordnungen der Auftraggeberin haben Verfügungscharakter (Ziff. II. Anhang 2).

4.3.2.2. *Leistungsprofil*

Eine vertiefte Überprüfung von Arbeitsabläufen, des Verhaltens der an der Erfüllung des Auftrags beteiligten Personen oder der Eignung von Sicherheitsmassnahmen ist nicht möglich.

4.3.2.3. *Aufwand*

Kontrollen sind für die Auftraggeberin mit relativ wenig Aufwand zu planen und durchzuführen und entfalten neben ihrer direkten Wirkung auch eine bedeutende präventive und bewusstseinsbildende Wirkung beim Anbieter.

4.3.3. Im engeren Sinne: Besuche

4.3.3.1. *Definition*

Der Besuch, als *angemeldete*, punktuelle Überprüfung der Sicherheitsvorgaben beim Lieferanten mit Fachgespräch über die Umsetzung ist ein eigentlicher Realakt (Ziff. I. Anhang 2) von Auftraggeberinnen, welche in der Regel nicht über vom Recht verliehene Aufsichts- und Vollzugskompetenzen verfügen¹⁷.

4.3.3.2. *Leistungsprofil*

Realakte zielen darauf ab, das *Verhalten des Adressatenkreises* zu beeinflussen, ohne dass jedoch bei Nichtbefolgung eine Rechtsfolge damit verbunden wäre. Da der Mensch in der Informationssicherheit die grösste Schwachstelle darstellt und Realakte eben gerade an dessen Verhalten ansetzen, kann die positive Wirkung von Besuchen nicht genug hoch eingeschätzt werden.

4.3.3.3. *Aufwand*

Sollen Besuche ihre Wirkung entfalten, sind sie sorgfältig vorzubereiten z. B. durch Erstellen von Ausbildungsunterlagen, Merkblättern, Leitfäden etc. Es ist somit ein relativ erheblicher Vorbereitungsaufwand damit verbunden.

¹⁶ Verordnung über das Betriebssicherheitsverfahren (SR 128.41)

¹⁷ Vgl. hierzu z. B. auch das Thema «Sensibilisierungsgespräche» in Ziffer 2.2 [Aufsicht Cybersicherheit der ElCom - Weisung 1-2024](#)

4.3.4. Im engeren Sinne: Audits

4.3.4.1. *Definition*

Das Audit, als Besuch mit vorbereitetem und mit dem Lieferanten vereinbarten Prüfprogramm, durchgeführt von der Auftraggeberin oder von einer damit von der Auftraggeberin speziell beauftragten Organisation, ist das umfassende Aufsichtsinstrument der Informationssicherheit bei Lieferanten. Es vereint die Leistungsprofile von Kontrollen und Besuchen und wird häufig zur Überprüfung von Prozessen eingesetzt.

4.3.4.2. *Leistungsprofil*

Seine Spannweite reicht damit von einer Umsetzungskontrolle über die Prozessprüfung bis zur Prüfung menschlichen Verhaltens. Umsetzungsanordnungen der Auftraggeberin haben entweder Verfügungscharakter (Ziff. II. Anhang 2) oder die Form eines verwaltungsrechtlichen Vertrags (Ziff. III. Anhang 2.). Die Wirkung von Audits hängt im Wesentlichen vom im Einzelfall festgelegten Auditprogramm ab.

4.3.4.3. *Aufwand*

Wirkungsvolle Audits müssen gründlich vorbereitet und in der Regel mit nicht zu unterschätzendem Aufwand nachbereitet werden, da solch eingehende, oft mehrere Tage dauernde Untersuchungen häufig Abweichungen vom Soll-Zustand zu Tage fördern, die vom Lieferanten behoben werden müssen (Korrektur der Abweichungen). Ein solches Lieferantenaudit, insbesondere die Behebung allenfalls daraus hervorgehender Abweichungen ist zeitlich auf mehrere Monate ausgelegt und hängt nicht zuletzt vom Umfang des Prüfprogramms ab.

4.4. Instrumente der indirekten Aufsicht

4.4.1. Selbstdeklarationen

4.4.1.1. *Definition*

Als Massnahme der indirekten Aufsicht zeichnet sich die Selbstdeklaration dadurch aus, dass der Lieferant anhand der ihm auferlegten Sicherheitsanforderungen eine Selbsteinschätzung vornimmt und darin erklärt, die Anforderungen einzuhalten. Auf Verlangen weist er der Auftraggeberin entsprechende Belege vor. Beispiele sind etwa Geheimhaltungserklärungen.

4.4.1.2. *Leistungsprofil*

Grundsätzlich kann darauf vertraut werden, dass Selbstdeklarationen von den Lieferanten wahrheitsgemäss erfolgen, weil sie an der Auftragserteilung und der Geschäftsbeziehung zum Bund interessiert sind. Als «Mittel der ersten Stunde» können sie risikounabhängig *in der Breite* eingesetzt werden, der Auftraggeberin obliegt es, vertiefte Abklärungen zu treffen, wenn sie Zweifel an den Angaben der Lieferanten hat.

Falsche Selbstdeklarationen dürften als schriftliche Lügen gelten und wohl noch nicht unter die Urkundendelikte fallen.

4.4.1.3. *Aufwand*

Solange die Auftraggeberin den Angaben der Lieferanten vertraut und kein Anlass für Zweifel an diesen besteht, ist die Selbstdeklaration ein relativ aufwandarmes Instrument.

4.4.2. Externe Audits und Zertifikate

4.4.2.1. *Definition*

Auftraggeberinnen können Lieferanten auch damit beauftragen, sich selber auditieren zu lassen und periodisch über die Ergebnisse dieser Audits mittels entsprechender Zertifikate zu berichten.

4.4.2.2. *Leistungsprofil*

Je nach Auditauftrag können an die Zertifikate hohe Erwartungen an die Beweiskraft gestellt werden, da diese Audits in der Regel ebenfalls durch akkreditierte Organisationen, welche zertifizieren dürfen, durchgeführt werden. Durch die Zertifizierung des Lieferanten kann von einer Einhaltung des Standards ausgegangen werden, welche sich in der Qualität der Prozesse widerspiegelt und der Sicherheit zuträglich ist.

4.4.2.3. *Aufwand*

Für die Auftraggeberin ergibt sich hier ebenfalls minimaler Aufwand. Da hier für die Lieferanten Kosten entstehen, kommt dieses Regime nur in Frage, wenn damit ein entsprechendes Risiko spürbar minimiert werden kann.

4.4.3. Betriebliche Informationssicherheitsmanagementsysteme (ISMS)

4.4.3.1. *Definition*

ISMS, insbesondere die auf ISO 27001 abgestützten, gelten als international anerkannte Best Practices (vgl. Ziff. 2.3.3.). Die Auftraggeberin verlangt vom Lieferanten die Etablierung eines (in der Regel) zertifizierten ISMS, welches periodisch gemäss Ziffer 4.3.2. auditiert wird. Die Auftraggeberin lässt sich die Prüfergebnisse vorlegen.

4.4.3.2. *Leistungsprofil*

Auditergebnisse haben insbesondere dann hohe Beweiskraft, wenn nachgewiesen wird, dass ein ISMS etabliert wurde und darüber hinaus auch wirkungsvoll gelebt wird. Auch diese Audits werden zudem in der Regel durch unabhängige akkreditierte Organisationen vorgenommen werden.

4.4.3.3. *Aufwand*

Auch hier minimiert die Auftraggeberin ihren Aufwand. Unter einem solchen Regime fallen aber für den Lieferanten in der Regel sehr hohe Kosten an. Ein ISMS muss daher auch hohen Anforderungen an die Verhältnismässigkeit, Wirksamkeit und Wirtschaftlichkeit genügen.

4.5. Sonderfall: Aufsicht in der Lieferkette

4.5.1. *Ausgangslage*

Viele öffentliche Aufträge werden nicht alleine durch den Lieferanten erfüllt, welcher im Vergabeverfahren den Zuschlag erhalten hat (Erstlieferant). Hinter der Erbringung einer staatlichen Leistung stehen oft lange und weitverzweigte Lieferketten, deren Ursprünge nicht selten jenseits der Landesgrenzen liegen.

Für jeden einzelnen Lieferanten in einer solchen Kette, soweit er bei der Erfüllung seiner vertraglichen Leistung mit Informationen oder Informatikmitteln des Bundes in Berührung kommt,

müssen konsequenterweise die gleichen Regeln, sprich Sicherheitsvorgaben, gelten. Somit müssen auch die vorerwähnten Aufsichtsinstrumente entlang der ganzen Lieferkette vertraglich vereinbart und zur Anwendung gebracht werden können. Andernfalls könnten sich durch ein Leck bei einem – eventuell relativ unbedeutenden Lieferanten – die – eventuell hochwertigen – Sicherheitsmassnahmen bei den anderen Gliedern der Kette als nutzlos erweisen.

4.5.2. Problematik

Die staatliche Auftraggeberin, welche öffentliche Aufträge vergibt, tut dies immer gegenüber einem Erstlieferanten. Nur bei diesem kann sie sich die Lenkungsfunktion des Beschaffungsprozesses sowie die Möglichkeit der Vertragsgestaltung direkt zu Nutze machen (Auswahl und Instruktion, vgl. Ziff. 3.2.2.). Der Erstlieferant ist jedoch im Rahmen von Artikel 8 BöB und Artikel 68 OR frei, Teile seiner vertraglichen Verpflichtung auf einen anderen Lieferanten zu übertragen (Substitution, vgl. Ziff. VII Anhang 1) oder sich durch andere Lieferanten bei seiner Leistung unterstützen zu lassen (Vergabe von Aufträgen an Sublieferanten, vgl. Ziff. VII Anhang 1), soweit es sich dabei nicht um die für das Rechtsgeschäft charakteristische Leistung handelt¹⁸.

Verträge sind grundsätzlich streng zweiseitig, das heisst, die Auftraggeberin ist an einem Vertragsverhältnis zwischen Erstlieferant und Substituenten und Sublieferanten gar nicht beteiligt und hat damit keinen direkten Zugriff auf letztere. Dadurch wird die durchgängige Aufsicht über die Lieferkette erheblich erschwert. Die Problematik verschärft sich weiter, wenn ausländische Sublieferanten im Spiel sind. Diese können sich dem Zugriff durch schweizerische Behörden weitgehend entziehen.

4.5.3. Lösung

Will sich die staatliche Auftraggeberin den Risiken, welche diese doch recht übliche Art der Leistungserbringung mit sich bringt, nicht unkontrolliert aussetzen, muss sie bereits dem Erstlieferanten entsprechende Verpflichtungen im Vertrag bzw. mittels der vereinbarten Allgemeinen Geschäftsbedingungen des Bundes auferlegen. Diese können wie folgt aussehen:

- *Überbindungspflicht* von Sicherheitsanforderungen auf Substituenten und Sublieferanten (muss in jedem Vertrag Standard sein);
- *Verbot* der Substitution und der Vergabe von Unteraufträgen;
- *Genehmigungspflicht* für Substitution und die Vergabe von Unteraufträgen;
- *Meldepflicht* für Substitution und die Vergabe von Unteraufträgen mit Widerspruchsrecht der Auftraggeberin.
- Verbindliche *Deklaration von Substituenten und Lieferketten* in der Offerte mit Gewährung eines Ausschlussrechts für die Auftraggeberin.

Haben Sublieferanten ihren Sitz im Ausland, ist in Erwägung zu ziehen, den schweizerischen Erstlieferanten für die Handlungen und Unterlassungen seines ausländischen Sublieferanten per Vertrag haftbar zu machen.

¹⁸ Vgl. Artikel 68 des Obligationenrechts: «Der Schuldner ist nur dann verpflichtet, persönlich zu erfüllen, wenn es bei der Leistung auf seine Persönlichkeit ankommt.»

4.6. Exkurs: Auslagerung der Aufsicht

Wie in Kapitel 4.4 dargestellt, müssen Prüfhandlungen nicht in jedem Fall von der Auftraggeberin selber vorgenommen werden, es besteht die Möglichkeit der Auslagerung an Dritte.

Solche Dritten dürfen Untersuchungshandlungen vornehmen, soweit sie nicht in das staatliche Gewaltmonopol eingreifen (negative Voraussetzung) und darüber hinaus entsprechend durch eine rechtliche Grundlage legitimiert sind (positive Voraussetzung). Zu beachten ist schliesslich, dass einem durch Dritte auditierten Lieferanten immer ein Vetorecht gegen die prüfende Organisation einzuräumen ist, falls er glaubhaft machen kann, dass ihm aus der Prüfung ein wettbewerbsrelevanter Nachteil erwachsen könnte.

4.7. Zwischenfazit

Zur Gewährleistung einer rechtskonformen Aufsicht über Lieferanten ergeben sich folgende Erkenntnisse:

- Aufsichtsmassnahmen gegenüber Lieferanten benötigen einen rechtlichen Rahmen. Dieser kann sich aus dem Beschaffungsvertrag oder aus dem Sicherheitskonzept im Betriebssicherheitsverfahren ergeben.
- Die verschiedenen Aufsichtsinstrumente haben unterschiedliche Leistungs- und Aufwandprofile. Bei deren Einsatz sind Kosten-/Nutzenüberlegungen nach den Kriterien der Verhältnismässigkeit, Wirksamkeit und Wirtschaftlichkeit zu tätigen.
- Die Auftraggeberin muss berücksichtigen, dass hinter der Erbringung einer vertraglichen Leistung eines Lieferanten häufig eine komplexe Lieferkette mit verschiedenen Lieferanten steht. Wenn sie es versäumt, den «Erstlieferanten» durch vertragliche Vereinbarungen entsprechend zu instruieren, werden die Risiken innerhalb der Lieferkette immer schwerer kontrollierbar.
- Die Auslagerung von Aufsichtstätigkeiten an Lieferanten (z. B. Auditdienstleistungen) ist möglich, findet ihre Grenze aber beim staatlichen Gewaltmonopol, das heisst bei der Durchsetzung von behördlichen Anordnungen. Lieferanten, die ihrerseits von einem nichtstaatlichen Prüforgan beaufsichtigt werden, müssen das Recht haben, solche abzulehnen, wenn sie durch die Prüfung einen Wettbewerbsnachteil erleiden könnten (Vetorecht).

5. Lösungsvorschläge

5.1. Vorbereitungshandlungen

5.1.1. Konsequente Rollenteilung und -zuweisung

Wie in Ziffer 3.1. gesehen, sind am Beschaffungsprozess verschiedene Rollenträger beteiligt. In diesem Zusammenhang muss auf eine sorgfältige und die Lieferkette durchdringende Vertragsgestaltung geachtet werden. Die Absprache zwischen Bedarfsstelle und Beschaffungsstelle muss somit einwandfrei funktionieren. Mit der Bedarfsmeldung nach Artikel 14 Org-VöB obliegt es der Bedarfsstelle, die Beschaffungsstelle hinsichtlich des zu beschaffenden Gutes exakt zu instruieren. Dazu gehören eben auch die Sicherheitsanforderungen für die Beschaffung und die Auftragserfüllung.

Ebenso müssen Aufgaben, Kompetenzen und Verantwortlichkeiten zwischen der Bedarfsstelle und dem Lieferanten vertraglich definiert werden. Diesem Aspekt wie auch dem Prinzip der *cura in eligendo, instruendo und custodiendo* (vgl. Ziff. 2.3.4) hat die Beschaffungsstelle bei der Vertragsgestaltung hinreichend Rechnung zu tragen.

Mit den beiden Gesetzes- bzw. Verordnungsnovellen (ISG und Org-VöB) könnte es unter Umständen nützlich sein, die Beschaffungsprozesse mit entsprechenden Kontrollpunkten zu versehen.

5.1.2. Konsequente Anwendung des risikobasierten Ansatzes

Die Aufsicht über Lieferanten muss – nicht zuletzt mit Blick auf die allorts knappen Mittel – zwingend dort Schwerpunkte setzen, wo für die Sicherheit der Schweiz die grössten Risiken zu erwarten sind. Sie erfordert damit von den Auftraggeberinnen und Vollzugsbehörden die Vornahme entsprechender Risikobeurteilungen. Der Gesetzgeber hat mit den Klassifizierungsstufen für Informationen und den Sicherheitsstufen für Informatikmittel die Vorarbeit zu einer Kategorisierung und somit risikomässigen Abstufung geleistet. Den Vollzugsbehörden obliegt es nun, die vorhandenen Mittel nach den Grundsätzen der Wirksamkeit, der Wirtschaftlichkeit und der Verhältnismässigkeit einzusetzen.

5.1.3. Nutzung des Beschaffungsprozesses, Vertragsgestaltung

Wie in Ziffer 3.2. erkannt, bietet das Beschaffungsrecht den Bedarfsstellen insbesondere im frühen Stadium der Bedarfserhebung und der Ausschreibung (oder Einladung zur Offertstellung) geeigneten Raum, um die Vorgaben der Informationssicherheit zum *Inhalt des Rechtsgeschäftes* mit dem Lieferanten zu machen. Das trägt einerseits zur sorgfältigen *Auswahl* und – bei entsprechend gezielter Formulierung des Vertragsinhaltes – zur *Instruktion* des Lieferanten bei. Die dem Lieferanten überbundenen Vertragsinhalte sind Grundlage und Schranken der Aufsicht zugleich.

5.1.4. Bildung von Kategorien

Nach dem Vorerwähnten und auf Grundlage der Systematik des ISG drängt es sich auf, die mit den Lieferanten abgeschlossenen Rechtsgeschäfte in die nachfolgenden Kategorien einzuteilen, welchen gezielt jene Aufsichtsinstrumente zugewiesen werden, die dem tatsächlichen Risiko für die Sicherheit nach den Grundsätzen der Wirksamkeit, der Wirtschaftlichkeit und der Verhältnismässigkeit am besten entsprechen. Entlang der Ziffern 1–4 wird das Risiko immer kleiner.

Innerhalb der Ziffern sind die Buchstaben a–c mögliche Sachverhalte, welche aus dem Bereich der Informationssicherheit vom Rechtsgeschäft mit dem Lieferanten erfasst werden.

Kategorien (K)

- | | |
|----------|--|
| 1 | <ul style="list-style-type: none"> a Bearbeitung «geheim» klassifizierter Informationen b Verwaltung, Wartung und Überprüfung von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz» c Betrieb von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz» (externer Leistungserbringer¹⁹) |
| 2 | <ul style="list-style-type: none"> a Bearbeitung «vertraulich» oder «intern» klassifizierter Informationen oder von Personendaten sowie besonders schützenswerten Personendaten b Verwaltung, Wartung und Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz» c Betrieb von Informatikmitteln der Sicherheitsstufe «hoher Schutz» (externer Leistungserbringer) |
| 3 | <ul style="list-style-type: none"> a Bearbeitung von Informationen, die dem BGÖ²⁰ unterliegen b Verwaltung, Wartung und Überprüfung von Informatikmitteln der Sicherheitsstufe «Grundschutz» c Betrieb von Informatikmitteln der Sicherheitsstufe «Grundschutz» (externer Leistungserbringer) |
| 4 | <ul style="list-style-type: none"> a Bearbeitung von Informationen, die dem BGÖ unterliegen b Kein Umgang mit Informatikmitteln des Bundes c Kein Betrieb von Informatikmitteln (externer Leistungserbringer) |

5.2. Einsatz des risikoangemessenen Aufsichtsinstruments

5.2.1. Sehr hohe Risiken

In der Kategorie **1** kann das Rechtsgeschäft mit dem Lieferanten einen *sicherheitsempfindlichen öffentlichen Auftrag* (Ziff. IV. Anhang 1) beinhalten. Das Sicherheitsrisiko bewegt sich regelmäßig im sehr hohen Bereich, weshalb diese Lieferanten besondere Schutzkonzepte umzusetzen haben und eingehend zu überwachen sind. Folgende Aufsichtsinstrumente erscheinen als risikoangemessen:

K 1 a Selbstdeklaration / Kontrolle / Besuche / Audit durch Auftraggeberin

K 1 b Selbstdeklaration / ISMS / Externes Audit und Zertifikat / Audit durch Auftraggeberin

¹⁹ Unter den externen Leistungserbringern sind auch die **Cloud-Dienstleister** zu verstehen. Das typische Merkmal ist einerseits der für die Auftraggeberin flexible und wirtschaftlich günstige Zugriff auf die bereitgestellten Rechenkapazitäten für die Informationsverarbeitung, andererseits aber auch die Datenhaltung außerhalb des Herrschaftsbereichs der Auftraggeberin.

²⁰ Öffentlichkeitsgesetz (SR 152.3)

K 1 c Selbstdeklaration / ISMS / Externes Audit und Zertifikat / Audit durch Auftraggeberin / Besuche

Substitution und Beizug von Sublieferanten müssen vertraglich mindestens einer *Genehmigungspflicht* im Einzelfall unterstellt werden. Ist es dem Lieferanten objektiv möglich, die vertragliche Leistung alleine zu erfüllen, sollen die Substitution und der Beizug von Sublieferanten verboten werden. Der Lieferant ist in jedem Fall zu verpflichten, die Einhaltung der festgelegten Sicherheitsmassnahmen auf den Substituenten oder Sublieferanten zu überbinden.

5.2.2. Hohe Risiken

In der Kategorie **2** kann das Rechtsgeschäft mit dem Lieferanten ebenfalls einen sicherheitsempfindlichen öffentlichen Auftrag (Ziff. IV. Anhang 1) oder die Bearbeitung von «intern» klassifizierten Informationen oder von Personendaten und besonders schützenswerten Personendaten beinhalten. Das Sicherheitsrisiko bewegt sich im hohen Bereich. Diese Lieferanten sind eingehend zu überwachen. Folgende, in der *Kompetenz der Auftraggeberin* liegende Aufsichtsinstrumente erscheinen als risikoangemessen:

K 2 a Selbstdeklaration / Kontrolle / Besuche / Audit durch Auftraggeberin

K 2 b Selbstdeklaration / ISMS / Externes Audit und Zertifikat

K 2 c Selbstdeklaration / ISMS / Externes Audit und Zertifikat / Besuche

Substitution und Beizug von Sublieferanten sollten nur auf Grundlage einer vorgängigen *verbindlichen Deklaration* von Substituenten und Lieferketten möglich sein. Die Auftraggeberin muss sich in jedem Fall den Ausschluss von Substituenten und Subunternehmen vorbehalten. Ist es dem Lieferanten objektiv möglich, die vertragliche Leistung alleine zu erfüllen, sollen die Substitution und der Beizug von Sublieferanten verboten werden. Der Lieferant ist in jedem Fall zu verpflichten, die Einhaltung der festgelegten Sicherheitsmassnahmen auf den Substituenten oder Sublieferanten zu überbinden.

5.2.3. Mittlere Risiken

In der Kategorie **3** beinhaltet das Rechtsgeschäft mit dem Lieferanten keinen sicherheitsempfindlichen öffentlichen Auftrag. Die betroffenen Informationen sind im Sinne des BGÖ grundsätzlich öffentlich zugänglich. Das Sicherheitsrisiko bewegt sich im mittleren bis tiefen Bereich. Diese Lieferanten sind zu überwachen. Folgende, in der *Kompetenz der Auftraggeberin* liegende Aufsichtsinstrumente erscheinen als risikoangemessen:

K 3 a Selbstdeklaration / Kontrolle / Besuche

K 3 b Selbstdeklaration / Kontrolle / Besuche

K 3 c Selbstdeklaration / Audit / Besuche

Substitution und Beizug von Sublieferanten müssen vertraglich mindestens einer *Meldepflicht* im Einzelfall mit Widerspruchsrecht der Auftraggeberin unterstellt werden. Der Lieferant ist in jedem Fall zu verpflichten, die Einhaltung der festgelegten Sicherheitsmassnahmen auf den Substituenten oder Sublieferanten zu überbinden.

5.2.4. Geringe Risiken

In der Kategorie 4 beinhaltet das Rechtsgeschäft mit dem Lieferanten einen *öffentlichen Auftrag* ohne besondere Informationsschutzbedürfnisse. Die betroffenen Informationen sind im Sinne des BGÖ grundsätzlich öffentlich zugänglich. Das Sicherheitsrisiko bewegt sich im tiefen Bereich. Bei diesen Lieferanten sind aus Kosten-Nutzen-Überlegungen nur geringfügige Aufsichtshandlungen oder gar keine zu vollziehen. Folgende, in der *Kompetenz der Auftraggeberin* liegende Aufsichtsinstrumente erscheinen als risikoangemessen:

K 4 a Selbstdeklaration / Kontrolle / Keine

K 4 b Keine

K 4 c Keine

Substitution und Beizug von Sublieferanten können grundsätzlich zugelassen werden. Der Lieferant ist in jedem Fall zu verpflichten, die Einhaltung der festgelegten Sicherheitsmassnahmen auf den Substituenten oder Sublieferanten zu überbinden.

5.3. Überprüfung des Mitteleinsatzes

Der vorliegende Bericht betrachtet die Mittelknappheit (personell und finanziell) für die Aufsicht als Konstante, was zwar den risikobasierten Ansatz alternativlos macht, jedoch nicht bedeutet, dass die Mittelallokation nicht von Zeit zu Zeit überprüft werden sollte. Auslösende Elemente für solch eine Lagebeurteilung wären zum Beispiel:

- neue Technologien,
- eine auffällige Erhöhung des Anteils ausländischer Lieferanten oder die Häufung von Übernahmen von schweizerischen Lieferanten durch ausländische Organisationen,
- eine Verschlechterung der allgemeinen Sicherheitslage,
- eine auffällige Häufung von Sicherheitsvorfällen bei Lieferanten,
- die zunehmende Abhängigkeit von systemrelevanten²¹ Lieferanten.

Mittelallokation setzt Entscheidungskompetenz, in der Regel auf hoher politischer Ebene, voraus, weshalb sie von Bedarfs- und Beschaffungsstellen oder Sicherheitsorganisationen nur bedingt beeinflusst werden kann. Diesen Stellen obliegt aber die vorgenannte Lagebeurteilung sowie eine angemessene Berichterstattung an die Entscheidorgane, um allenfalls mittelbar auf die zur Verfügung stehenden Mittel einzuwirken.

5.4. Retrospektive auf das «Österreichischer Modell»

Nach nun erfolgter Analyse sei nochmals kurz auf das sog. «Österreichischer Modell» zurückgeblickt. Die nachfolgende Aufzählung wiederholt nochmals die Eckpunkte des Modells, in Klammer sind die jeweiligen Berichtsziffern vermerkt, wo die einzelnen Punkte abgehandelt werden:

- Vorgabenkatalog (2.2.2.),
- eine Selbstdeklaration der Anbieterin (4.3.1.),

²¹ Der Ausfall systemrelevanter Lieferanten würde z. B. bewirken, dass die Bundesverwaltung oder Teile davon nicht mehr in der Lage wäre, ihre Aufgaben zu erfüllen.

- eine Auslagerung der Aufsicht an Non-Profit-Organisationen (4.5.),
- eine Auditpflicht (5.2.),
- eine Abstufung der Anforderungen (5.1.2.).

Anhang 1: Begriffe

I. Informationssicherheit

Um die Schutzkriterien²² der Vertraulichkeit, der Verfügbarkeit, der Integrität und der Nachvollziehbarkeit in der Zusammenarbeit mit Lieferanten erfüllen zu können, muss vom Lieferanten das folgende Verhalten verlangt werden (gilt auch für Substituenten und Sublieferanten):

- Der Lieferant bearbeitet die ihm anvertrauten Informationen des Bundes während der gesamten Erfüllung seiner vertraglichen Pflichten gemäss den sich aus dem ISG ergebenden Weisungen der Auftraggeberin. Das umfasst auch die Bearbeitung mit betrieblichen Informatikmitteln (Ziff. II. Anhang 1).
- Befasst sich der Lieferant mit der Verwaltung, der Wartung, der Entwicklung und/oder der Überprüfung von Informatikmitteln des Bundes, hat er dies während der gesamten Erfüllung seiner vertraglichen Pflichten gemäss den sich aus dem ISG ergebenden Weisungen der Auftraggeberin zu tun.
- Werden betriebliche Informatikmittel für die Bearbeitung von Informationen des Bundes oder für die Verwaltung, die Wartung, die Entwicklung und/oder die Überprüfung von Informatikmitteln des Bundes eingesetzt, müssen diese bezüglich Sicherheit mindestens dem jeweils aktuellen Stand der Technik entsprechend aufdatiert sein.
- Erbringt der Lieferant mit betrieblichen Informatikmitteln Leistungen, die mit einem Leistungserbringer nach Artikel 9 VDTI vergleichbar sind, hat er die gleichen Vorgaben zu erfüllen wie der Letztere.

II. Informatikmittel

Gemäss Artikel 5 Buchstabe a ISG gelten als Informatikmittel alle Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen.

Innerhalb dieser Definition gilt es für die Zusammenarbeit mit Lieferanten zu unterscheiden zwischen:

- *Informatikmitteln des Bundes*: Hierbei handelt es sich um Informatikmittel, die von einem internen IKT-Leistungserbringer nach Artikel 9 VDTI verwaltet, betrieben, gewartet, kontrolliert und/oder überprüft werden.
- *betrieblichen Informatikmitteln*: Hierbei handelt es sich um Informatikmittel, deren Verwaltung, Betrieb, Wartung, Kontrolle und/oder Überprüfung in der Verantwortung des Lieferanten liegt und deren Eigentümer er in der Regel ist (Server, Rechenzentren, Clouds).

III. Öffentlicher Auftrag

Ein öffentlicher Auftrag ist gemäss Artikel 8 Absatz 1 BÖB²³ ein Vertrag, der zwischen Auftraggeberin und Lieferant abgeschlossen wird und der Erfüllung einer öffentlichen Aufgabe dient. Er ist gekennzeichnet durch seine Entgeltlichkeit sowie den Austausch von Leistung und

²² Vgl. Artikel 6 Absatz 2 ISG.

²³ Bundesgesetz über das öffentliche Beschaffungswesen (SR 172.056.1)

Gegenleistung, wobei die charakteristische Leistung durch den Lieferanten (Anbieterin) erbracht wird.

IV. Sicherheitsempfindlicher öffentlicher Auftrag

Zu den sog. sicherheitsempfindlichen Tätigkeiten gehören nach Artikel 5 Buchstabe b ISG die Bearbeitung von «vertraulich» oder «geheim» klassifizierten Informationen, die Verwaltung, der Betrieb, die Wartung und die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» sowie der Zugang zu Sicherheitszonen, insbesondere zu Schutzzone 2 oder 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen. Ein sicherheitsempfindlicher öffentlicher Auftrag beinhaltet mindestens eine dieser Tätigkeiten.

V. Auftraggeberin

a. Vorbemerkung

Das ISG bezeichnet die Behörde oder Organisation des Bundes, welche einen öffentlichen Auftrag vergibt, mit dem allgemeinen Begriff «Auftraggeberin» (vgl. Art. 51, 53, 54, 58, 60, 61, 62, 63, 67, 71). Ein Blick ins Beschaffungsrecht zeigt jedoch, dass die nachfolgenden Differenzierungen zwingend nötig sind.

b. Bedarfsstelle

Gemäss Artikel 2 Buchstabe c Org-VöB²⁴ handelt sich um eine Einheit der zentralen oder dezentralen Bundesverwaltung, die zur Erfüllung ihrer Aufgaben Waren und Dienstleistungen benötigt.

c. Zentrale Beschaffungsstelle

Zentrale Beschaffungsstellen²⁵ sind gemäss Artikel 2 Buchstabe b Org-VöB Einheiten der zentralen Bundesverwaltung, die für die Bedarfsstellen Waren und Dienstleistungen zentral beschaffen. Bei sicherheitsempfindlichen öffentlichen Aufträgen übernimmt die zentrale Beschaffungsstelle gemäss Artikel 12 Org-VöB im Einvernehmen mit der Bedarfsstelle die Aufgaben einer Auftraggeberin nach den Artikeln 55–67 ISG.

d. Delegationsempfängerin

Delegationsempfängerinnen sind Bedarfsstellen, die auf Antrag und in begründeten Ausnahmefällen die Kompetenz erhalten, Waren und Dienstleistungen, deren Beschaffung eigentlich den zentralen Beschaffungsstellen vorbehalten ist, selber zu beschaffen. Ab dem Zeitpunkt der Delegation obliegen der Delegationsempfängerin die Rechte und Pflichten einer zentralen Beschaffungsstelle (Art. 17–20 Org-VöB).

²⁴ Verordnung über die Organisation des öffentlichen Beschaffungswesen der Bundesverwaltung (SR 172.056.15)

²⁵ Zentrale Beschaffungsstellen nach Artikel 5 Org-VöB: Bundesamt für Bauten und Logistik, Bundesamt für Rüstung, Bundesamt für Strassen, Bundesreisezentrale.

e. **Dezentrale Beschaffungsstelle**

Wenn Waren und Dienstleistungen nicht der zentralen Beschaffung unterliegen, so beschaffen die Bedarfsstellen eigenständig (Art. 22 Abs. 1 Org-VöB). Bei sicherheitsempfindlichen öffentlichen Aufträgen übernimmt die dezentrale Beschaffungsstelle gemäss Artikel 26 Org-VöB alle Aufgaben einer Auftraggeberin nach den Artikeln 49–69 ISG.

VI. Lieferant

Der Begriff «Lieferant» stammt aus der Org-VöB und wird für den vorliegenden Bericht gleichbedeutend verwendet mit:

- dem Begriff der *Anbieterin* nach BöB, und
- dem Begriff des *Betriebs* nach ISG.

Gemäss Artikel 3 Buchstabe a BöB handelt es sich somit um eine natürliche oder juristische Person des privaten oder öffentlichen Rechts oder eine Gruppe solcher Personen, die Leistungen anbietet, sich um die Teilnahme an einer öffentlichen Ausschreibung, die Übertragung einer öffentlichen Aufgabe oder die Erteilung einer Konzession bewirbt.

VII. Sublieferant und Substituent

Sublieferanten beteiligen sich an der Erfüllung der vertraglichen Verpflichtung eines Lieferanten, ohne mit der Auftraggeberin in einem Vertragsverhältnis zu stehen. Er tut dies entweder direkt gegenüber einem Lieferanten oder, als Teil einer Lieferkette, gegenüber einem anderen Sublieferanten.

Substituenten erfüllen die vertragliche Leistung direkt gegenüber der Auftraggeberin, jedoch anstelle des vertraglich gebundenen Lieferanten, aber ohne mit der Auftraggeberin in einem Vertragsverhältnis zu stehen.

VIII. Geheimnis/Geheimnisherr

Als *Geheimnisse* gelten nach bundesgerichtlicher Rechtsprechung²⁶ Tatsachen, die weder offenkundig noch allgemein zugänglich sind (relative Unbekanntheit), die ein *Geheimnisherr* geheim halten möchte (Geheimhaltungswille) und an deren Geheimhaltung der Geheimnisherr ein objektiv berechtigtes Interesse hat (objektives Geheimhaltungsinteresse).

IX. Aufsicht

Im demokratischen Rechtsstaat ist unter Aufsicht die Befugnis einer übergeordneten Stelle, Handlungen zu veranlassen, zu überprüfen und zu korrigieren, zu verstehen. Die Kriterien der Aufsicht sind²⁷:

- *Rechtmässigkeit*: wird geltendes Recht eingehalten?
- *Ordnungsmässigkeit*: werden interne Weisungen beachtet?
- *Zweckmässigkeit*: ist ein Umsetzungsmodell zweckmässig?
- *Wirksamkeit*: stimmt das Verhältnis zwischen geplanten und erzielten Wirkungen?

²⁶ Vgl. z. B. BGE 142 II 268.

²⁷ Vgl. Artikel 26 Absatz 3 Parlamentsgesetz (SR 171.10)

- *Wirtschaftlichkeit*: stimmt das Verhältnis zwischen Mitteleinsatz und Leistungen?

Aus der jahrelangen Erfahrung der Fachstelle Betriebssicherheit (früher Fachstelle Industriesicherheit des VBS) können folgende Kategorien einer umsetzbaren Aufsicht bei Lieferanten unterschieden werden (Beschrieb und Leistungsprofile der verschiedenen Instrumente in Ziff. 4.2. und 4.3.):

- Kontrollen,
- Besuche,
- Audits,
- Selbstdeklarationen,
- Externe Auditierung mit Zertifizierung,
- Informationssicherheitsmanagementsysteme.

Anhang 2: Formen staatlichen Handelns

I. Informelles Verwaltungshandeln: Realakt

Die sog. Realakte kommen formlos zustande und zielen darauf ab, das Verhalten des Adressatenkreises zu beeinflussen²⁸, ohne dass jedoch bei Nichtbefolgung eine Rechtsfolge damit verbunden wäre. Beispiele solch tatsächlichen oder schlichten Verwaltungshandelns sind etwa Auskünfte, Belehrungen, Empfehlungen, Warnungen, amtliche Berichte oder Vernehmlassungen²⁹.

Dieses Instrument ist insbesondere für Behörden und Organisationen von grossem Wert, welche nicht über vom Recht verliehene Aufsichts- und Vollzugskompetenzen verfügen (z. B. Fachstellen).

II. Rechtliches Verwaltungshandeln: Verfügung

Die Grundform staatlichen Handelns ist die Verfügung nach Artikel 5 VwVG³⁰. Es handelt sich dabei um eine Anordnung der Behörde im Einzelfall, die sich auf öffentliches Recht des Bundes stützt und insbesondere die Begründung, Änderung oder Aufhebung von Rechten und Pflichten des Adressaten zum Gegenstand hat.

Verfügungen haben damit grundsätzlich zwingenden Charakter und können von einer Rechtsmittelinstanz überprüft, aufgehoben oder an die erlassende Behörde zum Neuentscheid zurückgewiesen werden. Ihr Zustandekommen bedingt das Durchlaufen aller Prozessschritte des jeweils anwendbaren Verfahrensrechts.

III. Rechtliches Verwaltungshandeln: Verwaltungsrechtlicher Vertrag

Das Instrument des verwaltungsrechtlichen Vertrags ist dann angezeigt, wenn eine staatliche Aufgabe durch Schaffung einer dauerhaften Rechtsbeziehung besser erledigt werden kann als durch einen einseitigen hoheitlichen Einzelakt. Er dient unmittelbar der Erfüllung einer öffentlichen Aufgabe. Für den vorliegenden Bericht ist insbesondere der sog. subordinationsrechtliche Vertrag, geschlossen zwischen dem Staat und Privaten, von Interesse. Der Staat handelt jedoch bei dieser Vertragsform immer noch als Hoheitsträger und muss sich dabei stets eine Kontrollmöglichkeit vorbehalten. Die Prinzipien von Artikel 5 BV bleiben massgebend (vgl. Ziff. 2.2.1.1).

Der subordinationsrechtliche Vertrag hat damit wie die Verfügung zwingenden Charakter. Die Überprüfung durch eine Rechtsmittelinstanz geschieht häufig dadurch, dass bei Streitigkeiten der Erlass einer Verfügung erwirkt wird, welche dann dem Instanzenzug einer solchen folgen wird.³¹

IV. Rechtliches Verwaltungshandeln: Privatrechtlicher Vertrag

Güter und Dienstleistungen, die am Markt erhältlich sind, beschafft der Staat üblicherweise wie jeder andere Einkäufer mittels privatrechtlicher Verträge. Der Markt bietet heute insbesondere

²⁸ Z. B. Plakate, die vor den Gefahren des Rauchens warnen, Einladungen zur Gemeindeversammlung, behördliche Informationsveranstaltungen etc.

²⁹ [Vgl. hierzu KLEY, Andreas, *Verwaltungsverfahrenrecht, Ziffer 3.2, Lehrstuhl für öffentliches Recht, Verfassungsgeschichte sowie Staats- und Rechtsphilosophie*](#)

³⁰ Verwaltungsverfahrensgesetz (SR 172.021).

³¹ [Vgl. hierzu KLEY, Andreas, *Verwaltungsverfahrenrecht, Ziffer 3.3.3, Lehrstuhl für öffentliches Recht, Verfassungsgeschichte sowie Staats- und Rechtsphilosophie*](#)

im Dienstleistungssektor zahlreiche Angebote, die für den Staat auch im Bereich der Aufsicht interessant sein können.