Rika Koch, Lara Biehl, Thomas M. Fischer

Alles neu?
Die Beschaffungswelt im Wandel

Konferenzband zur 12. IT-Beschaffungskonferenz der Berner Fachhochschule BFH und der Universität Bern

weblaw

Rika Koch, Lara Biehl, Thomas M. Fischer

Alles neu?
Die Beschaffungswelt im Wandel.

Konferenzband zur 12. IT-Beschaffungskonferenz am 22. August 2023 der Berner Fachhochschule BFH und der Universität Bern

Tagungsband

Editions Weblaw, Bern 2024

O Codex
I Commentatio
II **Colloquium**
III Dissertatio
IV Doctrina
V Liber amicorum
VI Magister
VII Monographia
VIII Thesis
IX Scriptum
X Anthologia

Editions Weblaw

ISBN 978-3-03916-218-5 (Print)

INHALTSVERZEICHNIS

Einleitung: Die IT-Beschaffungskonferenz 2023 – die Beschaffungswelt im Wandel 1
Thomas M. Fischer

«Es muss anders werden, wenn es gut werden soll» – Die Beschaffungswelt im Wandel 11
Marco Fetz / Lara Biehl

Open Source Software im EMBAG 21
Rika Koch / Simon Schlauri

Abhängigkeiten von ICT-Herstellern reduzieren: Wiederkehrende Wartungsverträge, Vermeidung von «Ausnahmefreihändern», Beschaffung von Open Source Software etc. 39
Chantal Lutz / Cédric Miehle

Soziale Nachhaltigkeit in der Beschaffung von IKT-Produkten 55
Lara Biehl

Öffentliche Beschaffungen und ESG 83
Paula Zimmermann

Datensicherheit und Meldepflichten nach DSG und ISG im Beschaffungsprozess 99
Nicole Beranek Zanon

Ich bin jung und muss noch lernen? 113
Sven Kohlmeier

Cloud und Datenschutz – Was ist zu beachten? 135
Dominika Blonski

Gemeinsame Beschaffungen – Möglichkeiten und Grenzen 155
Martin Zobl

Die Schlüsselrolle des Pflichtenhefts in Ausschreibungen 171
Josef Schreiber / Roland Füllemann

Abkürzungsverzeichnis 189

EINLEITUNG: DIE IT-BESCHAFFUNGSKONFERENZ 2023 – DIE BESCHAFFUNGSWELT IM WANDEL

Thomas M. Fischer

Thomas M. Fischer ist Rechtsanwalt, stellvertretender Leiter des Amts für Informatik und Organisation des Kantons Bern (KAIO) sowie Vorsitzender der kantonalen Beschaffungskonferenz.

«Die Beschaffungswelt im Wandel» – der Titel der diesjährigen IT-Beschaffungskonferenz fasst die Herausforderungen zusammen, denen sich die IT-Beschaffungsverantwortlichen der öffentlichen Hand sowie die IT-Branche gegenüberstehen. Der Wandel ist sowohl rechtlicher wie auch technischer und wirtschaftlicher Natur:

Zum einen sind die Kantone mitten im Prozess der Einführung des total revidierten öffentlichen Beschaffungsrechts, das sie in der IVöB 2019 kodifiziert haben. Dies tun sie im gewohnt gemächlichen föderalistischen Tempo. Am 1. Oktober 2023 war die IVöB 2019 erst in vierzehn Kantonen in Kraft (AG, BL, BS, AI, BE, FR, GR, LU, SG, SO, SH, SZ, TG, UR, VD, ZH), während sich sechs im Beitrittsverfahren befanden (NE, GL, JU, NW, VS, ZG). Vier Kantone (AR, GE, OW, TI) hatten das Beitrittsverfahren noch nicht gestartet, womit sie weiterhin die bisherige IVöB 1994/2001 anwenden.[1] Rund vier Jahre nach dem Beschluss des revidierten Konkordats und fast drei Jahre nach dem Inkrafttreten des neuen Rechts für den Bund wenden damit immer noch fast die Hälfte der Kantone das alte Recht an.

Dies ist eine Herausforderung vor allem für die landesweit tätigen Anbieter von IT-Leistungen: Sie müssen sich nicht nur weiterhin mit den (auch im neuen Recht teils fortbestehenden) Eigenheiten des kantonalen öffentlichen Beschaffungsrechts auseinandersetzen,[2] sondern müssen auf absehbare Zeit je nach Kanton sowohl das neue wie auch das alte Recht berücksichtigen. Das verstärkt einen in der Praxis noch wenig diskutierter Trend: Angesichts der Kleinräumigkeit der Schweiz und der entsprechend geringen Grösse der

---

1 Schweizerische Bau-, Planungs- und Umweltdirektoren-Konferenz BPUK, 2023.

2 Siehe zu den Unterschieden auch Beitrag von Martin Zobl in diesem Band, Kapitel 7.

einzelnen kantonalen und kommunalen IT-Beschaffungsaufträge führt die langsame Harmonisierung dazu, dass führende nationale und internationale IT-Anbieter sich noch häufiger als bisher dafür entscheiden werden, an öffentlichen Beschaffungsverfahren *nicht* teilzunehmen. Für sie rechtfertigt das relativ geringe Auftragsvolumen den Aufwand für das Ausarbeiten eines Angebots und die Auseinandersetzung mit den Besonderheiten des kantonalen Beschaffungsrechts und der Beschaffungspraxis oftmals nicht. Dies schränkt den Markt in wettbewerblichen Verfahren ein und kann IT-Auftraggeber dazu verleiten, noch häufiger auf das freihändige Verfahren zurückzugreifen, um marktführende Lösungen berücksichtigen zu können, als sie dies ohnehin schon tun.[3] Die föderale Fragmentierung des öffentlichen Beschaffungsrechts in der Schweiz wird damit immer deutlicher zum Risiko für den funktionierenden Binnenmarkt.[4]

Dabei wäre bereits der technische und wirtschaftliche Wandel Herausforderung genug. Zu den Metatrends, die die IT-Branche bereits in den letzten Jahren im Atem hielten – Nachhaltigkeit, Lieferengpässe, Cybersicherheit, Fachkräftemangel, Cloud Computing – gesellte sich 2023 erstmals in vollem Umfang die künstliche Intelligenz (KI), nachdem der durchschlagende Erfolg von generativen KI-Systemen wie ChatGPT zu einem Wettrüsten der grossen Technologiekonzerne und zur raschen Integration von KI-Modellen in Endbenutzerprodukte wie Suchmaschinen und Office-Anwendungen führte. Vor diesem Hintergrund erstaunt es nicht, dass sich am 22. August 2023 an der ausgebuchten IT-Beschaffungskonferenz 2023 über 400 Fachleute aus dem öffentlichen Beschaffungswesen und der Informatikbranche im Von-Roll-Areal in Bern versammelten, um sich über diese Herausforderungen auszutauschen, und um sich über neue Grundlagen und Trends in der öffentlichen Beschaffung und bei IT-Ausschreibungen zu informieren.

---

3 In der Schweiz werden rund 40% der auf simap.ch publizierten IT-Zuschläge im freihändigen Verfahren vergeben, aber nur rund 20% aller Zuschläge gesamthaft (siehe für die Visualisierung dieser Statistik Intelliprocure.ch).

4 Abhilfe schaffen könnten hier gemeinsame Beschaffungen, siehe Beitrag von Martin Zobl in diesem Band.

1. DIE BEITRÄGE DER IT-BESCHAFFUNGSKONFERENZ 2023

Einleitend zeigte **Benedikt Würth,** Ständerat des Kantons St. Gallen (Die Mitte) die «**Druckstellen zwischen dem Beschaffungsrecht und der Politik**» auf. Er stellte die Erwartungen der Politik an eine neue Vergabekultur vor, wie den verstärkten Fokus auf die Qualität statt nur den Preis sowie die Berücksichtigung der Nachhaltigkeit. Diese Forderungen, so Ständerat Würth, fordern die Auftraggeber heraus: Halten sie sich weiterhin an «harte», einfach zu bewertende Kriterien wie den Preis, oder nutzen sie den erweiterten Werkzeugkasten des neuen Rechts, zu dem verstärkt auch «weiche», nichtpreisliche Kriterien gehören, die aber mit mehr Aufwand und vermutet höheren Beschwerderisiken verbunden sind? Die angestrebte neue Vergabekultur verlangt laut Ständerat Würth nach mehr Professionalität im Vergabeverfahren. Er führte aus, wie der Kanton St. Gallen das neue Beschaffungsrecht umsetzt und mit einem E-Government-Gesetz die staatsebenenübergreifende Zusammenarbeit und die Nutzung von Skaleneffekten bei der Digitalisierung verbessern will.

Den Blick aus der Praxis auf diese Fragestellungen vermittelte anschliessend **Marco Fetz** (Leiter Projektbeschaffung Tiefbau der SBB), und forderte: «**Es muss anders werden, wenn es gut werden soll**». Er wies darauf hin, dass die methodischen Neuerungen des neuen Rechts wie Rahmenverträge oder Digitalisierung weitgehend Forderungen und Ansätze der Praxis aufgreifen und legitimieren. Seiner Meinung nach verlangt der disruptive Wandel im IT-Beschaffungswesen nach Mut der Beschaffenden, den vom Gesetzgeber geschaffenen Spielraum auszunutzen und Beschaffungen neu zu gestalten, um den Herausforderungen zu begegnen. In der anschliessenden Diskussionsrunde waren sich Marco Fetz und Bundesverwaltungsrichter **Marc Steiner** einig, dass das Gesetz weniger wichtig ist als die Ausnützung seiner Ermessensspielräume durch die Beschaffenden. **Dr. Daniel Markwalder,** Delegierter des Bundesrates für digitale Transformation und IKT-Lenkung, hielt dem die Risikowahrnehmung der Projektverantwortlichen entgegen: «Das grösste Risiko ist das Beschaffungsrecht. Einfach keine Beschwerde, dann sind wir tot», höre er oft. Er unterstrich, dass es für einen Vergabekulturwandel beide Seiten brauche.

In der ersten Fachsession, «**Beschaffung von Cloud-Leistungen**», beschrieb **Martin Strässler** (Head of Sourcing Advisory, rete AG), die «Vergleichbarkeit von Cloud und On-Premise Angeboten in einer Submission»: Die Herausforderung, unterschiedliche Bereitstellungsmodelle von IT-Leistungen (Cloud oder on premise) vergleichbar zu machen, kann seiner Meinung nach mit verschiedenen Ansätzen gelöst werden: man fällt den Modellentscheid vorab, oder schreibt lösungsneutral aus – mit oder ohne modellspezifische Rangliste. Einen Dialog oder bei fehlendem Wettbewerb auch eine freihändige Vergabe hielt er ebenfalls für prüfenswert. Anschliessend ging **David Rosenthal** (Partner, VISCHER AG) auf die «datenschutzrechtliche[n] Anforderungen an eine Cloud-Ausschreibung – und die resultierenden Knacknüsse für das Beschaffungsrecht» ein. Er beschrieb Methoden, wie das von ihm erarbeitete Hilfsmittel CCRA-PS, mit denen die vielfältigen Cloud-Datenschutzrisiken bewertet und behandelt werden können. Seiner Meinung nach sind Erfolgsfaktoren bei Cloud-Beschaffungen eine Standardisierung der Vertragsbedingungen v.a. der Hyperscaler auf einem für öffentliche Organe akzeptablen Niveau, und mehr Erfahrungsaustausch unter den Beschaffenden, weil sich die Projekte und Lösungen oft stark ähneln.

In der Fachsession «**Agilität in der Beschaffung**» fragte **Sebastian Strzelczyk** (ti&m) zuerst: «HERMES 2022 und Agilität – Was ändert in der Beschaffung?». Er beschrieb die in der neuesten HERMES-Fassung vorgesehenen agilen Projektmanagementmethoden und hob die organisatorischen und kulturellen Voraussetzungen hervor, die agile Projekte erfolgreich machen. «Der agile Festpreis mit Scrum» war anschliessend das Thema von Michael Kaufmann (CEO Xebia/Xpirit Germany). Er zeigte auf, wie man mit Kooperationsverträgen, welche die Interessen beider Seiten ausgleichen, mit agilem Anforderungsmanagement und agilen Schätzmethoden das toxische Feilschen über die Mehrkosten von Changes vermeiden kann. Und **Max Reichen** (Legal, Procurement Specialist, Liip AG) stellte unter dem Titel «Agile Beschaffung – Ja, aber…» vor, wie im Rahmen des öffentlichen Beschaffungsrechts möglichst gute Voraussetzungen für agile Projekte geschaffen werden können. Dazu gehören seiner Meinung nach z.B. ein entschädigtes Vorprojekt im Rahmen eines Dialogs, oder die Durchführung von Wettbewerben.

«**Beschaffung und Open Source Software**» war das Thema der dritten Fachsession. **Simon Schlauri** (Partner, Ronzani Schlauri Anwälte) stellte zunächst den Stellenwert

von «Open Source Software [OSS] im neuen Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG)» dar. Wie er zeigte, sieht das EMBAG grundsätzlich die Freigabe von Bundes-Software als OSS vor.[5] **Chantal Lutz und Cédric Miehle** (beide Senior Associate, Domenig & Partner Rechtsanwälte AG) ging es anschliessend darum, wie man die «Abhängigkeiten von ICT-Herstellern reduzieren» kann. Sie beschrieben den Einsatz von OSS als Ansatz dazu und hoben hervor, dass der Auftraggeber verpflichtet sei, wettbewerbsausschliessende Situationen, die zu Folge-Freihandvergaben zwingen, zu vermeiden. Abschliessend stellte **Clarisse Schröder** (Consultant, APP Unternehmensberatung AG) «OSS-Beispiele aus der öffentlichen IT in Deutschland» vor. Dort koordiniere etwa das nationale «Zentrum digitale Souveranität» auf der Basis von OSS die Erarbeitung eines «souveränen Arbeitsplatzes», der bis Ende 2023 verfügbar sein soll.

Die Fachsession «**Supply Chain Management und Nachhaltigkeit**» eröffnete **Lara Biehl** (wissenschaftliche Assistentin, IPST) mit dem Thema «Soziale Verantwortung beim Einkauf von IKT-Produkten: Herausforderungen und Möglichkeiten bei der Überprüfung der ILO-Kernarbeitsnormen». Sie empfahl, auf der Basis einer länderspezifischen Risikoanalyse Nachweise unabhängiger Dritter einzuverlangen, wie die Mitgliedschaft in einer Standard-Initiative mit Auditbericht (z.B. amfori, BSCI oder RBA), ein Produktzertifikat (z.B. TCO-Certified), ein Fabrikzertifikat (z.B. SA-8000), oder die Überprüfung durch «Electronics Watch». **Andrea Fimian** (CEO und Gründerin, fips consulting) fragte anschliessend nach «Diversität und Inklusion in der Lieferkette?». Sie beschrieb, wie Unternehmen unter dem Titel «Supply Chain Diversity & Inclusion» unterrepräsentierte Gruppen wie Frauen, ethnische Minderheiten, LGBTIQ+-Personen und Menschen mit Beeinträchtigungen in ihrer Lieferkette berücksichtigen, und wie das Schweizer, EU-, US- und UK-Beschaffungsrecht diese Themen adressieren. Und **Paula Zimmermann** (Rechtsanwältin, Laux Lawyers AG) zeigte auf, wie «ESG in Lieferantenverträgen» berücksichtigt werden kann. Sie stellte die gesetzlichen Vorschriften zur «environmental and social governance» und zur Berichterstattung darüber in der EU und der Schweiz vor. Sie empfahl, die Anbieter auf der Basis einer Analyse der spezifischen Lieferkette

[5] Der Verfasser dieser Einleitung erlaubt sich an dieser Stelle den Hinweis, dass dies seit März 2023 auch im Recht des Kantons Bern gilt; vgl. Art. 26 des Gesetzes vom 7. März 2022 über die digitale Verwaltung (DVG); siehe dazu näher: www.be.ch/dvg.

vertraglich zur Berichterstattung und auf KPIs für ESG-Aspekte zu verpflichten, sowie auf Standards oder Zertifizierungen.

Während der Mittagspause hatten die Teilnehmenden die Gelegenheit, unter dem Titel «**Ask a lawyer**» drei auf öffentliche Beschaffungen spezialisierten Anwältinnen und Anwälten – **Dr. Wolfgang Straub** (Krneta Avokatur Notariat), **Julia Bhend** (Probst Partner) und **Dr. Christoph Jäger** (Kellerhals Carrard) – Fragen aus ihrer Praxis zu stellen. Unter dem Titel «**Ask a Consultant**» stellten sich die Berater **Roland Füllemann** (IT-Beschaffungsberater, example consulting gmbh) und **Josef Schreiber** (Inhaber, Schreiber IT-Consulting) am Ende der Konferenz ebenfalls zur Beantwortung von Fragen zur Verfügung.

In der Fachsession «**KI und Informationssicherheit**» behandelte **Sven Kohlmeier** (Partner, Wicki Partners AG Rechtsanwälte) anhand der Frage «Ich bin jung und muss noch lernen?» rechtliche und ethische Themen in der Beschaffung von KI im öffentlichen Sektor. Ihm zufolge darf der Staat zwar grundsätzlich KI-Software beschaffen und einsetzen, muss aber Grundrechte beachten und sein Handeln auf gesetzliche Grundlagen stützen. Der Staat müsse namentlich Fragen des Datenschutzes, der Haftung, des geistigen Eigentums und des Berufsgeheimnisses klären, und bei der Vorbereitung von Entscheiden mit KI auch solche des rechtlichen Gehörs und der Ermessensausübung. Vor dem Hintergrund dieser und ethischer Fragen des KI-Einsatzes empfahl Sven Kohlmeier Transparenzregeln und eine einheitliche Verwaltungspraxis für die KI-Beschaffung. **Nicole Beranek Zanon** (Partnerin, HÄRTING Rechtsanwälte AG) stellte anschliessend die «Datensicherheit und Meldepflichten nach DSG und ISG im Beschaffungsprozess» vor. Sie zeigte die Vorschriften des neuen Datenschutzgesetzes und des Informationssicherheitsgesetzes des Bundes auf, insbesondere die sich daraus für Private und Bundesorgane ergebenden Meldepflichten. Als «Revolution in der Beschaffung! GovTechs und der Public Sector» beschrieben **Jana Janze** (Geschäftsführerin, GovMarket GmbH) und **Sebastian Singler** (Senior Manager, PwC Switzerland) ihren Ansatz, um GovTechs (innovative Start-ups, die Behörden Digitalisierungstechnologien anbieten) bei Beschaffungen zu berücksichtigen. Diese könnten der Verwaltung einen Innovationsschub bringen, vor allem in Bereich von KI und Big Data, was das öffentliche Beschaffungsrecht aber oft verkompliziere.

«**Nachhaltigkeit ist Verhandlungssache**», hiess es in der nächsten Fachsession. **Ivette Djonova** (Head of Legal & Public Affairs, Swico) beschrieb den «ICT-Beschaffungsdialog», den der Branchenverband Swico mit der Bundesverwaltung führt. Dort werde etwa besprochen, was ICT-KMU brauchen, um vermehrt an Ausschreibungen teilzunehmen, oder wie Beschaffungsverfahren digitalisiert werden können. Dank Fallbesprechungen könnten Erkenntnisse aus früheren Ausschreibungen in spätere einfliessen. **Felix Elschner** (Leitung Fachbereich öffentliche Auftraggeber, Epson Deutschland GmbH) und **Ilse Beneke** (Kompetenzstelle für Nachhaltige Beschaffung, Beschaffungsamt des Bundesministeriums des Inneren) stellten anschliessend die «Soziale Nachhaltigkeit in der öffentlichen ITK-Beschaffung in Deutschland – die Verpflichtungserklärung zur Einhaltung von Arbeits- und Sozialstandards» vor. Diese Verpflichtungserklärung hätten die deutschen Behörden und der Branchenverband Bitkom gemeinsam erarbeitet, um eine praxistaugliche Umsetzung der gesetzlichen Vorschriften auf der Basis anerkannter Zertifikate (SA8000, RBA, Amfori, TCOcertified) zu ermöglichen. Sie werde Vertragsbestandteil und sehe Auditmöglichkeiten und Konventionalstrafen vor.

Die Fachsession «**Ausschreibungen im Wettbewerb um Anbieter**» begann mit einem Perspektivenwechsel: Unter dem Titel «Das Lesen und Bewerten von Zuschlagskriterien auf Anbieterseite» ermöglichten **Kathrin Kölbl** (Mitglied der Geschäftsleitung, Abraxas Informatik AG) und **Levis Pereira** (CTO, Abraxas Informatik AG) einen Schulterblick in die «Bid Calls» eines Anbieters. Sie zeigten auf, wie ein ICT-Unternehmen Ausschreibungen prüft und sich für oder gegen eine Teilnahme entscheidet. Letzteres werde umso wahrscheinlicher, je kürzer die Unterlagen sind, je höher die Qualität gewichtet wird, je mehr Zeit für das Angebot zur Verfügung steht und je transparenter und interaktiver das Verfahren ist. «Nachhaltigkeit aus Lieferantensicht – ein Erfahrungsbericht» wurde sodann von **Christian Möller** (Head of Legal, Risk & Compliance, Adnovum) und **Julian Osborne** (Gründer und CEO, Pelt8) erstattet. Anhand der Erfahrungen des Softwareherstellers Adnovum sollten Auftraggeber beurteilen können, welche Nachhaltigkeitsanforderungen sich eignen und vor welche Herausforderungen sie die Anbieter stellen. Und die «Herausforderungen und Chancen aus Anbietersicht» stellte **Magdalena Koj** (Head eGovernment, ti&m) vor. Sie beschrieb, was es für Anbieter bedeutet, bei jeder Ausschreibung aufs Neue auf die immer gleichen Kriterien eingehen

zu müssen (wie Referenzen, Lösungskonzept, Präsentation), und machte Vorschläge für ihre anbieterfreundliche Ausgestaltung.

In der letzten Fachsession, «**Gemeinsame Beschaffungen und Rahmenverträge**», blickten die Teilnehmenden noch einmal über die Grenze: **Sirko Hunnius** (Leiter Public Sector Consulting,]init[) stellte «Flächendeckende Online-Services im Föderalstaat: Das EfA-Umsetzungsmodell in Deutschland» vor. Er beschrieb, wie die die deutschen Bundes- und Landesbehörden unter dem Titel «Einer für alle» digitale Services, die von einer Behörde entwickelt und betrieben werden, allen anderen Behörden zur Verfügung stellen. Zum Thema «Gemeinsame Beschaffungen – Chancen und Stolpersteine» führte **Martin Zobl** (Partner, Walder Wyss) aus Schweizer Sicht aus, in welchen Situationen sich gemeinsame Beschaffungen anbieten und wie sie erfolgreich und rechtlich korrekt durchgeführt werden. Dabei ging er auf organisatorische Aspekte, die Wahl des anwendbaren Rechts und kartellrechtliche Schranken der Zusammenarbeit ein. Und die «Rahmenverträge in der IT-Beschaffung: das 'neue' Vergabeinstrument und seine Grenzen» stellten **Simon Oeschger** und **Benjamin Hundius** (Partner bzw. Associate, Suffert Neuenschwander & Partner) vor. Sie beschrieben die Spielarten, Mindestinhalte und Rahmenbedingungen von Rahmenverträgen im öffentlichen Beschaffungsrecht, und empfahlen den Auftraggebern namentlich, das Abrufverfahren transparent, sachlich und unter Berücksichtigung der Vergabegrundsätze auszugestalten.

Ihren Abschluss fand die IT-Beschaffungskonferenz mit dem Vortrag von **Dr. Dominika Blonski**, der die Frage aufwarf: «**Cloud und Datenschutz – Was ist zu beachten?**». Die Datenschutzbeauftragte des Kantons Zürich beschrieb, welche Datenschutzrisiken typischerweise mit einer Cloud-Auftragsdatenbearbeitung verbunden sind, und unter welchen Voraussetzungen Behörden Daten in die Cloud auslagern können: wenn dies nicht gesetzlich oder vertraglich verboten ist, und wenn die Behörden ihre datenschutzrechtliche Verantwortung wahrnehmen können, insbesondere durch risikoangemessene Massnahmen des Datenschutzes und der Informationssicherheit (ISDS). Die anschliessende Podiumsdiskussion zeigte unterschiedliche Einschätzungen David Rosenthals und Dominika Blonskis zur Tragweite des US-CLOUD-Acts und gesetzlicher Geheimhaltungspflichten auf. **Rika Koch** (BFH IPST) erwähnte die Herausforderung, ISDS mit dem Beschaffungsprozess in Einklang zu bringen. Auch Dominika Blonski stellte fest, dass ISDS-Vorschriften in Beschaffungsvorhaben oft ungenügend berück-

sichtigt würden. Sie unterstrich die grosse Verantwortung des Staates für die Daten der Bevölkerung. **Simon Graber** (Projektleiter, educa) beschrieb, wie die Fachagentur für den digitalen Bildungsraum Schweiz mit der Unterstützung des Verbands der Datenschutzbeauftragten (privatim) einen Vertrag mit Microsoft zur Nutzung der Cloudlösung M365 aushandelte, der einen Mindeststandard darstelle. **David Rosenthal** beschrieb das sorgfältige Abarbeiten der vielen Risiken bzw. Prüfpunkte als zentrale Herausforderung. Seiner Erfahrung zufolge sei das Aushandeln von mit dem Schweizer Recht konformen Verträgen mit grossen US-Anbietern zwar sehr aufwändig und zeitraubend, aber möglich – wobei es illusorisch sei, Schweizer AGB vorgeben zu wollen.

2. ZUR KONFERENZ UND ZU DIESEM BAND

Die oben zusammengefassten Konferenzbeiträge sind fast vollständig als Präsentationen und teilweise als Videos auf der Webseite der IT-Beschaffungskonferenz verfügbar.[6] Erstmals erscheint als Ergänzung zur Konferenz der vorliegende Tagungsband. Er ermöglicht es den Vortragenden, die dies wünschen, ihre Beiträge in einem wissenschaftlichen Format zu veröffentlichen, und ihre Erkenntnisse damit einem breiteren Publikum aus der Beschaffungs- und Rechtspraxis zugänglich zu machen.

Organisiert wurde die Konferenz vom Institut Public Sector Transformation (IPST) der Berner Fachhochschule (BFH) und vom Institut für Wirtschaftsinformatik (IWI) der Universität Bern. Die Konferenzleitung stellte Matthias Stürmer (IPST) sicher, und die Organisation Lara Biehl. Dem Programmkomitee gehörten Thomas M. Fischer (Amt für Informatik und Organisation des Kantons Bern, KAIO), Matthias Günter (CH Open), Greg Hernan (Digitale Verwaltung Schweiz, DVS), Rika Koch (IPST), Reto Maduz (Xebia), Daniel Markwalder (Bundeskanzlei), Mario Marti (suisse.ing), Thomas Myrach (IWI), Stephan Sutter (ti&m), Marc Steiner (IPST), Andrea Sägesser (APP Unternehmensberatung) und Wolfgang Straub (Krneta Advokatur Notariat) an.

Daneben profitierte die Konferenz von Praxis-Partnerschaften aus der öffentlichen Verwaltung und der Wirtschaft, ohne die die Konferenz nicht möglich gewesen wäre. Dazu

[6] Präsentationen: https://www.bfh.ch/wirtschaft/de/aktuell/fachveranstaltungen/it-beschaffungskonferenz-2023/detailprogramm/, Videos: https://www.youtube.com/playlist?list=PLZs42uSUfwzgrHr1Qe_GIeRnq2xLYE057.

gehören neben den Mitgliedern des Programmkomitees der Schweizerische Verband der Telekommunikation (asut), das Digital Impact Network, die Information Security Society Switzerland (ISSS), procure.ch, Swico und suisse.ing.

«ES MUSS ANDERS WERDEN, WENN ES GUT WERDEN SOLL» – DIE BESCHAFFUNGSWELT IM WANDEL

Marco Fetz / Lara Biehl

Marco Fetz (Autor des Referats) ist Leiter Einkauf Bauprojekte SBB AG, Infrastruktur.

Lara Biehl (Redaktion des Referats) ist Wissenschaftliche Assistentin an der Berner Fachhochschule

EINLEITUNG

«*Es muss anders werden, wenn es gut werden soll*»:

Das Zitat von Christoph Lichtenberg passt perfekt zum derzeitigen Stand im Beschaffungswesen. Eine neue Ära steht vor den Toren und die Transformation geht rasend schnell. ChatGPT, S4, ARIBA, Ecovadis: Diese beispielhaften Stichworte lassen uns nicht unberührt. Doch wie werden sie die IT-Beschaffung verändern? Und welche Rolle spielt dabei das neue Beschaffungsrecht? Diesen beiden Fragen widmet sich die folgende Einführung und unternimmt den Versuch, einen Ausblick auf das zu geben, was uns in den nächsten drei Jahren erwartet. Eines steht bereits fest: Wir sprechen von «Gamechangern», also grundlegenden Systemveränderungen, die viel Innovation, aber auch einige Herausforderungen versprechen.

Meine Erinnerungen an die Gründung der IT-Beschaffungskonferenz sind lebendig. Ich war von Anfang an dabei und stand am 22. August 2023, zwölf Jahre später, vor einem vollen Haus. Die Konferenz war mit 400 Teilnehmenden ausgebucht und zog zahlreiche Einkaufsspezialist*innen an. Ich konnte deshalb mit Freude zur Kenntnis nehmen, dass sich die Konferenz im Laufe der Jahre zu einer eigentlichen Institution entwickelt hat. Dabei hat sie nicht nur mehr Interesse für den Beruf geweckt, sondern sich auch kontinuierlich professionalisiert und eine engagierte Community geschaffen. Als Redner im Plenum der diesjährigen Konferenz stand ich somit vor einem Publikum, das mein Interesse an Fachthemen teilte.

Als ich vor einigen Monaten von der Konferenzorganisation gefragt wurde, ob ich bei der diesjährigen Konferenz als Plenumssprecher zur Verfügung stehen würde, habe ich schnell zugesagt. Warum? Weil der Titel passt. «**Alles neu? Beschaffungswelt im Wandel**». Zu diesem Thema wollte ich meinen Beitrag leisten und meine Sichtweise einbringen. Ständerat Benedikt Würth, mein Vorredner, beleuchtete die politische Ebene und betrachtete den Wandel von der Gesetzesebene her. Er berichtete über die Erwartungen der Politik an die neue Vergabekultur. Ich beleuchte den Wandel nun von einer etwas anderen Seite – von der Praxis der Vergabestellen aus. Die folgenden Ausführungen geben meine persönliche Meinung wieder.

DER DERZEIT LAUFENDE WANDEL IST FUNDAMENTAL

Der Wandel findet statt, und er ist grundlegend. Der Wandel hat nicht nur mit der Revision des Gesetzes zu tun, sondern auch mit einer Welt, die sich verändert. Vor allem in der IT war die zweite Art der Veränderung spürbar. Spätestens seit der Covid-Pandemie ist auch der und dem Letzten klar geworden, was mit IT alles möglich ist. Vom Home-Office über KI bis zur Digitalisierung in Städten und Gemeinden; die IT ist auf dem Vormarsch und auch die Vergabestellen beginnen zunehmend, ihre Prozesse zu digitalisieren. ChatGPT, S4, ARIBA, Ecovadis usw. – daran müssen wir uns gewöhnen.

Die Entwicklungen rund um die **künstliche Intelligenz (KI) sind für mich ein echter Gamechanger**. Ein Professor hat einmal gesagt, dass die Auswirkungen von ChatGPT für ihn so einschneidend sind wie die Einführung des Internets. Bei dem Gedanken bekomme ich Gänsehaut. Ich weiss zwar nicht, ob das stimmt, aber die Evolution der KI scheint keine gewöhnliche iterative Entwicklung zu sein. Es ist etwas Neues. Diese Situation birgt Chancen, die wir vielleicht nutzen können. Und auch der öffentliche Sektor ist bestrebt, diese neuen Möglichkeiten zu erschliessen.

Um KI zu nutzen und die Digitalisierung voranzutreiben, muss Big Data aber in die Cloud verlagert werden – und hier ist aus Datenschutzgründen Vorsicht geboten, wie jüngste Beispiele aus China und den USA zeigen. Gleichzeitig benötigen wir IT-Sicherheitsexpert*innen auf höchstem Niveau, die derzeit kaum am Markt verfügbar sind. **Das wird keine leichte Aufgabe**.

Und es ist ebenso keine leichte Aufgabe, den Bedürfnissen und Anforderungen der Nutzer*innen gerecht zu werden. Denn die Erwartung lautet: **Einfachheit und mehr Benutzerfreundlichkeit bei all den Innovationen**.

Neben dem technischen Fortschritt haben sich auch das internationale Umfeld und der Handel verändert. Lieferengpässe sind an der Tagesordnung. Das traf auch die SBB. Plötzlich standen wir ohne Chips für die Bahnhofsanzeigen da. Weil die ganze Dynamik im Markt viel volatiler geworden ist, müssen wir im Einkauf schneller reagieren. Das ist nicht mehr das Geschäft, das wir gewohnt sind. Und um die Sache noch interessanter zu machen, lastet jetzt auch noch der Kostendruck auf uns. Der Bund, die SBB, die Nationalbank – alle müssen sparen. Die Zeit drängt, und **wir müssen Wege finden, um mit knappen Ressourcen trotzdem etwas zu erreichen**.

URSPRUNG VOM BESCHAFFUNGSRECHT: FAIRER WETTBEWERB UND KORRUPTIONSPRÄVENTION

Technologischer Wandel und internationale Marktveränderungen erfordern Anpassungen. Alle diese Veränderungen sind grundlegend und werden uns in Zukunft beschäftigen. Das führt uns zu der **Frage: Wenn die Veränderungen grundlegend sind, brauchen wir dann etwas Neues, um damit adäquat und effizient umgehen zu können, oder ist das, was wir bisher haben, ausreichend?** Um diese Frage zu beantworten und die Ausgangsituation zu verstehen, werfen wir einen kurzen Blick zurück. Die öffentliche Hand gibt nicht einfach ihr eigenes Geld aus, sondern das Geld der Bürger*innen. Dies war der Ausgangspunkt für die Forderung nach Korruptionsprävention, und wenn zusätzlich der Wettbewerb gefördert wird, können sogar bessere Konditionen erzielt werden.

Das internationale Gremium, das dies vorantrieb, hatte damals die Vision, die Grenzen zwischen den Ländern zu öffnen. Ihr Ansatz war überzeugend: **Wer Korruption verhindern will, braucht Transparenz. Um fairen Wettbewerb zu ermöglichen, braucht es Gleichbehandlung**. Ein – so scheint mir – richtiger Ansatz. Auch die Schweiz hat auf diese Veränderungen reagiert und im Januar 2021 ist das revidierte Beschaffungsrecht in Kraft getreten. Neben der Harmonisierung des Rechts zwischen den Kantonen stellt es weitere Instrumente zur Verfügung, um Themen wie Nachhaltigkeit und Innovation

anzugehen und zu berücksichtigen. Bevor darauf näher eingegangen wird, soll kurz auf die spezifischen vergaberechtlichen Anforderungen hingewiesen werden, mit denen sich Jurist*innen, Einkäufer*innen und Anbieter*innen auseinandersetzen müssen.

Wie gehen Jurist*innen mit den oben genannten Voraussetzungen um? Insbesondere im Verwaltungsrecht brauchen sie eine greifbare Grundlage, auf die sie sich in einem Gerichtsverfahren berufen können, um etwas zu schützen. Diese Grundlage hat die Form einer Verfügung. Sie können sich das so bildlich vorstellen, als wäre die Verfügung ein Haken, an dem Sie Ihre Kleider, also die Beschwerde, aufhängen können. Zumindest wurde die Besonderheit des Vergabeverfahrens als fortlaufender Prozess erkannt. Deshalb **müssen Unstimmigkeiten sofort gerügt werden**: Wenn jemandem während des Ausschreibungs- und Bewerbungsprozesses etwas auffällt, muss es sofort kommuniziert werden, sonst kommt jede Intervention zu spät. Diese Eigendynamik ist ein wesentlicher Aspekt des Beschaffungsverfahrens.

Das wäre eigentlich eine gute Ausgangslage. Aber die Gesetzgeber, und in ihrem Schlepptau die Richter, haben sich – in guter Verwaltungsrechtsmanier – nicht nur auf das sogenannte Anfechtungsobjekt (Verfügung) und auf gewisse Grundsätze beschränkt. Sie begannen, der Beschaffungsstelle detailliert inhaltliche Vorgaben für ihre Entscheide vorzugeben. Um nur einige Beispiele zu nennen: Beschaffungsstellen müssen bestimmte Mindestanforderungen definieren und sinnvolle Kriterien auflisten. Bei den Zuschlagskriterien müssen sie zudem die Rangfolge und Gewichtung anfügen, wobei sie eine Mindestgewichtung für den Preis respektieren müssen. Ausserdem gibt es vorgegebene Fristen und fix definierte Verlängerungs- und Verkürzungsmöglichkeiten – all diese Elemente greifen ineinander und machen den Prozess kompliziert. Schliesslich wurde sogar der Verhandlungsprozess reglementiert, so dass z.B. Preisangebote nicht mehr möglich sind. Und das sind nur wenige Beispiele (vgl. die Anforderungen an einen Ausschluss von Anbietenden etc.).

REFORM DES BESCHAFFUNGSRECHTS: EIN ERFOLG?

Der Markt ist im Wandel. Die Einkaufsprozesse sind aufgrund der zu detaillierten Vorgaben vom Beschaffungsrecht kompliziert. Nachdem die Ausgangslage somit geklärt ist, kommen wir zur Frage: War die Vergaberechtsrevision 2021 erfolgreich? Meine

Antwort lautet im Grundsatze: Ja. Geht man vom erklärten **Ziel der Reform** aus, die **Bestimmungen zwischen den Kantonen und dem Bund zu harmonisieren** – so **ist dieses erreicht**. Zudem wurde ein besonderes Augenmerk auf die Nachhaltigkeit gelegt, und ich denke, dass auch das Ziel, die nachhaltige Beschaffung zu fördern, erreicht wurde. Ich bin fest davon überzeugt, dass Nachhaltigkeit für uns und unsere zukünftigen Generationen von grosser Bedeutung ist. Und diese Überzeugung hält nun Einzug ins Gesetz – und langsam auch in die Praxis.

Betrachten wir die Reform des Vergaberechts aber über die deklarierten Ziele hinaus etwas kritischer und fragen: Hat sich die Dauer der quälend langen Verfahren (sowohl in der Vergabe als auch bei einer Beschwerde) verkürzt? Nein, die Verfahren sind nach wie vor zeitraubend und langwierig. Hat die Revision die Verfahren vereinfacht? Nein, das glaube ich nicht. Die Verfahren sind nach wie vor kompliziert und die Angst vor möglichen Beschwerdeverfahren bleibt bestehen. Dennoch gibt es überwiegende positive Aspekte des neuen Gesetzes, auf die ich im Folgenden näher eingehen werde. Der Kern dieses Optimismus liegt darin, dass uns das Gesetz einen erheblichen Ermessensspielraum lässt. Das Gesetz ist lediglich ein Rahmen, den es geschickt zu nutzen gilt. Doch: Wie kann dieser Rahmen am besten genutzt werden? Und wie wird dieser Rahmen heute bereits genutzt?

Eine Möglichkeit besteht darin, durch **Rahmenverträge** längerfristige Lieferantenbeziehungen aufzubauen. Doch nicht nur das: Wurden in einem Vergabeverfahren Partner für Rahmenverträge ausgewählt, kann der Abruf von Leistungen ausserhalb vom Vergaberecht schnell und unbürokratisch erfolgen. Es muss nicht für jede einzelne Lieferung oder Leistung ein neues Vergabeverfahren durchgeführt werden. Um den Wettbewerb bei Abrufen weiterhin zu gewährleisten, kann innerhalb der gewählten Vertragspartner ein sogenanntes Mini-Tender durchgeführt werden. Rahmenverträge bieten daher Flexibilität in Bezug auf die Menge der benötigten Waren oder Dienstleistungen sowie in Bezug auf mögliche Vertragsanpassungen.

Neu wird auch der **Dialog** im Vergabeprozess genutzt. Ziel des Dialogs ist es, ein besseres Verständnis zwischen öffentlichen Beschaffer*innen und potenziellen Lieferanten bei komplexen Beschaffungen zu erreichen, was nicht nur den Informationsaustausch, sondern auch die Entwicklung innovativer Lösungen erleichtern soll. Zudem kann

im Dialog auch explizit das Preis-Leistungsverhältnis vertieft thematisiert werden. Allerdings ist die Umsetzung davon sehr aufwändig. Alles wird minutiös protokolliert, und in vielen Schritten, damit der Prozess nachvollziehbar ist – für den Fall, dass es vor Gericht geht. Das ist aber mit den neuen Technologien besser lösbar (z.B. Videoaufnahmen per Teams).

Weiter gibt es, wie bereits erwähnt, vermehrt erste Schritte in Richtung **Umwelt- und Sozialstandards**. Auch das öffentliche Beschaffungswesen soll die ökonomische, ökologische und soziale Nachhaltigkeit im Beschaffungsprozess berücksichtigen und fördern. Und wo stehen wir heute? Wir versuchen uns anzunähern. Aber auch das ist nicht immer einfach. Ich bin einem Beispiel zur Reparierbarkeit von Kopfhörermuscheln begegnet, wo die Reparaturkosten die Kosten eines Neukaufs um ein Vielfaches übersteigen – lohnt sich da eine Reparatur? Sollen wir reparieren, auch wenn das zu Mehrkosten führt? Oder sollen aus Preisgründen der weniger nachhaltige Neukauf in Betracht gezogen werden? Generell ist es zwar eine Herausforderung, Nachhaltigkeit in Prozesse zu integrieren. Aber diese Chance muss nun endlich genutzt werden.

Nachdem einige Neuerungen im Beschaffungsrecht diskutiert wurden, frage ich mich: Ist das genug? **Nutzen wir mit diesen Instrumenten wirklich die Gelegenheit, uns den aktuellen Herausforderungen zu stellen?** Nachfolgend meine Antwort: Bisher lautete das Credo vieler Einkäufer*innen: «Wir bündeln, um bessere Preise zu erzielen». Dieses Credo wird jedoch durch die Instabilität der Lieferketten zunehmend aufgeweicht. Mit anderen Worten: Um stabil zu bleiben, braucht man mehrere Lieferanten und Zulieferbetriebe. Wenn ein Lieferant ausfällt, hat man immer noch andere, auf die man sich verlassen kann. Mit der Zeit wird deshalb das Credo der Bündelung zugunsten der Liefersicherheit in den Hintergrund treten. Das wiederum führt uns dazu, wieder mehr in der Heimat zu beschaffen. Denn wenn die Lieferanten zu weit weg sind, entzieht sich mir die Kontrolle über sie. Das heisst: Die Preisvorteile bei Bündelungen werden zwecks Erhöhung der Resilienz relativiert, was zu mehr «**Nearshoring**» führt – **der Verlagerung von Geschäftsprozessen in das eigene Land oder nahegelegene Länder**. Dies wiederum kann eine Verteuerung nach sich ziehen. Zieht man das Nearshoring einer genaueren Analyse vor, zeigt sich, dass die Herausforderung darin besteht, dass sich der Markt allmählich ausdünnt und die Gefahr von Preissteigerungen droht, da der Kostendruck anhält.

Wie kann die öffentliche Hand dem entgegenwirken? Soll sie eine Kostenobergrenze einführen? Oder schafft ein **Bonus-Malus-System** Abhilfe? Nach dem Motto: «Wenn es Ihnen als Anbieter gelingt, durch intelligente Lösungen die Kosten bei gleichbleibender Qualität zu senken, dann teilen wir uns die Einsparungen». Diese Überlegungen existieren. Wir führen solche Bonus-Malus-Systeme bereits ein, aber die Umsetzung davon ist sehr anspruchsvoll, insbesondere was den Malus betrifft. In Zeiten, in denen die öffentliche Verwaltung unter finanziellem Druck steht, ist aber auch die Frage der Boni schwierig.

Und wenn wir schon bei den aktuellen Herausforderungen sind: Auch das Problem des **Fachkräftemangels** darf nicht unerwähnt bleiben. Wie können wir darauf reagieren? Hierzu möchte ich ein konkretes Beispiel anführen, ohne jedoch konkrete Namen zu nennen: Ein Unternehmen berichtete, dass seine IT-Lieferanten nur über eine begrenzte Anzahl qualifizierter Projektleiter verfügen. Nun kommt es vor, dass diese Projektleiter bei einem Kunden nicht optimal agieren können und deshalb aus dem Projekt abgezogen werden. In solchen Fällen wendet sich der Kunde an die SBB und sagt: «Wir haben hier jemanden, der in unserem Projekt nicht erfolgreich war, aber ein hervorragender Experte oder eine hervorragende Expertin ist, den oder die wir sofort einsetzen möchten». Ich möchte nicht darüber spekulieren, wie ein Einsatz dieser Personen im Rahmen des Vergaberechts umgesetzt werden kann. Aber das sind Ansätze, die sich langsam durchsetzen, einfach weil qualifizierte Expert*innen auf dem Markt knapp sind.

Eine weitere Herausforderung ist der neue Fokus auf den **Qualitätswettbewerb**: wie kommen wir von der Fokussierung auf den Preis zur grösseren Berücksichtigung messbarer Qualität? Die ersten Ansätze ähneln denen im privaten Sektor: Wenn wir irgendwo einkaufen oder eine Dienstleistung in Anspruch nehmen, fragen wir uns: «War das gut? War der/die Handwerker*in kompetent? War der Computer oder die Software von guter Qualität?». Verneinen wir diese Fragen, suchen wir nach Alternativen. Auch im öffentlichen Beschaffungswesen bewerten wir die Qualität im Nachhinein sowie während der Nutzungsdauer, und diese Erfahrungen fliessen in künftige Aufträge ein. Um mehr Qualität zu fordern, sollten daher die bisherigen Erfahrungen als Kriterium für zukünftige Vergaben herangezogen werden. Doch auch hier stellen sich wieder Fragen: Ist das gemäss Vergaberecht zulässig? Wie bewerten wir diejenigen, die noch nie für uns gearbeitet haben und deren Produkt oder

Dienstleistung wir nie testen konnten? Wer nimmt die Bewertung vor und wer wird öffentlich angehört? Die Chance und die Devise kann hierbei nur lauten: Machen - Ausprobieren – Experimentieren!

Auch die Forderung nach **Nachhaltigkeit** stellt uns vor die Suche nach neuen Lösungen, was deren Umsetzung betrifft: Um nachhaltiger zu beschaffen, müssen wir höhere Anforderungen an die Transparenz in der Lieferkette stellen – dafür ist ein zentrales Datenmanagement unerlässlich. Das ist vielerorts im Aufbau, aber auch dieser gestaltet sich nicht ganz einfach, ist aber notwendig, um effizient zu arbeiten.

Was sich ebenfalls im Aufbau befindet, ist das **Allianzmodell**. Was ist damit gemeint? In einem solchen Modell sitzen wir gemeinsam in einem Boot und führen das Projekt von Anfang bis Ende gemeinsam durch. Auch Gewinn und Verlust werden gemeinsam getragen. Die ersten Allianzmodelle sind bereits vertraglich fixiert und können umgesetzt werden. Man versucht, diesen Weg gemeinsam zu gehen – und dies eröffnet neue Chancen. Doch auch hier können wieder tausend Fragen aufgeworfen werden: Wie wähle ich die Partner aus, damit alles passt? Eine mögliche Antwort ist: Ganz einfach, ich suche mir erstmals jemanden, der die Bereitschaft zeigt, mit mir diesen Weg zu gehen, und wir schauen dann gemeinsam, wie es am besten funktioniert. Wichtig ist, dass wir für solche Experimente offen sind und uns nicht davon abhalten lassen, Spielräume zu nutzen und Neuartiges auszuprobieren, nur weil es vergaberechtlich schwierig ist.

FAZIT

Mein Resümee – und jetzt werde ich ein wenig provokativ: Ich glaube, diejenigen, die im öffentlichen Beschaffungswesen auf der Auftraggeberseite stehen, stehen derzeit vor Herausforderungen. Aber auch vor vielen Chancen. Entweder man entscheidet sich, es «gäng wie gäng» zu machen (wie man in Bern zu sagen pflegt), denn das geht: mit den bekannten Problemen und den bewährten Lösungen. Aber mein Ansatz wäre ein anderer. Ich glaube, dass sowohl das alte als auch das neue Vergaberecht **Spielraum** bietet, es nicht nur anders, sondern auch besser zu machen. Diesen müssen wir jetzt **nutzen**. Zuerst sollten wir uns überlegen, wie wir das machen wollen. Und wichtig ist dabei, dass wir uns von Bedenken und Ängsten überwältigen und behindern zu lassen. Das heisst natürlich nicht, dass wir uns nicht an das Recht halten sollen. Dass wir das

tun, ist eine Voraussetzung. Ich appelliere vielmehr, den Spielraum, den wir innerhalb des Rechts haben, so gut wie möglich zu nutzen.

Zu Beginn einer Beschaffung sollte sich die Beschaffungsstelle klar werden, was sie überhaupt will. Ist dies klar, dann muss sie **mutig sein und ihr Ermessen ausschöpfen**. Lasst die Bedenken nicht überhandnehmen und gestaltet das Verfahren so, wie ihr es auch privat machen würdet. Ein Beispiel: Manchmal unterliegt die SBB nicht dem Vergaberecht und kauft privatrechtlich Software, die sie also «frei» beschaffen kann, auch ohne Ausschreibung an alle möglichen Lieferanten. Ich habe dann die Einkäufer*innen gefragt, wie sie das machen. Hier deren Antwort: Sie beschränken sich darauf den (aufwändigen) Wettbewerb auf einige wenige, aber gemäss ihren eigenen Erfahrungen zuverlässige Lieferanten zu beschränken. Daraufhin fragte ich nach, warum wir das nicht im öffentlichen Teil, der dem Vergaberecht unterliegt, ebenfalls machen können. Das ginge nicht, war die oft gehörte Ansicht meiner Kolleg*innen. Steht man vor so einer Aussage, soll man sich überlegen: «Stopp, geht das wirklich nicht?» Denn den Lieferanten ist es eigentlich egal, wie etwas in der konkreten Beschaffung funktioniert. Es muss nur schnell und fair gehen. Wenn die Vergabestelle am Anfang des Verfahrens mitteilt: «Wir spielen Basketball auf dem Fussballfeld» – was solls? Das ist mir als Lieferant egal, ich muss es einfach wissen. Anders ausgedrückt: Wenn ich die Bedingungen kenne und weiss, wie etwas umgesetzt wird, dann kann ich mich darauf einstellen und meine Leute darauf vorbereiten, auf dem Fussballfeld Basketball zu spielen. Und schliesslich haben wir ja zu Beginn gesehen, dass das Beschaffungsrecht im Grund nur eines will: Transparenz und Gleichbehandlung als Mittel für einen nachhaltigen Wettbewerb und zur Verhinderung von Korruption.

Mein konkreter Vorschlag – oder vielmehr mein Appell – für eine **mutige Herangehensweise** wäre deshalb: Vergabestellen, ihr seid völlig frei, sofern ihr zu Beginn des Verfahrens die «Spielregeln» transparent und nicht-diskriminierend vorgibt. Nützt dabei auch die Möglichkeit, die Vergabeverfahren zu beschleunigen. Wenn man dann die versprochene Beschleunigung einhält und vielleicht das Ganze mit einem Bonus-Malus-System würzt, dann, so meine These, werden die Lieferanten sagen: «Endlich haben sie es kapiert».

Das ist mein Schlusswort. Ich hoffe, dass ich nicht ganz falsch liege und auch in zehn Jahren … wieder an die IT-Beschaffungskonferenz kommen kann.

OPEN SOURCE SOFTWARE IM EMBAG

Analyse des neuen Art. 9 des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

Rika Koch / Simon Schlauri

Rika Koch ist Dozentin an der Berner Fachhochschule und Co-Leiterin der Fachgruppe Public Procurement.

Simon Schlauri ist Partner bei Ronzani Schlauri Anwälte.

Abstract: Der vorliegende Beitrag diskutiert, wie sich das neue Digitalisierungsgesetz des Bundes, das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG), auf die Entwicklung und Beschaffung von Software durch Bundesbehörden auswirken wird. Art. 9 des EBMAG führt ab 1. Januar 2024 namentlich neu die Pflicht ein, einschlägige Software unter eine Open-Source-Lizenz (OSS-Lizenz) zu stellen. Anhand einer Analyse des Wortlauts, Gesetzeszwecks und der Geschichte von Art. 9 EMBAG beleuchten die Autorin und der Autor, was dieser Paradigmenwechsel hin zu OSS für die Bundesverwaltung bedeutet, auch in Hinblick auf IT-Beschaffungen.

INHALTSVERZEICHNIS

1. Einleitung 22
2. Was bezweckt das EMBAG und was trägt OSS dazu bei? 23
3. Pflicht zur offenen Lizenzierung und Freigabe von Software (OSS-Pflicht, Art. 9 Abs. 1 und Abs. 2 EMBAG) 25
   - 3.1 Offenlegung des Quellcodes 25
   - 3.2 …sowie freie Nutzung, Weiterentwicklung und Weitergabe 25
   - 3.3 Geltungsbereich 26
     - 3.3.1 Für welche Behörden gilt das EMBAG? 26
     - 3.3.2 Für welche Software gilt das EMBAG? 27

3.4 Ausnahmen: Rechte Dritter und sicherheitsrelevante Gründe 29
3.4.1 Wortlaut und Vorgeschichte 29
3.4.2 Rechte Dritter 30
3.4.3 Sicherheitsrelevante Gründe 30
4. Lizenzen (Art. 9 Abs. 3 und Abs. 4 EMBAG) 31
4.1 Grundlagen 31
4.2 Welche Lizenz soll gewählt werden? 32
4.3 Soll eine Lizenz mit Copyleft verwendet werden? 33
4.4 Haftungsansprüche insbesondere 34
5. Ergänzende Dienstleistungen (Art. 9 Abs. 5 und Abs. 6 EMBAG) 34
6. Fazit: Kein Allheilmittel, aber ein guter Anfang 36
Bibliographie 37

1. EINLEITUNG

Während Open Source Software (OSS)[1] in der Privatwirtschaft etabliert ist, entwickelt die öffentliche Verwaltung immer noch vorwiegend proprietäre Software (Poledna, Schlauri & Schweizer, 2017, Rz. 483 oder generell OS-Studie Schweiz 2021). Dies ist wohl darauf zurückzuführen, dass die Frage, ob Behörden die von ihnen entwickelte und genutzte Software (Behördensoftware) unter eine Open-Source-Lizenz (OSS-Lizenz) stellen dürfen oder gar sollen, in der Schweiz lange mit Rechtsunsicherheit behaftet war.

Die Diskussion über OS-Behördensoftware ist über 12 Jahre alt (Stürmer 2023). Sie geht auf die Gerichtssoftware «Openjustitia» zurück, die das Bundesgericht unter eine OSS-Lizenz stellte, um anderen Gerichte deren kostenlose Nutzung zu ermöglichen (Netzwoche 2014). Dies warf die daraufhin kontrovers diskutierte Frage auf, ob OS-Behördensoftware zu Konkurrenzierung der Privatwirtschaft und zu Wettbewerbsverzerrungen führen würde. Im Rahmen dieser Kontroverse wurden mehrere politische Vorstösse (siehe z.B. Interpellation Weibel 12.4247, Postulate Glättli 14.4275 und Graf-Litscher 14.3532) und zwei Rechtsgutachten veröffentlicht: Das erste Gutachten äusserte sich skeptisch

[1] Für eine Begriffsdefinition von OSS vgl. ISB, 2019, S. 3.

zur Notwendigkeit von OS-Behördensoftware, befürwortete die «Bildung einer Closed Community» und verlangte eine gesetzliche Grundlage auf Verfassungsstufe (Müller & Vogel, S.30). Das zweite Gutachten hingegen hob die Vorteile von OSS hervor, stellte diese in einen staatspolitischen Kontext und analysierte die Notwendigkeit einer gesetzlichen Grundlage differenzierter (Poledna, Schlauri & Schweizer Rz. 281 und Rz. 482).

Diese Entwicklungen führten schliesslich zu einem Umdenken, welches die Bedenken in Bezug auf die Wettbewerbsneutralität von OSS in den Hintergrund rücken liessen. Es stellte sich immer mehr die Erkenntnis ein, dass OSS auch bzw. vor allem für die öffentliche Verwaltung aus Gründen der Effizienz, Transparenz und Inklusivität gewichtige Vorteile gegenüber proprietärer Software hat. Das 2021 verabschiedete «Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben» (EMBAG) besiegelte schliesslich den Paradigmenwechsel und führte zu einer Kodifizierung von OSS als Standard für Behördensoftware in Art. 9 EMBAG.

Der vorliegende Beitrag beleuchtet diese neue Rechtsnorm, die den unterstellten Behörden eine Pflicht zur OSS-Lizenzierung gewisser Software auferlegt (OSS-Pflicht). Im Folgenden analysiert der Beitrag den Umfang und die Schranken der neuen OSS-Pflicht in Art. 9 EMBAG, die Ausnahmen davon sowie die damit einhergehenden Spielräume. Dabei soll auch auf die Frage eingegangen werden, was die OSS-Pflicht in Art. 9 EMBAG für die öffentliche Beschaffung von Behördensoftware bedeutet.

2. WAS BEZWECKT DAS EMBAG UND WAS TRÄGT ES ZU DIESEN ZWECKEN BEI?

Das EMBAG verfolgt zwei Ziele (Botschaft EMBAG, S. 6 und S. 7): Erstens will es eine Rechtsgrundlage schaffen für die digitale Transformation des Bundes. Deshalb wird das Gesetz umgangssprachlich auch als «eGov-Gesetz» bezeichnet. In diesem Sinne normiert das EMBAG nebst OSS in Art. 9 EMBAG auch die Veröffentlichung von Verwaltungsdaten (Open Government Data, Art. 10 EMBAG) oder die Festlegung von Standards durch den Bund (Art. 12 EMBAG). Zweitens zielt das Gesetz darauf hin, die Zusammenarbeit zwischen den verschiedenen föderalen Ebenen zu verbessern.[2]

[2] Siehe auch Beitrag von Chantal Lutz und Cédric Miehle in diesem Band (Kapitel 4).

OSS spielt zur Erreichung beider Ziele eine wichtige Rolle. Sie verspricht einen gesamtgesellschaftlichen Mehrwert durch die transparente und gemeinschaftliche Nutzung von mit öffentlichen Geldern finanzierten Softwarelösungen («Public Money, Public Code»). Zudem ermöglicht die Übernahme bestehender OSS-Lösungen Effizienzgewinne und somit Kosteneinsparungen für die öffentliche Hand. Im Weiteren beinhaltet OSS ein partizipatives Element, weil sie eine aktive Teilnahme und Mitgestaltung bei der Pflege und Weiterentwicklung nicht nur ermöglicht, sondern aktiv fördert (vgl. statt vieler Poledna, Schlauri & Schweizer, 2017; ISB, 2019 und Straub, 2024).[3]

Auch in Bezug auf die verstärkte Zusammenarbeit zwischen den Behörden kann OSS eine wichtige Rolle spielen: Durch die Freigabe können bewährte Softwarelösungen von Behörden getreu dem Motto «einmal entwickeln – mehrfach nutzen» auch von einer anderen Behörde übernommen und genutzt bzw. adaptiert werden kann. Der sog. «Einer-für-alle-Ansatz» (EfA) bedeutet, dass z.B. ein Kanton (oder eine Gemeinschaft von Kantonen) eine Leistung zentral entwickelt und betreibt und diese anschliessend anderen Kantonen oder Gemeinden zur Verfügung stellt. Die Kosten werden geteilt (dazu Bundesministerium des Inneren und für Heimat, 2023; Schlauri, 2023).

Art. 9 EMBAG statuiert die Pflicht, von Behörden entwickelte Software grundsätzlich unter eine OSS-Lizenz zu stellen. Vorbehalten bleiben die im Gesetz umschriebenen Ausnahmen (Art. 9 Abs. 2 EMBAG, vgl. sogleich, Ziff. 3.4). Somit schafft Artikel 9 nicht nur Rechtssicherheit für die Freigabe von OSS durch Behörden, sondern geht einen Schritt weiter und verankert OSS gar als Pflicht für Behördensoftware.

Weil der Gesetzeswortlaut von der ursprünglich fakultativen «Kann-Bestimmungen» abgekommen ist und nun einen obligatorischen Charakter aufweist, wird vorliegend von einer eigentlichen OSS-Pflicht gesprochen.

[3] Für weitere Vorteile von OSS gegenüber Closed Source Software bzw. proprietäre Software vgl. statt vieler ISB, S. 4 – S.5.

3. PFLICHT ZUR OFFENEN LIZENZIERUNG UND FREIGABE VON SOFTWARE (OSS-PFLICHT, ART. 9 ABS. 1 UND ABS. 2 EMBAG)

3.1 OFFENLEGUNG DES QUELLCODES…

Art. 9 Abs.1. und 2 EMBAG verankern den OS-Grundsatz, bzw. beschreiben, welcher Pflicht die unterstellten Behörden nachzukommen haben. Abs. 1 bezieht sich auf die Offenlegung des Quellcodes:

> *Die diesem Gesetz unterstehenden Bundesbehörden legen den Quellcode von Software offen, die sie zur Erfüllung ihrer Aufgaben entwickeln oder entwickeln lassen, (…). (Art. 9 Abs. 1, erster Teilsatz)*

Die Offenlegung des Quellcodes, auch Sourcecode genannt (d.h. der für Menschen lesbare Text eines Computerprogrammes; vgl. etwa Straub, 2024, Rz. 7), ist der Grundstein des OSS-Gedankens, denn ohne diese Offenlegung kann die Software nicht insbesondere nicht durch Dritte angepasst werden (für eine detailliertere Schilderung vgl. ISB, 2019, S. 9). OSS unterscheidet sich von «Closed Source Software» gerade im Wesentlichen darin, dass Open Source Lizenzen grundsätzlich allen die urheberrechtlichen Nutzungsrechte am Quellcode einräumen (Poledna, Schlauri & Schweizer, 2017, Rz. 17 m.H.).

3.2 …SOWIE FREIE NUTZUNG, WEITERENTWICKLUNG UND WEITERGABE

In einem zweiten Schritt spezifiziert Absatz 2 einen weiteren Grundsatz von OSS, namentlich die kostenlose Nutzung, Weiterentwicklung und Weitergabe der Software ohne Zweckbindung:

> *Sie erlauben jeder Person, die Software zu nutzen, weiterzuentwickeln und weiterzugeben, und erheben keine Lizenzgebühren. (Art. 9 Abs. 2 EMBAG)*

Die kostenlose Nutzung, Weiterentwicklung und Weitergabe ist wesentliches Merkmal von Open Source Software (früher deshalb auch «free software» genannt, vgl. Poledna, Schlauri & Schweizer, 2017, Rz. 16): Diese zeichnet sich ja eben genau dadurch aus, dass Dritten die genannte Nutzung der Software erlaubt wird, und dabei keine Lizenzgebühren erhoben werden (wobei für die Weitergabe oder für das Kopieren Ge-

bühren erhoben werden können, vgl. z.B. Botschaft EMBAG, S. 26 oder Straub, 2024, Rz. 717 mit Hinweis auf Ziff. 4 Abs. 2 GLP v3). Dabei ist wichtig zu betonen, dass diese Nutzungsrechte gemäss Art. 9 EMBAG grundsätzlich gegenüber allen eingeräumt werden müssen, und sich nicht auf spezifische Personen(gruppen) beschränken dürfen, wie es bei gebührenpflichtigen Lizenzmodellen der Fall ist. Auch eine Beschränkung auf bestimmte Einsatzbereiche (z.B. nur nicht-kommerzielle Nutzung) ist nicht mit dem Grundgedanken von OSS vereinbar (Schlauri, 2023).[4]

3.3 GELTUNGSBEREICH

3.3.1 Für welche Behörden gilt das EMBAG?

Als erstes stellt sich die Frage, welche Behörden OS-pflichtig werden: Das EMBAG gilt für die zentrale Bundesverwaltung, also die Departemente des Bundes und die Bundeskanzlei, sowie die dazugehörigen Generalsekretariate und Bundesämter (Art. 2 Abs. 1 EMBAG i.V.m. Art. 7 der Regierungs- und Verwaltungsorganisationsverordnung RVOV). Während der Entwurf des EMBAG die dezentrale Bundesverwaltung von der Unterstellung befreien wollte, verpflichtet Art. 2 Abs. 2 EMBAG in der finalen Version auch die dezentrale Bundesverwaltung (Art. 7a RVOV), also diejenigen Bundesbehörden mit eigener Rechtspersönlichkeit (z.B. Aufsichtsorgane, Stiftungen, Hochschulen oder Forschungsinstitute). Der Bundesrat kann allerdings Ausnahmen vorsehen; der Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei veröffentlicht dazu eine Liste der Bundesbehörden, die nach Absatz 1 dem EMBAG unterstellt sind, sowie der für sie geltenden Bestimmungen des EMBAG (Art. 1 Abs. 2 EMBAV).

Dabei ist wichtig zu betonen, dass das EMBAG nur für die Behörden des Bundes gilt. Den kantonalen oder kommunalen Behörden kann es mangels Bundeskompetenz im Bereich Digitalisierung keine Verpflichtungen auferlegen, auch wenn dies gelegentlich von den Vernehmlassungsteilnehmenden gefordert wurde (vgl. z.B. Vernehmlassungsantworten der SP oder der GLP, Vernehmlassungsbericht, S. 7).

Den Kantonen steht es selbstverständlich frei, eigene Gesetzgebungen zu implementieren zu implementieren. So hat der Kanton Bern beispielsweise seit 2022 ein «Gesetz über die

[4] Im Gegensatz zu bestimmten «Creative-Commons»-Lizenzen, welche die kommerzielle Nutzung von Werken verbieten können (Schlauri, 2023).

digitale Verwaltung» (DVG, BSG 109.1), das in Artikel 26 ebenfalls den Grundsatz von OSS und Open Government Data (OGD) «by default» verankert. In Zürich liess zudem der Regierungsrat auf ein an die Berner Vorlage angelehntes Postulat hin verlauten, bei noch zu erarbeitenden Vorgaben für die Applikations-, Daten- und Technologiearchitektur von Software sollten bezüglich des Themas OSS die im Postulat geforderten Massnahmen angemessen berücksichtigt werden (Regierungsrat Zürich, 5). Ansonsten kennen noch wenige Kantone eine OSS-Regelung. Wie Straub anmerkt, könnten sich aber auch Kantone bei der Auslegung (oder Ausgestaltung) ihres Rechts bezüglich der Verwendung von Open Source Software am EMBAG orientieren (Straub, 2024, Rz. 1171).

3.3.2 Für welche Software gilt das EMBAG?

Weiter umfasst der Wortlaut des EMBAG nicht alle Software, sondern nur diejenige Software, die eine Behörde a) «entwickelt oder entwickeln lässt» und b) die «der Erfüllung einer öffentlichen Aufgabe» dient.

Als erstes Kriterium stellt der Wortlaut «entwickeln oder entwickeln lassen» klar, dass nur Neuentwicklungen unter die OSS-Pflicht fallen; also Software, die der Bund einerseits selbst neu entwickelt/programmiert, oder andererseits auf Markt von privaten Softwarefirmen neu entwickeln lässt. Weiterentwicklungen bereits bestehender Behördensoftware müssen nicht als OSS lizenziert werden (was rechtlich und technisch gesehen wohl gar nicht möglich wäre, zumindest sofern der Bund sich nicht die Rechte hat abtreten lassen oder im Fall von Eigenentwicklungen originäre Rechte erworben hat). Ebenfalls nicht unter die OSS-Pflicht fällt der Kauf bestehender Software, die «von Dritten unverändert erworben wird» (Botschaft EMBAG, S. 119). Somit steht es den Behörden weiterhin offen, eine proprietäre Software «von der Stange» zu kaufen.

Die neue Regelung hat auch beschaffungsrechtliche Implikationen: Diejenige Software, die eine Bundesbehörde auf dem privaten Markt einkauft oder entwickeln lässt, untersteht den Regeln des Bundesgesetzes über das öffentliche Beschaffungsrecht (BöB). Das bedeutet, dass sich die jeweilige Beschaffungsbehörde für Neuentwicklungen zumindest ein Recht des Bundes zur Unterlizenzierung als OSS in der Ausschreibung (und idealerweise auch im Vertragsentwurf) vorzubehalten hat. Sofern die Behörde – wie beispielsweise gemäss Art. 24.1.1 der AGB der SIK vorgesehen – die Rechte an den

Arbeitsergebnissen ohnehin an den Bund abtreten lässt, entfällt dies aber, weil die Behörde ohnehin frei ist, die Ergebnisse als OSS zu lizenzieren. Auch Erfahrung im Bereich von OSS könnte als Eignungs- oder Zuschlagskriterium verlangt werden. Die öffentliche Beschaffung von bereits bestehender Software ist nicht von der OSS-Pflicht erfasst und erfordert keine entsprechenden Kriterien in der Ausschreibung.

Dabei ist wichtig zu betonen, dass die Frage welche Software genau beschafft oder entwickelt werden soll und ob diese selbst oder extern entwickelt werden soll («Make-or-Buy»-Entscheid) weiterhin im freien Behördenermessen liegt und von der OSS-Pflicht in Art. 9 EMBAG nicht tangiert wird (vgl. auch Straub, 2024, Rz. 722; Poledna, Schlauri & Schweizer, Rz. 342 ff.).

Das zweite Kriterium, «zur Erfüllung öffentlicher Aufgaben», ist weniger klar. Grob können all diejenigen Aufgaben zu den «öffentlichen Aufgaben» gezählt werden, welche die jeweilige Behörde aufgrund ihres gesetzlichen Auftrags wahrnimmt.[5] Was genau zur öffentlichen Aufgabe der jeweiligen Behörde gehört, ergibt sich in der Regel aus dem Gesetz, bzw. kann aus diesem abgeleitet werden. Die Rechtsprechung im Kontext des öffentlichen Beschaffungswesens zeigt,[6] dass dieser Begriff breit gefasst ist und im Zweifelsfall von einer öffentlichen Aufgabe ausgegangen werden muss (vgl. BGE 144 II 177 mit Referenzen oder WTO Appellate Body Report *Canada – Certain Measures Affecting the Renewable Energy Generation Sector/Measures Relating to the Feed-in Tariff Program* vom 6. Mai 2013, para. 5.58).

Von den öffentlichen Aufgaben abzugrenzen sind «kommerzielle Dienstleistungen». Dazu gehören Dienstleistungen, die eine Behörde im Ausnahmefall gegen Entgelt wahrnehmen kann, obwohl dies nicht direkt der Erfüllung ihrer öffentlichen Aufgaben dient (so z.B. auch die «ergänzenden Dienstleistungen» i.S.v. Art. 9. Abs. 5 EMBAG, siehe nachstehend Ziff. 5). Kommerzielle Dienstleistungen durch Behörden sind aufgrund des Legalitätsprinzips und der Wettbewerbsneutralität nur dann möglich, wenn dies

---

5 Aufgrund des Legalitätsprinzips darf eine Behörde grundsätzlich nicht tätig werden, ohne dass dies in einem Gesetz umschrieben ist.

6 Auch im öffentlichen Beschaffungsrecht ist die Definition des «öffentlichen Auftrags» gem. Artikel 8 des Bundesgesetzes über das öffentliche Beschaffungswesen (BöB) davon abhängig, ob der Auftrag «der Erfüllung einer öffentlichen Aufgabe dient». Rechtsprechung in diesem Bereich kann deshalb auch im Kontext des EMBAG als Interpretationshilfe dienen.

in der jeweiligen gesetzlichen Grundlage verankert ist, da sonst die Gefahr von Wettbewerbsverzerrungen besteht.[7]

Somit ergibt sich die Frage, ob die jeweilige Software der Erfüllung öffentlicher Aufgaben dient, oder eher dem Bereich der kommerziellen Dienstleistungen zuzuordnen ist aus der Analyse der jeweiligen gesetzlichen Grundlage der Behörde.

Schliesslich muss die zu entwickelnde Software zur öffentlichen Aufgabe der jeweiligen Behörden in einem kausalen Zusammenhang stehen, also deren Erfüllung dienen.

3.4 AUSNAHMEN: RECHTE DRITTER UND SICHERHEITSRELEVANTE GRÜNDE

3.4.1 Wortlaut und Vorgeschichte

Art. 9 EMBAG sieht zwei Ausnahmetatbestände vor, die eine unterstellte Behörde von der OSS-Pflicht befreien. So stellt Art. 9 Abs. 1 EMBAG die Offenlegung des Quellcodes unter folgenden Vorbehalt:

> Die diesem Gesetz unterstehenden Bundesbehörden legen den Quellcode von Software offen, die sie zur Erfüllung ihrer Aufgaben entwickeln oder entwickeln lassen, *es sei denn die Rechte Dritter oder sicherheitsrelevante Gründe würden dies ausschliessen oder einschränken.*

Der von den Räten verabschiedete Wortlaut sieht nur zwei Ausnahmetatbestände vor: vorbestehende Rechte Dritter und sicherheitsrelevante Gründe. Bemerkenswert ist, dass die Entwurfsfassung von Art. 9 EMBAG die Ausnahmen noch sehr viel offener formulierte: Die Norm beschränkte den OSS-Grundsatz auf diejenigen Fälle, in denen die Offenlegung des Quellcodes «sinnvoll und möglich ist». Dieser schwammig formulierte Vorbehalt, der den unterstellten Behörden ein grosses Ermessen eingeräumt hätte, wurde in der parlamentarischen Debatte in Befolgung eines Minderheitsantrages gestrichen. Diese Streichung ist zu begrüssen, da der Vorbehalt ein wahrscheinlich allzu

[7] So sieht Art. 4 des Bundesgesetzes über die Meteorologie und Klimatologie (MetG, SR. 429.1) explizit vor, dass das Bundesamt für Meteorologie und Klimatologie «erweiterte Dienstleistungen» unter gewissen Bedingungen leisten kann. Auch das ETH-Gesetz (ETHG, SR. 414.110) ermächtigt die ETH dazu, private Dienstleistungen zu tätigen, solange sie dies den Wettbewerb nicht verfälscht (Art. 10 ETHG).

willkommenes Schlupfloch im Gesetz dargestellt hätte, auf die Lizenzierung als OSS zu verzichten (vgl. schon Schlauri, 2023).

3.4.2 Rechte Dritter

Die OSS-Pflicht gilt dann nicht, wenn eine Offenlegung des Quellcodes und die freie Einräumung der Nutzungsrechte bestehende «Rechte Dritter» verletzen würde. Solche Rechte sind primär Immaterialgüterrechte und Rechte, die sich aus Lizenzen ergeben und das geistige Eigentum der Softwarentwickler*innen schützen. Vorbestehende proprietäre Lizenzen beispielsweise erlauben keine Offenlegung des Quellcodes und somit keine OSS-Freigabe. Deshalb gilt die OSS-Pflicht auch nur für Neuentwicklungen (vgl. oben, Kapitel 3.3.2).

Problematisch bleiben insbesondere Fälle, in denen Software zumindest teilweise auf vorbestehenden Modulen von mit der Entwicklung beauftragten Drittunternehmen abstellt. Sofern vom Hersteller nicht das Recht erhältlich ist, auch jene Teile unter eine Open-Source-Lizenz zu stellen (was aus Nutzersicht regelmässig die einfachste Lösung sein wird), sind jedenfalls die neu entwickelten Teile der Software als OSS freizugeben. Wer diese Teile verwenden will, kann sich diesfalls zumindest um eine (kommerzielle) Lizenz des Herstellers für die vorbestehenden bemühen oder diese nachentwickeln.

Weitere «Rechte Dritter» könnten sich aus dem Datenschutzecht ergeben. Weil Software typischerweise keine personenbezogenen Daten beinhaltet, läuft die Veröffentlichung von Software-Code i.d.R. aber nicht Gefahr, Datenschutzrechte zu verletzen. Nichtsdestotrotz ist es mit zunehmender Verbreitung von OSS umso wichtiger darauf zu achten, dass nicht (absichtlich oder unabsichtlich) personenbezogene Daten (wie nicht-fiktive Beispieldaten) im Code genannte werden.

3.4.3 Sicherheitsrelevante Gründe

Weit weniger klar ist der zweite Ausnahmetatbestand, der sich auf «sicherheitsrelevante Gründe» bezieht. Eine rein grammatikalische Auslegung dieses Wortlauts ist zwar deutlich: gemeint sind Gründe, in denen eine Offenlegung des Quellcodes die Sicherheit gefährden würde. Doch welche Gründe das sein könnten, bleibt bislang weitgehend unbeantwortet und wurde weder in der bundesrätlichen Botschaft zum EMBAG noch in der parlamentarischen Debatte thematisiert.

Der Ausnahmetatbestand dürfte auf Bedenken zurückzuführen sein, dass die Offenlegung des Quellcodes bei OSS potenziellen Angreifenden Einblicke in die Funktionsweise der Software und mögliche Angriffspunkte bieten könnten, die durch eine Geheimhaltung des Quellcodes und eine eingeschränkte Nutzung abgewehrt werden können («Security by Obscurity»). Dieser Ansatz wird jedoch kritisiert (vgl. Schlauri, 2023), weil die Sicherheit einer Software nicht im Wesentlichen von der Geheimhaltung des Quellcodes abhängt, sondern von anderen Faktoren wie Qualität der Programmierung und regelmässigen Updates und Patches. In diese Richtung geht auch das Argument, dass die Offenlegung des Quellcodes eine bessere Sicherheit ermöglicht, da eine grössere Gemeinschaft von Entwickelnden potenzielle Schwachstellen identifizieren und beheben kann.

4. LIZENZEN (ART. 9 ABS. 3 UND ABS. 4 EMBAG)

4.1 GRUNDLAGEN

Lizenzen sind privatrechtliche Vertragsinstrumente, mithilfe deren die Lizenzgeber*innen ihren Vertragspartner*innen (Lizenznehmer*innen) das Recht zur Nutzung und allenfalls Weiterentwicklung der Software einräumen. Dies wird so auch in Art. 9 Abs. 3 EMBAG wiedergegeben:

> *Die Rechte nach Absatz 2 werden in der Form von privatrechtlichen Lizenzen erteilt (…). (Abs. 3, erster Teilsatz)*

Definitionsgemäss hat jede OSS-Lizenz den Lizenznehmer*innen das Recht zur Nutzung und Weiterentwicklung einzuräumen (vgl. dazu im Detail Straub, 2024, Kapitel 7).

Was den darüberhinausgehenden Regelungsinhalt der Lizenz anbelangt, ist dieser je nach OSS-Lizenz unterschiedlich: So erfordern einige OSS-Lizenzen wie die GNU General Public License (GPL), dass Weiterentwicklungen (sog. «abgeleitete Werke») unter denselben strengen Bedingungen weitergegeben werden müssen («Copyleft»)[8], während andere Lizenzen weniger restriktiv sind (statt vieler, vgl. Straub, 2024; Schlauri, 2023).

[8] Copyleft ist ein Lizenzierungsprinzip, das sicherstellt, dass abgeleitete Werke einer Software die gleichen Freiheiten und Offenheitsbedingungen wie das Originalwerk beibehalten müssen (Straub, 2024, Kap. 7.4).

4.2 WELCHE LIZENZ SOLL GEWÄHLT WERDEN?

Das EMBAG stellt es den Behörden frei, unter welcher OSS-Lizenz sie ihre Software stellen. Art. 9 Abs. 3 und Abs. 4 EMBAG spezifizieren lediglich, dass die jeweilige OSS-Rechte nach Abs. 2 in der Form von privatrechtlichen Lizenzen erteilt werden, die wie der Vertrag im öffentlichen Beschaffungswesen privatrechtlicher Natur sind (Abs. 3)[9], und die nach Möglichkeit «international etabliert» sein sollen (Abs. 4):

> *Soweit möglich und sinnvoll sind international etablierte Lizenztexte zu verwenden. Haftungsansprüche von Lizenznehmern sind auszuschliessen, soweit dies rechtlich möglich ist. (Abs. 4)*

Nur schon aus Gründen der Rechtsicherheit empfiehlt es sich, international etablierte Lizenztexte zu verwenden,[10] da diese den Entwickler*innen und Nutzenden gleichermassen bekannt sind. Zudem fördern etablierte Lizenzen die globale Zusammenarbeit innerhalb der OSS-Community, weil sie weit verbreitet und verstanden sind, was die Integration und Weiterentwicklung von Projekten erleichtert. Schliesslich gewährleisten solche Lizenzen die langfristige Verfügbarkeit und somit die Nachhaltigkeit der Software, da sie die Weitergabe und Nutzung unter klaren Bedingungen sichern. Eigene oder lokale, international nicht etablierte Lizenzen könnten die internationale Community abschrecken und sie daran hindern, an der Weiterentwicklung mitzuwirken.

Ebenfalls aus Gründen der Rechtsicherheit empfiehlt es sich, die Wahl der Lizenzen bereits als Teil der Projektinitialisierungsphase zu klären und in denjenigen Fällen, in denen die Entwicklung extern in Auftrag gegeben wird, die Wahl der Lizenz in den Ausschreibungsunterlagen als technische Spezifikationen festzuhalten.

Nicht-etablierte Lizenzen können sich im Beschaffungsverfahren als Wettbewerbshindernis auswirken für Anbieter*innen, welchen eine solche Lizenz nicht bekannt ist. Bei regional etablierten Lizenzen würde sich dieser Wettbewerbsnachteil auf ausländische Anbieter*innen beschränken, was dem Diskriminierungsverbot des Government

---

9 Weiter besagt Art. 9 Abs. 3 auch, dass im Streitfall ein Zivilgericht und nicht wie beispielsweise bei einem Zuschlag im öffentlichen Beschaffungswesen ein Verwaltungsgericht zuständig ist.

10 Die Frage, welche Lizenzen als «international etabliert» gelten und welche nicht, ist nicht abschliessend geklärt und müsste im Streitfall von einem Gericht definiert werden. Klar ist, dass die üblichen, MIT-etablierten Lizenzen oder die GPL.

Procurement Agreements (GPA) der Welthandelsorganisation (WTO) widersprechen könnte (Art. X:2 GPA).

4.3 SOLL EINE LIZENZ MIT COPYLEFT VERWENDET WERDEN?

Aus unserer Sicht ist die Verwendung von Lizenzen mit Copyleft je nach Kontext sinnvoll. Zu bedenken ist zwar einerseits, dass zwar die Freiheit einer wirtschaftlichen Nutzung des Codes durch das Copyleft eingeschränkt wird, andererseits liegt Ziel der Verwendung von Lizenzen mit Copyleft darin, den einmal freigegebenen Code nachhaltig frei zu halten eine Art Tauschverhältnis zu etablieren: Wer sich am öffentlich verfügbaren «Pool» von OSS bedient, soll seine Ergebnisse auch wieder in diesen Pool zurückleiten, sodass die Community wieder profitiert (vgl. Stürmer 2009, S. 4). Dieses Tauschverhältnis ist je nach Anwendungsfall zentral, oder tritt in den Hintergrund.

Aus unserer Sicht sind daher die folgenden Grundsätze zu beachten:

- Eine Lizenz mit Copyleft ist in jedem Fall dann zu wählen, wenn vorbestehende Teile der Software schon unter Copyleft lizenziert sind. Diesfalls ist das Gesamtprojekt schon aufgrund der Lizenzbedingungen der vorbestehenden Software unter die entsprechende Lizenz zu stellen.
- Liegt das Ziel der Freigabe einer Software als Open Source in einer langfristigen, nachhaltige Verfügbarkeit der Software, setzt dies den Aufbau einer Community voraus, die auch im Sinne des genannten Tauschverhältnisses längerfristig Beiträge liefert (vgl. Stürmer 2009, S. 4). Solches ist ohne Lizenz mit strengem Copyleft kaum zu erreichen.
- Eher gegen eine Lizenz mit Copyleft spricht eine Software, welche die Basis einer digitalen Kerninfrastruktur schaffen soll (Software-Bibliotheken mit grundlegenden Funktionen). Diesfalls ist eher eine Lizenz mit schwachem Copyleft oder gar eine solche ohne Copyleft zu wählen.
- Gegen die Verwendung einer Software mit Copyleft spricht auch, wenn es schon weit verbreitete vergleichbare Produkte auf dem Markt gibt, die nicht unter Copyleft-Lizenzen stehen, weil diesfalls die Gefahr besteht, dass die durch den Bund neu veröffentlichte Software wenig genutzt wird.

4.4 HAFTUNGSANSPRÜCHE INSBESONDERE

Ferner statuiert Art. 9 Abs. 3 EMBAG, dass Haftungsansprüche von Lizenznehmer*innen auszuschliessen sind. So kann eine Beschaffungsbehörde ausschliessen, dass sie für Fehler haften, die sich in Weiterentwicklungen eingeschlichen haben und bei der Nutzung dieser zu Schäden führen. Bei (international) etablierten Lizenzen ist ein solcher Haftungsausschluss typischerweise bereits durch den Lizenztext abgedeckt, was wiederum für die Verwendung (international) etablierter Lizenzen spricht. Nicht vertraglich wegbedungen werden kann die Haftung für grobe Fahrlässigkeit oder Vorsatz, was in der Praxis aber wenig Relevanz aufweisen wird.[11]

5. ERGÄNZENDE DIENSTLEISTUNGEN (ART. 9 ABS. 5 UND ABS. 6 EMBAG)

Schliesslich stellen die letzten beiden Absätze von Art. 9 EMBAG klar, dass die unterstellten Behörden auch sog. «ergänzende Dienstleistungen» im Zusammenhang mit ihrer OSS zur Verfügung stellen dürfen:

> *Die diesem Gesetz unterstehenden Bundesbehörden können ergänzende Dienstleistungen, insbesondere zur Integration, Wartung, Gewährleistung der Informationssicherheit und zum Support erbringen, soweit die Dienstleistungen der Erfüllung von Behördenaufgaben dienen und mit verhältnismässigem Aufwand erbracht werden können. (Abs. 5)*

Als «ergänzende» Dienstleistungen[12] gelten Dienstleistungen, welche die jeweilige Behörde nicht ausschliesslich zur Erfüllung der gesetzlichen Aufgabe erbringt (die aber typischerweise damit in einem Zusammenhang stehen), die sie aber «ergänzend» dazu auf privatwirtschaftlicher Basis erbringen kann, wenn Nachfrage besteht. Da diese Art von Dienstleistungen nicht direkt vom gesetzlichen Kernauftrag der jeweiligen Behörde

---

11 Während in der Botschaft vom EMBAG auf Art. 164 BV und somit auf das öffentliche Haftungsrecht verwiesen wird, wird hier die Meinung vertreten, dass sich eben gerade aus der privatrechtlichen Natur der Lizenzen Haftungsanspruche daraus nach dem OR richten (Schlauri, 2023).

12 Auch «gewerbliche» Dienstleistungen (Botschaft EMBAG, S.38) oder «erweiterte Dienstleistungen» genannt (Art. 4 MetG).

gedeckt ist und in einem Spannungsverhältnis zur verfassungsmässigen Wettbewerbsneutralität des Bundes steht, können Behörden diese möglicherweise nur mit einer gesetzlichen Grundlage erbringen. In Bezug auf OSS-Dienstleistungen stellt Art. 9 Abs. 5 EMBAG eine solche gesetzliche Grundlage dar.

Als Beispiel für ergänzende Dienstleistungen nennt Art. 9 Abs. 5 EMBAG die Integration oder die Wartung der entwickelten Software (für eine andere Behörde oder ein privates Unternehmen) sowie Dienstleistungen in Bezug auf die Informationssicherheit. Diese zusätzlichen Leistungen können notwendig sein, um die korrekte Implementation der Software zu gewährleisten und ihre Nutzung und Verbreitung zu fördern.

Um die Wettbewerbsneutralität des Staates zu gewährleisten, müssen die Behörden solche ergänzenden Dienstleistungen zu zumindest kostendeckendem Entgelt erbringen (9 Abs. 6 EMBAG).[13] Ausnahmen von diesem Grundsatz der Kostendeckung sind nur dann erlaubt, wenn der Bund ein überwiegendes öffentliches Interesse an der Erbringung der ergänzenden Dienstleistung hat (z.B. zur Förderung von OSS, vgl. Botschaft EMBAG, S. 69). Kostenlos erbrachte ergänzende Dienstleistungen sind aber nur dann möglich, wenn der private Markt diese nicht anbietet (Botschaft EMBAG, S. 69).

So oder so empfiehlt es sich aus Gründen des Projektmanagements, des Vertragsrechts und wo einschlägig auch des Beschaffungsrechts, sich früh zu überlegen, welche weiteren Dienstleistungen wie Wartungs- und Supportarbeiten bei der Implementierung der Software anfallen (so auch Praxisstudie BFH, S. 43). Bei OSS gehört dazu auch die Frage, ob die betreibende Behörde genug Kapazitäten für das sog. «Community Management» hat. Falls dies nicht der Fall ist, bzw. wenn die die OSS nutzende Behörde keine Kapazitäten für die mit der Implementierung zusammenhängenden Dienstleistungen hat (also der im umgekehrten Fall als in Art. 9 Abs. 5 EMBAG beschrieben) ist zu definieren, wer diese Rolle übernehmen soll. Wenn die jeweilige Software-Lösung auf dem freien Markt eingekauft wird, können diese Leistungen auch von der Anbieterin

[13] Die Angst vor Wettbewerbsverzerrungen durch das EMBAG bzw. die in Art.9 Abs. 5 EMBAG verankerte Möglichkeit zur Erbringung der ergänzenden Dienstleistungen wurde auch in der Vernehmlassung geäussert, vgl. Vernehmlassungsantworten von Economiesuisse und der FDP, Vernehmlassungsbericht EMBAG, S. 34.

eingefordert werden. Dies ist dann im Beschaffungsprozess jeweils in der Ausschreibung als Eignungs- oder Zuschlagskriterium festzuhalten (vgl. auch Stürmer & Koch, 2024).[14]

6. FAZIT: KEIN ALLHEILMITTEL, ABER EIN GUTER ANFANG

Ursprünglich durch Rechtsunsicherheiten und Vorbehalte geprägt, hat die Diskussion über OSS in Behördensoftware über die letzten Jahre hinweg zu einem Umdenken geführt. Das EMBAG markiert dabei einen Wendepunkt, indem es OSS als Standard für Behördensoftware in Art. 9 EMBAG kodifiziert. Dies ist ein wichtiger erster Schritt in Richtung wirtschaftlicher und digitaler Nachhaltigkeit von Behördensoftware. Die Norm kann zudem als Basis für die Umsetzung des «Einer-für-alle-Ansatzes» auch in der Schweiz darstellen, d.h. sie kann dazu beitragen, dass einmal entwickelte Software durch verschiedene Behörden (auch über verschiedene föderale Ebenen hinweg) mehrfach genutzt werden kann.

Die OSS-Pflicht im EMBAG hat auch beschaffungsrechtliche Implikationen (zumindest was Software betrifft, die nicht inhouse oder instate, sondern extern auf dem Markt entwickelt und öffentlich beschafft wird). So führt das Gesetz dazu, dass die Beschaffungsbehörden alle OSS-relevanten Kriterien (wie beispielsweise die Lizenz) in der Ausschreibung wiedergeben müssen. Diesbezüglich sind noch viele Fragen offen: Welche Kriterien sollen bei OSS-Ausschreibungen als notwendige technische Spezifikationen oder Eignungskriterien, welche als wünschenswerte Zuschlagskriterien aufgenommen werden? Wie sollen das Community-Management und weitere Wartungs- und Supportarbeiten gehandhabt werden? Besteht die Möglichkeit, eine Entwicklung oder Beschaffung gemeinsam in Kooperation mit anderen Behörden durchzuführen? Wenn ja, wer beteiligt sich in welchem Umfang? Obwohl z.B. der Kanton Zürich bereits in der Vernehmlassung auf die «Wichtigkeit von beschaffungsrechtlich einwandfreien Grundlagen» hingewiesen hat, wurden bislang keine solche Grundlagen zur Verfügung gestellt.

Abschliessend lässt sich in Anlehnung an die parlamentarische Debatte (Votum von Ständerat Benedikt Würth, parlamentarische Debatte zum EMBAG vom 1. Juni 2022) festhalten, dass man «von diesem Gesetz keine Wunder erwarten» kann, aber dass

[14] Dazu im Detail auch Beitrag von Chantal Lutz und Cédric Miehle.

es «ein wichtiges Element ist, damit wir in der digitalen Transformation besser und strukturierter voranschreiten können». Wie schnell und gut das Gesetz seine Ziele erreichen wird und wie das Instrument der OSS-Pflicht in der Praxis eingesetzt wird, wird sich im Laufe des Implementierungsprozesses zeigen.

BIBLIOGRAPHIE

Aegerter, J. (2012, 22. Oktober). Streit um Open-Source-Lösung «Openjustitia». *Netzwoche*. https://www.netzwoche.ch/news/2014-03-18/streit-um-open-source-loesung-openjustitia

Botschaft zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben. (2022, 4. März). BBl 2022 804. (zit.: Botschaft EMBAG).

Bundesministerium des Inneren und für Heimat (2023). *Einer für Alle – Einfach erklärt*.

https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/efa/efa-node.html

Eidgenössisches Finanzdepartement EFD. (2022, 4. März). *Vorentwurf des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBaG), Vernehmlassung vom 11. Dezember 2020 bis zum 25. März 2021 Bericht über die Ergebnisse der Vernehmlassung*. (Zit.: Vernehmlassungsbericht). https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87454.html.

Forschungsstelle Digitale Nachhaltigkeit. (2021, 17. Juni). Open Source Studie Schweiz. (zit.: OSS-Studie 2021). www.oss-studie.ch.

Informatiksteuerungsorgan des Bundes (ISB). (2019). *Praxis Leitfaden, Open Source Software in der Bundesverwaltung*. (Zit.: Praxisleitfaden ISB.). Abgerufen von: https://www.bk.admin.ch/dam/bk/de/dokumente/dti/ikt-vorgaben/strategien/oss/Praxis-Leitfaden_OSS_Bundesverwaltung_V_1-0.pdf.download.pdf/Praxis-Leitfaden_OSS_Bundesverwaltung_V_1-0.pdf.

Müller, G., & Vogel, S. (2014, 26. März). *Rechtsgutachten zur verfassungsrechtlichen Zulässigkeit der Randnutzung von Software im Verwaltungsvermögen, insbesondere der*

Veröffentlichung und Verbreitung von Open-Source Software durch Träger von Bundesaufgaben. https://www.news.admin.ch/NSBSubscriber/message/attachments/37015.pdf.

Parlamentarische Debatte zum EMBAG vom 01. Juni 2022. Ständerat, dritte Sitzung. Amt.Bull. S 2022.022. www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=57030.

Poledna, Th., Simon S. & Samuel S. (2017). *Rechtliche Voraussetzungen der Nutzung von Open-Source Software in der öffentlichen Verwaltung, insbesondere des Kantons Bern*. Berlin – Bern: Carl Grossman Verlag. www.carlgrossmann.com/poledna-schlauri-schweizer-rechtliche-voraussetzungen-der-nutzung-von-open-source-software-in-der-oeffentlichen-verwaltung-insbesondere-des-kantons-bern.

Antrag des Zürcher Regierungsrates vom 15. September 2021 für einen Beschluss des Kantonsrates zum Postulat KR-Nr. 65/2019 betreffend Synergien beim Software-Einsatz im Kanton Zürich

Nutzen, KR-Nr. 65/2019.

Schlauri, S. (2023). *Open Source Software im neuen Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG).* [PPT-Präsentation gehalten an der IT-Beschaffungskonferenz am 22. August 2023.] *www.bfh.ch/dam/jcr:4a363a57-b139-476f-9f27-83d32dc9eb0c/Pr%C3%A4sentation%20-%20Simon%20Schlauri.pdf.*

Straub, W. (2024). *Softwareschutz – Urheberrecht, Patentrecht, Open Source* (2. Aufl.). Dike.

Stürmer, M. (2023). *«Open by default» als Gesetz*. www.societybyte.swiss/2023/07/12/open-by-default-als-gesetz.

Stürmer, M. (2009). *How Firms Make Friends: Communities in Private-Collective Innovation.* ETH Zürich, Doctoral Dissertation No. 18630. www.researchgate.net/publication/228536679_How_Firms_Make_Friends_Communities_in_Private-Collective_Innovation

Stürmer, M. & Koch, R. (2024). *Whitepaper zur öffentlichen Beschaffung von Open Source Software gem. Art. 9 EMBAG.* Erscheint demnächst auf Societybyte.

ABHÄNGIGKEITEN VON ICT-HERSTELLERN REDUZIEREN: WIEDERKEHRENDE WARTUNGSVERTRÄGE, VERMEIDUNG VON «AUSNAHMEFREIHÄNDERN», BESCHAFFUNG VON OPEN SOURCE SOFTWARE ETC.

Chantal Lutz / Cédric Miehle

Chantal Lutz, Rechtsanwältin, verfügt über Weiterbildungen im Datenschutz und in der Cybersecurity.

Cédric Miehle, Rechtsanwalt, verfügt über das CAS öffentliche Beschaffung und ist seit 2020 als Senior Associate bei Domenig & Partner tätig.

Abstract: *Überschwellige Freihandvergaben können Anbieter vom Markt ausschliessen oder langfristige Abhängigkeiten schaffen. Deshalb ist es wichtig, Freihandvergaben restriktiv handzuhaben und gut zu begründen.*

INHALTSVERZEICHNIS

1 Einleitung 40
2 Gesetzliche Voraussetzungen 40
2.1 Gesetzliche Grundlage 40
2.2 Zweck der überschwelligen Freihandvergabe 41
2.3 Problemfelder 41
3 Rechtliche Problemfelder 43
4 Lösungsvorschlag 45
5 Schlussfolgerung 51
Bibliografie 52

*Die Autor*Innen zeigen in diesem Beitrag auf, wie das neue Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) Grundlagen zur künftigen Reduktion der schafft. Das EMBAG sieht die Veröffentlichung von Software-Quellcodes vor. Durch die Förderung von Open-Source-Software (OSS) soll die digitale Souveränität und Interoperabilität innerhalb der Verwaltung gestärkt werden. Dies hat das Potenzial, die Digitalisierung effizienter und kostengünstiger zu gestalten. Kantone und Gemeinden können von mehr frei verfügbarer Software langfristig profitieren. Dies fördert den Aufbau von Open Source Communities, die die Softwarequalität in der Verwaltung nachhaltig verbessern können.*

1 EINLEITUNG

Im Bereich der Bundesverwaltung wurden im Jahr 2020 von 1'321 Vergaben über dem WTO-Schwellenwert 610 Vergaben im überschwelligen freihändigen Verfahren vergeben. Dies entspricht einem Anteil von 46,1%, obwohl das freihändige Verfahren eine Ausnahme darstellt. In absoluten Zahlen wurden somit CHF 3.92 Mill. von insgesamt CHF 8.11 Mill. überschwellig freihändig vergeben. CHF 1.91 Mill. des Vertragsvolumens der überschwellig freihändigen Vergaben im Jahr 2020 basieren auf den Ausnahmetatbeständen der technischen Besonderheiten bzw. aus Gründen des Schutzes des geistigen Eigentums oder des unzumutbaren Anbieterwechsels (BKB, 2020, S. 12 ff.). Damit spielt die Lieferantenabhängigkeit bzw. die Abhängigkeit von einem bestimmten, proprietären Produkt eine massgebende Rolle bei Beschneidung des freien Wettbewerbs im Vergabeverfahren. Chantal Lutz und Cédric Miehle zeigen in diesem Beitrag auf, dass die zunehmende Beschaffung von nicht proprietärer Software (sog. Open Source Software, nachfolgend «OSS») diese Abhängigkeiten verringern kann. Ausserdem gehen sie darauf ein, wie der Lieferantenabhängigkeit mittels vertraglicher Mechanismen vorgebeugt werden kann.

2 GESETZLICHE VORAUSSETZUNGEN

2.1 GESETZLICHE GRUNDLAGE

Das freihändige Verfahren ist bei der Beschaffung von Bauleistungen unter CHF 300'000.00 sowie bei Lieferungen und Dienstleistungen unter CHF 150'000.00 stets zulässig. Wer-

den diese Schwellenwerte erreicht oder überschritten, sind freihändige Vergaben nur bei Vorliegen einer der in Art. 21 Abs. 2 und 3 des Bundesgesetzes über das öffentliche Beschaffungswesen vom 21. Juni 2019 (BöB) genannten Ausnahmen erlaubt.

Die aufgezählten Tatbestände in Art. 21 Abs. 2 und 3 BöB sind abschliessend. Das bedeutet, dass keine weiteren Ausnahmen hinzugefügt oder auf ähnliche Weise interpretiert werden können.

2.2 ZWECK DER ÜBERSCHWELLIGEN FREIHANDVERGABE

Das überschwellige Freihandverfahren deckt Fälle ab, in welchen das Einladungs-, offene und selektive Verfahren nicht durchführbar oder nicht zweckmässig sind, z. B., weil ein Wettbewerb aus Gründen des Schutzes von Immaterialgüterrechten nicht möglich ist. Gleiches gilt z.B. für Folgebeschaffungen oder für aus unvorhersehbaren und nicht selbst verschuldeten Gründen dringliche Beschaffungen. Eine Besonderheit gilt für die Beschaffung von Leistungen, die für Verteidigungs- und Sicherheitszwecke unerlässlich sind. Eine freihändige Vergabe auf Grund von Sicherheits- und Verteidigungszwecken ist gerechtfertigt und völkerrechtlich unbedenklich, da solche Beschaffungen ausserhalb des Staatsvertragsbereichs erfolgen (Botschaft BöB,1926 und 1929). Die überschwellige Freihandvergabe soll als Ausnahme ermöglichen, die wirtschaftlichen Gegebenheiten, die Dringlichkeit, die rechtlichen Voraussetzungen oder im Rahmen der Sicherheitspolitik die Interessen der Schweiz berücksichtigen zu können. Es soll demnach Anwendung finden, wenn das Beschaffungsrecht an seine Grenzen stösst und nicht zweckdienlich ist, da entweder andere Grundsätze oder Rechtsgüter (z.B. Immaterialgüterrechte), als die des Beschaffungsrechts höher zu gewichten sind, oder das Beschaffungsrecht in zeitlicher Hinsicht keine Lösungsoption darstellt.

2.3 PROBLEMFELDER

Beim überschwelligen Freihandverfahren vergibt der Auftraggeber den Beschaffungsauftrag direkt und ohne Ausschreibung einem Anbieter. Der Auftraggeber tritt in diesem Fall direkt mit einem Anbieter in Verhandlungen, ohne vorab eine Ausschreibung durchgeführt zu haben. Entsprechend handelt es sich beim überschwelligen freihändigen Vergabeverfahren nicht um ein mit dem Einladung-, offenen oder selektiven Verfahren gleichwertigen Instrument, da nicht begriffsnotwendig ein Wettbewerb zwischen den

Anbietern stattfindet. Damit hat das überschwellige freihändige Verfahren zur Folge, dass die Grundsätze des Vergaberechts – Wirtschaftlichkeit, Transparenz, Wettbewerb – nur in abgeschwächter bzw. in keiner Form zum Tragen kommen (EFD, 2015, S. 24).

Im Jahr 2020 tätigte die gesamte Bundesverwaltung 1'321 Vergaben über dem WTO-Schwellenwert mit einem Volumen von CHF 8.11 Mill. 51.6% dieses Volumens, in Zahlen CHF 4.18 Mill.[1], wurden in einem Wettbewerbsverfahren (offenes Verfahren, selektives Verfahren oder Einladungsverfahren) vergeben.

In Gefahren- und Dringlichkeitslagen kann das Vergabeverfahren ausnahmsweise beschleunigt und vereinfacht werden. Wegen Dringlichkeit aufgrund unvorhersehbarer Ereignisse kann überschwellig freihändig vergeben werden (vgl. Art. 21 Abs. 2 Bst. d BöB): Das freihändig vergebene Vertragsvolumen unter Bst. d erhöhte sich im Rahmen der Pandemie von um rund CHF 54 Mio. 2019 (CHF 21 Mio.) auf CHF 75 Mio. in 2020 und schwankt seither (siehe Beschaffungscontrolling des Bundes, 2023). Dies kann auf verschiedene Ursachen zurückgeführt werden. Die Covid-19-Pandemie begründet sicherlich den grössten Anteil der Zunahme der freihändigen Vergaben über dem WTO-Schwellenwert (ca. CHF 450 Mio.): Das Volumen der freihändigen Vergaben ist im Verhältnis zum Gesamtvolumen aller Vergaben über dem WTO-Schwellenwert gegenüber dem Vorjahr um 23 Prozentpunkte angestiegen (von CHF 2.22 Mill. auf CHF 3.92 Mill.; BKB, 2020, S. 3 f.). Der Anteil der überschwelligen Freihandvergaben war schon in den Jahren vor der Covid-19-Pandemie hoch und ist nicht nur aufgrund der Covid-19-Pandemie angestiegen. Insofern lohnt es sich hinzusehen, wo ausser bei der Dringlichkeit, die Vergaben freihändig im überschwelligen Bereich getätigt wurden, um die Problemfelder zu eruieren.

Die Dringlichkeit ist mit Ausnahme des Covid-19 Jahr 2020 bei den überschwelligen Freihandvergaben kein grosses Problem, da sie selten als Begründung beigezogen wird. Vielmehr sind die Probleme bei überschwelligen Freihandvergaben aufgrund von technischen oder künstlerischen Besonderheiten der Vergabegegenstände oder

[1] Diese Kennzahl ist inkl. der aufgrund von Art. 10 Abs. 4 BöB vom Beschaffungsrecht ausgenommen Beschaffungen aufgrund Schutz und Aufrechterhaltung der Sicherheit, Schutz der Gesundheit oder des Lebens von Menschen und ähnliches. Beschaffungen in diesem Bereich beliefen sich im Jahr 2020 auf CHF 424 Mio. im Gegensatz zu CHF 3 Mio. im Jahr 2019.

des Schutzes geistigen Eigentums. Bei spezifischen Vergaben, wie z.B. spezifizierter Software, besteht die Möglichkeit, dass nur ein Anbieter auf dem Markt ist, jedoch sind die überschwelligen Vergaben heikel im Bereich von Folgeaufträgen oder wenn noch gar keine Abhängigkeiten bestehen (Sonntagszeitung, 13.09.2019, S. 4 – S.5). Insofern wird in diesem Beitrag der Fokus auf überschwellige Freihandvergaben im Bereich von Folgeaufträgen sowie Abhängigkeiten und technischen Voraussetzungen beim Beschaffungsgegenstand gelegt.

3 RECHTLICHE PROBLEMFELDER

Bei einer Freihandvergabe ist bereits relevant und zu prüfen, ob eine frühere und möglicherweise unzulässige Beschaffungsstrategie dazu geführt hat, dass ein Markt weiterhin abgeschottet wird und anderen potentiellen Anbietern nicht mehr offensteht (Schneider-Heusi & Mazzariello, 2011, S. 6.).

Wenn Sachzwänge vorliegen, können sich langjährige Abhängigkeiten von einem proprietären Anbieter ergeben, die einen vom Beschaffungsrecht beabsichtigten Wettbewerb faktisch verunmöglichen. Wenn sich die Einreichung von allenfalls wirtschaftlicheren Konkurrenzofferten selbst für Teilbereiche wie Wartung und Support erübrigt, ist das ein grosses Warnsignal, dass solche Sachzwänge vorliegen (Poledna & do Canto, 2009, S. 5). Obwohl das Beschaffungsrecht als Zweck die Verhinderung von Kollusionen hat, sind die Mittel des Vergaberechts diese Abhängigkeiten und allenfalls kartellrechtlich unzulässigen Verhaltensweisen zu lösen, nur begrenzt vorhanden (Schneider-Heusi & Mazzariello, 2011, S. 6.). Dies bedeutet aber nicht, dass eine eingeschlagene Beschaffungsstrategie nicht mehr korrigiert werden darf bzw. sogar korrigiert werden muss.

Eine langjährige Zusammenarbeit mit einem Anbieter darf für die Vergabestelle keinen Grund darstellen, dass ein Beschaffungsgegenstand nicht mehr ausgeschrieben wird. Zudem sind die von Dritten bezogenen Leistungen stets periodisch zu überprüfen. Die überschwellige freihändige Vergabe zugunsten eines einmal ausgewählten ursprünglichen Anbieters muss auf zwingenden, von Art. 21 Abs. 2 Bst. e BöB legitimierten Gründen, und nicht aufgrund bestehender Sachzwänge beruhen. Zu hohe Kosten beim Wechsel des Anbieters, zusätzlicher Aufwand und/oder mehr Zeitbedarf bei einem Wechsel

eines Anbieters oder einer Bau- oder Dienstleistung sind in aller Regel unzureichende Gründe für eine überschwellige freihändige Vergabe.

Die Vergabestelle hat stichhaltig und schriftlich zu begründen, weshalb es an der Austauschbarkeit fehlt. Hinsichtlich der erwarteten Mehrkosten liegt die Schwelle hoch: Nicht jede Erhöhung der erwarteten Kosten berechtigt zum Ausschluss des Wettbewerbs. Vielmehr muss feststehen, dass die Mehrkosten unverhältnismässig sind, das heisst, dass sie in keinem angemessenen Verhältnis zum Auftragspreis der fraglichen überschwelligen Freihandvergabe stehen. Gemäss Art. 15 Abs. 4 BöB dürfen deshalb Daueraufträge die Dauer von fünf Jahren in der Regel auch nicht überschreiten.

Folgebeschaffungen setzen einen vergaberechtskonformen Grundauftrag voraus. Wenn der Auftragswert für eine Folgebeschaffung den Schwellenwert für eine offene oder selektive Ausschreibung erreicht, so muss auch der Grundauftrag offen oder selektiv ausgeschrieben werden. In Ausnahmefällen, wenn stichhaltige Begründungen vorliegen, darf der Auftragswert eines Folgeauftrags höher sein als der Auftragswert eines Grundauftrags, wobei der Grundauftrag in diesem Fall zumindest im Einladungsverfahren vergeben worden sein muss. Bei Beschaffungen gemäss Art. 20 Abs. 3 BöB gilt dies ohne Beachtung der Schwellenwerte (Botschaft BöB, 1927 f.).

Die Vergabestelle kann sich zudem nicht auf Art. 21 Abs. 2 lit. a BöB berufen und geltend machen, es liege ein erfolgloses vorangegangenes Verfahren vor, wenn das vorangegangene Verfahren in Verletzung der Regeln über die Verfahrenswahl z.B. als Einladungsverfahren organisiert wurde, obwohl es als selektives oder öffentliches Verfahren hätte durchgeführt werden müssen. Des Weiteren darf sich die Vergabestelle auch nicht auf diese Klausel stützen, wenn die wesentlichen Erfordernisse und Bedingungen der Beschaffung im Vergleich zum vorangegangenen, abgebrochenen Verfahren wesentlich verändert wurden (VGer TI 52.2018.305 vom 14.11.2018).

Erstvergaben, als überschwellige Freihandvergaben, sind gemäss Art. 21 Abs. 2 lit. c BöB nur dann zulässig, wenn ein Auftrag aufgrund seiner technischen oder künstlerischen Besonderheiten oder aus Gründen des Schutzes des geistigen Eigentums nur an einen bestimmten Anbieter erteilt werden kann. Dies ist zum Beispiel dann

der Fall, wenn dieser Anbieter mangels angemessener Alternativen als einziger in der Lage ist, ein entsprechendes Produkt zu liefern beziehungsweise eine entsprechende Bau- oder Dienstleistung zu erbringen. Zur Rechtfertigung der überschwelligen Freihandvergabe ist der Auftraggeber nicht nur zur Dokumentierung der technischen Gründe verpflichtet, sondern er muss auch glaubwürdig darlegen und nachweisen, dass diese Gründe die überschwellige Freihandvergabe unbedingt erforderlich machen (Botschaft BöB,1926 f.).

Die Vergabestelle kann sich nicht auf Art. 21 Abs. 2 lit. c BöB berufen mit der Argumentation des Vorliegens von rechtlichen Besonderheiten, wenn die Ausschliesslichkeitsrechte, die bei einem bestimmten Anbieter liegen, auf einen durch die Vergabestelle zu einem früheren Zeitpunkt vergebenen Vertrag zurückzuführen sind, in dem sich die Vergabestelle den Erwerb dieser Rechte hätte ausbedingen können. Die Vergabestelle ist bei ihren Vertragsschlüssen dazu verpflichtet, darauf zu achten, wettbewerbsausschliessende Situationen zu vermeiden (Beyeler, 2020, Rz. 110; VGer SG B 2016/146, 22.2.2018).

4 LÖSUNGSVORSCHLAG

Die Problemfelder sind bei überschwelligen Freihandvergaben offensichtlich technische oder künstlerische Besonderheiten der Vergabegegenstände oder der Schutz des geistigen Eigentums mit CHF 572 Mio. und Folgeaufträge aufgrund bestehender Abhängigkeiten mit CHF 740 Mio. im Jahr 2022 (BKB, 2022, S. 21). Im Vergleich dazu beliefen sich die Zahlen im Jahr 2020 auf CHF 1.49 Mill. für überschwellig freihändige Beschaffungen (im Folgend «IT-Freihänder») basierend auf dem Ausnahmetatbestand der technischen Besonderheiten oder aus Gründen des Schutzes geistigen Eigentums sowie auf CHF 425 Mio. wegen bestehender Abhängigkeiten (BKB, 2020, S. 14 f).

Insbesondere im IT-Bereich sind überschwellige Freihandvergaben weit verbreitet. So machten die IT-Freihänder in den letzten drei Jahren im Durchschnitt 43.5% sämtlicher Beschaffungen in diesem Bereich aus. Dies im Vergleich zu den Freihändern insgesamt, deren Anteil bei ca. 20% liegt.

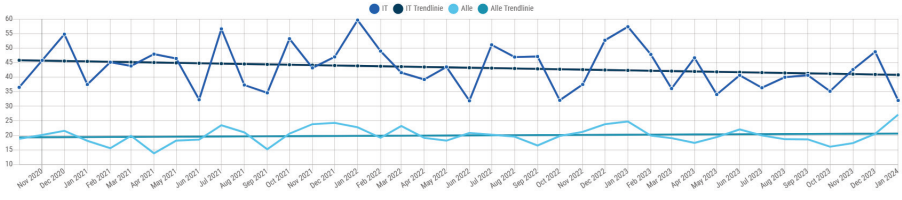

Abbildung 1. Anzahl Freihänder in Prozent im Vergleich zu den Freihändern insgesamt, Messzeitraum 09.10.2020 bis 09.10.2023. (Intelliprocure.ch)

Um überschwellige Freihandvergaben bei der Softwarebeschaffung, deren Weiterentwicklung und den dazugehörigen Dienstleistungen wie Wartung effektiv und nachhaltig zu reduzieren, müssen folgende Problemfelder angegangen werden:

1. Die Bedarfsstelle wird den Grund der technischen Besonderheiten vor allem dann anführen, wenn es auf den ersten Blick nur einen Softwareanbieter auf dem Markt gibt, dessen Produkt die geforderten Eigenschaften erfüllt. Es kann auch sein, dass die geeignete Lösung bislang noch nicht vorliegt und die Weiterentwicklung von bereits am Markt etablierter Software eine vielversprechende Option darstellt. Was auf eine solche Vergabe folgt, ist ein sog. Vendor Lock-In.
2. Gibt es keine Software, welche die Bedürfnisse der Bedarfsstelle erfüllt, werden die technischen Besonderheiten weniger relevant sein, da eine Neuentwicklung notwendig ist. In einem solchen Fall besteht die Gefahr von Sachzwängen, die sich daraus ergeben, dass künftig nur der Zuschlagsempfänger in der Lage sein wird, die beschaffte Software weiterzuentwickeln oder zu warten. Dies kann daran liegen, dass der Knowhow-Transfer zur Bedarfsstelle nicht als Vergabekriterium definiert oder ein solcher mangels interner Ressourcen der Bedarfsstelle nicht erfolgt ist.

Die dargestellten Sachzwänge werden vom neuen Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben vom (EMBAG) aufgegriffen. Es verlangt die konsequente Veröffentlichung von Quellcode von Eigen- oder Fremdentwicklungen unter Verwendung von international etablierten Lizenztexten durch die Bundesverwaltung. Lediglich bei Sicherheitsbedenken oder wenn Teile der Software

proprietär sind, kann von der Veröffentlichung abgesehen werden (vgl. Art. 9 Abs. 1 EMBAG).[2]

Mit diesem Schritt verankert der Bund seine strategischen Überlegungen zum Einsatz von OSS[3] auf Gesetzesebene. Diese beinhalten insbesondere die Beschleunigung der Digitalisierung durch effiziente Softwareentwicklung sowie auch die kostengünstige Beschaffung von Software, indem Lizenzgebühren eingespart und an anderen Orten wie bei der Wartung und Weiterentwicklung eingesetzt werden können (ISB, 2019a, S. 4 f.).

Das EMBAG fördert ausserdem die Verbreitung von OSS. Betrachtet man die Open Source Studie 2021 (Open Source Studie Schweiz, n.d.)[4] ist ersichtlich, dass 43.8% der befragten Personen aus Kantons- und Gemeindeverwaltungen die Relevanz von OSS in ihrer Organisation als «*eher zugenommen*» einstufen. 60.8% dieser Befragten gaben als wichtigsten Grund für den Einsatz von OSS die Unterstützung von interoperablen Standards, d.h. die Kommunikation und Integration über verschiedene Systeme hinweg, an. Veröffentlicht die Bundesverwaltung nun vermehrt den Quellcode von eigen- und fremdentwickelter Software, wird dies vermutlich einen positiven Effekt auf die digitale Zusammenarbeit auf allen Verwaltungsstufen und mit öffentlichen Organisationen haben. Hiermit erhofft sich der Bundesrat eine Stärkung der digitalen Souveränität der Verwaltung in der Schweiz (Botschaft EMBAG, S. 36 f.).

Die Verwaltungsträger auf Stufe Kanton und Gemeinden werden vermehrt auf bestehende, insbesondere von Bundesbehörden veröffentlichte und frei verfügbare Software zurückgreifen können. In der Folge werden entsprechende Beratungs-, Integrations-, Weiterentwicklungs-, Betriebs-, Wartungs- und Supportleistungen für OSS kostenpflich-

---

[2] Für eine genaue Analyse von Art. 9 EMBA siehe auch Beitrag von Rika Koch und Simon Schlauri in diesem Band.

[3] Die Botschaft zum EMBAG definiert OSS wie folgt: «*Als OSS wird Software bezeichnet, deren Quellcode offengelegt wird und die von jedermann lizenzgebührenfrei benutzt, studiert, verändert, weiterentwickelt und weitergegeben werden darf. Die Verbreitung erfolgt üblicherweise mittels Lizenz, eine Lizenzgebühr wird jedoch nicht geschuldet.*» (Botschaft EMBAG, S. 36).

[4] Ausgewählte Kriterien: Funktion: 7/7, Bezüger/Anbieter: 2/4 (Interner IT-Anbieter und Informatik-Nutzer/Bezüger/Anwender), IT-Budget: 9/9, Branche/Sektor: 2/16 (Kantonsverwaltung und Stände- und Gemeindeverwaltung), Organisationsgrösse: 7/7.

tig beschafft werden müssen. Um entsprechenden Sachzwängen im Zusammenhang mit Folgeaufträgen bei der Beschaffung dieser Leistungen vorzubeugen, sieht das EMBAG eine gesetzliche Grundlage vor, um die Bildung von sog. Open Source Communities zu fördern. Lebendige Communities tragen entscheidend zur Verbesserung des Quellcodes in qualitativer und sicherheitsrelevanter Hinsicht bei (Schluchen, 2019, S. 15). Gemäss Art. 9 Abs. 5 EMBAG dürfen Bundesbehörden neu ergänzende Dienstleistungen wie Wartung, Support etc. im Zusammenhang mit dem veröffentlichten Quellcode für ein kostendeckendes Entgelt erbringen. Solche Dienstleistungen müssen allerdings der Erfüllung von Behördenaufgaben dienen und verhältnismässig erfolgen.[5] Damit dürfen die Dienstleistungen im Vergleich zur ursprünglichen Verwaltungsaufgabe lediglich ein untergeordnetes Ausmass annehmen und die Privatwirtschaft darf nicht konkurrenziert werden (vgl. Art. 9 Abs. 6 EMBAG; Botschaft EMBAG, S. 67.).

Um Freihänder basierend auf technischen Besonderheiten effektiv zu verhindern, müssen somit auf Ebene Bedarfsstelle freiwillige Massnahmen getroffen werden. Christian Schluchen propagiert im Zusammenhang mit OSS Beschaffungen im Bundesamt für Umwelt BAFU folgende, strategische Massnahmen:

- *«Einführen einer Bedürfnisstrategie, welche die Bedürfnisse der Stakeholder berücksichtigt und zu einer Ausschreibungsvariante führt.*
- *Einführen eines Open Source Technologie-Stacks, welcher etablierte OSS Produkte beinhaltet zu welchen es Dienstleistungs-Anbieter und aktive Communities gibt»* (Schluchen, 2019)

Es scheint insbesondere auch an konkretem Wissen über die Open Source Landschaft, das Vorhandensein von aktiven Open Source Communities und die verschiedenen Open Source Lizenzmodelle zu fehlen (Schluchen, 2019, S. 27, 30 f.). Der Bund hat diese Wissenslücke erkannt und vor knapp vier Jahren reagiert, indem er den Praxis-Leitfaden Open Source Software in der Bundesverwaltung veröffentlichte, worin z.B. eine Übersicht zur Kompatibilität von Open Source Lizenzen enthalten ist (IBS, 2019, S. 11 f.). Auch Initiativen wie die von CH Open betriebene Plattform OSS Directory können die Bedarfsstelle dabei unterstützen, das passende Softwareprodukt zu finden.

[5] Siehe dazu im Detail auch den Beitrag von Rika Koch und Simon Schlauri (Kapitel 5) in diesem Band.

Mit der Inkraftsetzung des EMBAG und der Förderung von weiteren, freiwilligen Massnahmen hat der Bund den Weg für die Verbreitung von OSS in der Verwaltung weiter geebnet. Was ist nun aber bei der Ausschreibung und der anschliessenden Vertragsverhandlung im Zusammenhang mit OSS konkret zu beachten?

Christian Schluchen hat im Rahmen seiner Abschlussarbeit ein Ablaufdiagramm entwickelt, das einer Bedarfsstelle helfe «*während der Beschaffung die richtigen Fragen in der richtigen Reihenfolge zu stellen*» (Schluchen, 2019, S. 36) um zur richtigen Ausschreibungsvariante zu gelangen (zwingend proprietär, zwingend OSS, OSS bevorzugt, Gleichbehandlung beider Varianten). Kommt OSS in Frage, muss vor der Ausschreibung geklärt werden, ob und wie der Quellcode veröffentlicht wird oder nicht, wer sich um das Community Building kümmert und welches Lizenzmodell mit der Veröffentlichungsstrategie kompatibel ist. Gegebenenfalls müssen die entsprechenden Nebenleistungen beim Anbieter mitbeschafft werden (Schluchen, 2019, S. 40 ff.). Insbesondere dort, wo die Software anschliessend von weiteren Verwaltungsträgern (bspw. Gemeinden) genutzt wird, muss sich die Bedarfsstelle im Klaren darüber sein, welche Betreuungsobliegenheiten sie über die Bereitstellung des Quellcodes hinaus hat. Ohne anfängliche Betreuung erfolgt ggf. keine Community Building und der positive Effekt der Qualitätsverbesserung der Software realisiert sich nicht, womit Sachzwänge bei der Beschaffung von Wartungs- und Weiterentwicklungsleistungen nicht effektiv vermieten werden.

Die für die Veröffentlichung beabsichtigte OSS-Lizenz sollte bereits bei der Ausschreibung mitberücksichtigt werden, denn sie bestimmt, inwiefern Weiterentwicklungen künftig veröffentlicht werden müssen und ob deren Kommerzialisierung zulässig ist. Das EMBAG sieht in diesem Zusammenhang die Verwendung etablierter OSS-Lizenzen vor. Dies könne für die Zusammenarbeit zwischen Gemeinwesen günstig sein, da diese Lizenztexte viele rechtliche Fragen unkompliziert und im Paket regeln (Botschaft EMBAG, S. 65). Es müsse zudem geprüft werden, ob vorbestehende Rechte Dritter an Teilen der zu beschaffenden Software eine Veröffentlichung des Quellcodes verhindern könnte. Die Bedarfsstelle muss sich also die nötigen Rechte ausbedingen. Der Bundesrat schlägt in seiner Botschaft zum EMBAG vor, *«dass in einem Beschaffungsverfahren die für das betreffende Projekt relevanten Merkmale von OSS als Eignungs- oder Zuschlagskriterium definiert wird.»* (Botschaft EMBAG, S. 39)

Christian Schluchen und Reto Scholl empfehlen allerdings, kein spezifisches OSS-Lizenzmodell vorzugeben, sondern lizenzneutral auszuschreiben und höchstens den Ausschluss gewisser Lizenzen zu deklarieren sowie zu begründen (Schluchen, 2019, S. 29; Scholl, 2019, S. 35). Um eine Teilnahme von möglichst vielen Anbietern zu begünstigen und den freien Wettbewerb zu fördern, sollte die Ausschreibung somit möglichst lizenz- und produkteneutral formuliert werden. Schlussendlich sollte es die Bedarfsstelle nicht verpassen, im Rahmen der Beschaffung die beabsichtigte Quellcodeveröffentlichung als Kriterium aufzunehmen und als Lösungsarchitektur auch Empfehlungen in Bezug auf die Wahl des richtigen Lizenzmodells oder die richtige Veröffentlichungsform zu verlangen. Eine entsprechend frühzeitige Berücksichtigung dieser Aspekte dient schlussendlich der Entwicklung einer effektiven Open Source Community, bei welcher ausreichend Entwickler Wissen über den Quellcode verfügen und eigene Weiterentwicklungen wieder in die Community zurückgeben können oder, je nach Lizenzmodell, müssen.[6]

In vertraglicher Hinsicht sollten namentlich folgende Aspekte berücksichtigt werden:[7]

1. Bei Neu-/Weiterentwicklung:
   a. Vornahme einer klaren Abgrenzung von vorbestehender Software des Anbieters und Übertragung des Urheberrechts an die Bedarfsstelle (ISB, 2019b, S. 19).
   b. Regelung der Rechtsgewährleistung durch den Anbieter, indem verlangt wird, dass er der Bedarfsstelle die zeitlich unbeschränkte Nutzungsmöglichkeit von vorbestehenden Softwarekomponenten rechtsgültig verschaffen kann (Schluchen, 2019, S. 92).

---

[6] Vgl. auch die Datenbank zu den verschiedenen OSS-Lizenzmodellen: https://opensource.org/licenses/, Filtermöglichkeit: «Popular / Strong Community».

[7] Weitere Hilfestellungen für Ausschreibungen und Verträge: Kompetenzzentrum Beschaffungswesen Bund KBB und Rechtsdienst Bundesamt für Bauten und Logistik BBL. (2015). *Merkblatt Software-Ausschreibungen: Sicherstellung eines breiten Wettbewerbs.* https://www.bkb.admin.ch/dam/bkb/de/dokumente/Hilfsmittel/Merkblaetter/13_Merkblatt_Software_Ausschreibungen_inkl_%20IT_ABG_und_Pflichtenheftbeilage.pdf.download.pdf/13_Merkblatt_Software_Ausschreibungen_inkl_%20IT_ABG_und_Pflichtenheftbeilage.pdf.

   c. Ggf. Regelung der Publikationspflicht und Veröffentlichungsart des Quellcodes durch den Anbieter, insbesondere bei OSS-Modellen mit Copy-Left Effekten (Schluchen, 2019, S. 91).
   d. Ggf. Aufbau und Pflege der Community.
2. Bei Wartungs- und Supportverträgen:
   a. Sicherung des Knowhow-Transfers sowie ggf. der Service Transition in Bezug auf den Betrieb des Service Desks oder der Weiterentwicklung zur Bedarfsstelle oder zu einem neuen Anbieter.
   b. Ggf. Regelung des Life-Cycles der Software wie allfällige Migration oder die Ablösungen von veralteter Software (Schluchen, 2019, S. 31).

5 SCHLUSSFOLGERUNG

Aufgrund der freien Verfügbarkeit des Quellcodes inkl. Dokumentation von OSS kann sich grundsätzlich jede Person das notwendige Wissen zur Software aneignen und diese verändern. Der Ausnahmetatbestand von Art. 21 Abs. 2 lit. c BöB bezüglich technischer Besonderheiten oder Schutz des geistigen Eigentums greift nur dort, wo noch kein angemessenes Alternativprodukt auf dem Markt existiert und eine Eigenentwicklung, namentlich aus Kosten- oder Zeitgründen, nicht in Frage kommt. Das EMBAG und diverse strategische Massnahmen inkl. Hilfestellungen des Bundes legen den Grundstein für eine zunehmende Verbreitung von neuen OSS-Produkten und den Aufbau des Wissens über Alternativprodukte in der Verwaltung. Mittels des Anreizes, ein kostendeckendes Entgelt zu fordern, werden die veröffentlichenden Bedarfsstellen dazu motiviert, in den Aufbau bzw. die Pflege von Open Source Communities zu investieren. Zwar implementiert das EMBAG kein Open Source First Prinzip, jedoch wird es künftig je nach gesuchter Funktionalität schwieriger begründbar sein, weshalb kein Alternativprodukt aus dem OSS-Bereich eingesetzt wird.

Ein weiterer Ausnahmetatbestand sieht vor, dass ein Wechsel der Anbieterin für Leistungen zur Ersetzung, Ergänzung oder Erweiterung bereits erbrachter Leistungen aus wirtschaftlichen oder technischen Gründen nicht möglich ist, erhebliche Schwierigkeiten bereiten oder substanzielle Mehrkosten mit sich bringen würde (Art. 21 Abs. 2 lit. e BöB). Mit einer gut durchdachten Erstausschreibung, welche potenzielle Nebenleistungen der OSS-Entwicklung bzw. Veröffentlichung sowie den Life-Cycle der Soft-

ware berücksichtigt, sowie mit Einbezug der nötigen vertraglichen Regelungen, werden spätere Sachzwänge effektiv reduziert. Potenzielle Anbieterabhängigkeiten können sich namentlich aus dem Spezialwissen ergeben, welches beim Anbieter vorliegt. Auch bei OSS kann sich Spezialwissen bei Anbietern ansammeln. Ein solches sollte zu einem späteren Zeitpunkt mittels Knowhow- und Servicetransfer zur Bedarfsstelle oder einem Drittanbieter übertragen werden können.

Gerade in diesem Zusammenhang könnten sich künftige Entwicklungen im Bereich der künstlichen Intelligenz (KI) als «Game Changer» erweisen, da die Bedarfsstelle Code Reviews und Vorschläge zur Verbesserung des Codes nicht mehr beim Anbieter, sondern via eine KI-Lösung beschaffen kann.[8]

BIBLIOGRAFIE

Beyeler, Martin. (2020). *Vergaberechtliche Entscheide 2018/2019, Bund, Kantone, Europäischer Gerichtshof.* Schulthess Verlag.

Bund schreibt jede dritte Beschaffung nicht aus. (2019, 13. September). *Sonntagszeitung*. S. 4-5.

Eidgenössische Finanzdirektion EFD. (2022). *Reportingset Beschaffungscontrolling Bundesverwaltung 2022*.

Eidgenössische Finanzdirektion EFD. (2020). *Reporting Set Beschaffungscontrolling 2020 der Bundesverwaltung* .

Botschaft zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben. (2022, 4. März). BBl 2022 804. (zit.: Botschaft EMBAG).

[8] Vgl. bspw. den GitHub Co-Piloten, der auf KI-Modellen von OpenAI basiert: https://github.com/features/copilot. Die Autorin und der Autor raten allerdings zur Vorsicht, entsprechende Tools sollten, falls noch keine etablierte Handhabungspraxis besteht, nur nach vorgängiger Risikoeinschätzung in Bezug auf die Sicherstellung des Amtsgeheimnisses, des Datenschutzes sowie der Informationssicherheit und nach Rücksprache mit der Rechtsabteilung, der Datenschutzbeauftragten und des Informationssicherheitsbeauftragten des jeweiligen Verwaltungsträgers eingesetzt werden.

Botschaft zum Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben. (15. Februar 2017). BBl 2017 1851. (zit. Botschaft BöB).

Poledna, T. & do Canto, Ph. (2009). IT-Beschaffungen des Bundes: Freihändige Vergabe mit gebundenen Händen. *Jusletter,* 5. https://jusletter.weblaw.ch/juslissues/2009/522/_7436.html

Schluchen, Ch. (2019). Beschaffungsstrategie für Open Source Software in der Bundesverwaltung am Beispiel des Bundesamtes für Umwelt BAFU (Abschlussarbeit des CAS ICT-Beschaffungen an der Wirtschafts- und Sozialwissenschaftlichen Fakultät der Universität Bern) [PDF]. https://www.digitale-nachhaltigkeit.unibe.ch/unibe/portal/fak_naturwis/a_dept_math/c_iinfamath/abt_digital/content/e90971/e925072/e925079/e925091/

e930674/e930675/e930677/BeschaffungsstrategiefrOpenSourceSoftwareinderBundesverwaltungamBeispieldesBAFU_ger.pdf

Schneider-Heusi, C. & Mazzariello, L. (2011). Die freihändige Microsoft-Vergabe der Bundesverwaltung. *Jusletter, 6*. https://jusletter.weblaw.ch/juslissues/2011/618/_9292.html

Scholl, R. (2019). Open Source Software – Handlungsempfehlungen für Ausschreibungen in der Bundesverwaltung am Beispiel des Bundesamt für Umwelt BAFU. (Abschlussarbeit des CAS ICT-Beschaffungen an der Wirtschafts- und Sozialwissenschaftlichen Fakultät der Universität Bern) [PDF]. https://www.digitale-nachhaltig-keit.unibe.ch/unibe/portal/fak_naturwis/a_dept_math/c_iinfamath/abt_digital/content/e90971/e925072/e925079/e925091/e930674/e930675/e930679/

OpenSourceSoftwareHandlungsempfehlungenfrAusschreibungeninder-Bundesverwaltung_ger.pdf

Open Source Studie Schweiz. (n.d.). https://www.oss-studie.ch/

Eidgenössisches Finanzdepartement. (2015). *Erläutender Bericht des EFD zur Revision des Bundesgesetzes über das öffentliche Beschaffungswesen* [PDF]. https://www.bbl.admin.ch/dam/bkb/de/dokumente/Oeffentliches_Beschaffungswesen/Revision_Beschaffungsrecht/BoeB_Erlaeuternder_Bericht.pdf.download.pdf/B%C3%B6B%20Erl%C3%A4uternder%20Bericht.pdf

Informatiksteuerungsorgan des Bundes ISB. (2019a). *Strategischer Leitfaden Open Source Software in der Bundesverwaltung* [PDF]. https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software.html

Informatiksteuerungsorgan des Bundes ISB. (2019b). *Praxis-Leitfaden Open Source Software in der Bundesverwaltung* [PDF]. https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software.html

SOZIALE NACHHALTIGKEIT IN DER BESCHAFFUNG VON IKT-PRODUKTEN

Forderung von Nachweisen zur Überprüfung der ILO-Kernarbeitsnormen

Lara Biehl

Lara Biehl ist Wissenschaftliche Assistentin an der Berner Fachhochschule

Abstract: Das revidierte Vergaberecht verlangt von Beschaffungsverantwortlichen, Nachhaltigkeitsaspekte in Ausschreibungen zu berücksichtigen. Dazu gehört auch die soziale Nachhaltigkeit, die vor allem die Einhaltung von Arbeitsschutzvorschriften umfasst. In einigen Branchen, z.B. im IKT-Sektor, sind Verstösse gegen die Normen der Internationalen Arbeitsorganisation (ILO) sehr ausgeprägt und erstrecken sich über alle Stufen der Lieferkette. Aus Gründen der Sorgfaltspflicht sind Beschaffungsstellen in der Verantwortung, die soziale Nachhaltigkeit in den Lieferketten der Produkte, die sie beschaffen, zu überprüfen und zu fördern. Der folgende Artikel zeigt einerseits auf, warum es notwendig ist, dass Beschaffungsstellen die Einhaltung der ILO-Kernarbeitsnormen überprüfen. Andererseits evaluiert er zwei Varianten, wie Beschaffer*innen eine solche Überprüfung im IKT-Bereich vornehmen können.

INHALTSVERZEICHNIS

1. Einleitung 56
2. Vom Rohstoffhandel zur Endmontage: Soziale Probleme innerhalb der IKT-Wertschöpfungskette 58
3. Die Einhaltung der ILO-Kernarbeitsnormen als zwingende Teilnahmebedingungen 60
   - 3.1 Notwendigkeit einer Risikoanalyse 62
   - 3.2 Nachweise: Sorgfaltspflicht geht über Selbstdeklaration hinaus 62
4. Die Überprüfung der ILO-Kernarbeitsnormen im IKT-Bereich 63

4.1 Variante A: Einforderung von Zertifikaten oder Verifizierungen 64
4.1.1 Chancen bei der Verwendung von Zertifikaten oder Verifizierungen 65
4.1.2 Herausforderungen bei Nachweisen, die auf Sozialaudits basieren 67
4.2 Variante B: Überprüfung der ILO-Normen durch Electronics Watch 70
4.2.1 Chancen eines Beitritts zu Electronics Watch für Beschaffungsstellen 70
4.2.2 Herausforderungen für Beschaffungsstellen beim Electronics-Watch-Modell 71
5. Exkurs: Humanitäre Krisen im Schatten der Rohstoffgewinnung – Beschaffung von Rohstoffen aus der Demokratischen Republik Kongo 73
6. Fazit 75
Bibliografie 76

1. EINLEITUNG

Mit der Vergaberechtsrevision von 2021 wurde das Wirtschaftlichkeitsprinzip im öffentlichen Beschaffungsrecht der Schweiz um das Prinzip der Nachhaltigkeit erweitert (Art. 2 des Bundesgesetzes über das öffentliche Beschaffungswesen, BöB). Dies bedeutet, dass sowohl ökonomische als auch ökologische und soziale Nachhaltigkeitsaspekte bei Beschaffungen zu berücksichtigen sind, um nicht nur einen Preiswettbewerb, sondern auch einen Qualitätswettbewerb zu erreichen (Art. 41 BöB).

Die Reform des Vergaberechts markiert einen «Paradigmenwechsel», da Nachhaltigkeit in ihren drei Dimensionen (ökonomisch, ökologisch, sozial) nun explizit als Gesetzesziel verankert ist (Steiner & Klingler, 2023; Steiner, 2020; Koch, 2023, S. 20). Hinsichtlich der sozialen Nachhaltigkeit regelt Art. 12 BöB die zwingenden Teilnahmebedingungen als obligatorische Mindestanforderungen. Dabei unterscheidet er zwischen Mindestanforderungen an Anbieter mit Leistungsort in der Schweiz (Art. 12 Abs. 1) und solchen mit Leistungsort im Ausland (Art. 12 Abs. 2). Liegt der Leistungsort in der Schweiz, müssen die Anbieter die Vorschriften über den Arbeitsschutz, die Arbeitsbedingungen und die Gleichbehandlung von Frau und Mann einhalten (Art. 12

Abs. 1 BöB). Befindet sich der Leistungsort im Ausland, so sind mindestens die acht Kernübereinkommen der Internationalen Arbeitsorganisation (ILO) verbindlich (Art. 12 Abs. 2 BöB), die unter anderem die Beseitigung der Zwangsarbeit und der Kinderarbeit sowie den Schutz des Vereinigungsrechts fördern. Art. 12 Abs. 5 sieht vor, dass die Auftraggeber die Einhaltung dieser Teilnahmevoraussetzungen überprüfen können – z.B. durch eine Selbstdeklaration oder durch anerkannte Zertifizierungssysteme wie Labels und Zertifikate.

Besonders im Bereich der Informations- und Kommunikationstechnologien (IKT) sind soziale Missstände entlang der Lieferkette ausgeprägt. Trotz regionaler Unterschiede sind fast alle Arbeiter*innen, die an der Herstellung von IKT-Produkten beteiligt sind, mit ausbeuterischen Arbeitsbedingungen konfrontiert und es besteht ein hohes Risiko, dass ILO-Kernarbeitsnormen verletzt werden. Hierzu zählen Niedriglöhne, unzureichender Gesundheitsschutz, ungeregelte und exzessive Arbeitszeiten sowie Zwangs- und Kinderarbeit. Konflikte in Rohstoffregionen verschärfen die humanitären Herausforderungen in diesem Sektor zusätzlich (siehe z.B. Verité, 2014; Ames & Schurath, 2018).

Dies stellt öffentliche Beschaffer*innen bei der Überprüfung der ILO-Kernarbeitsnormen in der Lieferkette von IKT-Produkten vor eine Reihe von Schwierigkeiten. Zum einen erschwert die hohe Komplexität der IKT-Wertschöpfungsketten die Rückverfolgbarkeit der Produktionsprozesse. Zum anderen sind viele Herausforderungen bei der Beschaffung von IKT-Produkten struktureller Natur. Hersteller und Händler von IKT-Geräten profitieren von systemischen Missständen wie gewerkschaftsfeindlichen Praktiken und ausbeuterischen Arbeitsbedingungen in Rohstoff- und Produktionsländern. Diese Missstände führen in der Regel zu niedrigeren Rohstoff- und Produktionskosten, was wiederum höhere Gewinnmargen für Markenunternehmen ermöglicht (Beck, 2013, S. 11 – 23).

In diesem Artikel wird untersucht, auf welche Nachweis- und Unterstützungsmöglichkeiten Beschaffungsstellen zurückgreifen können, um die Einhaltung der ILO-Kernarbeitsnormen bei ihren Lieferanten zu überprüfen. Es folgt eine Bewertung dieser Nachweise hinsichtlich ihrer Vorteile und möglicher Herausforderungen. Die Ausführungen beschränken sich auf Nachweismöglichkeiten, die auch von kleineren oder finanzschwächeren Beschaffungsstellen genutzt werden können. Komplexere Sozial-

auditsysteme oder andere Kontroll- und Einflussmechanismen, die nur von ressourcenstarken Beschaffungsstellen umgesetzt werden können, werden in diesem Beitrag nicht berücksichtigt oder nur am Rande erwähnt.

2. VOM ROHSTOFFHANDEL ZUR ENDMONTAGE: SOZIALE PROBLEME INNERHALB DER IKT-WERTSCHÖPFUNGSKETTE

Die Lieferketten der meisten IKT-Produkte sind stark globalisiert und umfassen zahlreiche Zulieferer, Hersteller und Fabriken. Die IKT-Wertschöpfungskette beginnt mit der **Gewinnung von Rohstoffen**, entweder durch Recycling oder durch Bergbau. Der Abbau von Rohstoffen, insbesondere von sogenannten Konfliktmineralien wie Zinn, Tantal, Wolfram und Gold (3TG) sowie Kobalt und Coltan, birgt das Risiko schwerer Menschenrechtsverletzungen (Osburg, 2015, S. 209f.; Barume et. al., 2016, S. 9ff.). Besonders die Demokratische Republik (DR) Kongo und ihre Nachbarländer sind von diesen Problemen betroffen. Bewaffnete Gruppen versuchen im Kongo, die Kontrolle über die Abbaugebiete zu erlangen. Diese Kämpfe um die rohstoffreichen Gebiete führen zu Zwangsvertreibungen und kriegsbedingten humanitären Krisen. In den Minen herrschen zusätzlich fast immer prekäre Arbeitsbedingungen, vor allem Zwangs- und Kinderarbeit sind weit verbreitet (Faber et al., 2017, S. 10; Ames & Schurath, 2018, S. 8). Die zweite Stufe der IKT-Wertschöpfung umfasst die **Verarbeitung und Vorproduktion**. Die abgebauten oder recycelten Mineralien werden in Schmelzhütten und Raffinerien zu Materialien für die Herstellung von IKT-Produkten verarbeitet. Anschliessend werden diese Materialien in einem weiteren Schritt an Fabriken zur **Herstellung von Unterkomponenten** weitergegeben (zumeist in Niedriglohnländer in (Süd-)Ostasien, Lateinamerika und Osteuropa) (Verbrugge, 2020, S. 4). Die **Endfertigung**, d.h. der Zusammenbau der einzelnen Komponenten zum fertigen Produkt, stellt den letzten Schritt bei der Herstellung von IKT-Produkten dar. Sie findet zum grössten Teil in China statt (Merk, 2021, S. 67). Auf allen Produktionsstufen finden sich Verstösse gegen die meisten ILO-Kernarbeitsnormen. Besonders problematisch sind überlange Arbeitszeiten, missbräuchliches Management, Verletzung von Gewerkschaftsrechten, unklare (oder fehlende) Arbeitsverträge, niedrige Löhne und unzureichender Arbeits- und Gesundheitsschutz beim Umgang mit giftigen Stoffen (Merk, 2021, S. 67; WEED 2015, S. 7ff.). Die Gründe für diese Missstände liegen

unter anderem in strukturellen Entwicklungen im internationalen Handel. Im IKT-Sektor befinden sich viele an der Produktion beteiligten Fabriken in einem Unterbietungswettlauf (sog. «race to the bottom»): Herstellungsfirmen und -fabriken versuchen, die Produktionskosten so weit wie möglich zu senken, um Aufträge von multinationalen Konzernen zu erhalten bzw. zu behalten. Um im Preiskampf mithalten zu können, werden Löhne gedrückt, Arbeitsschutzmassnahmen vernachlässigt und Umweltauflagen missachtet. Die Forderung nach immer schnelleren Produktionszyklen verschärft diese Problematik zusätzlich (Davies & Vadlamannati, 2013, S. 12; Kelly et. al., 2019, S. 5ff).

Die Intransparenz der IKT-Lieferkette erschwert die Überwachung sozialer Missstände weiter. Die meisten Markenunternehmen (wie Apple, Dell, Lenovo, HP, Nokia etc.), die als direkte Zulieferer für Konsument*innen und den öffentlichen Sektor auftreten, lagern einen Grossteil oder, wie im Fall von Apple, die gesamte Produktionskette aus (Peter, 2022, S. 6; Pun et al., 2016, S. 168f.). Markenunternehmen vergeben die Organisation der Lieferkette an Sublieferanten, sogenannte «Contract Manufacturer» bzw. «Kontraktfertiger» (z.B. Flextronic, Foxconn, Inventec). Obwohl vielen Endnutzer*innen die Namen der Kontraktfertiger nicht geläufig sind, haben sich diese in den letzten zwei Jahrzehnten zu multinationalen Konzernen entwickelt, die sich auf die Beschaffung von Materialien und die Organisation umfangreicher Arbeitsabläufe konzentrieren. Kontraktfertiger beziehen ihre Komponenten in der Regel von vielen verschiedenen Lieferanten und Sublieferanten, was die Rückverfolgbarkeit einzelner Produktkomponenten erschwert (Merk, 2021, S. 43ff.). Da Kontraktfertiger eine Schlüsselrolle im IKT-Lieferkettenmanagement spielen und erheblich an der Erfüllung der Leistung beteiligt sind, sind sie «**wichtige Dritte**»[1] für den Hauptlieferanten. Aufgrund der Tatsache, dass Kontraktfertiger den Grossteil der Arbeitskräfte im IKT-Sektor beschäftigen – und zwar von der Rohstoffgewinnung bis zur Endmontage – ist es unerlässlich, nicht nur die direkten Zulieferer auf die Einhaltung der ILO-Kernarbeitsnormen zu überprüfen, sondern auch deren wichtige Dritte.[2]

---

[1] Unter «wichtige Dritte» fallen diejenigen Sublieferanten, die einen erheblichen Bestandteil des Produkts herstellen, eine erhebliche Teilleistung erbringen oder in einem besonders risikoanfälligen Bereich oder Produktionsschritt tätig sind. Siehe zur Terminologie von «Dritten»: Beschaffungskonferenz des Bundes BKB, 2021, S. 12–13.

[2] In der EU werden Unternehmen in Zukunft gewissen Transparenzgrundsätzen in Bezug auf ihre Lieferketten einhalten müssen, wenn das Lieferkettengesetz (Corporate Sustainability Due Dil-

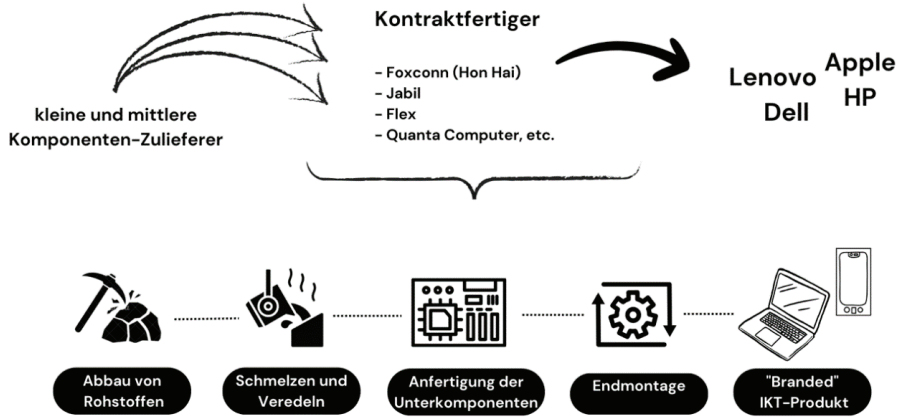

Abbildung 1 : Die wichtigsten Abschnitte der IKT-Lieferkette und ihre Hauptakteure. Im Durchschnitt lagern Markenunternehmen 70% ihrer Produktionskette auf Kontraktfertiger aus (Ibid., S. 52). Weil Kontraktfertiger mit vielen kleinen und mittleren Zulieferern zusammenarbeiten, ist die Rückverfolgbarkeit einzelner Produktkomponenten für den Endkunden schwierig bis unmöglich (Grafik der Autorin).

3. DIE EINHALTUNG DER ILO-KERNARBEITSNORMEN ALS ZWINGENDE TEILNAHMEBEDINGUNGEN

Das revidierte Gesetz bietet eine Grundlage, um Anbieter vom Wettbewerb auszuschliessen, wenn sie die ILO-Kernübereinkommen oder von der Schweiz ratifizierte ILO-Abkommen nicht einhalten (Art. 12 BöB i.V.m. Art. 4 VöB).[3] Die Übereinkommen der ILO sind internationale Verträge, die grundlegende Prinzipien und Rechte im Be-

ligence Directive, CSDDD) in Kraft tritt. Siehe dazu auch den Beitrag von Paula Zimmermann, Kapitel 2.1.4.

[3] Hier ist bemerkenswert, dass es das Gesetz (Art. 12 Abs. 2 BöB) vom Wortlaut her zwar erlaubt, den Nachweis über die «Einhaltung weiterer wesentlicher internationaler Arbeitsstandards» als zwingende Teilnahmebedingungen einzufordern, die Verordnung (Art. 4 VöB) die erlaubten Nachweise jedoch auf diejenigen ILO-Abkommen beschränkt, welche die Schweiz ratifiziert hat. Eine entsprechende Motion (Motion 22.3019 vom 21.02.2022), dies auf alle ILO-Abkommen – unabhängig von der Ratifizierung durch die Schweiz – auszudehnen, wurde abgelehnt.

reich der Arbeit festhalten. Mit der Ratifizierung verpflichtet sich ein Staat, geeignete rechtliche und praktische Schritte zu ergreifen und regelmässig über die Fortschritte bei der Umsetzung zu berichten (International Labour Organization, n.D.). Die Schweiz hat 62 Arbeitsübereinkommen der ILO ratifiziert, darunter die folgenden acht[4] Kernübereinkommen (SECO, n.D.):

Übersicht der ILO-Kernübereinkommen
Vereinigungsfreiheit und effektive Anerkennung des Rechts auf Kollektivverhandlungen: – Fundamentales Übereinkommen **Nr. 87** über die Vereinigungsfreiheit und den Schutz des Vereinigungsrecht – Fundamentales Übereinkommen **Nr. 98** über die Anwendung der Grundsätze des Vereinigungsrechtes und des Rechtes zu Kollektivverhandlungen
Abschaffung gewisser Formen der Zwangs- oder Pflichtarbeit: – Fundamentales Übereinkommen **Nr. 29** über Zwangs- und Pflichtarbeit – Fundamentales Übereinkommen **Nr. 105** über die Abschaffung der Zwangsarbeit
Beseitigung von Diskriminierung in Beschäftigung und Beruf: – Fundamentales Übereinkommen **Nr. 100** über die Gleichheit des Entgelts männlicher und weiblicher Arbeitskräfte für gleichwertige Arbeit – Fundamentales Übereinkommen **Nr. 111** über die Diskriminierung in Beschäftigung und Beruf
Abschaffung der Kinderarbeit: – Fundamentales Übereinkommen **Nr. 138** über das Mindestalter für die Zulassung zur Beschäftigung – Fundamentales Übereinkommen **Nr. 182** über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit (SECO, 2015)

[4] Inzwischen gibt es 10 ILO-Kernübereinkommen, wobei noch unklar ist, wie die zwei neuen Abkommen Eingang in Gesetzes- oder Verordnungsrecht finden.

Mit der Ausschlussmöglichkeit bei Nichteinhaltung der Kernarbeitsnormen (Art. 44 Abs. 2 lit. f BöB) soll verhindert werden, dass sich Anbieter einen Vorteil verschaffen können, indem sie bei der Produktion auf tiefe Löhne und ausbeuterische Arbeitsbedingungen setzen (Steiner, 2017, S. 44, S. 47f.). Ein weiteres Ziel dieser Massnahme ist die Vermeidung von Reputationsschäden für Schweizer Beschaffungsstellen bei Beschaffungen im Ausland.

Um festzustellen, ob ein Anbieter sowie seine wichtigsten Sublieferanten die ILO-Normen einhalten, müssen die Vergabestellen verschiedene Kontrollinstrumente einsetzen. Der Aufwand für die Überprüfung der Einhaltung der ILO-Normen ist nicht bei jeder Ausschreibung gleich, sondern hängt vom Ausschreibungsgegenstand und vom Sektor ab.

3.1 NOTWENDIGKEIT EINER RISIKOANALYSE

Nicht jeder Sektor oder jedes Produkt ist zwangsläufig von möglichen Verstössen gegen ILO-Normen betroffen. Selbst in Hochrisikosektoren oder bei Hochrisikoprodukten können verschiedene Normen unterschiedlich anfällig für Verstösse sein. Aus diesem Grund ist es in den meisten Fällen unumgänglich, eine Markt- bzw. Risikoanalyse der Lieferkette durchzuführen. Dabei geht es zuerst darum festzustellen, ob ein Produkt einer Risikobranche angehört, d.h. einer Branche, in der das Risiko der Verletzung von Arbeitsnormen üblich ist. In einem zweiten Schritt kann ermittelt werden, welche Normen genau einem Verletzungsrisiko ausgesetzt sind. Sind die Risikofaktoren identifiziert, können diese in den Ausschreibungsunterlagen gezielt abgefragt werden, indem spezifische Nachweise zu bestimmten Kernarbeitsnormen gefordert werden.[5]

3.2 NACHWEISE: SORGFALTSPFLICHT GEHT ÜBER SELBSTDEKLARATION HINAUS

Das Gesetz bietet verschiedene Möglichkeiten, wie öffentliche Beschaffungsstellen Nachhaltigkeitsnachweise fordern können. Die am häufigsten praktizierte Methode

[5] Mittlerweile gibt es eine Vielzahl von Instrumenten, die bei der Durchführung einer Risikoanalyse helfen können. Einige Instrumente, wie z.B. die Relevanzmatrix vom Bundesamt für Umwelt, geben einen Überblick über die ökologischen und sozialen Herausforderungen im Produktlebenszyklus verschiedener Produktkategorien und zeigen für jede Kategorie spezifische Handlungsoptionen auf: https://www.bafu.admin.ch/dam/bafu/de/dokumente/wirtschaft-konsum/fachinfo-daten/relevanzmatrix.pdf.download.pdf/relevanzmatrix-gesamt.pdf

ist die Verwendung einer «Selbstdeklaration» (Art. 26 Abs. 2 BöB), bei der der Anbieter auf Anfrage der Beschaffungsstelle ein Formular ausfüllt und bestätigt, dass die Vergabeanforderungen nach Art. 12 erfüllt sind. Unterzeichnet der Anbieter die Selbstdeklaration trotz Nichteinhaltung der Anforderungen, können Sanktionen bis hin zum Ausschluss vom Vergabeverfahren oder zum Widerruf des Zuschlags drohen (Art. 44 Abs. 2 Bst. f BöB). Ein Problem besteht darin, dass die in der Selbstdeklaration gemachten Angaben nicht unabhängig sind, d.h. von den Lieferanten oder Herstellern selbst stammen, und falsche oder verzerrte Angaben enthalten können, die ohne weitere Überprüfung nicht aufgedeckt werden können.[6] Es ist daher besonders wichtig, dass insbesondere in Risikobranchen aus Gründen der Sorgfaltspflicht eine unabhängige Verifizierung der Selbstdeklaration erfolgt, um sicherzustellen, dass die Teilnahmevoraussetzungen erfüllt sind (siehe auch Entscheid des BVGe B-1714/2022 vom 19. September 2023, E. 118). Mit einer Due Diligence-Prüfung, d.h. einer Prüfung und Bewertung sozialer Nachhaltigkeitsrisiken und -chancen, können Beschaffungsstellen sicherstellen, dass die von den Lieferanten gemachten Angaben korrekt sind und die zugesagten Standards auch tatsächlich eingehalten werden bzw. Schritte eingeleitet werden, um die Einhaltung zu gewährleisten.

4. DIE ÜBERPRÜFUNG DER ILO-KERNARBEITSNORMEN IM IKT-BEREICH

Im Folgenden werden zwei mögliche Vorgehensweisen bzw. Varianten zur Überprüfung der ILO-Kernarbeitsnormen (Art. 12 Abs. 5 BöB) vorgestellt und diskutiert.

Die erste Variante ist die Forderung von Zertifikaten oder Auditberichten. Diese Nachweise können von verschiedenen Nachweisgebern stammen, von denen die folgenden im IKT-Bereich am häufigsten verwendet werden:

---

[6] Vgl. z.B. https://www.srf.ch/play/tv/rundschau/video/dumping-auf-der-baustelle-die-methoden-der-eisenleger?urn=urn:srf:video:52e999ef-26f9-4d3e-998b-fb0ae1801f5a als Beispiel, warum Vergabestellen in Sektoren, in denen Verletzungen von ILO-Normen oder Arbeitsrechten bekannt sind, aus Gründen der Sorgfaltspflicht eine vertiefte Prüfung vornehmen müssen.

- Nachweis einer Mitgliedschaft in einer **Unternehmens/Standard-Initiative** mit Nachweis eines Auditberichts der relevanten Fabriken (z.B. amfori BSCI oder RBA);
- **Produktzertifikat** mit entsprechendem Nachweis (z.B. TCO-Certified);
- **Fabrikzertifikate** der relevanten Standorte (z.B. SA8000);
- Ein qualifizierter **Auditbericht** aller betroffenen Fabriken.[7]

Alle soeben aufgeführten Nachweisformen basieren auf sogenannten «Sozialaudits». Bei einem solchen Audit wird eine Produktionsstätte anhand einer Auditrichtlinie überprüft (z.B. Kontrollen im Bereich der Arbeitssicherheit sowie Kontrollen von Arbeitsverträgen, Lohndokumenten, Arbeitszeiten, Überstundenregelungen, Kinder- und Zwangsarbeit und von Diskriminierung). Erfüllt die Fabrik alle Anforderungen, wird sie zertifiziert bzw. bescheinigt. Werden Mängel festgestellt, muss die Fabrik in der Regel einen Korrekturmassnahmenplan vorlegen. In weiteren Audits werden die Fabriken erneut überprüft oder bei Mängeln die Verbesserungsmassnahmen bewertet.

Bei der zweiten Variante verlangt die Beschaffungsstelle nicht zwingend vorab Zertifikate oder Auditberichte, sondern überprüft die Einhaltung der ILO-Normen während der Vertragslaufzeit. In diesem Fall wird der Lieferant durch eine Vertragsklausel verpflichtet, den Standort und die Namen wichtiger Fabriken von sich und relevanten Sublieferanten offenzulegen. Während der Vertragslaufzeit werden diese Fabriken dann im Sinne eines Monitorings überwacht.

Die beiden Varianten können auch kombiniert werden. Im Folgenden werden beide Varianten sowie ihre wichtigsten Nachweisformen kurz vorgestellt und mögliche Herausforderungen diskutiert.

4.1 VARIANTE A: EINFORDERUNG VON ZERTIFIKATEN ODER VERIFIZIERUNGEN

Die Forderung nach Zertifikaten ist für die Vergabestellen die einfachste Möglichkeit, die Einhaltung der ILO-Normen zu überprüfen. Zertifikate bescheinigen die Einhaltung bestimmter Normen, Regelungen oder Anforderungen. Dabei wird zwischen Produkt-

[7] Siehe auch: Relevanzmatrix des BAFU (Faist & Schlierenzauer, 2020).

und Fabrikzertifikaten unterschieden. Produktzertifikate bestätigen, dass die Herstellung eines bestimmten Produkts einem Standard oder Kodex entspricht (Beschaffungsamt des BMI, 2021, S. 35). Sie haben den Vorteil, dass sie nur Grundkenntnisse über die Arbeitsbedingungen in der IKT-Branche voraussetzen und einfach und zeitsparend in die Ausschreibungsunterlagen integriert werden können. Fabrikzertifikate hingegen beziehen sich auf konkrete Fabriken und bescheinigen die Einhaltung bestimmter Standards in einer Fabrik (Ibid.) Produktzertifikate basieren meistens auf Fabrikzertifikaten bzw. umfassen mehrere davon.

4.1.1 Chancen bei der Verwendung von Zertifikaten oder Verifizierungen

Im IKT-Sektor werden vor allem «TCO-Certified» als Produktzertifikat und «SA8000» als Fabrikzertifikat für die Überprüfung sozialer Kriterien verwendet (vgl. Fuller & Rydell 2023; Social Accountability International, 2021 & 2023 für eine Erläuterung der Überprüfungsmechanismen der jeweiligen Zertifikate).[8] TCO-Certified zertifizierte Produkte gibt es in fast allen wichtigen Produktkategorien der IKT-Branche. Der «TCO-Certified Product Finder» bietet die Möglichkeit, nach Produktgruppen zu filtern und alle zertifizierten Modelle anzuzeigen. Aufgrund der Vielzahl von zertifizierten Produkten verschiedener Anbieter ist die Gefahr einer erheblichen Einschränkung des Marktes z.B. bei der Produktgruppe Notebooks (mehr als 355 Modelle der neuen Generation) kaum gegeben, während es bei Smartphones nur ein zertifiziertes Produkt gibt.[9]

Eine beispielhafte Formulierung in den Ausschreibungsunterlagen für die Einforderung eines Nachweises für ein Produktzertifikat könnte folgendermassen lauten:

> *Als Nachweis der Einhaltung der ILO-Kernübereinkommen im Rahmen der obligatorischen Teilnahmebedingungen, müssen die Angebotsunterlagen einen*

[8] Andere Produktzertifikate wie «Blauer Engel» gehen zwar einen Schritt in Richtung soziale Nachhaltigkeit, jedoch zertifizieren sie lediglich bestimmte Produktgruppen oder soziale Aspekte sind nur optional und decken nicht alle ILO-Kernarbeitsnormen ab. Diese Zertifikate können in den Ausschreibungsunterlagen erwähnt werden, sollten aber nicht als alleinige Voraussetzung für die Zertifizierung genannt werden.

[9] Siehe: https://tcocertified.com/de/product-finder/

Nachweis in Form eines TCO-Certified-Zertifikats oder eines vergleichbaren Zertifikats mit gleichwertigen Leistungsanforderungen enthalten.

Beschaffungsstellen sollten darauf achten, dass die aktuelle Version des Zertifikats verlangt wird und dass die exakte Produktkategorie angegeben wird. Wichtig ist zudem, dass gleichwertige Nachweise akzeptiert werden – einerseits, um den Markt nicht unnötig einzuschränken, und andererseits, um die Vielfalt von Zertifikaten in einigen Branchen, die vergleichbare Anforderungen oder Qualitätsstandards erfüllen, zu berücksichtigen. Dies kann in den Ausschreibungsunterlagen z.B. folgendermassen formuliert werden: *«Lieferanten müssen über ein gültiges TCO-Zertifikat [Nummer oder Version] oder einen gleichwertigen Nachweis für [Produktkategorie] verfügen».*

Neben Produkt- und Fabrikzertifikaten gibt es sogenannte «Unternehmens- oder Standard-Initiativen» wie Amfori BSCI oder die Responsible Business Alliance (RBA), bei denen es sich um einen Zusammenschluss verschiedener Unternehmen oder Stakeholder handelt, die sich nach einem definierten Standard richten wollen. Die an den Initiativen teilnehmenden Unternehmen erklären sich bereit, den Verhaltenskodex von Amfori BSCI bzw. RBA zu den Arbeitsprinzipien (u.a. ILO-Kernarbeitsnormen) umzusetzen und in ihren Lieferketten weiterzugeben.[10] Obwohl Standardinitiativen keine Zertifizierungsstellen sind, kann in der Ausschreibung auch ein amfori BSCI oder RBA Nachweis (Audit) für relevante Fabriken des Lieferanten und seiner wichtigen Dritten gefordert werden, da viele Standardinitiative mindestens die ILO-Kernarbeitsnormen in ihren Prüfrichtlinien integriert haben.[11] Die Forderung eines Audits einer Standardinitiative hat den Vorteil, dass viele Grossunternehmen der IKT-Branche über einen Standard wie RBA oder vergleichbare interne Richtlinien verfügen (Beschaffungsamt des BMI, 2021, S. 78.).

[10] Siehe z.B. Amfori BSCI-Systemhandbuch Teil II. (2018) für eine Übersicht der Regelungen und Zertifizierungen.

[11] Obwohl viele Initiativen und Zertifizierer die ILO-Kernarbeitsnormen berücksichtigen, können sich die Prüfungsrichtlinien unterscheiden. Es ist deshalb zu empfehlen, die jeweiligen Auditrichtlinien zu überprüfen und ggf. in den Ausschreibungsunterlagen festzulegen, was als «gleichwertiger» Nachweis bzw. Audit klassifiziert wird.

4.1.2 Herausforderungen bei Nachweisen, die auf Sozialaudits basieren

Überprüfungssysteme, die auf Sozialaudits basieren, sind mit einer Reihe von Herausforderungen konfrontiert. Erstens sind die Auditergebnisse nur eine Momentaufnahme und nicht zwangsläufig repräsentativ für die tatsächlichen Bedingungen in den Fabriken. Die Audits erfolgen stichprobenartig und meistens in Abständen von 24 bis 36 Monaten.[12] Eine Studie von Human Rights Watch zeigt ausserdem, dass auditierte Fabriken wiederholt versuchen, Auditfirmen zu täuschen (Human Rights Watch, 2022, S. 5). Dies geschieht beispielsweise durch die fehlerhafte Beantwortung von Fragebögen, die Fälschung von Unterlagen wie Lohnausweisen oder indem die Arbeitnehmer*innen gezielt darauf geschult werden, sich gegenüber Auditor*innen auf eine bestimmte Art und Weise zu verhalten (Ibid., S. 15). Erschwerend kommt hinzu, dass es sich bei den Auditfirmen in der Regel um private Unternehmen handelt, die miteinander im Wettbewerb stehen. Es wurde beispielsweise beobachtet, dass die Auditzeit in jüngster Zeit zunehmend verkürzt wurde, um den Auftraggebern einen besseren Preis anbieten zu können. Dies birgt die Gefahr, dass weniger Gespräche mit dem Personal geführt werden und weniger Zeit für detaillierte Inspektionen bleibt, was die Aussagekraft und Glaubwürdigkeit der Auditergebnisse beeinträchtigt (Terwindt & Armstrong, 2019, S. 7; Human Rights, 2022, S. 5).

Eine weitere Problematik ist der mangelnde öffentliche Zugang zu den Sozialauditberichten. Die Ergebnisse der Audits, inklusive der identifizierten Risiken und dokumentierten Korrekturmassnahmen, bleiben der Öffentlichkeit, den Beschäftigten und den Gewerkschaften verborgen. SA8000 veröffentlicht zwar die Namen und Standorte der zertifizierten Fabriken – die eigentlichen Auditberichte, die zur Zertifizierung geführt haben, sowie Mängel und Korrekturschritte bleiben jedoch versiegelt. Bei Amfori BSCI werden selbst die Namen und Standorte der zertifizierten Fabriken nicht veröffentlicht (Human Rights, 2022, S. 5 und S. 7; Kelly et al., 2019, S. 28). Dieser Mangel an Transparenz schafft Raum für unzureichende Audits, die unbemerkt bleiben können, da

[12] Siehe Abbildung 2 für einen Überblick über die Auditierungsintervalle der wichtigsten Zertifikate im IKT-Bereich.

weder die Gewerkschaften noch die betroffenen Arbeiter*innen die dokumentierten Missstände und damit die ausbleibenden oder erzielten Fortschritte verifizieren können (Terwindt & Armstrong, 2019, S. 19).

Eine weitere Schwierigkeit mit den vorgestellten Zertifizierungen besteht darin, dass aufgrund der Komplexität der IKT-Lieferketten in der Regel nur Fabriken der Endmontagewerke zertifiziert werden können, während die Zulieferer und Fabriken der vielen Zwischenschritte unberücksichtigt bleiben[13] (Verbrugge, 2020, S. 5, siehe Abbildung 2 für eine detailliertere Auflistung zur Umsetzung der Nachweise in der Lieferkette).

Auch wenn nicht die gesamte Lieferkette durch ein Zertifikat abgedeckt ist, bieten diese Nachweise einen höheren Kontrollmechanismus als die Selbstdeklaration und liefern zumindest für die Endfertigung einen Nachweis über die Einhaltung der ILO-Kernarbeitsnormen. Zudem beinhalten einige Produktzertifikate wie TCO-Certified im IKT-Bereich neben den sozialen auch ökologische Standards, so dass beide Aspekte berücksichtigt werden können. Gerade kleinere Institutionen mit wenig Ressourcen, wie Gemeinden, können so mit überschaubarem Aufwand die ökologische und soziale Nachhaltigkeit fördern. Die öffentliche Hand hat durch ihre Kaufkraft Einfluss auf den Markt, und die Forderung nach Zertifikaten kann die Nachhaltigkeitsbemühungen in der IKT-Lieferkette fördern. Zertifikate, die auf Sozialaudits basieren, können daher ein erster Ausgangspunkt für Beschaffungsstellen sein, um soziale Nachhaltigkeit in den Beschaffungsprozess zu integrieren. Aufgrund der genannten Defizite sollten sie jedoch nicht als Endpunkt einer umfassenden Strategie zur Förderung sozial nachhaltiger Beschaffung betrachtet werden.

[13] Siehe z.B. Amfori. (n.d.) für eine Stellungnahme bezüglich der Überprüfung von Rohstoffgewinnern und -herstellern.

	TCO-Certified	Amfori BSCI	RBA	SA-8000
Art des Zertifikats / der Verifizierung	**Produktzertifizierung** für Produktkategorien wie Computer, Monitore, Notebooks, Tablets und andere IT-Produkte.	**Unternehmens-Initiative:** Lieferanten orientieren sich am amfori BSCI Code of Conduct, der u.a. auf den Konventionen der International Labor Organization (ILO) gründet.	**Unternehmens-Initiative:** Mitglieder orientieren sich am RBA Code of Conduct , der u.a. auf den Konventionen der International Labor Organization (ILO) gründet.	**Fabrik-Zertifikat:** Der Standard basiert auf den Arbeitsnormen der Allgemeinen Erklärung der Menschenrechte und den ILO-Konventionen.
Überprüfung der ILO-Normen	**Sozial-Audits.** Bei vorliegendem SA-8000 Zertifikat werden Fabriken alle 36 Monate kontrolliert. In Risikogebieten alle 24 Monate. Korrekturmassnahmen müssen innerhalb von 24 Monaten erfolgen (RBA-VAP- oder SA8000-Audit), ansonsten wird die Fabrik aus der *TCO Certified Accepted Factory List* entfernt.	**Sozial-Audits**. Finden bei guter Bewertung der Fabrik alle zwei Jahre statt, bei mittlerer oder schlechter Bewertung alle 12 Monate. Bei festgestellten Verstössen werden ein Korrekturmassnahmenplan und Folgeaudits verlangt (GlobalGAP und SA8000-Audits werden akzepiert).	**Sozial-Audits**. Fragebögen zur Selbsteinschätzung, Audits durch unabhängige, von der RBA zugelassene Drittfirmen und Überwachung von Korrekturmassnahmen. Einteilung der Mitglieder/Fabriken je nach Befunden in **Platinum, Gold** oder **Silber**. Die Audits wiederholen sich alle zwei Jahre.	**Sozial-Audits.** Durchführung einer Kombination aus angekündigten, teilweise angekündigten und unangekündigten Audits während des dreijährigen SA8000-Zertifizierungszyklus. Die Anzahl der Audits variiert je nach Risikogebiet.
Umsetzung in den Lieferketten	**Endmontage**. TCO-Certified verlangt zusätzliche Massnahmen im Bereich der Konfliktmineralien (3TG und Kobalt) bezüglich Sorgfaltspflicht (z.B. Mitgliedschaft einer Multi-Stakeholder-Initiative für Verantwortung und Rückverfolgbarkeit).	Insbesondere **Endmontage**. Fordert zusätzlich die Einhaltung der Sorgfaltspflicht bezüglich Konfliktmineralien (OECD-Leitlinien zur Sorgfaltspflicht) bei den beteiligten Lieferanten.	RBA-Mitglieder müssen den Kodex als eine Initiative für die **gesamte Lieferkette** betrachten, d. h. sie müssen zumindest von ihren Zulieferern der nächsten Ebene verlangen, dass sie den Kodex anerkennen und umsetzen. Umsetzung in der Praxis aber insbesondere in der **Endmontage**.	Fabriken, die IT-Hardware herstellen, fertigstellen und verpacken.

Siehe: Langer (2023a); Langer (2023b); Fuller & Rydell (2023); Amfori BSCI-Systemhandbuch Teil II. (2018); amfori (n.d.); RBA (2022); RBA (2021); Social Accountability International (2021); Scott (2022)

Abbildung 2 : Übersicht der Nachweisformen (Grafik der Autorin)

4.2 VARIANTE B: ÜBERPRÜFUNG DER ILO-NORMEN DURCH ELECTRONICS WATCH

Einige der Nachteile von Sozialaudits können durch den Beitritt zu «Electronics Watch» und der Übernahme deren Vertragsbedingungen bzw. des «Code of Conduct» kompensiert werden. Diese Variante kann eigenständig oder in Kombination mit Variante A in den Beschaffungsprozess von IKT-Produkten integriert werden.

4.2.1 Chancen eines Beitritts zu Electronics Watch für Beschaffungsstellen

Electronics Watch (EW) ist eine dem IKT-Sektor einzigartige Monitoringorganisation, die öffentliche Beschaffungsstellen bei der fairen Beschaffung von IKT-Produkten unterstützt. Das EW-Modell basiert auf Monitoring – also der kontinuierlichen Überwachung und Bewertung von Arbeitsbedingungen der Zuliefererfabriken – und verfolgt den Ansatz «Vertragserfüllungsmanagement statt Zertifizierung» (Pawlicki, o. d., S. 88). Das bedeutet, dass Electronics Watch während der Vertragslaufzeit ein kontinuierliches Monitoring des «Code of Conduct» durchführt. Dabei werden anstelle von Sozialaudits in den Fabriken die Arbeitnehmer*innen ausserhalb der Fabriken in Interviews zu den Arbeitsbedingungen befragt.

EW arbeitet mit Monitoring-Partnern zusammen, die aus lokalen Gewerkschaften, NGOs und unabhängigen Menschenrechts- und Arbeitsrechtsexperten bestehen (für eine Auswahl an Partnern siehe: Monitoring-Partner, o. D.). Die Personen vor Ort handeln im Auftrag der EW-Mitglieder – also der öffentlichen Auftraggeber – und nicht der Wirtschaftsverbände oder der Hersteller. EW geht davon aus, dass Monitoring-Partner aufgrund ihrer Unabhängigkeit von der Privatwirtschaft eher in der Lage sind, das Vertrauen der Arbeiter*innen zu gewinnen als die von der Industrie beauftragten Auditor*innen. Dadurch erhöht sich gemäss EW die Chance, zusätzliche Informationen über die Arbeitsbedingungen in den Fabriken zu erhalten. Durch die lokale Präsenz der EW-Partner ist auch ein kontinuierliches Monitoring möglich, im Gegensatz zu den punktuellen Überprüfungen der Audits, die teilweise nur alle 12 – 32 Monate stattfinden. Ein weiterer Vorteil des EW-Modells ist, dass die Arbeiter*innen aktiv in den Optimierungsprozess einbezogen werden, indem sie Einsicht in die Auditunterlagen erhalten und über ihre Rechte aufgeklärt werden (Worker-Driven monitoring, o. d.).

Der Ansatz von EW konzentriert sich auf die Vertragserfüllung und nutzt den oben beschriebenen Zugang zu den Monitoring-Partnern als Überprüfungsmechanismus. Die Sicherstellung der Einhaltung der ILO-Normen erfolgt nicht wie bei Variante A durch eine «vorherige» Überprüfung des Lieferanten und seiner relevanten Dritten durch Zertifikate, sondern durch eine langfristige Überwachung während der Vertragslaufzeit. Zu diesem Zweck stellt EW Muster für Vertragsklauseln zur Verfügung, die in Vertrag mit den Lieferanten aufgenommen werden können. Zum einen wird darin geregelt, dass der Lieferant die Produktionsstätten offenlegen muss («Disclosure Form»), indem er alle Namen und Adressen der relevanten Fabriken in der Lieferkette angibt. Zum anderen enthält der Vertrag auch Vorgaben zur Einhaltung von Arbeitsschutzrechten, die im «Kodex» von EW definiert sind. Dazu gehört zum Beispiel, dass die Partner*innen von EW bei Verstössen gegen den Kodex Einsicht in den Fabrikbericht nehmen können, Zutritt zu allen relevanten Arbeitsstätten oder Wohnheimen erhalten oder Mitarbeiter*innenbefragungen in Abwesenheit von Autoritätspersonen durchführen können. Zudem verpflichtet sich der Lieferant die Monitoringberichte öffentlich zugänglich zu machen. Bei wiederholten Verstössen gegen den Kodex oder einer Verweigerung zur Behebung der Verstösse, kann die Beschaffungsstelle als Sanktion vom Vertragsverhältnis zurücktreten (Electronics Watch, 2019).

4.2.2 Herausforderungen für Beschaffungsstellen beim Electronics-Watch-Modell

Eine Herausforderung des EW-Modells ist die Abhängigkeit vom EW-Netzwerk. Die Mitgliedschaft bei EW ist mit Kosten verbunden, die sich nicht alle Beschaffungsstellen leisten können. Allerdings können Beschaffungsstellen Vertragsklauseln zu sozialen Aspekten, wie sie EW vorschlägt, teilweise auch ohne EW-Mitgliedschaft verwenden. So kann z.B. die Klausel, die den Lieferanten verpflichtet, die Standorte seiner Fabriken und die seiner Sublieferanten offen zu legen, auch dann eine Wirkung entfalten, wenn es keine Instanz gibt, die während der Vertragsdauer ein Monitoring durchführt. Denn auf diese Weise wird der Lieferant dazu angehalten, sich mit seiner eigenen Lieferkette auseinanderzusetzen und relevante Dritte sowie humanitäre Risiken zu identifizieren und zu lokalisieren. Um die Auseinandersetzung des Lieferanten mit der Produktwertschöpfungskette weiter zu fördern, können im Rahmen der Zuschlagskriterien auch «Anbieterkonzepte» bewertet werden, in denen der Lieferant aufgefordert wird,

detailliert auf Risiken in der Lieferkette hinzuweisen und Lösungsvorschläge zu unterbreiten, wie z.B. die Transparenz von Auditergebnissen erhöht und Korrekturmassnahmen besser umgesetzt werden können.[14] Bestimmte Lösungsvorschläge des Anbieters aus den Konzepten können dann vertraglich fixiert werden (z.B. dass der Lieferant der Beschaffungsstelle über Fortschritte berichtet oder dass Auditergebnisse transparent gemacht und mit der Beschaffungsstelle geteilt werden). Auf diese Weise kann die Beschaffungsstelle, auch wenn sie kein Monitoring durchführen kann, den vertraglichen Rahmen nutzen, um den Lieferanten für Risiken in der Lieferkette zu sensibilisieren und ihn zu verpflichten, über Verbesserungen oder Verschlechterungen zu rapportieren.

Neben der Abhängigkeit vom EW-Netzwerk besteht wie bei den Sozialaudits das Problem, dass sich die Überprüfung vor allem auf die Endfertigungsbetriebe erstreckt (allerdings gibt es bei EW Pilotprojekte, die das Monitoring auch auf Minen bzw. den Bergbau ausdehnen; siehe Electronics Watch, n. d.). Die Einhaltung der ILO-Kernarbeitsnormen beim Rohstoffabbau und -handel könnte, sofern der Beschaffungsgegenstand dies zulässt, durch eine zusätzliche Vertragsklausel oder durch den Nachweis der Mitgliedschaft des Lieferanten in einer Initiative für konfliktfreien Mineralienhandel näher spezifiziert werden (siehe Kapitel 5 für einen Exkurs zum Rohstoffhandel).

Ein weiterer potenzieller Nachteil des EW-Modells ist, dass die eigentliche Überprüfung der Fabriken erst nach dem Zuschlag stattfindet, da die Überwachung des EW-Kodex eine Vertragsbedingung ist. Der Lieferant muss 25 Tage nach Vertragsunterzeichnung das Compliance-Konzept vorlegen (Electronics Watch, 2017). Auch wenn der Vertrag Sanktionen bei Verstössen gegen den Kodex vorsieht (z.B. Kündigung des Vertragsverhältnisses), ist diese Option vor allem für Beschaffungsstellen mit langwierigen und planungsintensiven Beschaffungsprozessen ein Risiko.

Wichtig beim EW-Ansatz ist ausserdem, die «Verhältnismässigkeitsklausel» zu spezifizieren. Der EW-Vertragsentwurf verwendet die Formulierung, dass der Lieferant «angemessene und verhältnismässige Anstrengungen» unternehmen muss, um seine Sublieferanten zu überprüfen und den Kodex umzusetzen. Dies kann im Einzelfall

[14] Solche Anbieterkonzepte wurden bereits als Zuschlagskriterien formuliert und danach bewertet. Siehe für eine Musterausschreibung Evermann, 2016.

schwierig zu beurteilen sein, weshalb festgehalten werden soll, wie der Kodex umgesetzt werden soll und wie diese Umsetzung berichtet wird. Zudem könnte die Formulierung zu einer Verwässerung oder Abschwächung der sozialen Nachhaltigkeitsziele führen, indem die ursprünglich angestrebten Verbesserungen von Arbeitsbedingungen, fairer Entlohnung oder Menschenrechten nicht erreicht werden oder der Lieferant versucht, die Ziele zu umgehen. Die Formulierung «angemessene Anstrengungen» sollte nach Möglichkeit weiter konkretisiert werden und Mindestanforderungen sollten klar als solche dargestellt werden, da die Verhältnismässigkeitsklausel sonst die Definition von messbaren Zielen und Indikatoren erschweren könnte.

5. EXKURS: HUMANITÄRE KRISEN IM SCHATTEN DER ROHSTOFFGEWINNUNG – BESCHAFFUNG VON ROHSTOFFEN AUS DER DEMOKRATISCHEN REPUBLIK KONGO

Die in diesem Beitrag vorgestellten Zertifikate und Monitoringmöglichkeiten konzentrieren sich vor allem auf die Stufe der Endmontage von IKT-Produkten. Doch gerade am Ursprung der Lieferkette, dem Rohstoffabbau, kommt es häufig zu gravierenden Menschen- und Arbeitsrechtsverletzungen. Besonders betroffen davon sind die DR Kongo und ihre Nachbarländer. Seit Jahrzehnten herrschen in der DR Kongo bewaffnete Konflikte. Die sogenannten «Kongokriege» sowie die andauernden gewaltsamen Auseinandersetzungen zwischen verschiedenen Rebellengruppen und Milizen stehen in direktem Zusammenhang mit der Ausbeutung von Rohstoffen (vgl. z.B. OHCHR o. d.; Tsabora, 2014; Montague, 2002). Bewaffnete Gruppen versuchen sich meist durch Gewalt den Zugang zu Mineralvorkommen zu sichern oder erkämpfen sich die Kontrolle über Minen (auch Minen des Kleinbergbaus). Die beteiligten Gruppen versuchen dann, die erbeuteten Mineralien auf dem internationalen Markt zu verkaufen (Usanov et al., 2013, S. 57). Über Zwischenhändler gelingt es, die illegal gewonnenen Rohstoffe an westliche Händler zu vertreiben (Montague, 2002, S. 104, S. 107).

Grosse Teile der Zivilbevölkerung in der DR Kongo leiden stark unter den Kämpfen um die rohstoffreichen Gebiete. Zahlreiche Menschen werden Opfer von Vertreibung, Hunger, medizinischer Unterversorgung und Gewalttaten wie Mord, Vergewaltigung

und Entführung.[15] Bis zum Jahr 2023 wurden im rohstoffreichen Osten der DR Kongo fast sieben Millionen Menschen aus ihren Heimatgebieten vertrieben (Neiman, 2023; Record High Displacement in DRC At Nearly 7 Million, 2023). In den eroberten Gebieten wird die Zivilbevölkerung wiederum zur Arbeit im Rohstoffabbau gezwungen, wovon in hohem Masse Kinder betroffen sind (vgl. z.B. Cheruga et al., 2020). Die anhaltenden Kämpfe in den kongolesischen Rohstoffgebieten haben zu einer der schwersten humanitären Krisen der Gegenwart geführt.

Wer IKT einkauft, kommt kaum umhin, direkt oder indirekt Rohstoffe aus dem Kongo zu beziehen. 34% des weltweiten Kobalts und 10% des weltweiten Kupfers werden in Katanga – im Südostkongo – und in Sambia gefördert. In der kongolesischen Region Kivu lagern zudem 60-80% der weltweiten Coltanreserven, die für die Herstellung von Mobiltelefonen, Computern und anderen elektronischen Geräten unentbehrlich sind (OHCHR, o. d.). Was können Einkäufer*innen tun, um die soziale Nachhaltigkeit in den Rohstoffgebieten zu unterstützen? Die OECD-Leitsätze für einen verantwortungsvollen Einkauf von Rohstoffen aus Risikogebieten leistet einen ersten hilfreichen Ausgangspunkt. Die Leitsätze unterstützen Unternehmen, die Konfliktrohstoffe einkaufen, bei der Umsetzung der Sorgfaltspflicht in ihrer Lieferkette. Teilnehmende Unternehmen müssen beispielsweise jährlich Stellung zu ihren Bemühungen beziehen und offenlegen, wie sie die Leitsätze umsetzen. Zudem sind sie verpflichtet, Beschwerdemechanismen einzurichten (OECD, 2019). Der OECD-Leitfaden kann Beschaffungsstellen dabei helfen, ihre eigene Sorgfaltspflicht besser wahrzunehmen und die Bemühungen eines Unternehmens zur Beschaffung konfliktfreier Mineralien zu beurteilen und zu überprüfen.

Darüber hinaus existieren im Bereich des Rohstoffhandels einige Industrie- und Multi-Stakeholder-Initiativen. Eine der bekanntesten Initiativen ist die «Responsible Mineral Initiative» (RMI).[16] Sie verfolgt ein ähnliches Prinzip wie die in Kapitel 4.1.1 erwähnte «Responsible Business Alliance» (RBA). Die Mitgliedsunternehmen der RMI bekennen sich zu einer Verbesserung der Lieferkette im Rohstoffsektor. Ein Ziel der RMI ist

[15] Siehe z.B. Clashes in Eastern DR Congo Displace 450,000 in Six Weeks, 2023; Democratic Republic of Congo, 2023; Bitala, 2015; Human Rights Watch, 2023a; Human Rights Watch, 2023b.

[16] Andere Initiativen und Programme sind beispielsweise RJC (Responsible Jewellery Council), ITSCI (International Tin Supply Chain Initiative), EPRM (European Partnership for Responsible Minerals), RCI (Responsible Cobalt Initiative).

die Rückverfolgbarkeit der Rohstoffe herzustellen. Durch Auditprozesse und andere Überprüfungsmechanismen in den Schmelzen und Raffinerien soll sichergestellt werden, dass die Rohstoffe aus dokumentiertem Bergbau stammen und nicht illegal von Rebellen erworben wurden (vgl. RMAP Assessment Introduction vom RMI). Einige Zertifikate wie TCO-Certified oder EPEAT orientieren sich an den Vorgaben von Multi-Stakeholder-Initiativen im Rohstoffbereich und verlangen von Fabriken und Händlern die Umsetzung von Richtlinien zu Konfliktmineralien (siehe z.B. Langer, 2023b und GEC, 2022). Bei Mitgliedschaften in Initiativen besteht jedoch das Problem, dass die Mitgliedsunternehmen nicht verpflichtet sind, die RMI-Prinzipien umzusetzen und Rechenschaft abzulegen und auch Audit-Dokumente der Öffentlichkeit meist nur stark gekürzt oder gar nicht zugänglich sind (Peter, 2023a, S. 17f.).

Für Beschaffungsverantwortliche, die Rohstoffe aus Risikogebieten beziehen, ist es wichtig zu beachten, dass «frei von Konfliktmineralien» aus humanitären Gründen nicht gleichbedeutend mit «nicht aus der Demokratischen Republik Kongo» sein sollte. Ein genereller Boykott der DR Kongo ist problematisch, da der Rohstoffhandel ein wichtiger Wirtschaftszweig des Landes ist und viele Menschen von der Arbeit in diesem Sektor abhängig sind. Ein Wirtschaftsboykott würde die Handelsstrukturen des Landes weiter schwächen (Peter, 2023a, S. 22). Stattdessen sollte angestrebt werden, Mineralien in der DR Kongo aus dokumentiertem Bergbau (auch aus dem Kleinbergbau) zu beziehen.[17]

6. FAZIT

Der Artikel hat sich mit der Frage befasst, welche Mittel kleinen bis mittelgrossen Beschaffungsstellen zur Verfügung stehen, die ILO-Kernarbeitsnormen, die gemäss Art. 12 BöB als zwingende Teilnahmebedingungen definiert sind, zu überprüfen. Da IKT-Produkte innerhalb der Lieferketten ein hohes Risiko für Arbeitsrechtsverletzungen bergen, ist die Überprüfung dieser Normen über die Selbstdeklaration hinaus Gegenstand der Sorgfaltspflicht. Der Artikel hat zwei Ansätze identifiziert, die Beschaffungsstellen zur Überprüfung von ILO-Normen verfolgen können: Zum einen die Forderung nach

[17] Eine sehr hilfreiche und detaillierte Übersicht über die Beteiligung und Mitgliedschaft der meisten grossen Lieferanten in Rohstoffinitiativen findet sich in Peter, 2023a sowie eine Checkliste einiger ICT-Lieferanten in Peter, 2023b.

Nachweisen, die auf Sozialaudits basieren, und zum anderen vertragszentrierte Ansätze wie der von Electronics Watch (EW). Beide Ansätze wurden auf ihre Schwächen hin untersucht.

Die auf Sozialaudits basierenden Ansätze sehen sich mit dem Problem konfrontiert, dass Sozialaudits zunehmend in die Kritik geraten, weil die Inspektionen zu selten stattfinden und Fabrikmanager Verstösse gegen die ILO-Normen zu einfach verschleiern können. Das Problem beim EW-Ansatz ist, dass nur eine Verhältnismässigkeitsklausel eine zu starke Einschränkung des Marktes verhindern kann, was wiederum zu einer Verwässerung der Ansprüche an die soziale Nachhaltigkeit führen kann. Beide Ansätze konzentrieren sich hauptsächlich auf die letzte Stufe der Lieferkette, wobei die Stufe der Rohstoffgewinnung folglich weitgehend unkontrolliert bleibt. Hier müssten Beschaffungsstellen weitere Schritte unternehmen, um auch in diesem Bereich die Einhaltung der ILO-Normen zu überprüfen (siehe Kapitel 5 und Fussnote 17 für weiterführende Informationen). Trotz der diskutierten Schwächen ist die Umsetzung beider Varianten in der öffentlichen Beschaffung empfehlenswert und bedeutet einen Schritt in Richtung sozial nachhaltigere Lieferketten. Gerade im IKT-Bereich braucht es noch mehr Impulse, damit Lieferanten und ihre Sublieferanten soziale Missstände in der Lieferkette angehen. Die öffentliche Hand hat mit ihrer Kaufkraft die Chance, diese Impulse zu setzen.

BIBLIOGRAFIE

Ames, G. & Schurath, B. (2018). *Kobalt. kritisch³*. https://oenz.de/sites/default/files/kobaltstudie_0.pdf

Amfori BSCI-Systemhandbuch Teil II. (2018). *https://www.amfori.org/node/223/field_resource_language/german-10?search_api_views_fulltext=Systemhandbuch&field_resource_date_from=&field_resource_date_to=*

Amfori. (n.d.). *FTA Issues Statement on Conflict Minerals to Highlight Drawbacks of Draft Regulation*. Amfori.
https://www.amfori.org/news/fta-issues-statement-conflict-minerals-highlight-drawbacks-draft-regulation

Barume, B., Naeher, U., Ruppen, D. & Schütte, P. (2016). Conflict Minerals (3TG): Mining Production, Applications and Recycling. *Current opinion in green and sustainable chemistry*, *1*, 8–12.

Beck, S. (2013, 1. Januar). *Sozial verantwortliche Beschaffung von Informationstechnik*. ICCD, International Center for Development and Decent Work. https://kobra.uni-kassel.de/handle/123456789/2015030247562

Beschaffungskonferenz des Bundes BKB. (2021, Juni). *Nachhaltige Beschaffung: Empfehlungen für die Beschaffungsstellen des Bundes*. https://www.bkb.admin.ch/dam/bkb/de/dokumente/Oeffentliches_Beschaffungswesen/Nachhaltige_Beschaffung/Empfehlung_Nachhaltige%20Beschaffung_BKB_de_Neu.pdf.download.pdf/Empfehlung_Nachhaltige%20Beschaffung_BKB_de_Neu.pdf

Beschaffungsamt des BMI (2021). *Sozial-Audits als Instrument zur Überprüfung von Arbeitsbedingungen. Diskussion und Empfehlungen im Kontext der öffentlichen Beschaffung*.

Bitala, M. (2015, February 11). Krieg um Rohstoffe. *Süddeutsche.de*. https://www.sueddeutsche.de/politik/kongo-krieg-um-rohstoffe-1.930099

Cheruga, B., Liron, R., & Canavera, M. (2020). Ensuring children's social protection in the Democratic Republic of the Congo: A case study of combating child labour in the copper-cobalt belt. In D. Lawson, D. Angem, & I. Kasirye (Eds.), *What Works for Africa's Poorest Children. From measurement to action*. Practical Action Publishing.

Clashes in eastern DR Congo displace 450,000 in six weeks. (2023, November 24). UN News. https://news.un.org/en/story/2023/11/1143937

Davies, R. B. & Vadlamannati, K. C. (2013). A race to the bottom in labor standards? An empirical investigation. *Journal Of Development Economics*, 103, 1–14.

Electronics Watch (2017). *Contractor Guidance for Electronics Watch contract conditions, v 1.1*. Electronicswatch.org. https://electronicswatch.org/the-electronics-watch-contractor-guidance-september-2017_2525815.pdf

Electronics Watch. (2019). *Vertragsbedingungen für Lieferverträge*. Electronicswatch.org. https://electronicswatch.org/-2563231_2563231.pdf

Electronics Watch. (n. d.). *Electronics Watch stärkt Bergleute*. Electronicswatch.org. https://electronicswatch.org/de/electronics-watch-st%C3%A4rkt-bergleute_2621239

Evermann, A. (2016). Praxisbeispiele Sozial verantwortliche IT-Beschaffung. *WEED - World Economy, Ecology & Development*. https://www.weed-online.org/de/publikationen-detailansicht/praxisbeispiele-sozial-verantwortliche-it-beschaffung?file=files%2Fpublications%2Ffiles%2F2016%2FPraxisleitfaden-sozial-verantwor%2Fweed_2016_praxisleitfaden_it_bes.pdf

Faber, B., Krause, B. & De La Sierra, R. S. (2017). Artisanal mining, livelihoods, and child labor in the cobalt supply chain of the Democratic Republic of Congo. *RePEc: Research Papers in Economics*. https://escholarship.org/content/qt17m9g4wm/qt17m9g4wm.pdf

Faist, M. & Schlierenzauer, C. (2020). *Relevanzmatrix – Orientierungshilfe für Beschaffende und Bedarfsstellen Methodenbericht zu den ökologischen und sozialen Kriterien*. Im Auftrag des Bundesamtes für Umwelt (BAFU) https://www.bafu.admin.ch/dam/bafu/de/dokumente/wirtschaft-konsum/fachinfodaten/relevanzmatrix.pdf.download.pdf/relevanzmatrix-gesamt.pdf

Fuller, S. & Rydell, N. (2023, Juni 19). *Wie wird die Einhaltung der sozialen Kriterien in TCO certified*. TCO Certified. https://tcocertified.com/de/news/how-compliance-with-social-criteria-is-verified-in-tco-certified/

GEC (2022, Februar 3). *Überblick über die Auswirkungen der Nachhaltigkeit: Soziale Auswirkungen der Lieferkette*. Globaler Rat Für Elektronik. https://globalelectronicscouncil.org/de/resources/impact-guides/sustainability-impacts-overview-supply-chain-social-impacts/

Human Rights Watch (2022). *"Obsessed with Audit Tools, Missing the Goal". Why Social Audits Can't Fix Labor Rights Abuses in Global Supply Chains*. https://www.hrw.org/sites/default/files/media_2022/11/Social_audits_brochure_1122_WEBSPREADS_0.pdf

Human Rights Watch. (2023a, Januar 20). *Democratic Republic of Congo*. https://www.hrw.org/world-report/2023/country-chapters/democratic-republic-congo

Human Rights Watch. (2023b, 29. August). DR Congo: Killings, rapes by Rwanda-Backed M23 rebels. *Human Rights Watch*. https://www.hrw.org/news/2023/06/13/dr-congo-killings-rapes-rwanda-backed-m23-rebels

International Labour Organization. (n. d.). *How the ILO works*. International Labour Organization. https://www.ilo.org/global/about-the-ilo/how-the-ilo-works/lang--en/index.htm

Kelly, I. M., Miedema, C., Vanpeperstraete, B., & Winterstein, I. (2019). *FIG LEAF FOR FASHION. How social auditing protects brands and fails workers*. https://cleanclothes.org/file-repository/figleaf-for-fashion.pdf/view

Koch, R. (2023). *Öffentliche Beschaffungen im Bildungssektor Studie im Auftrag der Fachagentur Educa zur Verortung der (IKT-) Beschaffungen von Schulen nach dem revidierten öffentlichen Beschaffungsrecht*. https://www.bfh.ch/dam/jcr:4ab0c6b4-7308-4a71-9705-946958b8b871/%C3%96ffentliche%20Beschaffungen%20im%20Bildungssektor.pdf

Langer, A. (2023a, 11. Mai). *Mehr Transparenz macht Nachhaltigkeit zu einem guten Geschäft*. TCO Certified. https://tcocertified.com/de/news/increased-transparency-turns-sustainability-into-good-business/

Langer, A. (2023b, Mai 16). *In IT-Produkten verwendete Konfliktmineralien führen zu Kriegen und Menschenrechtsverletzungen*. TCO Certified. https://tcocertified.com/de/conflict-minerals/

Merk, J. (2021). *Human rights risks in the ICT supply chain*. https://www.ed.ac.uk/sites/default/files/atoms/files/human_rights_risks_in_the_ict_supply_chain_0.pdf

Monitoring-Partner. (o. D.). Electronics Watch. https://electronicswatch.org/de/monitoring-partner_2544003

Montague, D. (2002). Stolen Goods: Coltan and Conflict in the Democratic Republic of Congo. *SAIS Review (1989-2003)*, *22*(1), 103–118. https://www.jstor.org/stable/26996391

Neiman, S. (2023, December 5). Unease, uncertainty for displaced people in DR Congo ahead of Dec 20 vote. *Al Jazeera*. https://www.aljazeera.com/features/2023/12/5/unease-uncertainty-for-displaced-people-in-dr-congo-ahead-of-dec-20-vote

OECD (2019), *OECD-Leitfaden für die Erfüllung der Sorgfaltspflicht zur Förderung verantwortungsvoller Lieferketten für Minerale aus Konflikt- und Hochrisikogebieten: Dritte Ausgabe*, OECD Publishing, Paris, https://doi.org/10.1787/3d21faa0-de.

OHCHR (o. d.). *Violence linked to natural resource exploitation: DEMOCRATIC REPUBLIC OF THE CONGO 1993-2003.* UN Mapping Report. (n.d.). The Office of the High Commissioner for Human Rights (OHCHR).

Osburg, T. (2015). Erfolgreiche Ansätze zur Vermeidung von Konfliktmineralien. In E. Fröhlich (Hrsg.), *CSR und Beschaffung. Theoretische wie praktische Implikationen eines nachhaltigen Beschaffungsprozessmodells* (S. 207–221). Springer.

Pawlicki, P. (o. d.). *Electronics Watch – unabhängiges Monitoring für öffentliche Beschaffung, https://www.eineweltnetzwerkbayern.de/fileadmin/assets/Publikationen/14_Runder_Tisch/EWNB_-_14_RTB_-_S_85-91_-_ElectronicsWatch.pdf*

Peter, J. (2023a). ROHSTOFFE IM FOKUS. Wo steht die Elektronikbranche beim verantwortungsvollen Bezug von Rohstoffen?: Ein Update der Studie „Am anderen Ende der Lieferkette". In *WEED – Weltwirtschaft, Ökologie & Entwicklung e.V.* https://www2.weed-online.org/uploads/weed_2023_rohstoffe_im_fokus_web.pdf

Peter, J. (2023b). Steckbriefe der untersuchten IT-Hersteller. In *WEED – Weltwirtschaft, Ökologie & Entwicklung e.V.* WEED – Weltwirtschaft, Ökologie & Entwicklung e.V. https://www2.weed-online.org/uploads/weed_2023_rohstoffe_im_fokus_steckbriefe_web.pdf

Peter, J. (2022). Soziale Kriterien einfordern und überprüfen: Ansätze für eine faire öffentliche Beschaffung von IKT-Produkten. In *WEED – Weltwirtschaft, Ökologie & Entwicklung e.V.* https://www2.weed-online.org/uploads/weed_2022_ansaetze_fuer_eine_faire_oeffentliche_ikt_beschaffung_web_v2.pdf

Pun, N., Shen, Y., Guo, Y., Huilin, L., Chan, J., & Selden, M. (2016). Apple, Foxconn, and Chinese workers' struggles from a global labor perspective. Inter-Asia Cultural Studies, 17(2), 166–185. https://doi.org/10.1080/14649373.2016.1170961

RBA *(2022, 6. Februar), Frequently Asked Questions (FAQ). Regarding the VAP Audit Recognition Program*. https://eiccoalition.sharefile.com/share/view/s98ea4ce215024b-5fb19afa89e61624db

RBA Validated Assessment Program (VAP) Operations Manual. (2021). In *RBA*. https://www.responsiblebusiness.org/media/docs/AuditeeCAPmgt.pdf

Record High Displacement in DRC at Nearly 7 Million. (2023, 30. Oktober). International Organization For Migration. https://www.iom.int/news/record-high-displacement-drc-nearly-7-million

Responsible Minerals Initiative. (n.d.). https://www.responsiblemineralsinitiative.org/

RMAP *Assessment Introduction*. (n.d.). https://www.responsiblemineralsinitiative.org/responsible-minerals-assurance-process/

SECO. (n.d.). *Vertretung der Schweiz bei der Internationalen Arbeitsorganisation (IAO)*. https://www.seco.admin.ch/seco/de/home/Arbeit/Internationale_Arbeitsfragen/IAO.html

SECO (2015). Feuille d'information : Les conventions fondamentales de l'OIT et la Déclaration de 1998 sur les principes et droits fondamentaux au travail

Social Accountability International. (2023, June 16). *SA8000® Standard - SAI*. SAI. https://sa-intl.org/programs/sa8000/

Social Accountability International (2021, 14. Oktober). Unannounced SA8000 Audits - SAI. https://sa-intl.org/resources/unannounced-sa8000-audits/

Steiner, M. (2017). *Die Berücksichtigung sozialer Aspekte im Rahmen der öffentlichen Beschaffung*, erstellt im Auftrag der Interessengemeinschaft Ökologische Beschaffung Schweiz (IGÖB)

Steiner, M. (2020). Kurzabriss zu Entstehungsgeschichte und Zwecksetzung des BöB vom 21. Juni 2019. *Institut Für Schweizerisches Und Internationales Baurecht*, 8–10.

Steiner, M. & Klingler, D. (2023). The Revised Swiss Public Procurement Law: More Quality and Sustainability. European procurement & public private partnership law review, 18(1), 87–93. https://doi.org/10.21552/epppl/2023/1/12

Scott, P. (2022). Audit Requirements for Accredited Certification Bodies for the SA8000 Program. In *SAI - Social Accountability International*. https://sa-intl.org/wp-content/uploads/2021/10/SAAS_Procedure_200_v-4.2_March.2020.pdf

Terwindt, C. & Armstrong, A. (2019). Oversight and accountability in the social auditing industry: The role of social compliance initiatives. *International Labour Review*, 158(2), 245–272.

TRIAS – Leitfaden für öffentliche Beschaffungen. *Erstellung der Ausschreibung und Ausschreibungsunterlagen*. https://www.trias.swiss/erstellung-der-ausschreibung-und-ausschreibungsunterlagen#c971

Tsabora, J. (2014). Fighting the "resource wars" in the Democratic Republic of the Congo: an exploratory diagnosis of the legal and institutional problems. *The Comparative and International Law Journal of Southern Africa*, *47*(1), 109–128. http://www.jstor.org/stable/24585819

Usanov, A., de Ridder, M., Auping, W., Lingemann, S., Espinoza, L. T., Ericsson, M., Farooki, M., Sievers, H., & Liedtke, M. (2013). Coltan's connections to the conflict in the DRC. In *Coltan, Congo & Conflict: POLINARES CASE STUDY* (pp. 55–66). Hague Centre for Strategic Studies. http://www.jstor.org/stable/resrep12571.8

Verbrugge, B. (2020). Standaarden, certificaten, en monitoringsystemen in de ICT-sector: op weg naar een duurzame aankooppraktijk?

Verité (2014). *Forced Labor in the Production of Electronic Goods in Malaysia. A Comprehensive Study of Scope and Characteristics*. https://www.verite.org/wpcontent/uploads/2016/11/VeriteForcedLaborMalaysianElectronics2014.pdf

WEED (2015). *Die globalisierte Informations- und Kommunikationsbranche. Einflussmöglichkeiten der öffentlichen Beschaffung auf die Arbeitsbedingungen entlang der Lieferkette*. https://www2.weed-online.org/uploads/weed_ikt_einfluss_de_laser.pdf

Worker-Driven monitoring. (o. d.). Electronics Watch. https://electronicswatch.org/worker-driven-monitoring_2548297

ÖFFENTLICHE BESCHAFFUNGEN UND ESG

Wie können Beschaffungsstellen ESG nutzen, um das Nachhaltigkeitsziel umzusetzen?

Paula Zimmermann

Paula Zimmermann ist Politologin und Rechtsanwältin, Senior Adviser / Partnerin und Mitglied der Geschäftsleitung bei Laux Lawyers AG

Abstract: Unternehmen und öffentliche Hand im EU-Raum sind angesichts einer Vielzahl neuer Gesetze gezwungen, ihr Handeln zur Erfüllung von Nachhaltigkeitsstandard anzupassen und ihren «ESG-Reportingpflichten» nachzukommen. Was für die UnterN eine Herausforderung darstellt, bietet eine Chance für die öffentliche Hand der Schweiz, ihre Beschaffungsziele umzusetzen und Rechtssicherheit zu schaffen.

Der Artikel gibt einen Überblick über Begrifflichkeiten, Hintergründe sowie aktuelle Gesetzeslage im Bereich ESG und vermittelt gesetzlichen Grundlagen nachhaltiger Beschaffung für die öffentliche Hand in der Schweiz. Anschliessend wird gezeigt, wie sich das Thema ESG für die öffentliche Hand in Ausschreibungs- und Vertragsbedingungen umsetzen lässt.

Stand: Februar 2024

INHALTSVERZEICHNIS

1. Einführung: ESG und das Schweizer Beschaffungsrecht 84
   1.1 Was ist ESG? 84
   1.2 Das neue Nachhaltigkeitsziel im revidierten Schweizer Beschaffungsrecht 86
2. Gesetzliche Grundlagen und Verpflichtungen rund um ESG 87
   2.1 EU-Gesetzgebung 88

2.1.1 Nachhaltigkeitsberichterstattung (Corporate Sustainability Reporting Directive, CSRD) ... 89
2.1.2 Taxonomieverordnung 2020/852 ... 90
2.1.3 Sustainable Finance Disclosure Regulation (SFDR) ... 90
2.1.4 Lieferkettengesetz (Corporate Sustainability Due Dilligence Directive, CSDDD) ... 91
2.2 In der Schweiz: Verordnung zur nichtfinanziellen Berichterstattung ... 92
3. Umsetzung des neuen Nachhaltigkeitsziels im Rahmen der öffentlichen Beschaffung ... 93
Bibliographie ... 95

1. EINFÜHRUNG: ESG UND DAS SCHWEIZER BESCHAFFUNGSRECHT

1.1 WAS IST ESG?

Das Akronym „ESG" steht für Environmental, Social und Corporate Governance (zu Deutsch: Umwelt, Soziales und Unternehmensführung). Die drei nachhaltigkeitsbezogenen Verantwortungsbereiche gehen zurück auf die UN Sustainable Development Goals («SDGs») von 2015 (UNDP, n.d.), im Rahmen derer die Vereinten Nationen 17 Ziele für nachhaltige Entwicklung formulierte, um die Armut zu beenden, den Planeten zu schützen und sicherzustellen, dass bis 2030 alle Menschen in Frieden und Wohlstand leben.

Die ökologische Dimension (das «E»/Environment in ESG) steht für die umweltbezogenen Nachhaltigkeitsziele und dient zur Beschreibung von Unternehmenszielen und -verpflichtungen im Zusammenhang mit dem Klimawandel. Hier geht es z. B um das vielbesagte «Net-Zero» Klimaziel, das den Ausgleich aller Emissionen eines Unternehmens verlangt (z.B. über Emissionszertifikate) (Carbon Jargon, 2022 oder Frigo et. Al. 2022). Zu den Emissionen zählen nicht nur solche, die eine Unternehmung selbst emittiert («Scope 1» und «Scope 2»), sondern auch die Emissionen der Wertschöpfungskette ihrer Produkte oder Dienstleistungen («Scope 3») (Carbon Jargon, 2022 Hall,)[1].

[1] Emissionen, die «Upstream» durch den Einkauf (von Gütern) verursacht werden (z.B. je nach Geschäftsfeld Rohstoffe, Businessreisen), wie auch solche, die durch den Verkauf «Downstream» entstehen (z.B. Lieferungen, Finanzinvestitionen).

Dabei ist Nachhaltigkeit in der Unternehmensführung kein neues Thema. Bisher eher unter dem Begriff Coroporate Social Responsibilty («CSR») bekannt, bezog sich diese Terminologie aber auf Handlungsempfehlungen und Berichterstattungspflichten, ohne konkrete gesetzliche Grundlage. Aufgrund neuer gesetzlicher Vorgaben hat das Thema Nachhaltigkeit an Bedeutung gewonnen und eine neue Dimension der Rechenschaftspflichten von relevanten Akteuren erfahren (Europäischer Rat, 2022.)

Die Europäische Union (EU) hat das Ziel des Übereinkommens von Paris in eine langfristige europäische Wachstumsstrategie umgesetzt. Mit dem «Green Deal» hat die EU 2019 eine Reduktion der CO_2 Emissionen um 55% bis 2030 und Kilmaneutralität bis 2050 beschlossen. Zur Erreichung dieser Ziele soll die Wirtschaft über die Finanzen in die Nachhaltigkeit gelenkt werden.

Das Klimaschutzpaket, welche die Europäische Kommission (EC) am 14. Juli 2021 («Fit for 55»-Massnahmen) erlassen hat, beinhaltet Gesetze, die helfen sollen, bis 2050 Klimaneutralität zu erreichen; einerseits durch Emissionsreduktionen von 55%, andererseits durch Berichterstattungsvorgaben für mehr Transparenz.

Die Tatsache, dass es rund um ESG zunehmend konkrete gesetzliche Vorgaben zur Nachhaltigkeit gibt, insbesondere was die Klimaberichterstattung anbelangt, eröffnet auch der öffentlichen Hand Chancen wenn es darum geht, das neue Nachhaltigkeitsziel im Beschaffungswesen umzusetzen.

Denn wenn Unternehmen, also auch die Anbieter als Zulieferer der öffentlichen Hand im Beschaffungswesen, entweder selbst konkreten Gesetzesvorgaben zur Nachhaltigkeitsberichterstattung unterliegen, oder das jedenfalls auf Seiten ihrer Zulieferer der Fall ist, dann können diese gesetzlichen Pflichten auch in Ausschreibungsunterlagen und den Verträgen verankert werden.

Die Gesetze, die erlassen wurden, um die ESG-Ziele zu erreichen, beinhalten sowohl konkrete Vorgaben, um zum Beispiel die Ziele des Green Deals zu erreichen, als auch Berichterstattungspflichten für Messbarkeit und Transparenz. Je nach Sektor variieren die Berichterstattungsspflichten, wie wir im Folgenden sehen werden. Daher kann es sein, dass diese je nach Sektor die direkten Lieferanten von Beschaffungsstellen, beispielsweise aus der IT-Branche, nicht verpflichten Aber auf die Sub-Lieferanten dieser

könnten die Berichterstattungspflichten durchaus Anwendung finden.[2] Das bedeutet, dass sich von den Sub-Lieferanten unter Umständen konkrete Zahlen in Bezug auf ESG finden würden, wenn eine Beschaffungsstelle nach diesen verlangt. Anders gesagt: Auch wenn die Gesetze rund um ESG (noch) keine direkte Wirkung auf die IT-Branche entfalten, ergeben sich die indirekte Wirkung aus den Gesetzesvorgaben für den Energie- und Rohstoffsektor, der wesentlich ist in der IT Lieferkette[3] (siehe z.B. Europäische Komission, 2021a).

1.2 DAS NEUE NACHHALTIGKEITSZIEL IM REVIDIERTEN SCHWEIZER BESCHAFFUNGSRECHT

Das revidierte Bundesgesetztes über das Beschaffungswesen (BöB) sowie die revidierte Verordnung über das öffentliche Beschaffungswesen (VöB) sind am 1. Januar 2021 in Kraft getreten. Die Revision hat zu einem Paradigmenwechsel im Schweizer Beschaffungswesen geführt, der im Rahmen der Vergabe nicht mehr nur dem wirtschaftlichen, sondern auch den volkswirtschaftlich, ökologisch und sozial nachhaltigen Einsatz der öffentlichen Mittel verlangt (Art. 2 lit. a BöB/IVöB). Dementsprechend sollen auch die konkreten Vergabeanforderungen so ausgestaltet sein, dass sie das Kriterium der Nachhaltigkeit berücksichtigen. Aufgrund der expliziten Erwähnung der Nachhaltigkeit im Zweckartikel kann die Nachhaltigkeit nicht nur bei den Zuschlagskriterien (Art. 29 BöB), sondern auch bei den technischen Spezifikationen (Art. 30 BöB) und bei den Eignungskriterien (Art. 27 BöB) berücksichtigt werden (BKB 2022). Im Rahmen der zwingenden Teilnahmebedingungen (Art. 12 BöB) müssen gewisse Mindeststandards in Bezug auf die ökologische und sozialen Nachhaltigkeit sogar zwingend eingehalten werden.[4]

Dass Nachhaltigkeit nicht «nur» gesetzlich verankert und in den Ausschreibungskriterien zu berücksichtigen ist, sondern von den potentiellen Lieferanten anhand belastbarer Kriterien nachzuweisen ist, sieht das neue Vergaberecht zwar nicht explizit vor. Sofern aber in der Ausschreibung Nachhaltigkeitsanforderungen auf Basis von allgemeinen

---

2 Für die Bedeutung von Sub-Lieferanten bzw. siehe Beitrag von Lara Biehl in diesem Band.

3 Für die Bedeutung der Lieferketten siehe auch Beitrag von Lara Biehl in diesem Band.

4 Siehe zu den obligatorischen Mindestanforderungen in Bezug auf Nachhaltigkeit auch den Beitrag von Lara Biehl in diesem Band.

Standards gestellt werden, kann ein ungenügender Nachweis dieser ein belastbares Ausschlusskriterium sein (BVGe B-5897/2022).[5]

In der Praxis werden solche Nachweise in Bezug auf die Nachhaltigkeit eher selten eingefordert,[6] da deren Einforderung und Überprüfung mit Aufwand verbunden ist. Nichtsdestotrotz sind Nachweise und Transparenz ratsam und bisweilen notwendig, um das neue Nachhaltigkeitsziel auch effektiv einfordern zu können und überprüfbar zu machen. Diesem Ziel kommen die handfesten gesetzlichen Anforderungen an Nachhaltigkeitsberichterstattung entgegen, die sich auf EU-Ebene verdichten. Denn Dank der gesetzlichen Berichterstattungspflichten bzgl. Nachhaltigkeit (und der normierten Angaben auf Basis derer die Berichterstattung zu erfolgen hat), können Lieferanten konkret verpflichtet werden. Dies sowohl im Rahmen der Ausschreibungskriterien als auch bei Abschluss der Verträge. Damit wird Nachhaltigkeit definierbar und als Lieferantenpflicht konkret vereinbar.

2. GESETZLICHE GRUNDLAGEN UND VERPFLICHTUNGEN RUND UM ESG

Zur Erreichung der EU-Klimaziele, und der Reduktion der CO_2-Emissionen um 55% bis 2030 und Kilmaneutralität bis 2050 soll «die Wirtschaft» über die Finanzen in die Nachhaltigkeit gelenkt werden (Europäische Kommission,2021). Dazu wird auf EU-Ebene ein Set an Gesetzen erlassen, das die Unternehmen u.a. zur Nachhaltigkeitsberichterstattung verpflichtet (siehe dazu auch vorhergehend, 1.1) und deren ökologischen Fussabdruck in Zahlen nachweisbar und belastbar machen soll (Europäische Kommission, 2023).

Hinzu kommen nationale Gesetze, beispielsweise in der Schweiz zur Berichterstattung über nichtfinanzielle Belange, oder das deutsche Lieferkettensorgfaltspflichtengesetz, die ebenfalls Berichterstattung über ESG-Parameter zum Inhalt haben.

---

5 So das Bundesverwaltungsgericht in seinem Urteil vom 5. April 2023, B-5897/2022 zu der Anforderung an den Nachweis eines «genügenden Umweltmanagementsystems» auf Basis einer ISO14001-Zertifizierung.

6 Siehe auch Beitrag von Lara Biehl in diesem Band.

2.1 EU-GESETZGEBUNG

Auch wenn in diesem Beitrag nicht alle Gesetze im Detail adressiert werden können, sollen hier einige Beispiele aus EU- und nationaler Gesetzgebung genannt werden. Das Set an Regularien spannt sich gewissermassen wie ein Schirm auf und deckt alle Wirtschaftssektoren, von Finanzindustrie über produzierende Industriezweige ab (Pettingale et al.,2022).

Zielsetzung und Anforderungen an die Berichterstattung folgen bei allen Gesetzen denselben Prinzipien mit dem Ziel, «Greenwashing» zu verhindern, also den Versuch, sich vordergründig ein «grünes» oder nachhaltiges Image zu geben, ohne ensprechende Massnahmen umzusetzen:

- Indem Reporting standardisiert, Zahlen belastbar, vergleichbar und verfügbar gemacht werden.[7]
- Die jeweiligen Gesetze enthalten spezifische Reportingstandards, es kann aber auch ein anderer Ansatz gewählt werden; wenn gar nicht Bericht erstattet wird, wäre dies zu erklären («comply or explain») und es kann auch Bussen zur Folge haben.

[7] Unternehmen, die der CSRD unterliegen, müssen nach den European Sustainability Reporting Standards (ESRS) berichten. Die Standards bauen auf internationalen Standardisierungsinitiativen auf und wurden von der EFRAG (früher European Financial Reporting Advisory Group) entwickelt, einem unabhängigen Gremium, in dem verschiedene Interessengruppen vertreten sind. Die Standards decken das gesamte Spektrum an Umwelt-, Sozial- und Governance-Themen ab, einschließlich Klimawandel, biologischer Vielfalt und Menschenrechten. Sie liefern den Anlegern Informationen, um die Nachhaltigkeitsauswirkungen der Unternehmen, in die sie investieren, zu verstehen. Sie berücksichtigen auch die Diskussionen mit dem International Sustainability Standards Board (ISSB) und der Global Reporting Initiative (GRI), um ein hohes Maß an Interoperabilität zwischen den EU-Standards und den globalen Standards zu gewährleisten und eine unnötige Doppelberichterstattung der Unternehmen zu vermeiden. Die Angaben sind als Teil des Jahresberichts, digital vorzulegen, perspektivisch sollen sie über einen sogenannten European Single Access Point („ESAP"), eine EU Datenbank öffentlich zugänglich sein. Die SFDR-Stufe 1 verlangt von Finanzinstituten in der EU allgemeine, prinzipienbasierte Angaben zu ESG-bezogenen Aktivitäten sowohl bezüglich die Sektoren, in die sie investieren, als auch über ihre Portfoliounternehmen, zu machen. Die SFDR-Stufe 2 beinhaltet technische Kriterien zur Bewertung von negativen Auswirkungen auf die Nachhaltigkeit auf Produktebene („adverse sustainability impacts statement"). In der Schweiz muss das Reporting qualitative und quantitative (sämtliche Treibhausgasemissionen sowie deren Berechnungsgrundlage, um die Vergleichbarkeit zu ermögliche) finanziellen Parameter betreffend CO2 Zielen und deren Erreichung mittels Business Model, Strategie, Investitionen und Risikomanagement enthalten.

- Inhaltlich liegt der Fokus momentan auf Berichterstattung in Bezug auf Nachhaltigkeit und Klima. Längerfristig ist das Ziel, alle ESG-Faktoren davon zu erfassen.
- Unternehmen müssen im Sinne der «doppelten Wesentlichkeit» berichten: Einerseits sind die Auswirkungen des Unternehmens auf die Umwelt und die Gesellschaft zu beschreiben, andererseits ist darzulegen, wie sich ändernde Nachhaltigkeitsaspekte auf das Unternehmen auswirken.
- Zunehmend rückt auch die ganze Lieferkette in den Fokus. Es zeichnet sich eine Pflicht ab, bei der Berichterstattung die gesamte Lieferkette mit einzubeziehen. Nicht nur, weil eine umfassende Klimabilanz (inklusive Scope-3 Emissionen), diese notwendigerweise mit umfassen muss, sondern auch weil es ganz spezifische Gesetze mit entsprechenden Pflichten gibt.
- Mittels delegierter Rechtsakte sollen zudem sektor-spezifische Anforderungen hinsichtlich Reporting erstellt werden.
- Die Nachhaltigkeitsinformationen müssen in einem deutlich gekennzeichneten Abschnitt des Lageberichts des Unternehmens veröffentlicht werden, der öffentlich zugänglich sein muss.
- Sowohl Unternehmen aus der Industrie als auch Finanzwirtschaft müssen diesen Reportingpflichten nachkommen.
- Diese Pflichten sind momentan auf «grosse» Unternehmen anwendbar, perspektivisch sollen aber auch kleinere / KMUs erfasst werden (Europäischer Rat, Rat der Europäischen Union, Pressemitteilung, 28. November 2022).

2.1.1 Nachhaltigkeitsberichterstattung (Corporate Sustainability Reporting Directive, CSRD)

Was die Industrieunternehmen anbelangt, ist als erstes die «Richtlinie 2022/2464 hinsichtlich der Nachhaltigkeitsberichterstattung von Unternehmen» zu nennen (auf englisch «Corporate Sustainability Reporting Directive» [CSRD] genannt), die grosse Unternehmen zur Nachhaltigkeitsberichterstattung verpflichtet. Die von der Richtlinie erfassten Unternehmen müssen Angaben machen über Geschäftsstrategie, Widerstandsfähigkeit des Geschäftsmodells und Risikomanagement in den Bereichen Klimawandel und biologische Vielfalt, sowie über soziale Faktoren wie Arbeitsbedingungen, Gleichberechtigung, Nichtdiskriminierung, «Diversity und Inclusion», Menschenrechte.

2.1.2 Taxonomieverordnung 2020/852

Diese Berichterstattung erfolgt basierend auf einer weiteren EU-Vergabe, der EU-Verordnung 2020/852 über die Einrichtung eines Rahmens zur Erleichterung nachhaltiger Investitionen (im folgenden -Taxonomie-Verordnung genannt).Mit der Taxonomie-Verordnung wurde ein Klassifizierungssystem für ökologisch nachhaltige Wirtschaftstätigkeiten erschaffen, das Unternehmen und Investor*innen die Möglichkeit geben soll, Transparenz über ihre nachhaltigen Aktivitäten zu schaffen, indem sie definiert, was überhaupt als «nachhaltige Wirtschaftstätigkeit» definiert werden kann (Europäische Kommission,2021b).

Die EU-Taxonomie enthält derzeit sektorspezifischen, technischen Prüfkriterien für 70 Aktivitäten zur Eindämmung des Klimawandels und 68 Aktivitäten zur Anpassung an den Klimawandel. Wenn die EU Taxonomie in diesem Zusammenhang von nachhaltigen Tätigkeiten spricht, dann sind damit gemäss Art. 3 a solche Wirtschaftstätigkeiten gemeint, die einen wesentlichen Beitrag zur Verwirklichung von mindestens einem der Umweltziele aus Art. 9[8] leisten, Gleichzeitig gilt aber gemäss Art. 3 b, dass keines dieser Ziele wesentlich beeinträchtigt werden darf und soziale Mindeststandards erfüllt sein müssen (Art. 18);

So können diejenigen Unternehmen, die die in nachhaltige Aktivitäten investieren wollen, auf Basis dieser Kriterien Investitionsentscheidungen treffen. Von der Taxonomie-Verordnung sind allerdings nicht alle Unternehmen erfasst, die unter der CSRD berichten müssen (Niederdrenk & Kopp, 2021).[9]

2.1.3 Sustainable Finance Disclosure Regulation (SFDR)

Als Beispiel für eine Berichterstattungspflicht der Finanzindustrie zu nennen ist die EU-Verordnung 2019/2988 über nachhaltigkeitsbezogene Offenlegungspflichten im

[8] Klimaschutz und Anpassung an den Klimawandel sowie vier weitere Umweltziele wie z.B. Übergang zur Kreislaufwirtschaft.

[9] Die EU-Kommission geht davon aus, dass mit den bislang getroffenen Regelungen rund 40 Prozent aller börsennotierten Unternehmen im Euroraum (und damit 80 Prozent direkter Treibhausgasemissionen) unter Taxonomiegesichtspunkten betrachtet werden könnten; Die Taxonomie-Verordnung deckt derzeit die Sektoren Forst- , Landwirtschaft, Energie- / Wasserversorgung, Verkehr, Information und Kommunikation und Baugewerbe ab.

Finanzdienstleistungssektor (Sustainable Finance Disclosure Regulation, im Folgenden SFDR genannt).

Die SFDR verpflichtet die Unternehmen der Finanz- und Versicherungsbranche, sowohl auf Unternehmens-, als auch auf Produktebene offenzulegen, inwiefern sie nachhaltig sind. So soll der den Geldfluss in nachhaltige Aktivitäten in der gesamten EU gefördert werden, indem klarer dargelegt wird, welche Wirtschaftstätigkeiten am meisten zur Erreichung der Umweltziele beitragen. Finanzseitig setzt die SFDR Standards zur Offenlegung von Nachhaltigkeitsinformationen bzw. der Integration von ESG-Faktoren insgesamt sowohl für Finanzmarktteilnehmer selbst, als auch in Bezug auf ihre Produkte.

Bemerkenswert ist insofern, dass die Nachhaltigkeitsindikatoren unter der SFDR den Parametern der EU-Taxonomien entsprechen. Kein Wunder, denn die Finanzinstitute sind ja zur Berichterstattung auf eben diese Informationen durch die Industrieunternehmen angewiesen.

2.1.4 Lieferkettengesetz (Corporate Sustainability Due Dilligence Directive, CSDDD)

Das EU-Parlament hat im Juni 2023 die Richtlinie über die unternehmerische Sorgfaltspflicht im Bereich der Nachhaltigkeit, «Corporate Sustainability Due Dilligence Directive» («CSDDD») verabschiedet. Der genaue Gesetzeswortlaut wird nun mit den Mitgliedstaaten verhandelt. Die Richtlinie wird voraussichtlich 2025 in Kraft treten.

Die Lieferketten-Richtlinie verlangt von Unternehmen, die Auswirkungen ihrer Geschäftstätigkeit auf die Menschenrechte - und die Umwelt entlang der ganzen Wertschöpfungskette zu ermitteln. Dabei geht die CSDDD insofern einen Schritt weiter als die bisherigen Berichterstattungspflichten, als sie die Unternehmen nicht nur verpflichtet, Risiken zu identifizieren, sondern auch Strategien zur Risikominderung nachzuweisen, diese zu überwachen und einen Jahresbericht zu erstellen, der die Bemühungen und Ziele im Bereich der Sorgfaltspflichten abdeckt.

Die CSDDD sieht deutlich weiter gehende Sorgfaltspflichten vor, als die im Schweizer Obligationenrecht neu eingegangenen Bestimmungen zur Berichterstattung (siehe

nachfolgend, Kapitel 3.2). So konzentrieren sich die Schweizer Bestimmungen zu den Sorgfaltspflichten auf Unternehmen in spezifischen Sektoren und im Bereich Rohstoffhandel. Die CSDDD gilt hingegen für alle Unternehmen ab einer bestimmten Grösse. Trotz des eingeschränkten Geltungsbereichs der Berichterstattungspflichten in der Schweiz betreffen diese neuen Sorgfaltspflichten Grossunternehmen mit hohen Umsätzen und damit Unternehmen, die einen grossen Einfluss auf die Wertschöpfung in der Schweiz haben (Meyer et al., 2023).

2.2 IN DER SCHWEIZ: VERORDNUNG ZUR NICHTFINANZIELLEN BERICHTERSTATTUNG

Wenn man nun das Schweizer Gesetz zur nichtfinanziellen Berichterstattung unter die Lupe nimmt, überrascht es nicht, dass hier die Themen und Parameter der Berichterstattung entsprechend ausgestaltet sind. Die Verordnung zur nichtfinanziellen Berichterstattung, die als Gegenvorschlag zur Konzerverantwortungsinitiative vom Bundesrat erlassen wurde (Verordnung vom 30. März 2022 über die Berichterstattung über Klimabelange) erstreckt sich auf die bekannten „ESG-Themenbereiche" Umwelt und CO_2-Ziele, Soziales, Arbeitnehmerbelange, Menschenrechte und Korruptionsbekämpfung. Die Pflichten zur nichtfinanziellen Berichterstattung wurden in die Art. 964 a-c des Schweizer Obligationenrechts aufgenommen.

Der zweite Bereich der Berichterstattung (Art. 964 j-l OR) betrifft spezifisch Rohstoffunternehmen und erlegt diesen Sorgfalts- und Berichterstattungspflichten in den Bereichen „Konfliktmineralien" und „Kinderarbeit" auf; wie in Punkto Fokus nationaler Gesetzgebung eingangs angedeutet, erstrecken sich die Berichtspflichten hier auch auf die Wertschöpfungskette. [10] Das Ziel dieser Berichtspflichten ist auch hierzulande, «Green Washing» entgegenzuwirken, also eine verlässliche Basis für Investitionen und Finanzdienstleistungen zu schaffen und mittels Standardisierung und Harmonisierung

[10] Die Kriterien zur Berichterstattung wurden anhand den Empfehlungen der «Task-Force climate related financial disclosures» (TCFD) der G20 Staaten etabliert, womit ein seit 2017 anerkannter und international etablierter Standard zur Klimaberichterstattung aufgegriffen und in Gesetzesform gegossen wurden. Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens zur Verordnung über die Berichterstattung über Klimabelange, S. 8.

der Berichterstattung in ESG belangen, eine Erhöhung der Rechts- und Investitionssicherheit herbei zu führen (siehe EFD, 2022, S.4).[11]

3. UMSETZUNG DES NEUEN NACHHALTIGKEITSZIELS IM RAHMEN DER ÖFFENTLICHEN BESCHAFFUNG

Der Geltungsbereich der oben genannten Gesetze ist sektorspezifisch und findet nicht auf jeden Lieferanten bzw. Anbieter Anwendung. Die Schweizer Beschaffungsbehörden sind als nicht-EU Organe natürlich nicht direkt von den Gesetzen betroffen. Wenn eine Schweizer Behörde Im Rahmen der IT-Beschaffung einen neuen Software Dienstleister auswählen möchte, dann finden etwaige EU-Gesetze nur dann potentiell Anwendung, wenn dessen Muttergesellschaft im einem EU-Land ist und der lokale Anbieter zur Erfüllung deren Reportingpflichten beitragen muss. Inhaltlich untersteht ein IT-Anbieter weder der CSRD noch der SFDR, und auch nicht den Schweizer Anforderungen zur nichtfinanziellen Berichterstattung. Aber in mittelbarer Wirkung der bereits jetzt existierenden Gesetze sind die Chancen gross, dass ein hiesiger Softwaredienstleister die relevanten Zahlen oder mindestens nachhaltigkeitsbezogene Angaben eben doch, jedenfalls in Teilen, liefern kann. So untersteht der Stromanbieter des IT-Dienstleisters möglicherweise bereits der CSRD (Geiger et al., 2022)[12]. Die Berichterstattung in der EU muss für den Energiesektor bereits auf Basis der EU-Taxonomie erfolgen. Dementsprechend ist es plausibel, dass auch ein kleiner IT-Dienstleister, der einen grossen Stromanbieter für ein Rechenzentrum hat, von diesem die relevanten Zahlen erfragen kann. So liegt es bisweilen nahe, dass ein Lieferant von in der IT-Branche erforderlichen Rohstoffen sowohl unter der CSDDD auf EU-Ebene als auch gemäss

---

11 Unternehmen welche in der Schweiz die Berichterstattung unterlassen oder sogar Falschangaben in den Berichten über nicht finanzielle Belange veröffentlichen, riskieren nach Art. 325ter Strafgesetz buch eine Busse von 100'000 CHF. Bei Fahrlässigkeit beträgt die Busse noch 50'000 CHF. Weit einschneidender können dabei jedoch die daraus resultierenden Reputationsschäden und Vertrauensverluste von Investoren und Konsumenten sein.

12 Mit der CSRD werden weitaus mehr Rohstoffhändler und Energieversorger in der EU einer Pflicht zur Erstellung eines Nachhaltigkeitsberichts unterstehen, da unter CSRD die Kotierungsvoraussetzung wegfällt und der Schwellenwert von 500 auf 250 Mitarbeitende reduziert wird. In der Schweiz werden voraussichtlich ebenfalls die meisten der (untersuchten) Energieversorger und alle Finanzinstitute künftig der Nachhaltigkeitsberichterstattungspflicht unterstehen.

Schweizer Vorschriften zur Berichterstattung verpflichtet sind, zumal wenn diese als Konfliktmineralien gelten.

Für die Gestaltung von Ausschreibungen und Verträgen ergibt sich aus all den geschilderten Gesetzesanforderungen die Chance, diese mit ganz konkreten Kriterien bezüglich Nachhaltigkeit zu versehen und Lieferanten auf konkrete gesetzliche Vorgaben zu verpflichten. Diese sind branchenspezifisch zu formulieren. Dazu braucht es Kenntnis der bestehenden Gesetzeslandschaft. Nach einer ausführlichen Analyse der spezifischen Industrie, also beispielsweise IT-Branche und deren Klima- / Lieferkettenberichterstattungspflichten, können konkrete Vertragspflichten formuliert werden. Im Falle der IT-Branche sind diese von eher mittelbarer Geltung. Aber sie lassen sich dennoch vertraglich festlegen. Beispielsweise damit, dass die Kennzahlen des Energielieferanten des Rechenzentrums eines IT-Dienstleisters geliefert werden müssen. Denn dieser Energielieferant wiederum muss seine Zahlen gemäss CSRD auf Basis der EU-Taxonomie bekannt geben. Des Weiteren lässt sich vertraglich festhalten, dass die Anbieter in Bezug auf die eigene Lieferkette die Anforderungen von Art. 964j-l OR zu Konfliktmineralien und Kinderarbeit einhalten müssen, beispielsweise bei der Beschaffung von Rohmaterialien zur Chip-Herstellung. Entsprechendes lässt sich als Ausschreibungskriterium festlegen.

Zusätzlich bietet es sich für die öffentliche Hand (sowie sämtliche Unternehmen) an, in die Verträge mit den eigenen Zulieferern eine Pflicht zur Einhaltung sämtlicher nachhaltigkeitsbezogenen Unternehmensziele (wie z.B. Klimaziele) aufzunehmen und diese Verpflichtung auch auf ihre Unterlieferanten auszudehnen. Das Prinzip der sog. „Back-to-Back" Spiegelung vertraglicher Pflichten entlang der Lieferkette und der Risikoabwälzung auf Zulieferer lässt sich sowohl für kommerzielle Risiken, als auch in Bezug auf die Einhaltung von Nachhaltigkeitskriterien abbilden. Die eigenen Klimaziele an die eigenen Lieferanten weiter zu geben und sie auch auf deren Lieferanten auszuweiten, ist zur Einhaltung der eigenen Klimaziele erforderlich. Denn ein Unternehmen oder eine Behörde kann nur dann «net zero» sein, wenn es auch die eigenen Lieferanten sind. [13]

[13] Das heisst wenn es keine «Scope 3-Emmissionen» gibt und der CO2-Ausstoss auch entlang der Lieferkette «netto null» ist.

Zudem sei der Vollständigkeit halber erwähnt, dass es neben den gesetzlichen Verpflichtungen auch Zertifizierungen (Beschaffungskonferenz des Bundes BKB,2021)[14] eine verlässliche Grösse für die Angaben eines Unternehmens zur Nachhaltigkeit sein können, also auch diese als Vertragspflichten aufgenommen werden können, wobei auch wieder Branchenkenntnis und ein umfassendes Verständnis der existierenden Zertifizierungen[15] und deren Verlässlichkeit[16] erforderlich sind (siehe dazu auch Beitrag von Lara Biehl).

Die obigen Ausführen haben gezeigt, dass die gesetzlichen Vorgaben Möglichkeiten zur konkreten Formulierung vertraglicher Pflichten und auch Ausschreibungsunterlagen bieten. Dies schafft Rechtssicherheit für beide Seiten kann bei öffentlichen Beschaffungen das Beschwerderisiko mindern.

BIBLIOGRAPHIE

Beschaffungskonferenz des Bundes BKB. (2021, Juni). Nachhaltige Beschaffung: Empfehlungen für die Beschaffungsstellen des Bundes. In *Beschaffungskonferenz Des Bundes BKB*. www.bkb.admin.ch/dam/bkb/de/dokumente/Oeffentliches_Beschaffungswesen/Nachhaltige_Beschaffung/Empfehlung_Nachhaltige%20Beschaffung_BKB_de_Neu.pdf.download.pdf/Empfehlung_Nachhaltige%20Beschaffung_BKB_de_Neu.pdf

[14] Siehe hierzu Schweizer Eidgenossenschaft, Beschaffungskonferenz des Bundes BKB, Nachhaltige Beschaffung, Empfehlungen für die Beschaffungsstellen des Bundes, Juni 2021, Ziffer 2.1.3 «Eignungskriterien Formulieren Sie bei umweltrelevanten Beschaffungen auch umweltbezogene Eignungskriterien, wie z.B. eine spezielle technische Kompetenz oder ein spezielles ökologisches Know-how, das mit entsprechenden Zertifikaten bzw. Unterlagen nachgewiesen werden kann.»

[15] So zum Beispiel die Science Based Targets Initiative (SBTi), https://sbti.go-for-impact.ch/, nicht zu verwechseln sind Zertifizierungen, die wie die hier genannte, mittels derer die Klimaziele eines Unternehmens definiert und deren erfolgreiche Erreichung bestätigt werden, mit den CO_2-Zertifikaten, die zur Reduktion der eigenen CO_2 Bilanz eingekauft werden können.

[16] In Punkto Verlässlichkeit hat der Zertifikatsmarkt angesichts Kritik an Marktplätzen wie Verra und Southpole eingebüsst, und auch die ETH-Studie mit Auswertung von 2000 Klimaschutzprojekten kommt zu dem Schluss, dass nur 12% der Zertifikate tatsächlich zu Emissionsreduktion führen, weshalb es bei Angaben zur CO_2 Kompensation durch Lieferanten ratsam ist, auch eine Zertifizierung der eingekauften Klimazertifikate (z.B. der WWF Gold Standard) festzulegen. ETH-Studie abrufbar unter: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/620307/230706_WP_full_vf.pdf?sequence=9&isAllowed=y.

Eidgenössisches Finanzdepartement EFD. (2022, 30. März). *Verordnung über die Berichterstattung über Klimabelange, Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens*. www.newsd.admin.ch/newsd/message/attachments/73998.pdf

Meyer, N., Legler, V., Gailhofer, P., Schmitt, L., & Keller, T. (2023). *Auswirkungen der CSDDD auf Schweizer Unternehmen, Standortattraktivität und Wettbewerb*. Vertiefte Analyse zuhande des BJ und SECO. www.newsd.admin.ch/newsd/message/attachments/85536.pdf

Geiger, S., Veser, M., Amhof, K., & Caputo, M. P. (2022). EU-Offenlegungspflichten im Nachhaltigkeitsbereich und Schweizer Investitionen im Energiebereich. Studie im Auftrag des Bundesamt Für Energie BFE. https://pubdb.bfe.admin.ch/de/publication/download/10880

Europäische Kommission. (2021a, April 21). *Sustainable finance package*. https://ec.europa.eu/info/publications/210421-sustainable-finance-communication_en#taxonomy

Europäische Kommission. (2021b, April 21). *Questions and Answers: Taxonomy Climate Delegated Act and Amendments to Delegated Acts on fiduciary duties, investment and insurance advice*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_1805

Europäische Kommission (2021, Juli 6), *Strategie zur Finanzierung einer nachhaltigen Wirtschaft* https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021DC0390&from=EN

Europäische Kommission. (2023, July 31). The Commission adopts the European Sustainability Reporting Standards. European Commission. https://finance.ec.europa.eu/news/commission-adopts-european-sustainability-reporting-standards-2023-07-31_en

Europäischer Rat, Rat der Europäischen Union. (2022, November 28). *Rat gibt endgültiges grünes Licht für die Richtlinie über die Nachhaltigkeitsberichterstattung von Unternehmen* [Pressemitteilung]. https://www.consilium.europa.eu/de/press/press-releases/2022/11/28/council-gives-final-green-light-to-corporate-sustainability-reporting-directive/

Carbon Jargon. (2022, November 18). 100% Renewables. https://100percentrenewables.com.au/publications/carbon-jargon-your-guide-to-net-zero/

Pettingale, H., Kuenzer, J., Reilly, P., De Maupeou, S., & FTI Consulting. (2022, April 4). *EU Taxonomy and the Future of Reporting*. The Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2022/04/04/eu-taxonomy-and-the-future-of-reporting/

UNDP. (n.d.). *Sustainable development goals*. United Nations Development Programme. https://www.undp.org/sustainable-development-goals

Niederdrenk, L., & Kopp, M. (2021). Ein Meilenstein für mehr Nachhaltigkeitstransparenz: Was eine konsistente EU-Taxonomie erreichen kann. In *WWF Deutschland*. https://www.wwf.de/fileadmin/fm-wwf/Publikationen-PDF/Unternehmen/ein-meilenstein-f%C3%BCr-mehr-nachhaltigkeitstransparenz.pdf

DATENSICHERHEIT UND MELDEPFLICHTEN NACH DSG UND ISG IM BESCHAFFUNGSPROZESS

Nicole Beranek Zanon / Monika Abt

Nicole Beranek Zanon ist Partnerin bei HÄRTING Rechtsanwälte AG in Zug.

Monika Abt ist Substitutin bei HÄRTING Rechtsanwälte AG in Zug.

Abstract: In diesem Artikel wird die Bedeutung von Datenschutz und Informationssicherheit im öffentlichen Beschaffungsverfahren hervorgehoben, welche Pflichten sich aus dem revidierten Datenschutzgesetz (DSG) und der sich momentan in Revision befindenden Gesetzgebung rund um die Informationssicherheit (Informationssicherheitsgesetz ISG) ergeben. Dabei geht der Beitrag auf die Unterschiede dieser beiden Konzepte ein, beleuchtet die jeweiligen Ziele, Grundsätze und Mindestanforderungen und analysiert die Meldepflichten unter den beiden Gesetzen. Die Autorinnen betonten aber auch, dass die Einhaltung der rechtlichen Anforderungen die Notwendigkeit eines effektiven Incident-Managements und einer konsistenten Kommunikationsstrategie voraussetzen.

INHALTSVERZEICHNIS

I. Einleitung und thematische Einordnung 100
II. Datensicherheit gemäss Art. 8 DSG 101
III. Mindestanforderungen an die Datensicherheit gemäss DSV 103
1. Strafrechtlicher Aspekt der Verletzung der Datensicherheit 103
2. Grundsätze 103
1.1. Schutzbedarf der Personendaten 103
1.2. Risikobeurteilung 103
3. Ziele der Datensicherheit Art. 2 DSV 104
4. Technische und organisatorische Massnahmen nach Art. 3 DSV 104

5. Protokollierung nach Art. 4 DSV 105
6. Bearbeitungsreglement nach Art. 6 DSV 105
IV. Gewährleistung der Datensicherheit bei Bearbeitung durch Auftragsbearbeiter 106
1. Übertragung an einen Auftragsbearbeiter 106
2. Nicht jede Information ist dem Amtsgeheimnis unterstellt 106
3. Prüfungspflicht des Verantwortlichen 107
V. Datensicherheit gemäss ISG 107
1. Informationssicherheits-Management-System (ISMS) 107
2. Beurteilung des Schutzbedarfs 108
3. Risikomanagement 108
4. Klassifizierung von Informationen 108
5. Sicherheitsverfahren und Sicherheitsmassnahmen 109
6. Personeller und physischer Schutz 109
VI. Meldepflichten in a nutshell 110
1. Meldepflicht nach DSG 110
2. Meldepflicht nach ISG de lege ferenda 110
VII. Schlussbemerkungen 111

I. EINLEITUNG UND THEMATISCHE EINORDNUNG

Daten- und Informationssicherheit sind für die öffentliche Hand essenziell, wie der Fall «Xplain» mit seinen Auswirkungen auf die Bundesverwaltung zeigt (siehe z.B. NCSC, 2023).[1] Wie sehen die Pflichten im Rahmen von öffentlichen Beschaffungen aus im Hinblick auf die Daten- und Informationssicherheit und welche Meldepflichten müssen Bundesbehörden erfüllen, falls eine Datenschutz- oder Informationsschutzverletzung vorliegt? Dieser Beitrag beleuchtet die Frage der Datensicherheit nach dem revidierten

[1] Medienmitteilung des NCSC vom 8. Juni 2023, Hackerangriff auf die Firma Xplain: Auch die Bundesverwaltung ist betroffen, https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/medienmitteilungen/newslist.msg-id-95605.html.

Datenschutzgesetz (DSG) und gibt einen Ausblick auf das Informationssicherheitsgesetz (ISG), welches die Informationsschutzverordnung (ISchV) ablösen wird.

Das Datenschutzgesetz schützt die Persönlichkeit und Grundrechte von Personen, über welche Personendaten bearbeitet werden (Art. 1 DSG), während die Datensicherheit generell auf die bei Verantwortlichen oder Auftragsbearbeitern vorhandenen Personendaten abzielt. Datensicherheit ist massgebend, um Datenschutz zu gewährleisten (Husi-Stämpfli et al., 2023 S. 116). Individueller Datenschutz erfordert allgemeine technische Vorkehrungen zur Datensicherheit. Datenschutz und Datensicherheit beeinflussen sich gegenseitig, sind jedoch unterschiedliche Konzepte. Daraus ergibt sich auch die Abgrenzung der Pflicht zur Datensicherheit nach Art. 8 DSG, wonach sowohl der Verantwortliche als auch der Auftragsbearbeiter dazu verpflichtet ist, für seine Systeme eine geeignete Sicherheitsarchitektur vorzusehen (Botschaft rev. DSG 2017 6941, 7031).

Das Informationssicherheitsgesetz gewährleistet im Gegensatz zum Datenschutz – nicht aber zur Datensicherheit – die sichere Bearbeitung von Informationen unter Bundeshoheit (Art. 1 Abs. 1 revISG). Zudem muss der sichere Einsatz von Informatikmitteln des Bundes gewährleistet werden. Es umfasst Informationen als solche wie auch die Informatikmittel, dabei werden Informationen sowie Daten unter dem Begriff «Informationen» subsumiert (Botschaft rev. ISG 2017 2953, 3010).

Im öffentlichen Beschaffungsprozess müssen sowohl Datenschutz als auch Informationsschutz berücksichtigt werden, wobei der Informationsschutz den Datenschutz inkludieren sollte. Was dies beinhaltet, wir nachfolgend aufgezeigt.

II. DATENSICHERHEIT GEMÄSS ART. 8 DSG

Der Verantwortliche sowie der Auftragsbearbeiter müssen gemäss Art. 8 Abs. 1 DSG eine angemessene Datensicherheit durch technische und organisatorische Massnahmen gewährleisten.[2] Die Datensicherheit bezeichnet den Schutz von Daten hinsichtlich deren Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit (vgl. Art. 2 DSV).

[2] Siehe auch Beitrag von Dominika Blonski (Kapitel 3) in diesem Sammelband.

Elementar ist dabei, dass sich die Datensicherheit nach dem Risiko für die betroffene Person richtet und die Gewährleistung der Datensicherheit durch geeignete technische und organisatorische Massnahmen zu erfolgen hat, die es auch ermöglichen müssen, Verletzungen der Datensicherheit zu vermeiden (vgl. Art. 8 Abs. 2 DSG).

Darin wird einerseits der risikobasierte Ansatz betont, der fordert, dass je grösser das Risiko einer Verletzung der Datensicherheit ist, umso höher die Anforderungen an die zu treffenden Massnahmen sind (Husi-Stämpfli et al., 2023 S. 122). Weiter ist die Geeignetheit der Massnahmen erforderlich, d.h. eine Massnahme soll ermöglichen, eine Datensicherheitsverletzung zu vermeiden. Geeignete Massnahmen können beispielsweise sein: eine Pseudonymisierung von Personendaten, Massnahmen zur Wahrung der Vertraulichkeit und Verfügbarkeit des Systems oder dessen Dienste, die Entwicklung von Verfahren, mit denen regelmässig geprüft, analysiert und bewertet werden kann, ob die getroffenen Sicherheitsvorkehrungen wirksam sind (Botschaft rev. DSG 2017 6941, 7031).

Eine Datensicherheitsverletzung ist gemäss Art. 5 lit. h DSG eine Sicherheitsverletzung, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert oder Unbefugten zugänglich gemacht werden. Gemäss der Botschaft liegt auch eine Datensicherheitsverletzung vor, wenn «lediglich die Möglichkeit bestand, dass die Personendaten Unbefugten offengelegt oder zugänglich gemacht wurden, oder ob ein solcher Zugang tatsächlich stattgefunden hat» (Botschaft rev. DSG 2017 6941, 7022). Damit wäre jeder Verlust eines Laptops oder Mobiltelefons bereits eine Datenschutzverletzung. Dies aber nur, wenn wirklich auf Personendaten zugegriffen werden kann, was namentlich bei einer genügend verschlüsselten Harddisk nicht vorliegt.

Der Bundesrat muss gemäss Art. 8 Abs. 3 DSG Mindestanforderung an die Datensicherheit erlassen. Dazu wurden in Art. 1 bis 3 DSV Vorgaben definiert. Es sind jedoch nicht klare Vorgaben, sondern Kriterien, die zu berücksichtigen, und Leitlinien, wie konkrete Massnahmen auszugestalten sind (Bundesamt für Justiz [BJ], Erläuternder Bericht DSV, 2022, S. 10). Diese Kriterien stützen sich dabei auf ISO 27001/2:2022. Ob Art. 1 ff. DSV aber für die Bestimmtheit der Norm zu genügen vermag, wird sich in Zukunft ergeben.

III. MINDESTANFORDERUNGEN AN DIE DATENSICHERHEIT GEMÄSS DSV

1. STRAFRECHTLICHER ASPEKT DER VERLETZUNG DER DATENSICHERHEIT

Die Nichteinhaltung der Mindestanforderungen der Datensicherheit kann auf Antrag mit einer Busse von bis zu CHF 250'000 bestraft werden (Art. 61 lit. c DSG), vorausgesetzt die private Person (recte gemäss Botschaft rev. DSG 2017 6941, 7099: natürliche Personen) handelt vorsätzlich. Der Gesetzgeber hatte Unternehmen im Fokus, es aber unterlassen, natürliche Personen von Bundesorganen gemäss Art. 2 Abs. 2 lit. b DSG auszunehmen. Es ist derzeit unseres Erachtens offen, ob die Strafbestimmungen damit auch leitende Bundesangestellte treffen können.

2. GRUNDSÄTZE

1.1. Schutzbedarf der Personendaten

Zur Gewährleistung einer angemessenen Datensicherheit müssen gemäss Art. 1 Abs. 1 DSV sowohl der Verantwortliche und der Auftragsbearbeiter den Schutzbedarf der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen. Die Kriterien des Schutzbedarfs umfassen die Art der bearbeiteten Daten gemäss Art. 1 Abs. 2 lit. a DSV, wobei entscheidend ist, ob besonders schützenswerte Daten bearbeitet werden, sowie den Zweck, die Art und den Datenbearbeitungsumfang gemäss Art. 1 Abs. 2 lit. b DSV. Der Bearbeitungszweck richtet sich insbesondere auf die Prüfung, ob dieser ein erhöhtes Risiko für die Persönlichkeitsrechte und die Grundrechte mit sich bringt; bei der Art der Bearbeitung ist von Interesse, wie die Daten bearbeitet werden. Die Umstände der Bearbeitung erfassen Aspekte, welche im Einzelfall Auswirkungen auf andere Kriterien haben und dienen insofern als Auffangbecken (BJ, Erläuternder Bericht DSV, 2022, S. 19; m.w.H. Husi-Stämpfli et al., 2023 S. 123 f.).

1.2. Risikobeurteilung

In Art. 1 Abs. 3 DSV werden wie für die vorangehende Beurteilung des Schutzbedarfs die Kriterien zur Beurteilung des Risikos einer Persönlichkeits- oder Grundrechtsver-

letzung aufgeführt. Die Beurteilung erfolgt nach fachlichen Kriterien (Beariswyl, 2023, S. 125). Im Unterschied zur Schutzbedarfsbeurteilung erfolgt die Risikobeurteilung gemäss einem Kaskadensystem (lit. a bis d). Das Ergebnis der Beurteilung ist massgebend für die weitere Risikobeurteilung (BJ, Erläuternder Bericht DSV, 2022, S. 19 f.; Husi-Stämpfli et al., 2023 S. 124 ff.).

3. ZIELE DER DATENSICHERHEIT ART. 2 DSV

Art. 2 DSV ergänzt Art. 1 DSG hinsichtlich des Gesetzeszweckes und konkretisiert die Ziele zur Gewährleistung der angemessenen Datensicherheit. Vertraulichkeit nach Art. 2 lit. a DSV bedeutet, dass Daten nur Berechtigten zugänglich sind und umfasst Authentifizierung sowie Methoden und Systeme zur Verwaltung und Einschränkung des Zugriffs (BJ, Erläuternder Bericht DSV, 2022, S. 22). Verfügbarkeit wird nach Art. 2 lit. b DSV gewährleistet, indem die Daten jederzeit eingesehen werden können. Das Ziel der Integrität gemäss Art. 2 lit. c DSV wird gewährleistet, wenn die Daten nicht unberechtigt oder unbeabsichtigt verändert werden und umfasst Authentizität, Zurechenbarkeit sowie die Nichtabstreitbarkeit. Abschliessend muss die Datenbearbeitung nachvollziehbar sein, wie es in Art. 2 lit. d DSV dargestellt wird, um Missbrauch oder unbefugte Zugriffe zu identifizieren, was für das Verfahren relevant ist und Kontrolle sowie Überwachung erleichtert (BJ, Erläuternder Bericht DSV, 2022, S. 22 f.).

4. TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN NACH ART. 3 DSV

Technische Massnahmen bezeichnen alle Vorkehrungen, die sicherstellen, dass die Datenbearbeitung rechtmässig erfolgt (Baeriswyl et al., 2023, S. 116). Darunter fallen Datenverschlüsselungen, Einrichten von Back-Ups oder Protokollierungen (Baeriswyl et al., 2023, S. 128). Organisatorische Massnahmen hingegen sind Vorgaben, welche die Prozesse beim Verantwortlichen und das Verhalten dessen Mitarbeitenden betreffen (Baeriswyl et al., 2023, S. 116).

Art. 3 DSV sieht vor, dass organisatorische und technische Massnahmen im Einzelfall ergriffen werden müssen, um die Ziele von Artikel 2 zu erreichen. Art. 3 DSV nennt dabei jeweils Massnahmen für die einzelnen Ziele. Beispielsweise wird die

Vertraulichkeit (Art. 2 lit. a DSV) durch risikoreduzierende organisatorische und technische Massnahmen aus Art. 3 Abs. 1 DSV gewährleistet (Baeriswyl et al., 2023, S. 125). Darunter fallen die Zugriffskontrolle (Berechtigte dürfen nur auf diejenigen Personendaten zugreifen, die sie zur Aufgabenerfüllung benötigen), die Zugangskontrolle (so dass nur Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden) sowie die Benutzerkontrolle (Unbefugte können automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen).

5. PROTOKOLLIERUNG NACH ART. 4 DSV

Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt und können die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen gemäss Art. 4 Abs. 1 DSV der *private* Verantwortliche und sein *privater* Auftragsbearbeiter gewisse Bearbeitungsvorgänge protokollieren. Gemäss Absatz 2 protokollieren das verantwortliche Bundesorgan und sein Auftragsbearbeiter bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten. Dies sind die gleichen Bearbeitungsvorgänge, die auch der private Verantwortliche protokollieren muss, allerdings muss dies bei Bundesorganen in grösserer Anzahl Fälle (bei jeder automatisierten Bearbeitung) erfolgen.

6. BEARBEITUNGSREGLEMENT NACH ART. 6 DSV

Art. 6 DSV verpflichtet das verantwortliche Bundesorgan und sein Auftragsbearbeiter beim Vorliegen gewisser Voraussetzungen ein Bearbeitungsreglement für automatisierte Bearbeitungen zu erstellen. Eine Pflicht besteht gemäss Art. 6 Abs. 1 lit. a–f DSV in verschiedenen Szenarien, wie beispielsweise, wenn besonders schützenswerte Personendaten bearbeitet werden oder ein Grundrechtseingriff besteht. Inhaltlich muss das Reglement, gleichermassen wie das Reglement für private Verantwortliche, Angaben zu interner Organisation, Datenbearbeitungs- und Kontrollverfahren und Massnahmen zur Gewährleistung der Datensicherheit enthalten (Beariswyl, 2023, S. 136).

IV. GEWÄHRLEISTUNG DER DATENSICHERHEIT BEI BEARBEITUNG DURCH AUFTRAGSBEARBEITER

1. ÜBERTRAGUNG AN EINEN AUFTRAGSBEARBEITER

Die Übertragung der Bearbeitung von Personendaten an einen Auftragsbearbeiter ist zulässig, wenn Daten so bearbeitet werden, wie der Verantwortliche es selbst tun dürfte und keine Geheimhaltungspflichten eine Übertragung verbieten (Art. 9 DSG).[3] Es gibt nur sehr wenige Gesetze, die explizit die Übertragung an einen Dritten verbieten[4]. Vielmehr ist damit gemeint, dass Geheimhaltungspflichten einer Übertragung entgegenstehen, wenn die Auftragsbearbeiter nicht als Hilfspersonen im Sinne von Art. 320 Ziff. 1 Abs. 1 bzw. 321 Ziff. 1 Abs. 1 StGB im Rahmen des Amts- oder Berufsgeheimnisses zu qualifizieren sind (Meier, 2011, Rz. 1227; Schwarzenegger et al., 2019, S. 23; andere aber unseres Erachtens überholte Ansicht Wohlers, 2016, S. 144 ff.).

Hingegen ist unseres Erachtens jedoch zu berücksichtigen, ob das strafrechtlich verankerte Berufs- oder Amtsgeheimnis nach Art. 320/321 StGB auch bei einer Übertragung ins Ausland gewahrt werden kann – sprich die Frage ist zu stellen, ob eine fremde Rechtsordnung das Schweizerische Amts- oder Berufsgeheimnis schützt. Dies ist nicht in allen Ländern der Fall, weshalb eine Übertragung an eine Hilfsperson im Ausland mit Zurückhaltung und erst nach einer entsprechenden Beurteilung der Rechtslage im Ausland zu erfolgen hat. Ausserdem sind auch in diesen Fällen allfällige weitere Garantien im Sinne von Art. 16 Abs. 2 DSG zu berücksichtigen.

2. NICHT JEDE INFORMATION IST DEM AMTSGEHEIMNIS UNTERSTELLT

Informationen, über die nach dem Öffentlichkeitsgesetz Auskunft zu erteilen ist, unterstehen per se nicht dem Amtsgeheimnis. Eine Vielzahl von Informationen kann folglich rechtskonform durch Dritte bearbeitet werden und die Prüfung der Wahrung

---

[3] Siehe auch Beitrag von Dominika Blonski in diesem Sammelband.

[4] Als Beispiel: Art. 5 Abs. 3 des Standeskommissionsbeschlusses über die Informatiknutzung des Kantons Appenzell Innerroden, (GS 172.315), der eine Cloud-Speicherung explizit verbietet.

des Amtsgeheimnisses bei der Übertragung an einen Auftragsbearbeiter im Ausland erübrigt sich.

3. PRÜFUNGSPFLICHT DES VERANTWORTLICHEN

Auch wenn gemäss Art. 8 DSG der Verantwortliche und der Auftragsbearbeiter für die Datensicherheit verantwortlich sind, so muss sich insbesondere der Verantwortliche vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten (Art. 9 Abs. 2 DSG). Dies setzt voraus, dass der Verantwortliche über umfassende Auditrechte verfügt. In der Praxis ist dies oft nicht der Fall oder gar nicht möglich. Hier hat es der Gesetzgeber unseres Erachtens verpasst anzumerken, dass einer solchen Kontrollpflicht genüge getan wäre, wenn entsprechende aktuelle Prüfzertifikate nach internationalen Standards wie z.B. ISO 27001/2:2022 oder SOC II beim Auftragsbearbeiter vorliegen.

V. DATENSICHERHEIT GEMÄSS ISG

Das Informationssicherheitsgesetz betrifft grundsätzlich nur Bundesbehörden und -organisationen, wie die Bundesversammlung, den Bundesrat oder die Schweizerische Nationalbank (vgl. Art. 2 ISG). Bei Zusammenarbeit mit Dritten muss gemäss Art. 9 ISG sichergestellt werden, dass Anforderungen und Massnahmen des Gesetzes in den entsprechenden Vereinbarungen und Verträgen festgehalten werden.

1. INFORMATIONSSICHERHEITS-MANAGEMENT-SYSTEM (ISMS)

Das Gesetz verlangt zunächst die Implementierung eines Informationssicherheits-Management-Systems (ISMS). Dessen Ziel ist es, ein angemessenes Schutzniveau für Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen (vgl. Art. 6 Abs. 2 ISG) im festgelegten Geltungsbereich zu erreichen. Die Pflichten umfassen dabei die Bewertung des Schutzbedarfs der bearbeiteten Informationen und Ergreifung angemessener Schutzmassnahmen, um unbefugten Zugriff, Verlust, Störungen und Missbrauch zu verhindern sowie die Klassifizierung von Informationen in enger Verbindung mit der Kontrolle und Minimierung von Risiken, sowohl intern als auch bei der Zusammenarbeit mit Dritten.

2. BEURTEILUNG DES SCHUTZBEDARFS

Der Schutzbedarf der Informationen wird hinsichtlich der potenziellen Beeinträchtigung der Interessen nach Art. 1 Abs. 2 ISG erhoben und in Bezug auf die detaillierten Ziele von Absatz 2 (Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit) definiert.

Die verpflichteten Behörden und Organisationen müssen somit den Schutzbedarf beurteilen und bestimmen, wie und in welcher Hinsicht die Informationen geschützt werden müssen. Der Schutz der Vertraulichkeit ist beispielsweise erforderlich, wenn sie aus einem rechtlichen Grund gewährleistet werden muss. Bestimmte Informationen können höhere Anforderungen an den Schutz ihrer Integrität oder Verfügbarkeit haben, ohne dass diese besonderen Anforderungen gesetzlich festgelegt sind, etwa dann, wenn die entsprechenden Informationen für die Aufgabenerfüllung einer Behörde unbedingt richtig oder verfügbar sein müssen (Botschaft ISG 2017 2953, 3017).

3. RISIKOMANAGEMENT

Risiken für die Informationssicherheit werden laufend beurteilt. Behörden und Organisationen müssen Risiken in ihrem Zuständigkeitsbereich und bei der Zusammenarbeit mit Dritten regulieren. Massnahmen zur Risikovermeidung und -reduzierung sollten geeignet sein, wobei Restrisiken deutlich identifiziert und akzeptiert werden müssen. Die Entscheidungsträger sind für ihre diesbezügliche Güterabwägung in dokumentierter Form auf diese Risiken und potenziellen Auswirkungen hinzuweisen, da ansonsten eine Verletzung der Datensicherheit vorliegt (Botschaft ISG 2017 2953, 3018 f.).

4. KLASSIFIZIERUNG VON INFORMATIONEN

Nach Art. 11 ISG müssen die verpflichteten Behörden und Organisationen sicherstellen, dass als intern, vertraulich oder geheim eingestufte Informationen klassifiziert werden (vgl. auch Art. 13 ISG). Eine Klassifizierung ist zwingend, sofern die entsprechenden Kriterien erfüllt sind. Gemäss Botschaft ISG 2017 muss die Klassifizierung angesichts des Öffentlichkeitsprinzips und des mit der Klassifizierung verbundenen Aufwands jedoch die Ausnahme darstellen. Der Schutzbedarf von Informationen nimmt mit der Zeit oftmals ab oder erübrigt sich nach einem bestimmten Ereignis (z. B. Veröffentlichung eines Berichts oder Abschluss einer bestimmten Massnahme). Die Klassifizierung

derartiger (beispielsweise nicht mehr aktueller) Informationen rechtfertigt sich dann nicht mehr. Sie würde bloss unnötigen Aufwand verursachen (3020).

5. SICHERHEITSVERFAHREN UND SICHERHEITSMASSNAHMEN

Das Sicherheitsverfahren nach Art. 16 ISG umfasst die Beurteilung des Schutzbedarfs der Informationen vor dem Einsatz von Informatikmitteln, die Umsetzung von Sicherheitsmassnahmen und deren Überprüfung, die Zuständigkeit für die Sicherheitsfreigabe von Informatikmitteln und das Vorgehen bei der Veränderung der Risiken. Für die Durchführung des Sicherheitsverfahrens ist die verpflichtete Behörde oder Organisation zuständig, die den Einsatz der Informatikmittel beschliesst.

Nach Art. 17 ISG können die Informatikmittel in Grundschutz, hoher Schutz und sehr hoher Schutz eingestuft werden. Die Sicherheitsstufe des Grundschutzes gilt für alle Informatikmittel, wenn diese nicht höher eingestuft werden müssen. Zur Sicherheitsstufe des hohen Schutzes gehören Informatikmittel, bei denen eine Verletzung der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit der Informationen, die damit bearbeitet werden, die Interessen nach Art. 1 Abs. 2 ISG erheblich beeinträchtigen können. Der hohe Schutz gilt ebenfalls für Informatikmittel, wenn ein Missbrauch oder eine Störung des Informatikmittels die Interessen nach Art. 1 Abs. 2 ISG erheblich beeinträchtigen können. Die Sicherheitsstufe des sehr hohen Schutzes gilt für Informatikmittel, wenn die oben genannten Interessen schwerwiegend beeinträchtigt werden können.

6. PERSONELLER UND PHYSISCHER SCHUTZ

Behörden und Organisationen müssen gemäss Art. 20 ISG sicherstellen, dass Personen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes haben, sorgfältig ausgewählt und risikogerecht identifiziert werden. Sie müssen über die Anforderungen des Informationsschutzgesetzes informiert und stufengerecht ausgebildet werden. Ausserdem müssen Risiken durch physische Bedrohungen wie menschliche Handlungen und Elementarschäden reduziert werden und Sicherheitszonen können Räumlichkeiten und Bereichen zugewiesen werden, die mit Kontrollen verbunden sind.

VI. MELDEPFLICHTEN IN A NUTSHELL

1. MELDEPFLICHT NACH DSG

Mit der Revision des Datenschutzgesetzes fand auch eine Pflicht zur Meldung von Verletzungen der Datensicherheit Eingang in das Gesetz. Bei der Verletzung der Datensicherheit handelt es sich gemäss Legaldefinition in Art. 5 lit. h DSG um eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Beispiele sind der Verlust oder Diebstahl von Datenträgern, Datenverluste durch Stromausfälle, IT-Ausfälle, Brände oder Naturkatastrophen.

Die Meldung an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten muss so rasch wie möglich erfolgen, ohne Aufschub nach Kenntniserlangung (Botschaft rev. DSG 2017, 7064). Wobei Bundesorgane einen Vorfall den Datenschutzberatenden melden müssen (Baeriswyl et al., 2023, S. 288 f.). Nicht jede Verletzung löst hingegen eine Meldepflicht aus; nur solche mit voraussichtlich hohem Risiko für die Persönlichkeit oder Grundrechte der Betroffenen sind meldepflichtig (vgl. Art. 24 Abs. 1 DSG).

Bezüglich des Inhalts der Meldung stellt Art. 24 Abs. 2 DSG gewisse Mindestanforderungen auf. Art. 15 DSV konkretisiert den Inhalt weiter: Art der Verletzung (Vernichtung, Löschung, Verlust, Veränderung oder Bekanntgabe von Daten), Zeitpunkt und Dauer, Kategorien und ungefähre Anzahl der Personendaten sowie der Personen, Folgen einschliesslich der Risiken, für die betroffenen Personen, die getroffenen oder vorgesehenen Massnahmen sowie den Namen und die Kontaktdaten einer Ansprechperson. Zu prüfen bleibt im jeweiligen Einzelfall, ob auch die betroffene Person zu informieren ist, wenn es entweder zu ihrem Schutz erforderlich ist oder vom EDÖB verlangt wird (vgl. Art. 24 Abs. 3 DSG).

2. MELDEPFLICHT NACH ISG DE LEGE FERENDA

Gemäss dem provisorischen Gesetzestext betreffend die Änderung des Informationssicherheitsgesetzes (Botschaft rev. ISG 2023 85) sind die vom Geltungsbereich erfassten Behörden und Organisationen verpflichtet dafür zu sorgen, dass dem Nationalen

Zentrum für Cybersicherheit (NCSC) Cyberangriffe auf ihre Informatikmittel gemeldet werden. Bei einem Cyberangriff handelt es sich um einen Cybervorfall, der absichtlich ausgelöst wurde (Art. 5 lit. e ISG). Bei einem Cybervorfall handelt es sich wiederum um ein Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist (Art. 5 lit. d ISG).

Die Meldepflicht gilt nur für Cyberangriffe mit erheblichem Schadenspotenzial, während menschliches Fehlverhalten und Schwachstellen in Informatikmitteln davon ausgenommen sind (Botschaft rev. ISG 2023 85, S. 16).

Erhält das NCSC Kenntnis von einer Schwachstelle, informiert es umgehend die Hersteller der betroffenen Soft- oder Hardware und setzt ihnen eine angemessene Frist zur Behebung der Schwachstelle. Die nicht fristgerechte Behebung oder Missachtung kann gemäss Art. 73b Abs. 3 ISG gar beschaffungsrechtlich sanktioniert werden.

Grundsätzlich geht das Öffentlichkeitsgesetz dem Informationsschutzgesetz gemäss Art. 4 Abs 1 ISG vor. Dies bedeutet, dass alle Personen Zugang zu amtlichen Dokumenten und Informationen des Bundes haben, sofern keine Ausnahmen oder Interessensabwägungen vorliegen. Durch die Revision des Informationsschutzgesetzes wird mit dem neuen Art. 4 Abs. 1bis ISG von dieser Regelung eine Ausnahme gemacht. Informationen von Dritten, von denen das NCSC durch die Entgegennahme und Analyse von Meldungen zu Cybervorfällen Kenntnis erhält, dürfen nicht nach dem Öffentlichkeitsgesetz zugänglich gemacht werden. Aber was wäre eine Ausnahme ohne Gegenausnahme: nicht als Dritte gelten Behörden, Organisationen und Personen nach Art. 2 Abs. 1 BGÖ. Enthält also eine Meldung Informationen namentlich über die Bundesverwaltung oder Parlamentsdienste, kann über das Öffentlichkeitsgesetz um Zugang zu diesen Informationen ersucht werden.

VII. SCHLUSSBEMERKUNGEN

Datenschutz und Informationssicherheit dürfen zwar nicht als Synonyme verwendet werden, spielen aber im Grundsatz zusammen und überschneiden sich teilweise. Die Herausforderung in der Zukunft wird sein, die verschiedenen Meldepflichten mit ziel-

gerichteter Kommunikation im Sinne von «One Voice» zu erfüllen. Dies bedingt ein Incident- und Krisenmanagement, das bereits im Vorfeld definiert wurde und die internen und externen Rollen und Ressourcen sowie die Kommunikation zumindest betreffend Umfang, Inhalt und Adressaten festlegt. Die einem Vorfall («Incident») nachgelagerten Meldepflichten sind deshalb auch Bestandteil der Preparedness und der Betriebskontinuität.

Literaturverzeichnis:

Baeriswyl, B., Pärli, K. & Blonski, D. (2023). *Stämpflis Handkommentar zum Datenschutzgesetz*. Stämpfli.

Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941. (zit. Botschaft rev. DSG 2017 6941)

Botschaft vom 22. Februar 2017 zum Informationssicherheitsgesetz, BBl 2017 2953. (*zit*. Botschaft rev. ISG 2017 2953, 3010)

Bundesamt für Justiz BJ. (2022). Erläuternder Bericht vom 31. August 2022 zur Verordnung über den Datenschutz (Datenschutzverordnung, DSV). https://www.newsd.admin.ch/newsd/message/attachments/75623.pdf

Husi-Stämpfli, S., Morand, A. & Sury, U. (2023). *Datenschutzrecht*. Schulthess.

Meier, P. (2011). *Protection des données: fondements, principes généraux et droit privé*. Stämpfli.

Schwarzenegger, C., Thouvenin, F. & Stiller, B. (2019). *Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte = Utilisation des services de cloud par les avocates et avocats*. Schriften aus dem ITSL, 4. https://digital.sav-fsa.ch/documents/1060627/1169162/Gutachten_Thouvenin_Schwarzenegger_Schiller.pdf/of612227-5274-943b-a82f-c1d6d99acefo?t=1614770740068

Wohlers, W. (2016). *Outsourcing durch Berufsgeheimnisträger, Patienten- und Mandantengeheimnisse als Schranke bei der Auslagerung von Datenverarbeitungen*. digma.

KI - ICH BIN JUNG UND MUSS NOCH LERNEN?

Rechtliche und ethische Themen der Beschaffung und des Einsatzes von Künstlicher Intelligenz (KI) im öffentlichen Sektor

Sven Kohlmeier

Sven Kohlmeier ist Rechtsanwalt und Fachanwalt für IT-Recht (D) und Co-Head des «Digital Education Institute».

Abstract: Ziel des Beitrages ist es, eine rechtliche Einordnung für die (öffentliche) Beschaffung und den Einsatz von KI-Systemen zu geben. KI-System können derzeit als unterstützende Hilfssysteme rechtmässig eingesetzt werden, bei fortschreitender Automatisierung stellt sich jedoch die Frage nach einer spezifischen Rechtsgrundlage. Der Beitrag beleuchtet verschiedene rechtliche Aspekte im Zusammenhang mit dem Einsatz von KI-Systemen. So wird das Spannungsverhältnis zu den datenschutzrechtlichen Grundsätzen, aber auch urheberrechtlichen Fragen und einer bundesgerichtlichen Entscheidung zu Substitution von Aufgaben aufgezeigt. Da sich der Beschaffungsvorgang aus dem beabsichtigten Einsatz des KI-Systems ergibt, wird ein Vorschlag unterbreitet, welche Anforderungen an die Ausschreibung von KI-Systemen bestehen sollten.

1. Einführung 114
2. Beschaffungsrecht im Allgemeinen 115
   - 2.1 Grundlagen staatlichen Handelns: Darf die öffentliche Verwaltung überhaupt KI beschaffen? 115
   - 2.2 Rechtsgrundlagen öffentlicher Beschaffungen 115
3. KI-Beschaffung für eine Anwendung durch den Staat im Spezifischen 116
   - 3.1 Datenschutzrechtliche Überlegungen im Rahmen der Beschaffung von KI-Anwendungen für (unterstützende) Verwaltungsarbeit 116
   - 3.2 Wahrung der Datenschutzrechte bei der Nutzung von KI 121
   - 3.3 Datengerüst der jeweiligen KI-Anwendung 123

3.4 Verwaltungsarbeit durch KI: Unterstützend oder beschliessend? 125
3.5 Urheberrechte bei der Nutzung von KI 128
3.6 KI-Anwendungen als Substituten in der Vertragserfüllung..... 129
4. Was gilt es zu beachten bei der Beschaffung von KI-Anwendungen für die öffentliche Hand?..... 130
Literaturverzeichnis 132

1. EINFÜHRUNG

Ganz neu ist der Einsatz von KI-Tools in der Verwaltung nicht. So nutzt etwas das Handelsregister St. Gallen einen Chatbot auf seiner Webseite und auch das Migrationsamt des Kanton Zürich setzt auf einen digitalen Chatbot. Beides sind mögliche Einsatzgebiete von KI-Tools. Durch die öffentliche Berichterstattung über ChatGPT (von OpenAI) und sein Pendent Bard (von Google) scheinen die Möglichkeiten der Vereinfachung in vielen Bereichen der Verwaltung aber ein neues Level erreicht zu haben: Die Auswertung und Analyse grosser Datenmengen, die Auswertung von Gerichtsentscheiden, die KI-automatisierte Prüfung von Anträgen, Entscheiden und Stellungnahmen und die Anfertigung von Entscheiden. Auch im Cyber-Sicherheitsbereich sowie in der strafrechtlichen Ermittlungstätigkeit können KI-Tools eine wertvolle Unterstützung sein. So kann die Sichtung von strafrechtlich inkriminiertem Material im Internet von einem KI-Tool übernommen werden, anstatt sich Mitarbeitende der Untersuchungsbehörden dies anschauen müssen.

Die Vorteile von KI-Anwendungen liegen klar auf der Hand: Bessere Entscheidungsfindung, Zeit- und Kostenersparnis sowie eine erhöhte Effizienz der Verwaltungstätigkeit. Auf der anderen Seite stellen KI-Anwendungen auch eine Herausforderung für die Verwaltung dar: Bei vertraulichen oder personenbezogenen Daten können Risiken bei dem Einsatz von KI bestehen und auch das Vertrauen in staatliche Institutionen könnte leiden, wenn anstelle einer Amtsperson ein emotionsloses KI-Tool entscheidet.

Ein transparentes, aber flexibles Regelwerk, welches die Interessen der Bevölkerung schützt, aber keine unüberwindbare Hürde für Innovation darstellt, ist also wünschenswert. Wie dieses Regelwerk aktuell aussieht, bzw. insbesondere nach welchen recht-

lichen Grundlagen sich der öffentliche Sektor bei der Beschaffung von KI zu richten hat, wird im Folgenden aufgezeigt.

2. BESCHAFFUNGSRECHT IM ALLGEMEINEN

2.1 GRUNDLAGEN STAATLICHEN HANDELNS: DARF DIE ÖFFENTLICHE VERWALTUNG ÜBERHAUPT KI BESCHAFFEN?

Sämtliches staatliches Verwaltungshandeln muss auf einer hinreichenden gesetzlichen Grundlage beruhen (Art. 5 Abs. 1 BV). Dies gilt auch für die Bedarfsverwaltung (auch administrative Hilfstätigkeit genannt), also jedes Tätigwerden des Gemeinwesens, durch welches die zur Erfüllung der öffentlichen Aufgaben notwendigen Sachgüter und Leistungen beschafft werden. Dies erfolgt in der Regel durch den Abschluss von privatrechtlichen Verträgen. Die Bedarfsverwaltung dient mittelbar der Erledigung von Verwaltungsaufgaben und entfaltet grundsätzlich keine Wirkung nach aussen. Die gesetzlichen Grundlagen ergeben sich aus den Normen, welche die eigentlichen Verwaltungsaufgaben regeln, zu deren Erfüllung die Bedarfsverwaltung dient (Poledna et al., 2017).

Soll im Rahmen der Bedarfsverwaltung ein KI-System beschaffen werden, so wird die Frage, ob die Verwaltung überhaupt KI-Anwendungen beschaffen darf, durch die Sachgesetze, welche die Verwaltungsaufgabe an sich regeln, beantwortet (Tschentscher et al., 2019).

Grundsätzlich darf die Verwaltung auch KI-Anwendungen beschaffen und einsetzen, soweit die beschaffungsrechtlichen Vorgaben (Ziff. 2.2.) erfüllt sind und die weiteren hier dargestellten spezifischen Voraussetzungen erfüllt sind (Ziff. 3).

2.2 RECHTSGRUNDLAGEN ÖFFENTLICHER BESCHAFFUNGEN

Das Verfahren der Beschaffung von Sachmitteln, beispielsweise für den Erwerb von IT-Software, ist durch das öffentliche Beschaffungsrecht geregelt (Waldmann et al., 2019). Bei der Beschaffung von KI-Anwendungen gelten dieselben nationalen wie auch kantonalen beschaffungsrechtlichen Vorgaben, wie dies auch bei der Beschaffung jeder anderen ICT-Leistung gilt.

In Abhängigkeit der konkreten Arbeits- und Funktionsweise kann die Beschaffung von KI-Anwendungen sowohl eine beschaffungsrechtliche Lieferung, Dienstleistung oder aber eine Mischung aus Lieferung und Dienstleistung darstellen. Dabei sind die entsprechenden Schwellenwerte zu beachten, insbesondere hinsichtlich der Berechnung bei Dienstleistungsverträgen mit bestimmter oder unbestimmter Laufzeit.

Das öffentliche Beschaffungsrecht enthält Vorschriften, wie der Staat solche Leistungen am Markt einkaufen darf. Das Vergabeverfahren soll gemäss Art. 2 BöB/IVöB die transparente, nachvollziehbare und willkürfreie, objektiv begründbare Vergabe des öffentlichen Auftrags an einen (privaten) Leistungserbringer unter mehreren interessierten Anbietern gewährleisten. Dass dies mit einigen Herausforderungen bei der Beschaffung von KI-Systemen verbunden ist, wird nachfolgend dargestellt.

3. KI-BESCHAFFUNG FÜR EINE ANWENDUNG DURCH DEN STAAT IM SPEZIFISCHEN

Im engen Sinn wird die Beschaffung von KI-Anwendungen durch den Staat durch das öffentliche Beschaffungsrecht geregelt. Doch auch weitere Rechtsgebiete haben einen Einfluss auf die Beschaffung und die Anwendung von KI durch die öffentliche Hand. Der Staat ist in der Auslagerung von Tätigkeiten (bzw. im Beizug von unterstützenden Mitteln) weniger frei als ein privatwirtschaftlich handelndes Unternehmen (Sury, 2021). So ist der Staat insbesondere an die Grundrechte gebunden, und muss sein Handeln auf gesetzliche Grundlagen stützen können. Dies spielt auch dann eine Rolle, wenn der Staat im Rahmen seiner Verwaltungstätigkeit Daten im weitesten Sinne bearbeitet.

3.1 DATENSCHUTZRECHTLICHE ÜBERLEGUNGEN IM RAHMEN DER BESCHAFFUNG VON KI-ANWENDUNGEN FÜR (UNTERSTÜTZENDE) VERWALTUNGSARBEIT

Für die Bearbeitung von Personendaten durch Bundesorgane gilt das eidgenössische Datenschutzgesetz (DSG). Für kantonale sowie kommunale Behörden kommen die jeweiligen kantonalen Datenschutzgesetze zur Anwendung. Für den Kanton Zürich ist dies das Gesetz über die Information und den Datenschutz (IDG) (Volz, 2022).

Die Grundsätze der Datenbearbeitung – die Gesetzmässigkeit, die Zweckbindung und die Verhältnismässigkeit – gelten dann, wenn durch den Staat, beispielsweise auch durch Nutzung von künstlich intelligenten Systemen, Personendaten bearbeitet werden. Hinsichtlich der Gesetzmässigkeit gelten auch im Hinblick auf den Einsatz von KI-Anwendungen die üblichen Gültigkeitsvoraussetzungen der genügenden Normstufe und Normdichte. Sofern es sich beim Einsatz von KI um eine blosse Unterstützung der eigentlichen Verwaltungsleistung handelt, stützt sich diese i.d.R. auf die gesetzliche Grundlage der Haupttätigkeit. Teilweise wird die Auffassung vertreten, dass eine separate gesetzliche Befugnis für den Einsatz von KI-Systemen zur Bearbeitung von Personendaten dann erforderlich ist, wenn der Einsatz von KI als zusätzlicher Eingriff in die Rechte der Betroffenen, bzw. als eine Bearbeitung von besonderen Personendaten zu werten ist (Glass, 2023).

Vor dem Hintergrund der demokratischen Legitimation öffentlichen Handels, und insbesondere bei Verfahren, welche in einem Entscheid münden, stellt sich die Frage, ob auch für den unterstützenden Einsatz von KI eine zumindest materiell-gesetzliche Grundlage benötigt wird, wenn die Unterstützung der KI so weit geht, dass sie einen schriftlichen Entwurf vorbereitet, der vom Menschen lediglich geprüft werden muss. Die Hürde, Abänderungen vorzunehmen, ist wohl grösser bei Vorliegen von bereits verschriftlichten Outputs und der Mangel an Zeit und personellen Ressourcen macht es wahrscheinlich, dass eine gleichwertige intensive Prüfung wie bei einem Verzicht auf die Unterstützung von KI unterbleiben würde (Reiter, 2022).

Wann der Einsatz von KI faktisch zu einem Entscheid ohne menschliche Einwirkung führt und wie viel menschliches Einwirken benötigt ist um eine Entscheidung als «vom Mensch getroffen» zu qualifizieren, hat nicht nur Auswirkung auf das Verwaltungsverfahren, sondern auch auf die Gesetzmässigkeit der Verwaltung.

Sofern KI-Systeme nur als ein weiteres Hilfsmittel wie z.B. das Internet, Laptop, Druckerpapier zur Erfüllung der gesetzlichen Aufgabe angesehen werden, bedarf es keiner spezifischen Rechtsgrundlage. Werden KI-Systeme aber als selbständig automatisierte Entscheidungs- und Datenverarbeitungssysteme tätig und der menschliche Einsatz beschränkt sich nur noch darauf, das System zu starten oder zu warten, bedarf es nach meiner Auffassung einer ausdrücklichen fachspezifischen Rechtsgrundlage. Denn bis-

her dürfte der Gesetzgeber eher von einer menschlich intendierten Datenverarbeitung ausgegangen sein und nicht von einer weitgehend oder vollständig autonomen Datenverarbeitung.

Für das Datenschutzgesetz hat sich der Gesetzgeber die Präzisierung in der Datenschutzverordnung vorbehalten, wann von einer automatisierten Bearbeitung im Sinne von Art. 21 Abs. 1 DSG auszugehen ist. «Der Bundesrat wird in der Verordnung falls erforderlich präzisieren, wann eine Entscheidung vorliegt, die ausschliesslich auf einer automatisierten Bearbeitung beruht. Dies ist der Fall, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat. [...] Eine automatisierte Einzelentscheidung kann selbst dann vorliegen, wenn sie anschliessend durch eine natürliche Person mitgeteilt wird, falls diese die automatisch gefällte Entscheidung nicht mehr beeinflussen kann. Massgebend ist somit, inwieweit eine natürliche Person eine inhaltliche Prüfung vornehmen und darauf aufbauend die endgültige Entscheidung fällen kann.» (Botschaft, 7056 f.). Eine Auslegungsregelung findet sich in der DSV indes nicht, jedoch hat der EDÖB in einer Pressemeldung vom 9. November 2023 klargestellt, dass das geltende Datenschutzgesetz für KI-Anwendungen direkt anwendbar sei und das gesetzliche Recht auf Transparenz eng verbunden mit dem Anspruch der betroffenen Person sei, dass automatisierte Einzelfallentscheidungen von einem Menschen überprüft werden. (EDÖB, 2023).

Gestützt auf die bestehenden Rechtsgrundlagen können die derzeit auf dem Markt befindlichen KI-Systeme genutzt werden, da diese letztlich nur ein weiterer technischer Fortschritt der Digitalisierung sind und das DSG technologieoffen ist. Abhängig vom technischen Fortschritt und der zukünftigen Automatisierung solcher Systeme wird der Gesetzgeber gefordert sein, spezifische und angepasste Präzisierungen in der DSV vorzunehmen, um dem Grundsatz der Gesetzmässigkeit zu genügen.

Unabhängig von der Fragestellung einer ausreichenden Rechtsgrundlage, wird bei der Beschaffung von KI-Systemen zu berücksichtigen sein, welche datenschutzrechtliche Eingriffstiefe mit der Nutzung verbunden ist. Die – andauernde – Diskussion zum Einsatz von Cloud-Services zeigt, welche Herausforderungen gelten, insbesondere weil eine Datenübertragung in die U.S.A. erfolgen kann. Ebenso wie auch im Bereich von

Cloud-Diensten und Anwendungssoftware handelt es sich bei den derzeitigen Anbietern von KI-Systemen hauptsächlich um amerikanische Unternehmen.

Bei der Beschaffung von Cloud-Diensten wird teilweise der risikobasierte Ansatz vertreten, um die mit der Beschaffung von Cloud-Diensten und Auslagerung an einen U.S.-amerikanischen Konzern verbundenen Risiken der Personendaten durch den möglichen Zugriff von US-amerikanischen Behörden zu rechtfertigen. Begründet wird der risikobasierte Ansatz damit, dass dieser (i) differenzierter und ganzheitlicher als die Anleitung des EDÖB sei, (ii) dem schweizerischen Datenschutzrecht immanent sei, (iii) Schrems II den risikobasierten Ansatz zulässt und die Schweiz bei Aufgabe des risikobasierten Ansatzes internationale Datentransfers in Staaten wie die USA generell untersagen müsste (Vasella, 2022). Der EDÖB hat sich bisher nicht ausdrücklich dem risikobasierten Ansatz angeschlossen. Dieser ist ohnedies nur der «Hilfsanker», soweit es an einem angemessenen Datenschutzniveau in den USA fehlt, welches die EU-Kommission erst kürzlich durch seinen Angemessenheitsbeschluss (erneut) festgestellt hat. Die Schweiz hat – Stand Juli 2024 – bisher kein angemessenes Datenschutzniveau festgestellt, so dass der risikobasierte Ansatz ein Weg ist, um einen Datentransfer in die USA vorzunehmen.

Fraglich ist, ob der risikobasierte Ansatz auch bei der Beschaffung von KI-Systemen ein möglicher Ausweg ist, sofern kein Angemessenheitsbeschluss vorliegt. In beiden Fällen besteht die Gefahr des Zugriffs amerikanischer Behörden ohne ausreichende Rechtsschutzmöglichkeit für den Betroffenen, was dafürspricht, den risikobasierten Ansatz auch bei der Beschaffung von KI-Systemen anzuwenden. Dagegen spricht aber, dass bei einem KI-System der datenschutzrechtlich relevante Eingriff erheblich schwerwiegender sein dürfte. Es werden gerade nicht nur Daten gespeichert (und potentiell dem Zugriff von US-amerikanischen Behörden ausgesetzt), sondern die Funktionsweise der KI-Systeme lebt üblicherweise davon, aus den Input-Daten das System zu trainieren. Personendaten werden daher fortlaufend verarbeitet, im Übrigen ohne offenzulegen, in welchem Umfang die Datenverarbeitung erfolgt, wer letztlich Zugriff auf die Trainingsdaten hat und wie diese Daten für andere Produkte weiterverarbeitet werden.

Der derzeitige risikobasierte Ansatz für den Einsatz von Cloud-Diensten lässt sich daher nur eingeschränkt für die Beschaffung von KI-Anwendungen übertragen und

bedarf, wenn man diesem Ansatz folgen will, einer neuen Bewertung des Risikos für die verarbeiteten Personendaten.

Zur Bearbeitung von Personendaten durch öffentliche Organe ist zudem der Grundsatz der Zweckbindung zu berücksichtigen. Öffentliche Organe dürfen sich nicht ohne Weiteres für Private interessieren, sondern nur in Zusammenhang mit der Erfüllung einer ihnen zugewiesenen gesetzlichen Aufgabe (Glass, 2023). Dies spielt insbesondere auch bei der Datenerhebung eine Rolle. So wird im Kanton Zürich durch das kantonale Datenschutzgesetz die Zweckbindung dahingehend definiert, dass die öffentlichen Organe Personendaten nur zu dem Zweck bearbeiten dürfen, zu dem sie erhoben wurden (Art. 9 Abs. 1 IDG ZH).

Die Zweckbindung steht aber in Frage, wenn die Personendaten nicht nur ausschliesslich zur Erstellung eines verwaltungsrechtlichen Entscheides mittels KI-System genutzt werden, sondern zugleich, um die KI selbst zu trainieren und fortzuentwickeln. Dabei spielt es keine Rolle, ob die KI mittels Dienstleistungsvertrag von einem Anbieter bezogen wird, oder aber autonom in der Verwaltung nach Lieferung eines Softwareprodukts eingesetzt wird. Der Betroffene hat seine Daten lediglich für den Zweck der Bearbeitung seines Anliegens, nicht aber für Trainingszwecke einer KI zur Verfügung gestellt. Aus Sicht der Verwaltung ist der Zweck jedoch sowohl die Bearbeitung des Bürgeranliegens wie auch Trainingszwecke der KI. Nach Art. 6 Abs. 3 DSG dürfen die Personendaten nur zu einem bestimmten und für die Person erkennbaren Zweck beschafft werden. Der Zweck ist dann erkennbar, wenn die betroffene Person informiert wird, die Bearbeitung gesetzlich vorgesehen ist oder aus den Umständen klar ersichtlich ist. Die Erkennbarkeit der Datenbearbeitung zum Zwecke z.B. der Bewilligung von Sozialhilfe ergibt sich aus der jeweiligen Rechtsgrundlage im Fachgesetz. Im Fachgesetz fehlt jedoch eine Rechtsgrundlage für den Zweck des Trainings eines KI-Modells, und auch eine Information erfolgt in der Regel nicht.

Die grosszügige Auslegung des Zweckbindungsgrundsatzes von Rosenthal (Rosenthal, 2023), demnach vom ursprünglichen Primärzweck ein späterer weiterer Zweck (wie etwas das Training einer generativen KI) umfasst sei, dürfte zu weitgehend sein. In der Botschaft zum DSG (Botschaft, S. 7025) ist festgehalten: «Sowohl die Beschaffung der Daten als auch der Zweck ihrer Bearbeitung müssen erkennbar sein.» Dass der Bürger

bei der Beschaffung von Daten durch die Verwaltung erkennt, dass die Verwaltung die Daten auch zum Sekundär- oder Kollateralzweck des Trainings einer generativen KI verwendet, verlangt nahezu hellseherische Fähigkeiten des Bürgers und widerspricht dem gesetzgeberischen Anliegen einer Zweckbindung. Zuzustimmen ist Rosenthal insoweit, dass die Zweckbindung erfüllt ist, wenn die Daten in einer Weise bearbeitet werden, die mit dem ursprünglichen Zweck «vereinbar» sind.

Auflösen lässt sich das mit einer gesetzlichen Grundlage im entsprechenden Fachgesetz (Art. 34 Abs. 1 DSG) oder einer datenschutzrechtlichen Information und Einwilligung des Betroffenen (Art. 34 Abs. 4 lit. b. DSG). Auch die kantonalen Datenschutzgesetze stellen, wenn auch mit anderem Wortlaut, auf den Grundsatz der Zweckbindung ab (z.B.: Art. 4 Abs. 4 KDSG-LU (2021), Art. 5 Abs. 4 KDSG-BE (2013): «Treu und Glauben mit dem Zweck unvereinbar»; Art. 26 revIDG-ZH: ein anderer «Zweck ist zulässig, wenn es eine Rechtsgrundlage erlaubt oder die betroffene Person im Einzelfall eingewilligt hat»)

Zusammenfassend kann festgestellt werden, dass die Beschaffung von derzeitig verfügbaren KI-Systemen datenschutzrechtlich möglich und zulässig ist. Eine Herausforderung besteht darin, den Grundsatz der Zweckbindung und Erkennbarkeit der Datenverarbeitung einzuhalten. Eine weitere Herausforderung stellt dar, dass die technische Funktionsweise von KI-Systemen derzeit kaum bekannt ist oder den Geschäftsgeheimnissen der Anbieter unterliegen. Welche tatsächlichen Risiken für die Bearbeitung von Personendaten mit dem Einsatz von KI-Systemen einhergehen, lässt sich daher – anders als bei dem Einsatz von Cloud-Diensten, deren Funktionsweise und Risiken weitgehend bekannt sind – seriös kaum sagen. Bisherige Überlegungen, auf einen risikobasierten Ansatz abzustellen, lassen sich daher nicht ohne weiteres auf den Einsatz von KI-Systemen übertragen, da sich die Risiken für die betroffene Person derzeit nicht bewerten lassen, solange weder Algorithmus noch Wirkungsweise vom Anbieter veröffentlicht werden oder nachvollziehbar bekannt sind.

3.2 WAHRUNG DER DATENSCHUTZRECHTE BEI DER NUTZUNG VON KI

Das verfassungsmässig geschützte Recht auf Privatsphäre (Art. 13 BV) ist im Zusammenhang mit dem Einsatz von KI-Anwendungen regelmässig betroffen, da solche Anwendungen eine Bearbeitung von Personendaten voraussetzen. Konkretisiert wird dieser Schutz

durch das Datenschutzgesetz (DSG). Die Anwendbarkeit des DSG bei der Bearbeitung von Personendaten durch Bundesbehörden ergibt sich aus Art. 2 Abs. 1 lit. b DSG.

Datenschutzrechtlich bestehen seitens der Betroffenen gegenüber Datenbearbeitern nicht nur Informationsrechte über die Bearbeitung bzw. Einsichtsrechte in den Bestand über eigene Daten, sondern auch Rechte zur Beseitigung von Verletzungen. Die Informationspflicht im Hinblick auf die Bearbeitung von Personendaten mittels künstlicher Intelligenz unterscheidet sich kaum von der üblichen Erhebung von Personendaten. In beiden Fällen muss über die Datenerhebung vorgängig informiert werden, Art. 19 DSG.

Problematisch ist eher der Zugang zu, bzw. der Umfang der Einsicht in die vorhandenen Personendaten. So führt Glass aus: «In Bezug auf KI-Systeme dürfte das Zugangsrecht insbesondere gegenüber Outputdaten wirksam werden, da diese in der Regel als Ergebnis einer Datenbearbeitung gespeichert und weiterbearbeitet werden. Inputdaten werden hingegen nicht notwendigerweise gespeichert, zumindest nicht durch das Organ, welches den Input veranlasst. Nutzt eine Mitarbeiterin eines öffentlichen Organs beispielsweise eine Such- oder Übersetzungsmaschine, werden die Suchbegriffe in der Regel nicht durch das öffentliche Organ gespeichert. Unter Umständen besteht aber dennoch eine aus der Begründungs- und Dokumentationspflicht fliessende Pflicht die Inputdaten zu speichern oder eine entsprechende Aktennotiz zu erstellen. Dies erscheint denkbar, wenn die KI-Funktion einen Output generieren soll, der als Begründung für eine rechtlich relevante Entscheidung dient, und dessen Erklärungszusammenhang sich allein aus der KI-Funktion ergibt.» (Glass, 2023).

Das datenschutzrechtliche Auskunftsrecht erfasst alle Informationen, die erforderlich sind, damit die betroffene Person ihre Rechte nach dem Datenschutzgesetz geltend machen kann (Art. 25 Abs. 2 Satz 1 DSG). Die Aufzählung in Art. 25 Abs. 2 Satz 2 lit. a–g DSG ist nach dem Willen des Gesetzgebers nicht abschliessend. Die Generalklausel in Satz 1 erlaubt, dass die betroffene Person gegebenenfalls weitere Informationen verlangen kann, um ihre Rechte geltend zu machen, muss aber bei grossen Datenmengen gegebenenfalls präzisieren, auf welche Informationen und Bearbeitungsvorgänge sich das Auskunftsersuchen bezieht (Botschaft, S. 7076). Die vom Gesetzgeber für die automatisierte Einzelfallentscheidung angenommenen Auskunftstiefe dürfte auch für KI-Systeme entsprechend anwendbar sein. «Dabei müssen nicht unbedingt die Algorithmen

mitgeteilt werden, die Grundlage der Entscheidung sind, weil es sich dabei regelmässig um Geschäftsgeheimnisse handelt. Vielmehr müssen die Grundannahmen der Algorithmus-Logik genannt werden, auf der die automatisierte Einzelentscheidung beruht», so der Bundesrat in der Botschaft zum DSG (Botschaft, S. 7067). Wenn der Gesetzgeber bereits für das Kredit-Scoring verlangt, dass über die Menge und die Art der für das Scoring herangezogenen Informationen sowie deren Gewichtung informiert wird, dürfte für den Einsatz von KI-Systemen nichts anderes gelten. Demnach wäre über den Einsatz eines KI-Systems Auskunft zu erteilen, wie auch über die Grundannahmen der Algorithmus-Logik. Da letztere dem Geschäftsgeheimnis der Anbieter unterliegen, ist Glass insoweit zuzustimmen, dass sich aus der Dokumentations- und Begründungspflicht die Pflicht ergibt, Auskunft zu erteilen, welche (Personen-)Daten als Inputdaten verwendet wurden. Dies gewährleistet dem Betroffenen die Überprüfung, ob seine Personendaten datenschutzkonform eingesetzt werden. Es ist auch nicht unpraktikabel, da die Verwaltung die Vorgänge vielfach digitalisiert abarbeitet und entsprechend dokumentieren kann.

Bei Such- oder Übersetzungsmaschinen, auch mit der Möglichkeit des Uploads ganzer Dokumente, entsteht ein weiteres Problemfeld: Während die Eingaben oftmals durch die eingebende Person nicht explizit gespeichert werden, erfolgt dies möglicherweise durch den benutzten Service[1]. Dies stellt ebenfalls eine Datenbearbeitung dar, die nach Art. 34 DSG einer Rechtsgrundlage bedarf. Sofern die öffentliche Verwaltung solche Dienste nutzt, bedarf es für Bundesbehörden eines Gesetzes im formellen Sinne wenn es sich um besonders schützenswerte Personendaten handelt oder die Datenverarbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen kann (Art. 34 Abs. 2 DSG). Bei der Beschaffung solcher Dienste muss darauf geachtet werden, dass entweder eine Weiterverwendung der Daten durch den Anbieter vertraglich ausgeschlossen wird oder im Rahmen der Beschaffungskriterien der Schutz der Personendaten z.B. durch Anonymisierung Berücksichtigung findet.

3.3 DATENGERÜST DER JEWEILIGEN KI-ANWENDUNG

Eine weitere Problematik, die sich im Zusammenhang mit dem Einsatz von KI-Systemen durch die öffentliche Verwaltung stellt, ist, wie die Trainingsdaten entstanden

[1] So lässt es sich beispielsweise beim Übersetzungsdienst «DeepL» in der Gratis-Version nicht verhindern, dass die eingegebenen Texte für weitere Trainings verwendet und gespeichert werden.

sind, woher die Trainingsdaten stammen und auf welchen Algorithmen bzw. Vorgaben das System der KI-Anwendung basiert. Die Trainingsdaten bilden die Grundlage der Entscheidung des KI-Systems und können abhängig von der System-Vorgabe zu verzerrten, einseitigen oder sogar diskriminierenden Ergebnissen führen.

Eine Studie verschiedener Universitäten (Awad et al., 2018) hat gezeigt, dass es in unterschiedlichen Kulturen unterschiedliche Moralvorstellungen über das Alter, den sozialen Status oder die Herkunft gibt. So haben beispielsweise in Asien ältere Menschen einen hohen gesellschaftlichen Stellenwert. Solche Moralvorstellungen könnten in die Programmierung und den Algorithmus eingeflossen sein und haben mithin Auswirkungen auf das Ergebnis. Neben Moralvorstellungen können auch gesellschaftliche oder politische Gegebenheiten – ob bewusst oder unbewusst – bei der Programmierung und des Trainings von KI eine Rolle spielen.

Im Rahmen des Beschaffungsprozesses muss daher geprüft werden, wofür eine KI-Anwendung verwendet wird, bzw. auf Basis welcher Parameter sie zu welchem Zweck ein Ergebnis erstellen soll. Insbesondere hat auch Gewicht, welche Bedeutung ein Ergebnis für eine betroffene Person hat. Entsprechend sind mehr oder weniger strenge Voraussetzungen an das Training, die formalisierten Tests, die Transparenz der Vorgänge und weitere Qualitätsmerkmale gestellt (Rosenthal, 2022).

Dass auch die Prognosewertung bzw. Entscheidfindung im Allgemeinen durch eine natürliche Person von Vorurteilen («bias»), Lücken und subjektiven Erfahrungen gekennzeichnet sein kann, ist bekannt und wird gerade durch die Rechtsschutzmöglichkeiten einer ausreichenden Kontrolle unterworfen. Schwieriger stellt sich die Kontrolle einer algorithmischen Entscheidung dar: Weil deren Funktionsweise und Algorithmus in der Regel nicht bekannt und durch Geschäftsgeheimnisklauseln der Anbieter geschützt sind, sind diese einer tatsächlichen wie auch rechtlichen Überprüfung faktisch entzogen. Der Algorithmus kann auch – anders als ein Mensch – nicht im Rahmen einer dienstlichen Erklärung oder Zeugenerklärung befragt werden, warum er eine Entscheidung in einer bestimmten Weise getroffen hat. Das Risiko einer für sie gerichtlich nachteiligen Entscheidung trägt letztlich die einsetzende Behörde, und zwar unabhängig davon, ob ein Mensch oder ein KI-System gehandelt wird. Ist das Gericht nicht von der Rechtmässigkeit

überzeugt, und sei es, weil begründete Zweifel an der «Unvoreingenommenheit» des KI-Systems bestehen, ist der Verwaltungsakt rechtswidrig.

Umso wichtiger erscheint es daher, bereits im Beschaffungsprozess gegenüber dem Anbieter Vorgaben zu machen, mit welchen Trainingsdaten und nach welchen Masstäben die KI trainiert wird und ob und in welchem Umfang Algorithmen und die Herkunft der Trainingsdaten offen zu legen sind. Auch könnte im Rahmen der Beschaffung vorgegeben werden, dass der Quellcode zur Überprüfung durch eine vertrauenswürdige, neutrale oder verschwiegenheitsverpflichtete Stelle offengelegt werden muss.

Zudem ist bei der Beschaffung von KI-Anwendungen für die Verwendung im öffentlichen Sektor ein besonderes Augenmerk darauf zu legen, ob sie dem bestehenden Regelwerk (bspw. Gleichstellungsgesetz, Diskriminierungsverbot) entsprechende Entscheidungen und Resultate produzieren.

3.4 VERWALTUNGSARBEIT DURCH KI: UNTERSTÜTZEND ODER BESCHLIESSEND?

Es ist davon auszugehen, dass insbesondere in Verfahren, die sich durch eine hohe Standardisierung von Prozessabläufen auszeichnen, einzelne Prozessschritte automatisiert werden. Eine Grenze zu ziehen, wie viel menschliches Involvieren benötigt wird, um ein Entscheid, bzw. ein behördliches Handeln als „menschlich" und nicht „automatisiert" zu qualifizieren, ist pauschaliert kaum möglich. Dennoch ist genau diese Frage von Bedeutung.

Es stellt sich die Frage, ob eine Pflicht des Staates gegenüber den betroffenen Personen besteht, die beinhaltet, dass gewisse behördliche Entscheidungen durch Menschen getroffen werden (Braun Binder, 2023).

Aus den Vorgaben der Bundesverfassung, dem in Art. 29 Abs. 2 BV verankerten Anspruch auf rechtliches Gehör, kann sich die Notwendigkeit ergeben, dass behördliche Entscheidungen durch Menschen getroffen werden müssen. Art. 29 Abs. 2 BV lautet: "Die Parteien haben Anspruch auf rechtliches Gehör."

Wie das Bundesgericht in ständiger Rechtsprechung urteilt, besteht die Pflicht der Behörde, ihre Verfügungen und Entscheide zu begründen (BGE 129 I 232 E 3.2):

> „Der Grundsatz des rechtlichen Gehörs als persönlichkeitsbezogenes Mitwirkungsrecht verlangt, dass die Behörde das Vorbringen des vom Entscheid in seiner Rechtsstellung Betroffenen auch tatsächlich hört, sorgfältig und ernsthaft prüft und in der Entscheidfindung berücksichtigt. Daraus folgt die grundsätzliche Pflicht der Behörden, ihren Entscheid zu begründen. Der Bürger soll wissen, warum die Behörde entgegen seinem Antrag entschieden hat. Die Begründung eines Entscheids muss deshalb so abgefasst sein, dass der Betroffene ihn gegebenenfalls sachgerecht anfechten kann. Dies ist nur möglich, wenn sowohl er wie auch die Rechtsmittelinstanz sich über die Tragweite des Entscheids ein Bild machen können. In diesem Sinne müssen wenigstens kurz die Überlegungen genannt werden, von denen sich die Behörde leiten liess und auf welche sich ihr Entscheid stützt (BGE 126 I 97 E. 2b mit Hinweisen).“.

Eine behördliche Begründung erfolgt aber dann nicht mehr, wenn das KI-System völlig autonom zum Beispiel über den Bezug von Sozialhilfeleistung anhand der vom Antragsteller zur Verfügung gestellten Angaben eine Entscheidung trifft. Soweit es die Berechnung betrifft, stellt sich der Einsatz von KI als unkompliziert dar, da es nichts anderes ist als die Nutzung eines Taschenrechners. Wenn es aber um Einzelfallentscheidungen oder die Ausübung von der Behörde durch Gesetz eingeräumtes Ermessen geht, stellt der Einsatz von KI-Systemen auf den ersten Blick eine Herausforderungen dar.

So liegt ein Ermessensmissbrauch vor, wenn die Ermessensausübung nicht pflichtgemäss erfolgt, von sachfremden Kriterien geleitet oder “unmotiviert” ist (VGr ZH, 22.10.2004, VB.2004.00297, E. 2.3). Auch wenn wohl nicht jede menschliche behördliche Entscheidung besonders motiviert erfolgt, dürfte jedenfalls beim Einsatz von KI keinerlei „Motivation“ vorliegen. Und auch eine Ermessensunterschreitung kann vorliegen. Dies ist der Fall, wenn die Behörde das ihr eingeräumte Ermessen nicht ausschöpft, und beispielsweise ganz oder teilweise auf das ihr zustehende Ermessen verzichtet (VGr ZH, 9.11.2011, VB.2011.00573, E. 2), wenn besondere Umstände nicht berücksichtigt werden, obwohl das Recht dies vorsieht (VGr ZH, 8.2.2007, VB.2006.000369, E. 6), oder wenn die Behörde Fälle schematisch gleich behandelt, obgleich der Gesetzgeber eine differenzierte Behandlung bestimmter Fragen fordert (VGr ZH, 19.5.2004, VB.2004.00123, E. 4.3.1).

Vor der Beschaffung von KI-Systemen sind daher verwaltungsinterne Richtlinien zu erstellen, wie das rechtliche Gehör und die Ausübung des Ermessens unter schlussendlicher menschlicher Beteiligung erfolgen. Die Richtlinien können ebenso Vorgaben zur Erfüllung von Transparenzanforderungen oder Entscheidungs-Triagen enthalten. Diese Richtlinien bilden die Grundlage für die Beschaffungskriterien des zu beschaffenden Systems.

Oftmals kritisiert wird auch die mangelnde bzw. eingeschränkte Nachvollziehbarkeit maschineller Lernverfahren. Fraglich ist, ob eine Entscheidung durch eine KI-Anwendung dem rechtsstaatlichen Begründungserfordernis eines Rechtsaktes bzw. Gerichtsurteils genügen kann. Die Begründung dient dazu, Transparenz bezüglich der Entscheidungsgründe herzustellen. Sie soll es den Betroffenen ermöglichen, gegen den behördlichen Entscheid ein sachgerechtes Rechtsmittel einzureichen. (Braun Binder, 2019). Doch auch dies ist, konsequent betrachtet, lediglich eine Anforderung an die Ausgestaltung und Qualität der KI-Anwendung.

Selbst ohne tangierte Grundrechte erfordert der Einsatz von KI in der Verwaltung zu seiner demokratischen Legitimation eine genügend bestimmte gesetzliche Grundlage (Gesetzmässigkeitsprinzip). Denn grundsätzlich geht die demokratische Legitimation wohl aktuell davon aus, dass hoheitliches Handeln einem Menschen obliegt und von Menschen verantwortet werden. Es ist also unabhängig von der Art des Einsatzes unumgänglich, eine genügend bestimmte gesetzliche Grundlage zu schaffen, sofern die Nutzung von KI im Ergebnis die Rechtstellung von Personen betrifft, auch wenn sie nur unterstützend angewendet wurde (Reiter, 2022). Dieser Auffassung von Reiter ist insofern zuzustimmen, dass je selbstautonomer KI-Programme Entscheidungen treffen, die eine Auswirkung auf den Bürger haben, desto eher es einer gesetzlichen Grundlage bedarf. Denn KI-Tools die die menschliche Entscheidung ersetzen, sind gerade nicht nur einfach Hilfsmittel des Verwaltungsmitarbeiters, sondern ersetzen diesen. Erfolgt eine vollständige oder weitestgehende Ersetzung von Verwaltungsaufgaben durch autonome Systeme (z.B. denkbar auch autonome Polizeiroboter, wie diese für den New-Yorker Einsatz geplant sind[2] oder derzeit im Innovation Lab der Polizei

[2] https://arstechnica.com/gadgets/2023/04/nypd-robocops-hulking-400-lb-robots-will-start-patrolling-new-york-city/.

NRW entwickelt werden[3]) ist KI aber nicht nur Hilfsmittel ist, sondern «Entscheider» und bedarf wegen dem Gesetzmässigkeitsprinzip einer gesetzlichen Grundlage im entsprechenden Fachgesetz. Denn dies führt zu zweierlei: Der Gesetzgeber muss sich bei der Gesetzeserarbeitung (politisch) damit befassen, ob und in welchem Umfang er KI-Tools als Substituierung des Verwaltungsmitarbeitenden einsetzen will. Und der Bürger kann anhand der gesetzlichen Grundlage erkennen, ob (i) ein Verwaltungsmitarbeiter entscheidet, (ii) ein Verwaltungsmitarbeiter und eine KI entscheiden oder (iii) eine KI autonom entscheidet.

Dem kann entgegengehalten werden, dass auch der Output generativer KIs nichts anderes als die aggregierte und statistisch modellierte Meinung vieler Menschen ist, weil diese den Inputdaten der KI-Modelle zugrunde liegt. So betrachtet wären KI-Systeme «demokratischer» als viele andere Technologien.

Diese Auffassung übersieht aber, dass KI-Systeme mit einer bestimmten Moral- oder Grundvorstellung programmiert sein können (siehe zuvor) und sich die autonomen Fähigkeiten von KI-Systemen in der Zukunft fortentwickeln wird. Während in den Neunzigern von einigen dem World-Wide-Web eine Demokratisierung der Welt vorschwebte, zeigt sich heute, dass sich diese Hoffnung nicht unbedingt erfüllt hat (auch wenn das auch an anderen Umständen liegen könnte). Der Einsatz von KI-Systemen in der Verwaltung stellt sich für den Verfasser als unproblematisch dar, soweit die verfassungsrechtlichen Grundprinzipien und Rechtsschutzmöglichkeiten gewahrt bleiben. Neue Techniken brauchen angepasste gesetzliche Grundlagen: Das war bei der Eisenbahn so, bei dem Auto und auch bei dem Internet.

Wer KI-Systeme beschafft, wird die Thematik des rechtskonformen Einsatzes von zu beschaffenden KI-Systemen berücksichtigen müssen.

3.5 URHEBERRECHTE BEI DER NUTZUNG VON KI

Bei der Weiterverwendung von Ergebnissen, welche mittels einer KI-Anwendung erstellt wurden, stellt sich auch die Frage nach den Urheberrechten an diesen Ergebnissen. Art. 2 Abs. 1 Urheberrechtsgesetz (URG) definiert den Begriff des Werks wie folgt: «Werke

[3] https://www.polizei-dein-partner.de/themen/gewalt/gesellschaft/detailansicht-gesellschaft/artikel/high-tech-unterstuetzung-fuer-die-polizei.html.

sind, unabhängig von ihrem Wert oder Zweck, geistige Schöpfungen der Literatur und Kunst, die individuellen Charakter haben».

Aufgrund des Kriteriums der geistigen Schöpfung unterfallen die Ergebnisse von KI-Anwendungen nicht dem urheberrechtlichen Werk-Begriff. Etwas anderes kann sich daraus ergeben, dass ein Mensch einen kreativen Input (Prompt) vornimmt und damit das KI-Ergebnis überhaupt erst erzielt werden kann. Soweit das Bundesgericht (BGE 130 III 168 E. 5.2.) entschieden hat, dass ein Foto des bekannten Sängers Bob Marley auf einem Konzert Urheberrechtsschutz geniessen kann, dürfte diese Rechtsprechung auch auf die KI-Eingabe zu übertragen sein. Im richtigen Moment auf den Auslöser einer Kamera drücken (Bob Marley) ist ebenso schöpferisch wie eine kreative Eingabe bei einem KI-Tool.

Soweit für den KI-Input urheberrechtlich geschütztes Material oder Werke genutzt werden, muss der Verwender über die Nutzungsrechte verfügen oder sich diese einräumen lassen. Bei dem Input von einfachen Texten zum Beispiel in einem Antragsformular dürfte kein Urheberrechtsschutz bestehen. Aber bei dem Input von Fotos, Bildern oder Videos in ein KI-System ist das Urheberrecht zu beachten, insbesondere wenn das KI-System die Daten für Trainingszwecke weiterverarbeitet.

Eine Lösung könnte sein, dass bei der Beschaffung eine Weiterbearbeitung von Input-Daten für Trainingszwecke vertraglich ausgeschlossen wird. Eine andere Lösung könnte sein, verwaltungseigene KI-Agenten zu nutzen, bei denen die Input-Daten innerhalb des IT-Systems der Verwaltung bzw. Verwaltungseinheit verbleiben, so dass die Verarbeitung des Fotos des Antragstellers eine Verwaltungstätigkeit darstellt und keine Nutzung der Daten durch externe Anbieter des KI-Systems bzw. das Unternehmen erfolgt.

3.6 KI-ANWENDUNGEN ALS SUBSTITUTEN IN DER VERTRAGSERFÜLLUNG

Wird ein Teil der Arbeit durch KI-Anwendungen erbracht, stellt sich die Frage wie diese «Auslagerung» zu qualifizieren ist, und ob eine solche zulässig ist.

Das Bundesgericht setzte sich in BGer 4A_305/2021, E 7.3 mit der Rechtsfrage auseinander, ob ein algorithmisches System die Rechtsfigur der Substitutin im Sinne des OR ausfüllen kann. Dabei kam das Gericht zum Schluss, dass mit «Dritten» im Sinne von Art. 398

Abs. 3 OR andere natürliche oder juristische Personen gemeint sind. Dies ergebe sich daraus, «dass der Auftraggeber gemäss Art. 399 Abs. 3 OR Ansprüche, die dem Beauftragten gegen den Dritten zustehen, unmittelbar gegen diesen geltend machen kann. Dies setzt voraus, dass dem Dritten Rechtspersönlichkeit zukommt. Die Verwendung von Hilfsmitteln, wie beispielsweise eines Computers mit entsprechender Software, die das Market Making automatisiert durchführt, stellt keine Substitution dar, da diesen Hilfsmitteln keine Rechtspersönlichkeit zukommt.» (BGer 4A_305/2021, E 7.3.1).

Überträgt man diesen Rechtsgedanken auf das Verwaltungsrecht, dann würde auch der verwaltungsrechtliche Einsatz von KI-Systemen keine Substituierung der Verwaltungstätigkeit darstellen, sondern lediglich Hilfsmittel der Verwaltungstätigkeit sein.

Die verfassungsrechtlichen Vorgaben des Art. 29 Abs. 2 BV, wie auch das Vertrauen in die Nachvollziehbarkeit verwaltungsrechtlicher Entscheidungen, führen zwingend dazu, dass zwischen dem privatrechtlich-substituierenden Handeln und dem verwaltungsrechtlich-substituierenden Handeln zu unterscheiden ist. Zudem ist die Verwaltung nicht nach Auftragsgrundsätzen im Sinne des OR tätig, so dass die zivilrechtliche Rechtsprechung des Bundesgerichts nicht auf das Verwaltungsverfahren zu übertragen ist.

4. WAS GILT ES ZU BEACHTEN BEI DER BESCHAFFUNG VON KI-ANWENDUNGEN FÜR DIE ÖFFENTLICHE HAND?

Die Beschaffung von Systemen künstlicher Intelligenz für die Anwendung im öffentlichen Sektor unterscheidet sich nicht von der Beschaffung von ICT-Dienstleistungen oder -Produkten. Die Beschaffung von KI-Anwendungen ist für die öffentliche Hand, zumindest als Hilfsmittel, ohne Weiteres gestattet.

Die für Beschaffung von KI-Anwendungen absehbaren Problemfelder ergeben sich aus dem nach der Beschaffung beabsichtigten *Einsatz* des KI-Systems. Da der Staat in seinen Handlungen an die Grundrechte gebunden ist, sind diese stets zu berücksichtigen. Dabei ist es insbesondere das Recht auf Privatsphäre, welches Ausfluss im Datenschutzgesetz findet, zu beachten, da die KI-Systeme gewichtigsten Risiken für den Schutz von Personendaten mit sich bringen. Jede Anwendung von künstlicher Intelligenz setzt eine Bearbeitung von Daten, insbesondere zu Lern- und Trainingszwecken

voraus, um bessere Ergebnisse zu erzielen. Zudem ist das verfassungsmässige Recht auf Gleichbehandlung bzw. gegen Diskriminierung (Art. 8 BV) zu berücksichtigen. Der Staat hat in der Anwendung von KI zu gewährleisten, dass diese auf einer neutralen Datenbasis beruht.

Bei dem Einsatz von KI-Anwendungen in der öffentlichen Verwaltung könnten im Rahmen des Beschaffungsvorganges folgende Vorgaben bestehen:

1. **Transparenz**: Bei der Beschaffung von KI-Systemen bedarf es in der Ausschreibung Anforderungen an:

- die Offenlegung/Transparenz über die Herkunft der (Trainings-) Daten
- Transparenz über den Algorithmus der Entscheidungsfindung
- Idealerweise: Offenlegung des Quellcodes, jedenfalls gegenüber der Behörde
- In den Entscheiden ist z.B. durch einen „digitalen Fussabdruck" offenzulegen, dass der Entscheid unter Nutzung von KI-Systemen getroffen wurde. Das ermöglicht dem Bürger, den Bescheid und die verwendeten Hilfsmittel zu überprüfen[4].

2. **Richtlinien**: Aus den verwaltungsinternen Richtlinien müssen sich die Spezifikationen für die zu beschaffende KI-Software ergeben. Die Richtlinien sind vorgängig zur Beschaffung zu erstellen und sollten wesentliche Punkte zum Einsatz von KI-Anwendungen enthalten:

- Erfüllung der Triage-Checkliste für KI-Systeme (Checkliste 1, Braun Binder et al., 2021).
- Erfüllung der Transparenzanforderungen (Checkliste 2, Braun Binder et al., 2021)
- Technische Vorgaben, wie in den Entscheiden die eingesetzten KI-Tools durch eine Signatur oder „digitalen Fussabdruck" offengelegt werden
- Vorgaben über die eingesetzten Trainingsdaten und deren Herkunft
- Vorgaben zur Einhaltung von Gesetzen (u.a. Datenschutz, Urheberrecht)

[4] In einem Beitrag von IT-Inside haben die Rechtsanwälte Christian Laux und Sven Kohlmeier einen Vorschlag für eine Transparenzmeldung bei Einsatz von KI-Tools erarbeitet: https://www.inside-it.ch/kohlmeier-vs-laux-wie-weit-geht-transparenz-beim-einsatz-von-ki-in-der-verwaltung-20231019.

3. **Einheitlichkeit**: Es bedarf einer einheitlichen Verwaltungspraxis für die Ausschreibung von KI-Systemen durch Bund und Kantone im Hinblick auf:

- Ethische Grundsätze
- Einhaltung von Gesetzen (z.B. Datenschutz und Urheberrecht etc.)
- Beschreibung des zu beschaffenden Systems (z.B. Leistungsumfang, Hosting, Herkunft der Trainingsdaten und Anforderungen an die Anpassung der Trainingsdaten etc.)

Auch wenn kein umfassendes KI-Recht besteht, und ein solches aufgrund der Vielseitigkeit der Risiken und Möglichkeiten auch nicht sinnvoll wäre, es ist keineswegs so, dass sich die öffentliche Verwaltung aktuell bei der Beschaffung von KI in einem rechtsfreien Raum bewegt. Die Koordination der Problemfelder erscheint zwar auf den ersten Blick noch etwas unstrukturiert, bzw. dynamisch. Wenn man sich aber die Entwicklungsgeschwindigkeit von KI aktuell ansieht, wird klar, weshalb eine gewisse Flexibilität und Dynamik im rechtlichen Umgang mit ihr unabdingbar ist.

Sven Kohlmeier, Rechtsanwalt, Fachanwalt für IT-Recht (D), Wicki Partners AG

Mitarbeit: Raël Fein, Substitutin, Wicki Partners AG

Einen besonderen Dank bei der Redigatur gebührt Thomas M. Fischer, Rechtsanwalt.

LITERATURVERZEICHNIS:

Awad, E., Dsouza, S., Kim, R., Schulz, J., Henrich, J., Shariff, A., Bonnefon, J-F., Rahwan, I., The moral Machine Experiment, 2018, https://core.ac.uk/download/pdf/231922494.pdf

Braun Binder, N., Spielkamp, M., Egli, C., Freiburghaus, L., Kunz, E., Laukenmann, N., Loi, M., Mätzener, A., Obrecht, L., Wulf, J., Einsatz künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen, Schlussbericht, 2021, https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/kanton/digitale-verwaltung-und-e-government/projekte_digitale_transformation/ki_einsatz_in_der_verwaltung_2021.pdf

Braun Binder, Staat, Mensch, Algorithmen, BJM 2023, https://bjm.recht.ch/fr/artikel/01bjm0123auf/staat-mensch-algorithmen

Braun Binder , Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ 115/2019 S. 472

Botschaft zum Datenschutzgesetz, BBl 2017, 6941, https://www.fedlex.admin.ch/eli/fga/2017/2057/de

EDÖB, Geltendes Datenschutzrecht ist auf KI direkt anwendbar, 2023, https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/2023/20231109_ki_dsg.html

Glass, Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung / III. - IV., in: Widmer Michael (Hrsg.), Datenschutz - Rechtliche Schnittstellen, 2023, S. 208Poledna /Schlauri /Schweizer, Rechtliche Voraussetzungen der Nutzung von Open-Source-Software in der öffentlichen Verwaltung, insbesondere des Kantons Bern, 2017

Reiter, Künstliche Intelligenz im Verwaltungsverfahren, AJP 2022 S. 984 ff.

Rosenthal, Datenschutz und KI: Worauf in der Praxis zu achten ist, in: Jusletter IT, April 2022

Rosenthal, Datenschutz beim Einsatz generativer künstlicher Intelligenz, in: Jusletter, 6.11.2023

Sury, Digital in Law, Informatikrecht, 2021

Tschentscher/Lienhard /Sprecher, Öffentliches Recht, Verfassungsrecht, Verwaltungsrecht, öffentliches Verfahrensrecht, 2. Aufl., 2019

Vasella, D. (2022). EDÖB: Zweifel am risikobasierten Ansatz, https://datenrecht.ch/edoeb-zweifel-am-risikobasierten-ansatz/

Waldmann /Wiederkehr, Allgemeines Verwaltungsrecht, 2019

CLOUD UND DATENSCHUTZ – WAS IST ZU BEACHTEN?

Dr. iur., Dominika Blonski

Dr. iur., Dominika Blonski, Executive MPA Unibe, ist Datenschutzbeauftragte des Kantons Zürich, Herausgeberin und Autorin verschiedener Kommentare und Fachpublikationen sowie Dozentin zum Datenschutzrecht.

Abstract: Beschaffen Behörden eine Cloud-Lösung, liegt datenschutzrechtlich eine Auftragsdatenbearbeitung vor. Behörden als öffentliche Organe haben diese Datenbearbeitung – wie jede Datenbearbeitung – rechtmässig auszugestalten. Es stellen sich somit primär rechtliche Fragen: zunächst ist die Rechtsfrage zu beantworten, ob überhaupt ausgelagert werden darf, weil keine rechtliche Bestimmung der Auslagerung entgegensteht und der Auftraggeber seine Verantwortung wahrnehmen kann. Wird diese erste Frage bejaht, stellt sich in einem zweiten Schritt die Frage der angemessenen organisatorisch-technischen Massnahmen für die Datenbearbeitung. Diese Massnahmen werden anhand einer Risikoanalyse – je nach Art der Daten – festgelegt und damit die Frage gestellt, wie ausgelagert werden darf.

INHALTSVERZEICHNIS

1 Einleitung 136
2 Cloud Computing ist eine Auftragsdatenbearbeitung 137
2.1 Was ist Cloud Computing? 137
2.2 Was ist eine Auftragsdatenbearbeitung? 137
2.3 Besondere Risiken 138
3 Wann ist eine Auftragsdatenbearbeitung in der Cloud rechtmässig? 139
4 Was sind die Voraussetzungen einer Auftragsdatenbearbeitung in der Cloud? 141
4.1 Rechtsfrage: Darf in die Cloud ausgelagert werden? 142
4.1.1 Stehen rechtliche Bestimmungen entgegen? 142

4.1.1.1 Geheimhaltungspflichten 143
4.1.1.2 Weitere Bestimmungen, die der Auslagerung entgegenstehen können 146
4.1.2 Ist die Wahrnehmung der Verantwortung möglich? 146
4.2 Risikofrage: Wie darf in die Cloud ausgelagert werden? 148
5 Vorgehensweise zur Prüfung der Voraussetzungen 149
6 Übersicht Vorgaben 151
6.1 Rechtsfrage – Geheimnisse 151
6.2 Risikofrage – Art der Personendaten 151
7 Fazit 151
Literaturverzeichnis 152

1 EINLEITUNG

Cloud-Lösungen werden in immer mehr Bereichen eingesetzt, sowohl in privaten Unternehmen als auch bei öffentlichen Organen. Dafür gibt das Datenschutzrecht sowohl rechtliche als auch organisatorisch-technische Rahmenbedingungen vor. Dieser Beitrag beleuchtet die juristischen Vorgaben für öffentliche Organe (gem. Art. 5 lit. i DSG und auf kantonaler Ebene z.B. § 3 Gesetz über die Information und den Datenschutz des Kantons Zürich, LS 170.4 [IDG/ZH]), also Bundesorgane und öffentliche Organe in den Kantonen, die gleichzeitig auch als öffentliche Auftraggeber bzw. Beschaffungsbehörden auftreten, wenn die Cloud-Lösung auf dem privaten Markt im öffentlichen Beschaffungsprozess eingekauft wird.[1]

Die juristischen Vorgaben für öffentliche Organe bei der Auslagerung von Daten in die Cloud bleiben bei der Diskussion über den Einsatz von Cloud-Lösungen häufig im Hintergrund, was angesichts ihrer Relevanz für den Datenschutz als Grundrecht der Bürgerinnen und Bürger unhaltbar ist. Denn für die öffentlichen Organe ergeben sich spezifische Anforderungen aus dem öffentlichen Recht, die sich von jenen für private

[1] Im Folgenden wird deshalb entweder die datenschutzrechtliche Terminologie des «öffentlichen Organs» oder die beschaffungsrechtliche Terminologie der «Auftraggeber» oder «Beschaffungsbehörde» bedient.

Datenbearbeitende unterscheiden. Anhand der gesetzlichen Vorgaben führt dieser Beitrag Schritt für Schritt durch die Fragen, die sich für öffentliche Organe stellen, wenn sie Cloud-Lösungen öffentlich beschaffen, bzw. Daten in die Cloud an Dritte auslagern.[2]

2 CLOUD COMPUTING IST EINE AUFTRAGSDATENBEARBEITUNG

2.1 WAS IST CLOUD COMPUTING?

Aus technischer Perspektive ist Cloud Computing ein Netzwerk, auf das jederzeit und ortsungebunden zugegriffen werden kann. Es handelt sich um einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste), die mit minimalem Verwaltungsaufwand und minimaler Serviceprovider-Interaktion rasch bereitgestellt und freigegeben werden können. Cloud Computing ermöglicht damit insbesondere Flexibilität und Skalierbarkeit. Es gibt unterschiedliche Servicemodelle: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) und verschiedene Organisationsmodelle wie Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud (NIST, 2011; Blonski, 2022).

2.2 WAS IST EINE AUFTRAGSDATENBEARBEITUNG?

Im datenschutzrechtlichen Sinne liegt beim Beizug von Cloud-Dienstleistungen eine Auftragsdatenbearbeitung vor (gem. Art. 9 DSG und auch § 6 IDG/ZH), weil die Datenbearbeitung einem Dritten übergeben wird. Entsprechend sind die Vorgaben für die Auftragsdatenbearbeitung einzuhalten (Blattmann, 2021, Rz 1).

Wenn die öffentliche Hand sich also entscheidet, Cloud-Leistungen von externen Anbieterinnen einzukaufen, muss sie auch in der öffentlichen Ausschreibung beachten, dass die Vorgaben für die Auftragsdatenbearbeitung eingehalten werden. Wie bei jeder Auftragsdatenbearbeitung verbleibt auch bei der Auslagerung in eine Cloud das öffentliche Organ datenschutzrechtlich vollständig für die Datenbearbeitung verantwortlich. Eine

[2] Eine Abhandlung der verfassungs- und grundrechtskonformen Nutzung von Cloud-Diensten eines US-amerikanischen Anbieters durch öffentliche Organe findet sich in einem Gutachten, das für den Cloud-Einsatz in Gemeinden des Kantons Zürich erstellt wurde, siehe Schefer & Glass, 2023.

Auftragsdatenbearbeitung ist keine Datenbekanntgabe,[3] da die Auftragnehmerin eine Drittperson ist, die keine datenschutzrechtliche Verantwortung gegenüber denjenigen Personen hat, die von der Datenbearbeitungen des öffentlichen Organs betroffenen sind.[4]

Die Auftragnehmerin (bzw. die «Anbieterin» in der beschaffungsrechtlichen Terminologie) darf die Daten entsprechend nur so wie der öffentliche Auftraggeber/die Beschaffungsstelle bearbeiten und sie nicht für eigene Zwecke nutzen. Sie führt die Datenbearbeitung im Auftrag und nur auf Weisung des Auftraggebers durch. Dies gilt auch, wenn das Bearbeiten im Ausland stattfindet, wie dies bei der Inanspruchnahme von Cloud-Lösungen häufig der Fall ist (Privatim, 2022; Datenschutzbeauftragte des Kantons Zürich, 2022; Baeriswyl; 2019, S. 120). Geht eine Datenbearbeitung durch die Auftragnehmerin über das im Rahmen der Auslagerung Zulässige hinaus, z.B. wenn die Cloud-Anbieterin die Daten zu eigenen Zwecken nutzt, müsste dies von der Rechtsgrundlage des öffentlichen Organs gedeckt sein (Botschaft DSG, 7053; Epiney & Fasnacht, 2020, Rz 51 sowie Baeriswyl, 2019).

2.3 BESONDERE RISIKEN

Die Ausschreibung und Nutzung von Cloud-Lösungen bringt aus datenschutzrechtlicher Sicht besondere Risiken mit sich. Dazu gehört beispielsweise ungenügende Transparenz über die Bearbeitung von Personendaten durch die Cloud-Anbieterin, womit u.a. die Einhaltung der Zweckbindung nicht gewährleistet ist. Weitere Risiken sind erschwerte Kontrollmöglichkeiten, der Einfluss ausländischer Rechtsordnungen (wie beispielsweise der CLOUD-Act, siehe auch sogleich 3) und die Gewährleistung eines gleichwertigen Datenschutzes, die Portabilität der Daten und die Interoperabilität mit anderen Systemen sowie Datenverlust und Datenmissbrauch.

In der Praxis wird oft moniert, dass der Auftraggeber bei der Beschaffung von Cloud-Lösungen kaum Einflussmöglichkeiten auf das Angebot sowie die Ausgestaltung der

---

[3] Bei einer Datenbekanntgabe geht die datenschutzrechtliche Verantwortung für die Daten auf die Auftragnehmerin über. Zum Schutz der Grundrechte der betroffenen Personen, sind andere datenschutzrechtliche Rahmenbedingungen vorgesehen, die bei der Auftragsdatenbearbeitung nicht zur Anwendung kommen (vgl. Art. 36 DSG; z.B. §§ 16 und 17 IDG/ZH).

[4] Art. 9 DSG; z.B. § 6 IDG/ZH; Die Botschaft spricht davon, dass die Auftragnehmerin mit dem Beginn der vertraglichen Tätigkeit keine Drittperson mehr ist (Botschaft DSG, 7023).

Cloud-Lösung hat und sich entscheiden muss, das Angebot anzunehmen oder ganz darauf zu verzichten. In einer solchen Situation besteht die Gefahr, dass Rahmenbedingungen der Auslagerung insgesamt und im Besonderen bei der Bearbeitung von Personendaten Grundrechte und Persönlichkeitsrechte verletzt werden. Umso wichtiger ist es bei öffentlichen Beschaffungen, die oben genannten Risiken durch ein vollständiges Pflichtenheft, das alle datenschutzrechtlichen Anforderungen abdeckt und in die Ausschreibung aufnimmt, zu minimieren und somit auf die Ausgestaltung der Cloud-Lösung Einfluss zu nehmen.

3 WANN IST EINE AUFTRAGSDATENBEARBEITUNG IN DER CLOUD RECHTMÄSSIG?

Jede Datenbearbeitung muss rechtmässig – also unter Einhaltung aller rechtlicher Vorgaben – erfolgen, damit sie zulässig ist.[5] Für öffentliche Organe bedeutet dies insbesondere, dass das Legalitätsprinzip eingehalten sein muss, indem sich die Datenbearbeitung auf eine Rechtsgrundlage stützt. Neben dem Legalitätsprinzip sind durch die öffentlichen Organe des Weiteren die verfassungsmässigen Prinzipien und somit auch die Grundrechte einzuhalten und dürfen diese nicht unrechtmässig einschränken (Art. 36 der Bundesverfassung [BV, SR 101]). Diese verfassungsmässigen Vorgaben werden in den Datenschutzgesetzen sowie für einzelne Datenbearbeitungen in bereichsspezifische Gesetze konkretisiert und sind Teil der Rechtmässigkeit der Datenbearbeitung.

Für die Auftragsdatenbearbeitung, bei der ein Dritter im Auftrag des öffentlichen Organs die Daten bearbeitet (Art. 9 i.V.m. Art. 5 lit. k DSG; z.B. § 6 IDG/ZH.), bedeutet dies, dass aufgrund der spezifischen Risiken zusätzliche rechtliche Anforderungen gelten. Diese sind gesondert in den Datenschutzgesetzen festgehalten.[6]

Bei der Frage, ob eine Datenbearbeitung rechtmässig erfolgt, ist zudem die gesamte Rechtsordnung einzubeziehen, die im Rahmen einer Auftragsdatenbearbeitung involviert sein könnte. So beispielsweise auch ein Bezug zu ausländischem Recht: Sieht

---

5 Siehe dazu auch Dominika Blonski, Cloud – alles Risiko? Rechtliche Vorgaben für die Auslagerung von Datenbearbeitungen in die Cloud, in: SJZ 2023/20, S. 991 ff.

6 Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 4.

es z.B. vor, dass Behörden auf Daten zugreifen können, stellt sich die Frage, ob dieser Zugriff nach allgemein anerkannten rechtsstaatlichen Kriterien erfolgt (z.B. im Rahmen der internationalen Rechtshilfe). Ist dies nicht erfüllt und widerspricht eine ausländische Regelung beispielsweise dem ordre public der Schweiz – wie dies beim CLOUD Act[7] der USA der Fall ist[8] –, kann keine rechtmässige Auftragsdatenbearbeitung stattfinden, da ein rechtlicher Kontrollverlust stattfindet, der je nach Konstellation nicht kompensiert werden kann.[9] Dies ist bei der Auslagerung von Datenbearbeitungen an Cloud-Anbieterinnen, die dem US-amerikanischen Recht unterliegen, besonders zu beachten, denn diese können die Einhaltung des anerkannten internationalen Rechts nicht vorbehaltslos garantieren.

Bei öffentlichen Ausschreibungen von Cloud-Dienstleistungen hat die Beschaffungsstelle als Auftraggeberin diesen Umstand bei der Ausschreibung und somit bei der Wahl der Auftragnehmerin zu beachten. Nur so kann sie ihre rechtlichen Vorgaben einhalten.[10]

---

7 Clarifying Lawful Overseas Use of Data Act, abrufbar unter: <https://www.congress.gov/bill/115th-congress/ senate-bill/2383> (zuletzt besucht am 25.11.2023).

8 Der CLOUD Act ist ein Gesetz der USA, das es bestimmten US-Behörden ermöglicht, amerikanische Unternehmen zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, selbst wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Es handelt sich dabei somit um ein Gesetz mit extraterritorialer Wirkung. Dieses Verfahren und dieser Zugriff auf Daten ist mit dem Datenschutzrecht und dem übergeordneten schweizerischen Recht nicht vereinbar. Es verstösst gegen den ordre public der Schweiz, weil es eine Umgehung des internationalen Rechtshilfewegs darstellt (Bundesamt für Justiz, Bericht zum US CLOUD Act, 17. September 2021, S. 35).

9 Markus Schefer/Philip Glass, Der grundrechtskonforme Einsatz von M365 durch öffentliche Organe in der Schweiz. Eine Analyse am Beispiel des Kantons Zürich, S. 55 ff.

10 Im Zusammenhang mit dem CLOUD Act führt es nicht weiter, anhand einer Risikoanalyse mit Wahrscheinlichkeitsberechnung aufzuzeigen, dass der behördliche Zugriff unwahrscheinlich sei. Die Rechtsfrage kann damit nicht umgangen werden, denn ein öffentliches Organ hat das Recht immer zu beachten und sich rechtmässig zu verhalten («Legalitätsprinzip»). Zudem kann das Verhalten einer amerikanischen Strafbehörde mit einer Methode mit Wahrscheinlichkeitsberechnungen nicht vorausgesagt werden (Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 76.).

Im Ergebnis liegt eine rechtmässige – und damit zulässige – Datenbearbeitung vor, wenn alle rechtlichen Vorgaben eingehalten sind. Das heisst folglich, dass sich auch bei der Auftragsdatenbearbeitung primär rechtliche Fragen stellen.

4 WAS SIND DIE VORAUSSETZUNGEN EINER AUFTRAGSDATENBEARBEITUNG IN DER CLOUD?

Die Auslagerung von Datenbearbeitungen ist unter Einhaltung der spezifischen rechtlichen Vorgaben gemäss den Datenschutzgesetzen grundsätzlich zulässig. Dabei ist insbesondere zu beachten, dass die von der Datenauslagerung in die Cloud bzw. Auftragsdatenbearbeitung durch die Cloud-Anbieterin betroffenen Personen dadurch insgesamt nicht schlechter gestellt werden. Aufgrund der spezifischen Risiken, die bei der Auftragsdatenbearbeitung für die Grundrechte der betroffenen Personen bestehen, präzisieren die Datenschutzgesetze die Rahmenbedingungen für den Beizug einer Auftragsdatenbearbeiterin und geben kumulativ zwei Voraussetzungen für die Auslagerung vor (vgl. Art. 9 DSG, § 6 IDG/ZH).[11] Eine Auftragsdatenbearbeitung ist demnach zulässig und rechtmässig, wenn:

1. keine gesetzliche oder vertragliche Bestimmung der Auslagerung entgegensteht und
2. die datenschutzrechtliche Verantwortung durch den Auftraggeber wahrgenommen werden kann.

Diese beiden Voraussetzungen lassen sich in zwei Schritten abbilden, die einerseits rechtliche und andererseits organisatorisch-technische Anforderungen vorgeben:

In einem ersten Schritt ist zunächst die Rechtsfrage, das heisst die Rechtmässigkeit der Datenbearbeitung an sich, zu beantworten: **Darf ausgelagert werden?** Es ist somit zu prüfen, ob rechtliche Bestimmungen einer Auftragsdatenbearbeitung entgegenstehen. Entgegenstehende rechtliche Bestimmungen können beispielsweise Geheimhaltungspflichten, aber auch vertragliche Vereinbarungen, Klassifizierungen von Informationen oder weitere Regelungen sein (vgl. 4.1). Zur Rechtsfrage gehört aber auch die Prüfung, ob

[11] Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 4 f.

die Beschaffungsstelle/Auftraggeberin ihre Sorgfaltspflicht bei der Auswahl, Instruktion und Überwachung der Auftragnehmerin (analog Art. 55 Obligationenrecht [OR], SR 220) wahrnimmt. Zudem hat sie sicherzustellen, dass die Anbieterin/Auftragnehmerin die Daten nur so bearbeitet, wie es die Beschaffungsstelle selber auch tun dürfte. Um diese Verantwortungen wahrzunehmen, muss dies bereits in der Ausschreibung kommuniziert werden und die Einhaltung als Eignungskriterium eingefordert und nach dem Zuschlag vertraglich festgehalten werden.

Der zweite Schritt stellt die Beantwortung folgender Frage dar: **Wie darf ausgelagert werden?** Bei diesem Schritt – und nur hier – werden anhand einer klassischen Risikoanalyse angemessene organisatorisch-technische Massnahmen festgelegt (vgl. sogleich 4.2).

4.1 RECHTSFRAGE: DARF IN DIE CLOUD AUSGELAGERT WERDEN?

Damit eine Auftragsdatenbearbeitung rechtmässig erfolgt, ist zunächst die Rechtsfrage zu beantworten, ob rechtliche oder andere Bestimmungen der Auftragsdatenbearbeitung in einer Cloud-Lösung entgegenstehen.

Steht eine rechtliche oder andere Bestimmung entgegen, kann geprüft werden, ob technische Massnahmen eine rechtswidrige Kenntnisnahme der Personendaten durch die Cloud-Anbieterin verhindern können (Verschlüsselung mit Schlüsselmanagement beim öffentlichen Organ, Anonymisierung oder Pseudonymisierung mit Schlüssel zur Re-Identifizierung beim Auftraggeber) und, falls ja, dennoch ausgelagert werden kann.[12]

4.1.1 Stehen rechtliche Bestimmungen entgegen?

Im Rahmen einer Rechtsgrundlagenanalyse ist zunächst zu prüfen, ob rechtliche Bestimmungen einer Auslagerung entgegenstehen.[13]

---

[12] Wolfgang Wohlers, Auslagerung einer Datenverarbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten, 2015, S. 20; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 3.

[13] Astrid Epiney/Tobias Fasnacht, § 10 Besondere Grundsätze, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011,

4.1.1.1 Geheimhaltungspflichten

Ob eine Geheimhaltungspflicht einer Auftragsdatenbearbeitung entgegensteht, ist im Einzelfall zu eruieren. Bei dieser Prüfung spielt die Art der Personendaten keine Rolle, es geht einzig um die Frage des Geheimnisschutzes. Ob Geheimhaltungspflichten einer Auslagerung entgegenstehen, kann anhand folgenden zwei Fragen eruiert werden:

1. Was schützt das Geheimnis und wer ist somit «Geheimnisherr» oder «Geheimnisherrin»? Diese/r kann über das Geheimnis verfügen und entsprechend über die Durchbrechung der Geheimnispflicht entscheiden. Davon ist der/die GeheimnisträgerIn zu unterscheiden, der/die das Geheimnis zwar trägt, aber nicht darüber verfügen kann.
2. Findet mit der Auftragsdatenbearbeitung eine Offenbarung[14] des Geheimnisses statt? Eine Offenbarung findet nicht statt, wenn die Auftragnehmerin als Hilfsperson (im strafrechtlichen Sinne)[15] qualifiziert werden kann. Findet hingegen eine Offenbarung statt, ist die Auftragsdatenbearbeitung nicht zulässig, wenn die Geheimhaltungspflicht der Auslagerung entgegensteht.

So steht das im öffentlichen Arbeitsverhältnis geltende und strafbewehrte Amtsgeheimnis[16] einer Auslagerung grundsätzlich nicht entgegen. Denn beim Amtsgeheimnis ist die

---

N 46; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 34 ff.; Datenschutzbeauftragte des Kantons Zürich, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 5, abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 25.11.2023).

14 D.h. das Geheimnis wurde einer dazu nicht ermächtigten Drittperson zur Kenntnis gebracht (z.B. BGE 147 II 227, E. 7.3).

15 Da es bei der Auftragsdatenbearbeitung nicht auf die Haftung ankommt, ist der haftungsrechtliche Hilfspersonenbegriff (gemäss Art. 101 OR oder Art. 55 OR) nicht anwendbar. Es stellt sich vielmehr die Frage, ob ein Geheimnis aus strafrechtlicher Perspektive offenbart wird, wenn keine entsprechende Hilfspersonenqualität vorliegt.

16 Z.B. § 51 Personalgesetz des Kantons Zürich vom 27. September 1998 (PG/ZH), LS 177.10; Art. 320 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0 (wobei der Versuch strafbar ist (Art. 22 StGB) und damit bereits die Möglichkeit der Kenntnisnahme für die Bejahung der Strafbarkeit ausreicht (Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 43)).

öffentliche Hand Geheimnisherrin, da das Geheimnis primär die Funktionstüchtigkeit des Amtes schützt. Damit kann und muss das Amt selber darüber befinden, ob eine Information dem Amtsgeheimnis unterliegt oder nicht. Betroffene Personen werden nur geschützt, wenn ihre privaten Interessen einer Veröffentlichung überwiegen. Untersteht eine Information dem Amtsgeheimnis, ist durch den Auftraggeber zu prüfen, ob er mit der Auslagerung seine Verantwortung wahrnehmen kann. Ist dies der Fall, kann (und muss) das Amt der Auftragnehmerin bzw. deren Mitarbeitenden das Amtsgeheimnis vertraglich überbinden.[17]

Besondere (auch unter Art. 320 StGB oder direkt aus der spezialgesetzlichen Regelung strafbewehrte Amtsgeheimnisse, wie beispielsweise das Steuergeheimnis (z.B. § 120 Steuergesetz des Kantons Zürich, LS 631.1) oder das Sozialhilfegeheimnis (z.B. § 47 Sozialhilfegesetz des Kantons Zürich, LS 851.1), wurden geschaffen, weil in bestimmten Bereichen des Amtsgeheimnisses nicht nur die Funktionstüchtigkeit des Amtes an sich geschützt werden soll, sondern auch das Vertrauensverhältnis zwischen dem Amt und den betroffenen Personen. Entsprechend hat das Amt als Geheimnisherr bei der Entscheidung, ob eine Information dem besonderen Amtsgeheimnis unterliegt, die Interessen der betroffenen Personen einzubeziehen. Die besonderen Amtsgeheimnisse stehen daher einer Auslagerung grundsätzlich entgegen, wenn keine technische Lösung die Kenntnisnahme durch die Auftragnehmerin bzw. ihre Mitarbeitenden unterbindet, da mit der Auftragsdatenbearbeitung ein Offenbaren stattfindet.[18]

---

17 Entsprechend sieht die Strafbestimmung mit der Einwilligung der vorgesetzten Behörde nur einen Rechtfertigungsgrund vor und nicht auch die Einwilligung der betroffenen Person: Matthias Michlig, Öffentlichkeitskommunikation der Strafbehörden unter dem Aspekt der Amtsgeheimnisverletzung (Art. 320 StGB), in: ZStStr - Zürcher Studien zum Strafrecht Band/Nr. 68, 2013, S. 204; Matthias Michlig/Eva Wyler, Art. 320 Verletzung des Amtsgeheimnisses, in: Damian K. Graf (Hrsg.), StGB Annotierter Kommentar, 2020, Rn. 6; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 42 und 45.

18 Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 46 f. und 49.

Das ebenso strafbewehrte Berufsgeheimnis (z.B. § 15 Abs. 1 und 2 Gesundheitsgesetz des Kantons Zürich (GesG/ZH), LS 810.1; Art. 321 StGB). schützt die betroffene Person selber und damit auch das Vertrauensverhältnis zwischen dieser und der einer bestimmten Berufsgruppe zugehörigen Person. Geheimnisherr oder -herrin ist beim Berufsgeheimnis allein die betroffene Person. Entsprechend kann – anders als beim Amtsgeheimnis – nicht der Geheimnisträger oder die Geheimnisträgerin darüber befinden, ob dem Geheimnis unterliegende Informationen offenbart werden dürfen. Die Geheimhaltungspflicht kann nur im Einzelfall durchbrochen werden, wenn eine gesetzliche Bestimmung dies vorsieht, die betroffenen Person eingewilligt hat oder die vorgesetzte Behörde die Geheimhaltungspflicht aufgehoben hat. Anders als beim Amtsgeheimnis, ist beim Berufsgeheimnis die vertragliche Erweiterung des Kreises der Geheimnisträger durch den Geheimnisträger nicht möglich ist.[19] Bei einer Cloud-Lösung steht das Berufsgeheimnis somit einer Auslagerung grundsätzlich entgegen, es sei denn, eine technische Lösung verhindert die Kenntnisnahme durch die Auftragnehmerin bzw. ihre Mitarbeitenden.[20]

Geheimnis	**Schutz / Geheimnisherr**	**Offenbarung Geheimnis**
Amtsgeheimnis	Funktionstüchtigkeit Amt / Öffentliches Organ	Geheimnis vertraglich überbinden
Besondere Amtsgeheimnisse	Funktionstüchtigkeit Amt und Vertrauensverhältnis / Öffentliches Organ	Ja, stehen grundsätzlich entgegen, wenn keine technische Lösung
Berufsgeheimnis	Vertrauensverhältnis / Betroffene Person	Ja, steht grundsätzlich entgegen, wenn keine technische Lösung

[19] Dies, weil der strafrechtliche Hilfspersonenbegriff des Berufsgeheimnisses sehr eng gefasst ist.

[20] Wolfgang Wohlers, Auslagerung einer Datenverarbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten, 2015, S. 18 und 21 ff.; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 50 f. und 52 f.

4.1.1.2 Weitere Bestimmungen, die der Auslagerung entgegenstehen können

Auch vertragliche Vereinbarungen können der Auslagerung entgegenstehen. So kann der Auftraggeber beispielsweise mit der Auftragnehmerin vereinbaren, dass keine weiteren Unterauftragnehmenden beigezogen werden dürfen.[21]

Des Weiteren können Klassifizierungen der Auftragsdatenbearbeitung entgegenstehen. Das neue Informationssicherheitsgesetz des Bundes (ISG, SR 128) hält verschiedene Klassifikationen beispielsweise zum Schutz der Interessen der inneren und äusseren Sicherheit der Schweiz fest.

Schliesslich können weitere Bestimmungen einer Auslagerung entgegenstehen bzw. diese einschränken. So sieht beispielsweise die Verordnung über das elektronische Patientendossier (Art. 12 Abs. 5 Verordnung über das elektronische Patientendossier [EPDV, SR 816.11]) vor, dass sich die Datenspeicher, auf denen die Informationen des Patientendossiers abgelegt werden, in der Schweiz befinden müssen und dem Schweizer Recht zu unterstehen haben.

4.1.2 Ist die Wahrnehmung der Verantwortung möglich?

Da die öffentliche Auftraggeberin für die Datenbearbeitung verantwortlich bleibt, muss sie bei Auslagerungen – auch in die Cloud – ihre Verantwortung wahrnehmen können. Dies ist die zweite Voraussetzung für die Zulässigkeit der Auftragsdatenbearbeitung.

Dies erfordert zunächst die Wahrnehmung der Sorgfaltspflicht analog Art. 55 OR bei der Auswahl, Instruktion und Kontrolle der Auftragsnehmerin (Botschaft a-DSG, 463 f.).[22] Handelt es sich bei der Cloud-Auslagerung um eine öffentliche Beschaffung, darf bei der Ausschreibung nur eine Auftragnehmerin den Zuschlag erhalten, die die

---

21 Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 35 f.

22 Gemäss Botschaft zum alten DSG muss «Bei der Übertragung der Bearbeitung an einen Dritten [...] der Auftraggeber in Analogie zu Artikel 55 des Obligationenrechts alle gebotene Sorgfalt aufwenden, um Verstösse gegen das Datenschutzgesetz zu verhindern. Er muss den Auftragnehmer entsprechend auswählen, ihm die richtigen Instruktionen erteilen und ihn soweit als möglich auch überwachen.»

Anforderungen einhalten kann und die somit für die Auftragserfüllung geeignet ist.[23] Das öffentliche Organ hat dabei zu prüfen, wie die Auftraggeberin organisiert ist und wie sie arbeitet sowie in welchen (Rechts-)Umfeld sie sich befindet. Weiter muss das öffentliche Organ die Auftragnehmerin instruieren und sie bei der Aufgabenerfüllung überwachen. Das bedeutet, dass die Auftragnehmerin einem durchsetzbaren Weisungsrecht des Auftraggebers unterstehen muss. Zudem muss das öffentliche Organ jederzeit die Kontrollmöglichkeit haben, indem es überprüfen können muss, ob der Auftrag nach seinen Vorgaben und damit rechtskonform erfolgt.

Die Vorgaben, an die sich das öffentliche Organ zu halten hat, sind vertraglich auf die Auftragnehmerin zu übertragen.[24] Besonders hinzuweisen ist auf die Regelung der Vorgabe, dass die Auftragnehmerin die Daten nicht zu ihren eigenen Zwecken bearbeiten darf. Liegt keine Rechtsgrundlage für die Datenbekanntgabe durch das öffentliche

---

[23] Astrid Epiney/Tobias Fasnacht, § 10 Besondere Grundsätze, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011, N 43; Veronica Blattmann, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 16; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 2.

[24] Im Kanton Zürich sind die Grundzüge des Vertragsinhalts in der Verordnung über die Information und den Datenschutz festgehalten (§ 25 Verordnung über die Information und den Datenschutz des Kantons Zürich vom 28. Mai 2008 (IDV/ZH), LS 170.41; Datenschutzbeauftragte des Kantons Zürich, Leitfaden Bearbeiten im Auftrag, V 1.12 / August 2022, S. 8 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf> (zuletzt besucht am 25.11.2023).). Der Regierungsrat des Kantons Zürich hat die AGB Auslagerung Informatikleistungen (Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen des Kantons Zürich (AGB Auslagerung Informatikleistungen) vom 24. Juni 2015, abrufbar unter: <https://www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_auslagerung_informatikleistungen.pdf> (zuletzt besucht am 25.11.2023).) und die AGB Datenbearbeitung durch Dritte (Allgemeine datenschutzrechtliche Geschäftsbedingungen bei der Datenbearbeitung durch Dritte des Kantons Zürich (AGB Datenbearbeitung durch Dritte) vom 24. Juni 2015, abrufbar unter: <https:// www.zh.ch/content/dam/zhweb/bilder-dokumente/organisation/finanzdirektion/afi/agb_datenbearbeitung_ durch_dritte.pdf> (zuletzt besucht am 25.11.2023).) erlassen (RRB 2015/670 vom 24. Juni 2015.). Diese AGB sind durch die öffentlichen Organe der kantonalen Verwaltung in ihre Verträge einzubeziehen.

Organ an die Auftragnehmerin vor, ist eine Verwendung zu eigenen Zwecken durch die Auftragnehmerin strafbar..[25]

Schliesslich hat sich eine öffentliche Auftraggeberin zu vergewissern, dass die Auftragnehmerin in der Lage ist, die Datensicherheit zu gewährleisten. Sie hat dafür mittels einer Risikoanalyse festzuhalten, welche organisatorisch-technischen Massnahmen zu ergreifen sind und diese Verpflichtung der Auftragnehmerin vertraglich zu überbinden (siehe sogleich 4.2).

4.2 RISIKOFRAGE: WIE DARF IN DIE CLOUD AUSGELAGERT WERDEN?

Ergibt die Rechtsfrage, dass eine Auftragsdatenbearbeitung zulässig ist, stellt sich in einem letzten Schritt die organisatorisch-technische Frage der Umsetzung von angemessenen Massnahmen zum Schutz der Daten, also die Frage, wie ausgelagert werden darf.

Die Datenschutzgesetze sehen vor, dass Daten angemessen geschützt werden müssen.[26] Um die Angemessenheit von organisatorisch-technischen Massnahmen zu eruieren, wird eine Risikoanalyse durchgeführt. Welche Massnahmen angemessen sind, hängt von der Art der Daten ab. Die Risikoabwägung zeigt die zu ergreifenden angemessenen organisatorisch-technischen Massnahmen passend zur Art der Personendaten auf. Der Auftraggeber hat sich im Rahmen der Wahrnehmung seiner Verantwortung zu vergewissern, dass die Auftragnehmerin die notwendigen organisatorischen und technischen Massnahmen einhalten kann und damit die Datensicherheit gewährleisten kann – so wie wenn die Daten durch ihn selber bearbeitet würden.[27]

Im Rahmen der Risikoanalyse ist einzubeziehen, ob die Auslagerung in der Schweiz, in einem EU-Land oder in einem Land ohne angemessenes Datenschutzniveau stattfindet oder ob andere Rechtsordnungen Bestimmungen vorsehen, die sich auf die Auslagerung

---

[25] § 40 IDG/ZH; Bruno Baeriswyl, Wenn die Rechtsauslegung «nebulös» wird. Cloud-Computing in der Verwaltung verändert die Art und Weise der Datenbearbeitung – aber nicht das Recht, in: digma 2019, S. 119.

[26] Art. 8 DSG, z.B. § 7 IDG/ZH.

[27] Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 55.

auswirken können. Mit der Übermittlung von Personendaten ins Ausland im Rahmen der Auslagerung, steigen die Risiken für die Grundrechte der betroffenen Personen. Gleichzeitig steigen auch die Risiken für den Auftraggeber. Denn die sich im Ausland befindenden Daten sind einer dem Auftraggeber fremden Rechtsordnung ausgesetzt, deren Auswirkungen er nicht einschätzen kann. Damit werden Kontrollen durch den Auftraggeber erschwert, wobei er allenfalls weitere Massnahmen ergreifen muss. Keine zusätzlichen Massnahmen müssen hingegen ergriffen werden, wenn das Datenschutzniveau im konkreten Land dem schweizerischen Datenschutz angemessen ist – dies ist bei Anwendbarkeit der Konvention 108[28] der Fall.[29]

5 VORGEHENSWEISE ZUR PRÜFUNG DER VORAUSSETZUNGEN

Um die umschriebenen Schritte abzudecken, kann eine übliche Projektmethodik beigezogen werden (beispielsweise die beim Bund und beim Kanton Zürich verwendete Methode HERMES). Die im Rahmen dieser Vorgehensweise vorgesehenen Dokumente adressieren die sich stellenden Fragen.

So wird mit einer Rechtsgrundlagenanalyse die rechtliche Lage eruiert und bewertet. Sie beantwortet rechtliche Fragen, wie beispielsweise: Welche rechtlichen Grundlagen sind anwendbar? Welche Vorgaben halten diese fest? Welche Bestimmungen könnten einer Auftragsdatenbearbeitung entgegenstehen? Liegen Geheimnispflichten vor und was schützen diese? Welche ausländischen Regelungen haben auf die Auftragsdatenbearbeitung Einfluss?

Mit der Risikoanalyse werden die Risiken, deren Eintretenswahrscheinlichkeit sowie die Auswirkungen bzw. das Schadensausmass im Falle des Eintretens der Risiken eruiert und bewertet.

---

[28] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention 108), SR 0.235.1.

[29] § 19 IDG/ZH i.V.m. § 22 IDV/ZH; Veronica Blattmann, § 6 Bearbeiten im Auftrag, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Schulthess 2012, Rn. 27 f.; Bruno Baeriswyl, Art. 9, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar SHK, 2. Aufl., Stämpfli 2023, Rn. 65 ff.

Die Datenschutzgesetze geben für entsprechende Projekte zwei spezifische Schritte vor, die durch die öffentlichen Organe bei einer beabsichtigten Datenbearbeitung durchzuführen sind – auch bei der Absicht, eine Cloud-Lösung zu beschaffen. Damit ist zunächst eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Diese zeigt auf, ob im Anschluss das Projekt bei der Datenschutzbeauftragten zur Vorabkontrolle einzureichen ist (Art. 22 und Art 23 DSG; z.B. § 10 IDG/ZH). Beschaffungsstellen als öffentliche Organe sind verpflichtet, bei der Datenbearbeitung bestehende Risiken für die Grundrechte von Betroffenen zu identifizieren und mit geeigneten Massnahmen zu reduzieren. Diese können sie mit der Durchführung einer DSFA erkennen und bewerten.[30] In diesem Dokument definiert das öffentliche Organ zudem Massnahmen, um die Risiken zu reduzieren.

Weist die beabsichtigte Bearbeitung von Personendaten eines öffentlichen Organs besondere Risiken für die Grundrechte der betroffenen Personen auf, ist eine Vorabkontrolle durch die Datenschutzbeauftragten erforderlich.[31] In diesem Fall legt die Beschaffungsstelle das Projekt der oder dem jeweiligen Datenschutzbeauftragten vor. Diese prüft die rechtlichen, organisatorischen und technischen Rahmenbedingungen der beabsichtigten Datenbearbeitung und nimmt dazu Stellung. Sie hält insbesondere fest, welche weiteren Massnahmen zu ergreifen sind bzw. wie das Projekt datenschutzkonform umgesetzt werden kann.

Schliesslich sind immer auch alternative weitere Möglichkeiten der Datenbearbeitung zu evaluieren. So ist zu prüfen, ob eine On-premises-Lösung möglich wäre, ob eine hybride Cloud oder eine treuhänderische Cloud eingesetzt werden könnte, ob andere Produkte genutzt werden könnten oder ob eine eingeschränkte Nutzung des Produkts (beispielsweise Nutzung von nur einzelnen Diensten oder nur für einzelne Datenkategorien) möglich ist.

---

30 Datenschutzbeauftragte des Kantons Zürich, Merkblatt Datenschutz-Folgenabschätzung (DSFA), V 2.0 / Oktober 2023, S. 1 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_dsfa.pdf> (zuletzt besucht am 25.11.2023).

31 Datenschutzbeauftragte des Kantons Zürich, Merkblatt Vorabkontrolle, V 3.0 / Oktober 2023, S. 1 f., abrufbar unter: <https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_vorabkontrolle.pdf> (zuletzt besucht am 25.11.2023).

6 ÜBERSICHT VORGABEN

6.1 RECHTSFRAGE – GEHEIMNISSE

Amtsgeheimnis	Besondere Amtsgeheimnisse	Berufsgeheimnis
Steht grundsätzlich nicht entgegen	Stehen entgegen	Steht entgegen
Risikoanalyse und Festlegung organisatorisch-technischer Massnahmen	Technische Massnahmen, die Kenntnisnahme verhindern	Technische Massnahmen, die Kenntnisnahme verhindern

6.2 RISIKOFRAGE – ART DER PERSONENDATEN

Personendaten	Besondere Personendaten
Risikoanalyse und Festlegung organisatorisch-technischer Massnahmen	Technische Massnahmen, die Kenntnisnahme verhindern

7 FAZIT

Cloud Computing bringt als Auftragsdatenbearbeitung spezifische Risiken mit sich. Während sich das öffentliche Beschaffungsrecht dazu nicht äussert, sehen die Datenschutzgesetze aus diesem Grund klare Voraussetzungen für die grundsätzlich zulässige Auftragsdatenbearbeitung vor, denn die Verantwortung verbleibtauch bei der Auslagerung in die Cloud beim öffentlichen Auftraggeber.

Damit rechtmässig in die Cloud ausgelagert werden kann, müssen zwei rechtliche Voraussetzungen erfüllt sein: Es dürfen der Auslagerung keine rechtlichen Bestimmungen entgegenstehen und die datenschutzrechtliche Verantwortung des Auftraggebers muss wahrgenommen werden können.

Zur Einhaltung der ersten Bedingung hat das öffentliche Organ zu prüfen, ob das Amtsgeheimnis, ein besonderes Amtsgeheimnis oder das Berufsgeheimnis oder ob vertragliche Vereinbarungen, eine Klassifizierung von Informationen oder weitere Regelungen der Auslagerung entgegenstehen. Ist dies der Fall, kann geprüft werden,

ob eine technische Massnahme die Kenntnisnahme verhindern kann (beispielsweise, wenn die Informationen verschlüsselt werden und das Schlüsselmanagement beim öffentlichen Organ verbleibt, wenn die Personendaten anonymisiert oder pseudonymisiert werden) und dennoch ausgelagert werden kann. Andernfalls ist auf die Auslagerung in die Cloud bzw. auf die Beschaffung der Cloud-Lösung zu verzichten, weil diese nicht rechtmässig erfolgt.

Die zweite Voraussetzung sieht vor, dass das öffentliche Organ bei der Auswahl, Instruktion und Kontrolle der Auftragsnehmerin seine Sorgfaltspflicht wahrnimmt, die Vorgaben vertraglich auf die Auftragnehmerin weitergibt und sich vergewissert, dass die Auftragnehmerin die notwendigen organisatorischen und technischen Massnahmen einhalten kann. Sind diese beiden Voraussetzungen erfüllt und kann damit die Rechtsfrage, ob ausgelagert werden darf, bejaht werden, stellt sich die zweite Frage, wie ausgelagert werden darf. Um diese Frage zu beantworten, muss die Projektleitung bei öffentlichen Beschaffungen von Cloud-Dienstleistungen eine Risikoanalyse anhand der Art der Daten durchführen und angemessene organisatorisch-technische Massnahmen festlegen. Wenn dies umgesetzt wird, erfolgt die Auftragsdatenbearbeitung in der Cloud rechtmässig und die Cloud-Dienstleistungen dürfen öffentlich ausgeschrieben werden.

LITERATURVERZEICHNIS

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 7023.

Baeriswyl, B. (2019). Wenn die Rechtsauslegung «nebulös» wird. Cloud-Computing in der Verwaltung verändert die Art und Weise der Datenbearbeitung – aber nicht das Recht (S. 118 – 122). digma.

Blonski, D. (2021). Cloud Computing. Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich. In A Epiney & S Rovelli (Hrsg.), *Künstliche Intelligenz und Datenschutz. L'intelligence artificielle et protection des données* (S. 65 – S. 80),

Tagungsband zum Dreizehnten Schweizerischen Datenschutzrechtstag, 2. Oktober 2020. Schulthess.

Datenschutzbeauftragte des Kantons Zürich. (2022). Merkblatt Cloud Computing (V 1.6). https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf>

Privatim. (2022). Merkblatt Cloud-spezifische Risiken und Massnahmen. https://www.privatim.ch/wp-content/uploads/2022/02/privatim_Cloud-Merkblatt_v3_0_20220203_def._DE-1.pdf> (zuletzt besucht am 25.11.2023)

Schefer, M. & Glass, Ph. (2023). Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich. Edition Weblaw.

Blattmann, V. (2012). § 6 Bearbeiten im Auftrag. In Baeriswyl, B. & Rudin, B. (Hrsg.*). Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich.* Schulthess.

NIST (National Institute of Standards and Technology). (2011). *The NIST Definition of Cloud Computing* (Special Publication 800-145). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

GEMEINSAME BESCHAFFUNGEN – MÖGLICHKEITEN UND GRENZEN

Martin Zobl

Martin Zobl ist Partner bei Walder Wyss.

Abstract: *Gemeinsame Beschaffungen öffentlicher Auftraggeber kommen immer häufiger vor – mit der zunehmenden Digitalisierung der Verwaltung vor allem auch im IT-Bereich. Sie können sowohl auftraggeber- als auch auftragnehmerseitig zu Effizienz- und somit Kostengewinnen führen und den Aufwand reduzieren. Allerdings bergen gemeinsame Beschaffungen, vor allem interkantonale und interföderative, viele Herausforderungen juristischer, projektplanerischer und finanzieller Art. Der vorliegende Artikel zeigt, welche gemeinsamen Beschaffungsformen es gibt und worauf öffentliche Auftraggeber besonders achten sollten.*

INHALTSVERZEICHNIS

Einleitung 156
Rechtsgrundlagen 157
Ausgestaltung 159
Bezugspflicht vs. optionale Bezüge 161
Transparenz im Aussenauftritt 162
Regelung des Innenverhältnisses 163
Anwendbares Recht 163
Kartellrechtliche Schranken 165
Schluss 167
Literaturverzeichnis 168

EINLEITUNG

Schliessen sich mehrere öffentliche Auftraggeber für eine Beschaffung zusammen, spricht man von gemeinsamen Beschaffungen. Gemeinsame Beschaffungen kommen in verschiedensten Bereichen vor. Zu denken ist etwa an den Einkauf einheitlicher IT-Lösungen durch Kantonsverwaltungen und Schulen, die interkommunale Beauftragung von Abfallentsorgungs- oder Altkleidersammelunternehmen oder die gemeinsame Bestellung von Rollmaterial durch Eisenbahnunternehmen. Eines der bekannteren Beispiele aus jüngerer Zeit bildet eOperations. Diese von der öffentlichen Hand gehaltene Organisation ist u.a. zuständig für die zentrale Beschaffung von Telekommunikations- und Informatiklösungen für öffentliche Auftraggeber.[1]

Potenzial und Vorteile gemeinsamer Beschaffungen liegen auf der Hand (vgl. auch Pfändler & Koch, 2023). Sie bestehen insbesondere in der Nachfragebündelung, die im Vergleich zu individuellen Beschaffungen einzelner Auftraggeber vorteilhaftere Konditionen und insgesamt Effizienzgewinne erwarten lässt. Zudem versprechen gut geplante gemeinsame Beschaffungen eine Aufwandreduktion sowohl im Vergabeprozess als auch im Vertragshandling. Idealerweise profitieren die beteiligten Auftraggeber gegenseitig von der vorhandenen Expertise, etwa wenn es um die Ausarbeitung des Pflichtenhefts geht. Nicht selten sind gemeinsame Beschaffungen vom Wunsch nach einem gemeinsamen Anbieter bzw. Produkt getragen, z.B. mit Blick auf eine über die Beschaffung hinausgehende Zusammenarbeit oder die Systemkompatibilität im Rahmen des Informationsaustauschs.

Trotz dieser und weiterer Vorteile wird das Instrument der gemeinsamen Beschaffung immer noch eher selten genutzt. Mögliche Gründe mögen im Initial- und Koordinationsaufwand solcher Projekte sowie im Wunsch nach einer individuellen, auf die spezifischen Bedürfnisse des Auftraggebers zugeschnittenen Leistung liegen. Zuweilen ist auch ein gewisses «Konkurrenzdenken» der beteiligten Auftraggeber zu beobachten, gerade

[1] Vgl. die Informationen unter https://www.eoperations.ch/eoperations-schweiz/mission-organisation/. Weitere nennenswerte Institutionen im Kontext gemeinsamer Digitalisierungsvorhaben sind der Verein Schweizerische Städte- und Gemeindeinformatik (SSGI), der u.a. Beschaffungsvorhaben für Schweizer Städte und Gemeinden durchführt, und der Verein OneGov.ch, einem Zusammenschluss von Kantonen, Gemeinden und Fachpartnern im Bereich E-Government.

wenn es sich um dezentrale Verwaltungsträger oder private Organisationen handelt (z.B. Sektorunternehmen gem. Art. 4 Abs. 2 des Bundesgesetzes über das öffentliche Beschaffungswesen [BöB] und der Interkantonalen Vereinbarung über das öffentliche Beschaffungswesen [IVöB] oder private Träger öffentlicher Aufgaben gem. Art. 4 Abs. 4 IVöB). Nicht zuletzt dürften mangelnde Erfahrung und Rechtsunsicherheiten im Umgang mit gemeinsamen Beschaffungen öffentliche Auftraggeber davon abhalten, zu diesem vielversprechenden Mittel zu greifen.

In diesem Beitrag werden die (vergaberechtlichen) Möglichkeiten und Grenzen gemeinsamer Beschaffungen beleuchtet.

RECHTSGRUNDLAGEN

Zulässigkeit und Modalitäten von gemeinsamen Beschaffungen sind im internationalen Recht (WTO-Recht und bilaterales Abkommen zwischen der Schweiz und der EU)[2] gar nicht und auf Stufe Bund (im BöB) und Kantone (in der IVöB) nur punktuell geregelt. BöB und IVöB enthalten in Art. 5 Abs. 1 und 2 Bestimmungen zum anwendbaren Recht, falls sich Auftraggeber auf Stufe Bund und Kanton oder Auftraggeber unterschiedlicher Kantone an einer Beschaffung beteiligen (siehe dazu auch Kapitel 7). Gesetz- und Konkordatsgeber gehen somit von der grundsätzlichen Zulässigkeit gemeinsamer Beschaffungen aus, haben jedoch im Sinne der gesetzgeberischen Tradition der Schweiz darauf verzichtet, eine detaillierte Regelung dieses Instruments zu erlassen. Da zudem kaum einschlägige Gerichtspraxis zu verzeichnen ist, sind gemeinsame Beschaffungen mit gewissen Rechtsunsicherheiten behaftet, die gleichzeitig Handlungsspielräume eröffnen.

Immerhin normiert die Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (Org-VöB) zentrale Beschaffungen von Gütern und Dienstleistungen für die zentrale Bundesverwaltung sowie gewisse dezentrale Verwal-

[2] Gemeint sind insbesondere das revidierte Übereinkommen über das öffentliche Beschaffungswesen (GPA 2012) und das Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über bestimmte Aspekte des öffentlichen Beschaffungswesens (BilatAbk CH-EU).

tungseinheiten (gem. Art. 1 Abs. 2 Org-VöB).[3] Die Kantone kennen analoge Regelungen für zentrale Beschaffungen ihrer Verwaltungen. Diese Regelwerke können Anhaltspunkte für gemeinsame Beschaffungen auch ausserhalb ihres Anwendungsbereichs bieten.

Beachtenswert ist der Leitfaden für interkantonale Submissionen der Zentralschweizer Baudirektorenkonferenz, ZBDK (Leitfaden ZBDK, 2006). Wie der Name sagt, handelt es sich um unverbindliche Empfehlungen für öffentliche Auftraggeber der Zentralschweizer Kantone. Zwar stammt der Leitfaden aus dem Jahr 2006 und bezog sich insofern auf die frühere IVöB 1994/2001. Und gleich wie die heutige gesetzliche Regelung in Art. 5 BöB/IVöB behandelt der Leitfaden schwergewichtig die Frage des anwendbaren Rechts. Gleichzeitig enthält er jedoch in einem «Praktischen Teil» wertvolle allgemeine Hinweise rund um interkantonale (und damit gemeinsame) Submissionen, etwa zum Ablauf solcher Beschaffungen, den Mitwirkungsmöglichkeiten der beteiligten Auftraggeber und zur Transparenz gegenüber den Anbietern.

Im Vergleich zum schweizerischen Recht sind gemeinsame Beschaffungen im europäischen Recht etwas ausführlicher geregelt. Art. 37 ff. der sog. klassischen Vergaberichtlinie (RL 2014/24/EU) unterscheiden zwischen Beschaffungstätigkeiten zentraler Beschaffungsstellen, der gelegentlichen gemeinsamen Auftragsvergabe öffentlicher Auftraggeber und der Auftragsvergabe durch öffentliche Auftraggeber aus verschiedenen Mitgliedstaaten.[4] Diese letztgenannte Möglichkeit der grenzüberschreitenden bzw. internationalen Submission ist im schweizerischen Recht bislang nicht (explizit) vorgesehen. Im Rahmen der Vergaberechtsrevision wurde es verpasst, eine entsprechende Regelung einzuführen.

Mangels detaillierter gesetzlicher Vorschriften kommt bei gemeinsamen Vergaben den allgemeinen verwaltungs- und vergaberechtlichen Grundsätzen eine besondere Bedeutung zu. Eine vorrangige Rolle spielen die Gebote der Transparenz und der Gleichbehandlung der Anbieter. Weitere Pflichten können sich aus dem Willkürverbot und dem Grundsatz von Treu und Glauben ergeben. So sind den Anbietern etwa der Verfahrensablauf (z.B. Genehmigungsvorbehalte) und die Zuständigkeiten der beteiligten

---

[3] Die Beschaffung von Bauleistungen richtet sich nach der Verordnung vom 5. Dezember 2008 über das Immobilienmanagement und der Logistik des Bundes (VILB); vgl. Art. 1 Abs. 3 Org-VöB.

[4] Vgl. auch §4 der deutschen Vergabeverordnung (gelegentliche gemeinsame Auftragsvergabe; zentrale Beschaffung).

Auftraggeber genauso wie das resultierende Vertragskonstrukt (Mehrparteienvertrag, Rahmenvertrag mit Abrufmöglichkeit der beteiligten Auftraggeber etc.) transparent zu kommunizieren (siehe auch nachfolgend, Kapitel 5).

AUSGESTALTUNG

Die rechtskonforme Konzeption und Abwicklung gemeinsamer Beschaffungen liegen in der Verantwortung der jeweiligen öffentlichen Auftraggeber. Sie verfügen dabei trotz und gerade wegen der bloss rudimentären gesetzlichen Regelung über viel Gestaltungsspielraum. Insbesondere besteht keine vorgegebene Typologie zulässiger Kooperationsformen. Gemeinsame Beschaffungen sind möglich zwischen Auftraggebern unterschiedlicher Staatsebenen (Gemeinden, Kantone, Bund; sog. interföderative Beschaffungen). Auch spricht aus vergaberechtlicher Sicht nichts Grundsätzliches gegen gemeinsame Vergaben von zentralen Verwaltungsbehörden und dezentralen Verwaltungsträgern mit eigener Rechtspersönlichkeit (z.B. Aufsichtsorgane, Stiftungen, Hochschulen oder Forschungsinstitute), genauso wenig wie gegen Kooperationen zwischen Sektorenauftraggebern oder anderen privatrechtlichen Organisationen, die dem Beschaffungsrecht unterstellt sind (z.B. Listenspitäler). Vorbehalten bleiben spezialgesetzliche Regelungen und kartellrechtliche Schranken (siehe zu Letzterem, Kapitel 8, Kartellrechtliche Schranken).

Auf organisatorischer Ebene lassen sich zwei Grundmodelle unterscheiden (vgl. auch Lutz, 2014, S.2):

Bei einer spontanen gemeinsamen Beschaffung schliessen sich mehrere Auftraggeber (in der Regel *ad hoc*) zusammen, um einen gemeinsamen Bedarf zu decken. Definiert wird ein sog. federführender Auftraggeber, welcher die Beschaffung als Beschaffungsstelle im Namen und Auftrag der anderen Auftraggeber und insofern als deren (direkter) Stellvertreter abwickelt. Der Zuschlag wird im Namen der beteiligten Auftraggeber erteilt und der daraus resultierende Vertrag wird zwischen dem Anbieter und allen beteiligten Auftraggebern abgeschlossen. Angesichts der gemeinsamen Beschaffungstätigkeit erscheint es als konsequent, diesen Vertrag als multilateralen Vertrag (Mehrparteienvertrag) auszugestalten. Allerdings spricht nach meinem Dafürhalten auch nichts dagegen, dass jeder beteiligte Auftraggeber einen eigenen Vertrag mit dem Zuschlagsempfänger

abschliesst, solange dies im Rahmen der Ausschreibung transparent kommuniziert wird und so der Aufwand für die Anbieter vorherseh- und kalkulierbar ist.[5]

Ein alternatives Modell besteht in der gemeinsamen Beschaffung über eine zentrale bzw. gemeinsame Beschaffungsstelle, die etwa als Verein oder Aktiengesellschaft ausgestaltet wird. Die zentrale Beschaffungsstelle ist in dem Sinne institutionalisiert, als es zu ihren vertraglich definierten Aufgaben gehört, regelmässig Beschaffungen für (andere) öffentliche Auftraggeber abzuwickeln.[6] Typischerweise tritt die zentrale Beschaffungsstelle als indirekte Stellvertreterin der beteiligten Auftraggeber auf, was bedeutet, dass sie in eigenem Namen, aber auf fremde Rechnung handelt.[7] In dieser Funktion schliesst sie mit den Zuschlagsempfängerinnen Rahmenverträge ab, die idealerweise so ausgestaltet sind, dass alle Auftraggeber im Bedarfsfall Bezugs- bzw. Einzelverträge direkt mit den Zuschlagsempfängerinnen abschliessen können, ohne den Umweg über die zentrale Beschaffungsstelle nehmen zu müssen. Diesem Modell folgt etwa die eingangs erwähnte Organisation eOperations: Unter den von eOperations abgeschlossenen Rahmenverträgen können die Bedarfsträger direkt Leistungen abrufen.

Um *keine* gemeinsame Beschaffung im hier verstandenen Sinn handelt es sich bei einer Vergabe mehrerer Bedarfsträger innerhalb derselben juristischen Person über eine zentrale Beschaffungsstelle. Dies ist z.B. der Fall, wenn Bundesämter gemeinsame Beschaffungen über eine der vier zentralen Beschaffungsstellen (z.B. Bundesamt für Bauten und Logistik [BBL]) gemäss Org-VöB abwickeln. Bei Lichte betrachtet handelt hier nämlich ein- und derselbe Rechtsträger, die Schweizerische Eidgenossenschaft. Dies gilt sowohl für den Beschaffungsprozess selbst als auch den Vertragsschluss, bei welchem immer die Schweizerische Eidgenossenschaft (handelnd durch eine Bundesbehörde) Auftraggeberin ist.

---

5 Anders wohl Leitfaden ZBDK, Abschnitt C 1.2.

6 Vgl. Art. 2 Ziff. 16 RL 2014/24/EU, der zentrale Beschaffungsstellen definiert «als öffentliche[r] Auftraggeber, der zentrale Beschaffungstätigkeiten und eventuell Nebenbeschaffungstätigkeiten ausübt.»

7 Dabei ist nicht ausgeschlossen, dass die zentrale Beschaffungsstelle selbst als Bedarfsträgerin fungiert, d.h. (auch) für eigene Zwecke beschafft.

BEZUGSPFLICHT VS. OPTIONALE BEZÜGE

Öffentliche Auftraggeber haben regelmässig ein Interesse an grösstmöglicher Flexibilität beim Leistungsbezug. Zudem ist das Beschaffungsvolumen umso schwieriger zu bestimmen, je grösser der Kreis der beteiligten Auftraggeber ist. Für die Anbieter stehen demgegenüber die Planungs- und Kalkulationssicherheit im Vordergrund, weshalb ihnen an einer möglichst präzisen Leistungsbeschreibung auch in quantitativer Hinsicht gelegen ist. Von diesem Dilemma sind gemeinsame Beschaffungen regelmässig geprägt.

Es entspricht der Vergabepraxis und wird in der Lehre mehrheitlich anerkannt, dass Rahmenverträge ohne (Mindest-)Bezugspflicht der Auftraggeber ausgeschrieben werden dürfen (Beyeler, 2012, Rz. 2927; Cordey, 2021, S. 362. ff.; Zwischenentscheid des BVGer B-3238/2021, E.5.4.3). Der Bundesrat hat in der Botschaft zum revidierten BöB ebenfalls auf diese Möglichkeit hingewiesen (vgl. Botschaft BöB, S. 1936 zu Art. 25 Abs. 1 BöB). Auch eine Exklusivitätszusage der beteiligten Auftraggeber gegenüber der Zuschlagsempfängerin stellt nach der hier vertretenen Meinung keine zwingende Anforderung dar, solange die fehlende Exklusivität transparent ausgewiesen wird (anderer Meinung Lutz, 2014, S.2).

Trotz dieser Freiheiten gebieten es die vergaberechtlichen Grundprinzipien des Wettbewerbs und der Transparenz, dass eine Ausschreibung auf einem konkreten Bedarf beruht, der gewissenhaft geschätzt und gegenüber den Anbietern kommuniziert wird. Vergabeverfahren dienen nach gesetzlicher Konzeption der spezifischen Bedarfsdeckung, nicht der Aushandlung abstrakter Konditionen im Sinne von reinen «terms and conditions». Um den Anbietern eine seriöse Angebotserstellung zu ermöglichen und die Wirtschaftlichkeit der Beschaffung zu fördern, ist für jede Ausschreibung zu prüfen, ob den Anbietern wenigstens ein verbindliches Mindestvolumen («Grund- bzw. Sockelleistung» bzw. Fixum) zugesichert werden kann. Dies verschafft ihnen eine gewisse Planungssicherheit und ermutigt sie, wirtschaftliche Konditionen anzubieten. Allerdings bedingt dies eine vorgängige Verständigung der beteiligten Auftraggeber über die Verteilung dieser Grundleistung. Wird auf eine Mindestbezugsmenge verzichtet, empfiehlt sich zumindest eine Rabattstaffelung (schrittweise Preisreduktion bei zunehmendem Volumen).

TRANSPARENZ IM AUSSENAUFTRITT

Bei gemeinsamen Beschaffungen ist dem Transparenzgrundsatz besondere Beachtung zu schenken. Für Anbieter macht es aus naheliegenden Gründen einen grossen Unterschied, ob sie für einen, zwei oder mehrere Auftraggeber anbieten. Bei der Offertstellung ist es wichtig zu wissen, wer die zukünftigen Vertragspartner und Bedarfsstellen sind bzw. wer Leistungen nach welchen verfahrensrechtlichen Modalitäten abrufen kann. Nebst dem Transparenzgrundsatz gebietet die Pflicht zur vollständigen und klaren Leistungsbeschreibung die Bekanntgabe aller leistungsrelevanten Aspekte, wozu auch die Identität der zukünftigen Vertragspartner gehört. Auch das europäische Vergaberecht ist in dieser Hinsicht streng und sieht vor, dass die Parteien einer Rahmenvereinbarung beim Vertragsschluss eindeutig identifizierbar sind.[8]

Der Kreis und die Rolle der (potenziell) beteiligten Auftraggeber müssen daher vor jeder Beschaffung geklärt und den Anbietern in den Ausschreibungsunterlagen bekannt gegeben werden. Insbesondere muss definiert sein, wer federführende Vergabestelle bzw. zentrale Beschaffungsstelle, wer zukünftiger Vertragspartner und wer Leistungsbezüger (Bedarfsträger) ist. Der nachträgliche Beitritt von im Ausschreibungszeitpunkt unbekannten Auftraggebern lässt sich mit den erwähnten Grundsätzen kaum vereinbaren.[9]

Gleich wie bei «gewöhnlichen» Beschaffungen sind im Ausschreibungszeitpunkt das (maximale) Auftragsvolumen, eine allfällige Mindestbezugspflicht sowie ggf. eine Rabattstaffelung anzugeben. Beteiligen sich Auftraggeber aus mehreren Kantonen bzw. unterschiedlicher Staatsebenen an einer Beschaffung, ist im Falle einer Rechtswahl nach Art. 5 Abs. 2 BöB/IVöB auf das anwendbare Recht hinzuweisen (siehe auch Kapitel 7, Anwendbares Recht). Nicht zu vergessen sind schliesslich weitere Besonderheiten gemeinsamer Beschaffungen wie etwa allfällige Genehmigungsvorbehalte, Erfüllungsorte sowie Bezugs- und Abrufmodalitäten bei Rahmenverträgen.

---

8 Dies kann entweder durch namentliche Nennung oder durch andere Mittel geschehen, wie beispielsweise eine Bezugnahme auf eine bestimmte Kategorie von öffentlichen Auftraggebern innerhalb eines klar abgegrenzten geografischen Gebiets. Vgl. Art. 33 Abs. 2 und E. 60 RL 2014/24/EU.

9 Vgl. zum europäischen Vergaberecht KLINKMÜLLER, S. 40 m.H. auf VK Düsseldorf Beschluss vom 23.05.2008. VK-07/2008-L.

REGELUNG DES INNENVERHÄLTNISSES

So wichtig die Kommunikation im Aussenverhältnis, so entscheidend die Organisation und Regelung des Innenverhältnisses zwischen den beteiligten Auftraggebern. Basis einer erfolgreichen gemeinsamen Beschaffung bildet die sorgfältige Projektplanung, welche die Kompetenzen verteilt und die wichtigsten Verfahrensschritte regelt. Es wird daher dringend empfohlen, das Verhältnis zwischen den beteiligten Auftraggebern und die Eckpfeiler des Projekts im Rahmen eines Kooperationsvertrags zu regeln. Vertragsstruktur und -inhalt sowie Regelungsdichte hängen von Natur und Komplexitätsgrad der Beschaffung sowie von den Beteiligten ab.

Punkte, über die sich die Vertragspartner im Innenverhältnis verständigen sollten, umfassen u.a. den Ausschreibungsgegenstand, die Eckdaten des Beschaffungsverfahrens (Verfahrensart, Zeitplan, Abrufmodalitäten etc.) sowie des abzuschliessenden Auftrags (idealerweise einen Vertragsentwurf), die Kompetenzverteilung bzw. die Rechte und Pflichten der beteiligten Auftraggeber inkl. Informations- und Auskunftsrechte, die Bevollmächtigung der federführenden Vergabestelle bzw. zentralen Beschaffungsstelle zur Durchführung des Verfahrens und ggf. zum Vertragsschluss sowie das Entgelt für deren Leistungen.

Bei längerfristigen Kooperationen, die auf regelmässige gemeinsame Beschaffungen über eine zentrale Beschaffungsstelle abzielen (siehe dazu auch Kapitel 3), bietet es sich an, die Grundzüge der Zusammenarbeit in einem Rahmen- bzw. Dachvertrag zu regeln. Dieser Dachvertrag bildet die Grundlage für die Durchführung einzelner Beschaffungsprojekte, deren Modalitäten in Einzelverträgen spezifiziert werden.

ANWENDBARES RECHT

Eine weitere wesentliche Frage bei gemeinsamen Beschaffungen betrifft das anwendbare Recht. Diese Frage stellt sich immer dann, wenn Auftraggeber aus unterschiedlichen Kantonen oder unterschiedlicher föderativer Stufen miteinander kooperieren. Art. 5

Abs. 1 und 2 BöB bzw. Art. 5 Abs. 1 bis 3 IVöB regeln diese sog. Kollisionssachverhalte (Aufeinandertreffen verschiedener Rechtsordnungen) in detaillierter Weise.[10]

Die Bestimmung des auf eine konkrete Beschaffung anwendbaren Rechts bleibt trotz der mit der Vergaberechtsrevision erfolgten schweizweiten Harmonisierung von Bedeutung. Denn zum einen handelt es sich um eine zwar weitgehende, jedoch nicht vollständige Harmonisierung: Nach wie vor bestehen gewisse Unterschiede nicht nur zwischen dem (für Bundesvergaben geltenden) BöB und der (auf kantonale Vergaben anwendbaren) IVöB, sondern auch zwischen den Ausführungserlassen der 26 Kantone, d.h. den kantonalen Beitrittsgesetzen und Submissionsverordnungen. Diese Unterschiede umfassen etwa die Teilnahmebedingungen, die Zuschlagskriterien oder die Ausnahmen i.S.v Art. 10 IVöB (vgl. auch die in Art. 63 Abs. 4 erwähnten Restzuständigkeiten der Kantone).

Zum anderen kommt in Beschaffungsverfahren subsidiär zum Vergaberecht immer das allgemeine Verwaltungsverfahrensrecht zur Anwendung, d.h. bei Bundesvergaben insbesondere das Verwaltungsverfahrensgesetz (VwVG)[11] und bei kantonalen Vergaben das entsprechende Verwaltungsrechtspflegegesetz. Dies gilt nicht nur für das (erstinstanzliche) Verfügungs- bzw. Beschaffungsverfahren selbst, sondern auch und umso mehr für das verwaltungsgerichtliche Rechtsmittelverfahren. Denn der Rechtsweg und damit die zuständige Beschwerdeinstanz hängen vom anwendbaren Recht ab. Untersteht eine Beschaffung dem BöB, ist das Bundesverwaltungsgericht als erste Rechtsmittelinstanz zuständig, während Beschwerden gegen kantonalrechtliche Vergaben in der Regel an das zuständige kantonale Verwaltungsgericht zu erheben sind (Art. 52 Abs. 1 BöB und IVöB).

Ungeachtet der gesetzlichen Regelung der «Kollisionssachverhalte» enthält das revidierte Vergaberecht eine ausdrückliche Rechtswahlklausel (Art. 5 Abs. 2 BöB und Art. 5 Abs. 3 IVöB) für interkantonale oder interföderative Vergaben. Danach sind die Auftraggeber

---

[10] Art. 5 Abs. 5 IVöB, wonach eine Beschaffung «durch eine gemeinsame Trägerschaft» dem Recht am Sitz der Trägerschaft untersteht, ist nach meinem Dafürhalten für die meisten Konstellationen gemeinsamer Beschaffungen nicht anwendbar.

[11] Im Bund kommt etwa kraft des Verweises von Art. 55 BöB das VwVG zur Anwendung, in den Kantonen nach Massgabe von Art. 55 IVöB die kantonalen Gesetze über die Verwaltungsrechtspflege.

im gegenseitigen Einvernehmen befugt, eine gemeinsame Beschaffung dem Recht eines beteiligten Auftraggebers zu unterstellen. Bei diesem Entscheid kommt ihnen ein Auswahlermessen zu, in welches die (Verwaltungs-)Gerichte unter Vorbehalt des Willkürverbots bzw. missbräuchlicher Ermessensausübung nicht eingreifen können (Art. 56 Abs. 3 BöB und Art. 56 Abs. 4 IVöB). Immerhin ist Auftraggebern bei wiederholten gemeinsamen Beschaffungen zu empfehlen, aus Gründen der Rechtssicherheit das anwendbare Recht dauerhaft statt bei jeder Beschaffung neu zu bestimmen. Zudem ist den Anbietern eine allfällige Rechtswahl zu kommunizieren (vgl. auch vorne, Ziff. 5).

Wählen die beteiligten Auftraggeber das anwendbare Recht nicht oder können sie sich dazu nicht verständigen, greifen die Kollisionsregeln von Art. 5 Abs. 1 BöB bzw. Art. 5 Abs. 1 und 2 IVöB. Dabei sind zwei Konstellationen zu unterscheiden: Bei einer interföderativen Vergabe (Beteiligung Bundes- und kantonalen Vergabestellen), ist entscheidend, ob der Bund einen Finanzierungsanteil von mindestens 50 % trägt. Ist dies der Fall, untersteht die Beschaffung dem BöB. In allen anderen Fällen, d.h. bei interföderativen Vergaben mit einem Bundesanteil kleiner als 50 % oder bei reinen (inter-)kantonalen Vergaben, kommt die IVöB zur Anwendung. In Ergänzung zur IVöB greift das Ausführungs- und Verfahrensrecht desjenigen Kantons, welcher den grössten Finanzierungsanteil trägt (Art. 5 Abs. 2 IVöB).

KARTELLRECHTLICHE SCHRANKEN

Schliessen sich öffentliche Auftraggeber für eine gemeinsame Beschaffung zusammen, kann dies kartellrechtlich relevant sein. Die Thematik ist komplex und kann hier nur in den Grundzügen umrissen werden.

Das Kartellgesetz (KG) ist subjektiv anwendbar auf unternehmerische Tätigkeiten. Es gilt der weite, sog. funktionale Unternehmensbegriff (Art. 2 Abs. 1bis KG). Er erfasst auch unternehmerische Aktivitäten staatlicher oder staatsnaher Behörden. Dies bedeutet, dass auch Einheiten der dezentralen (z.B. Staatsunternehmen) und der zentralen Verwaltung (der «Staat» an sich) in den persönlichen Geltungsbereich fallen können, wenn sie unternehmerische Tätigkeiten entfalten (vgl. bereits Art. 2 Abs. 1 KG: «Unternehmen des privaten und des öffentlichen Rechts»; ferner Art. 2 Abs. 1bis: «…unabhängig von ihrer Rechts- oder Organisationsform», vgl. hierzu auch eingehend Amstutz & Carron, 2021,

N. 62 ff., insb. N.134 mit Nachweisen). Vom KG regelmässig erfasst werden insbesondere (aber nicht nur) Sektorenauftraggeber (i.S.v. Art. 4 Abs. 2 lit. a BöB/ IVöB), genauso wie gewisse Einrichtungen des öffentlichen Rechts (Art. 4 Abs. 1 IVöB) und private Träger kantonaler und kommunaler Aufgaben (Art. 4 Abs. 4 lit. a IVöB).

Soweit das KG subjektiv anwendbar ist, können gemeinsame Beschaffungen öffentlicher Auftraggeber den Effekt einer Einkaufsgemeinschaft (EKG) zeitigen. EKG unter Konkurrenten, die sich auf die Festsetzung von Einkaufspreisen auswirken, können Wettbewerbsabreden i.S.v. Art. 4 Abs. 1 KG darstellen, welche eine Wettbewerbsbeschränkung bewirken, eventuell sogar bezwecken[12]. Dies muss jeweils im Einzelfall abgeklärt werden; die Risiken sind indessen angesichts der WEKO-Praxis gross, dass EKG als Wettbewerbsabreden betrachtet werden. Denn aus beispielsweise fünf Einkäufern in einem konkreten Beschaffungsfall wird über eine EKG ein einziger Nachfrager. Stellt eine EKG eine Wettbewerbsabrede dar, so handelt es sich um horizontale Abreden über Preise und Preisbestandteile (der Einkaufspreis ist Preisbestandsteil), die gemäss gesetzlicher Vermutung den Wettbewerb beseitigen (Art. 5 Abs. 3 KG). Diese gesetzliche Vermutung lässt sich oftmals widerlegen, da weitere Auftraggeber sowie Private für Nachfrage-Restwettbewerb sorgen.

Selbst wenn die Vermutungsfolge beseitigt werden kann, verbleibt gemäss Bundesgericht regelmässig eine erhebliche Wettbewerbsbeeinträchtigung (Art. 5 Abs. 1 KG). Um kartellrechtlich zulässig zu sein, muss sie durch Gründe der wirtschaftlichen Effizienz gerechtfertigt werden können (Art. 5 Abs. 2 KG). In Frage kommen hier u.a. das Bilden von Gegenmacht gegenüber einer starken Anbieterseite oder effizientere Ressourcennutzung bzw. effizientere Beschaffungsverfahren seitens der involvierten öffentlichen Auftraggeber. Ob der Effizienzbeweis gelingt, hängt wiederum stark vom Einzelfall ab. Die Praxis der WEKO zu den Rechtfertigungsgründen ist streng.

Wichtig ist, dass die kartellrechtliche Beurteilung anhand des konkreten Beschaffungsgeschäfts frühzeitig erfolgt, insbesondere bevor das gemeinsame Beschaffungsverfahren

[12] Die Entscheidpraxis der WEKO und die Beratungspraxis ihres Sekretariats sind einerseits nicht widerspruchsfrei und lassen anderseits grosse Interpretationsfreiräume offen. Es müssen im Einzelfall eine Vielzahl von Faktoren berücksichtigt werden, was komplexe Abklärungen erfordert; hierauf kann im Rahmen dieses Beitrags nicht eingegangen werden.

eingeleitet wird. Zu bestimmen ist dabei u.a. der exakte Beschaffungsgegenstand. Entscheidend ist in einem ersten Schritt eine kartellrechtliche Marktanalyse zur Abgrenzung des sachlichen und räumlichen Markts - aus Sicht der Auftraggeber als Nachfrager (Beschaffungsmarkt) sowie aus Sicht der potenziellen Anbieter, die sich um diese Aufträge bewerben könnten (Absatzmarkt). Weitere Faktoren sind der kombinierte Marktanteil der an einem Projekt beteiligten Auftraggeber, die Eigenschaften der Marktgegenseite (d.h. Anbieterseite) etc.

SCHLUSS

Gemeinsame Beschaffungen bergen viel ungenutztes Potenzial. Zu den Vorteilen gehören die Nachfragebündelung und damit potenziell bessere Konditionen sowie Effizienzgewinne im Vergabeprozess. Trotzdem kommen gemeinsame Beschaffungen immer noch eher selten vor.

Im schweizerischen Beschaffungsrecht sind gemeinsame Beschaffungen nur punktuell geregelt. Angesichts dessen und mangels einschlägiger Gerichtspraxis bleiben sie mit Rechtsunsicherheiten behaftet. Gleichzeitig verfügen öffentliche Auftraggeber dadurch über viel Gestaltungsspielraum, den es unter Beachtung allgemeiner vergabe- und verwaltungsrechtlicher Grundsätze zu nutzen gilt.

Zwei Grundtypen haben sich etabliert: Bei spontanen gemeinsamen Beschaffungen schliessen sich Auftraggeber *ad hoc* zusammen, um einen gemeinsamen Bedarf zu decken. In diesem Modell führt in der Regel ein federführender Auftraggeber die Beschaffung im Namen und Auftrag aller beteiligten Auftraggeber durch. Alternativ kann bei längerfristigen, institutionalisierten Kooperationen eine zentrale bzw. gemeinsame Beschaffungsstelle errichtet werden (z.B. in Form eines Vereins oder einer Aktiengesellschaft), wie es etwa bei der Organisation eOperations der Fall ist.

Während öffentliche Auftraggeber regelmässig Flexibilität beim Leistungsbezug anstreben, ist aus Anbietersicht eine präzise Leistungsbeschreibung entscheidend. Das Vergaberecht erfordert auch bei gemeinsamen Beschaffungen eine vorgängige Bedarfsermittlung, dient ein Vergabeverfahren doch der spezifischen Bedarfsdeckung, auch ohne

Exklusivitätszusage. Es empfiehlt sich, Anbietern ein verbindliches Mindestvolumen zu bieten oder eine Rabattstaffelung vorzusehen.

Bei gemeinsamen Beschaffungen kommt der Einhaltung des Transparenzgrundsatzes eine grosse Bedeutung zu. Für Anbieter ist bei der Offertstellung wesentlich, ob sie für einen oder mehrere Auftraggeber anbieten und wer ihre zukünftigen Vertragspartner und Bedarfsstellen sind. Diese sollten im Angebotszeitpunkt zumindest identifizierbar sein. Ebenso wichtig ist die sorgfältige Regelung des Innenverhältnisses zwischen den beteiligten Auftraggebern. Vertraglich festgehalten werden sollten u.a. die Eckpfeiler des Beschaffungsprojekts, Zuständigkeiten sowie wesentliche Verfahrensschritte.

Bei interkantonalen und interföderativen Vergaben stellt sich sodann die Frage nach dem anwendbaren Recht. Die Frage ist nicht nur für das (erstinstanzliche) Beschaffungsverfahren selbst relevant, sondern auch für den Rechtsweg im Beschwerdefall. Das revidierte Vergaberecht enthält für interkantonale und -föderative Beschaffungen eine Rechtswahlklausel, welche die Bestimmung des anwendbaren Rechts in das Ermessen der beteiligten Auftraggeber stellt. Subsidiär (bei fehlender Regelung) kommen die gesetzlichen Bestimmungen zum Tragen, die im Wesentlichen darauf abstellen, welches Gemeinwesen den grössten Finanzierungsanteil trägt.

Nicht zu vergessen sind schliesslich kartellrechtliche Aspekte, da gemeinsame Beschaffungen den Effekt einer Einkaufsgemeinschaft haben, die als Wettbewerbsbeschränkung gilt. Unter Umständen muss der Nachweis erbracht werden, dass die Zusammenarbeit aus Effizienzgründen gerechtfertigt ist. Die kartellrechtliche Beurteilung sollte stets anhand des konkreten Beschaffungsgeschäfts erfolgen.

LITERATURVERZEICHNIS

Amstutz, M. & Carron, B. (2021). Artikel 2 KG. In Amstutz, M. & Reinert, M. (Hrsg.), *BSK Kartellrecht* (2. Auflage). Basel: Helbing Lichtenhahn Verlag.

Botschaft zur Totalrevision des Bundesgesetzes über das öffentliche Beschaffungswesen. (15. Februar 2017). BBl 2017 1851. (Zit.: Botschaft BöB).

Gehrer, C. (2020). Rahmenverträge. In J. Zufferey, B. Beyeler, & P. Scherler (Hrsg.), *Aktuelles Vergaberecht 2020* (S. 351 – S.367). Zürich: Schulthess.

Lutz, D. (2014, Januar*). Wenn Gemeinden oder Kantone zusammen einkaufen*. Kriterium, 36. Kriterium Nr. 36 (Wenn Gemeinden oder Kantone zusammen einkaufen) (zh.ch)

Pfändler, S. & Koch, R. (2023, 23. November). *Gemeinsam beschaffen, gemeinsam Digitalisieren. Innovative Beschaffungsmodelle im Bereich Digitalisierung und darüber hinaus*. Praxisstudie BFH in Partnerschaft mit OneGov.ch. https://www.bfh.ch/dam/jcr:d6263f2e-4280-40a6-88ce-3cfc6550e246/20231115_Web_BFH_Broschuere_A4.pdf

Zentralschweizer Regierungskonferenz (ZBDK). (2006, 7. Juli). *Leitfaden für Interkantonale Submissionen*. www.zrk.ch/dateimanager/lf-ik-subm.pdf

DIE SCHLÜSSELROLLE DES PFLICHTENHEFTS IN AUSSCHREIBUNGEN

Josef Schreiber / Roland Füllemann

Josef Schreiber ist selbständiger IT-Berater und Erstautor eines Fachbuchs.

Roland Füllemann ist IT-Beschaffungsberater für die öffentliche Hand bei der «example consulting gmbh» und Co-Autor eines Fachbuchs.

Abstract: Der vorliegende Auszug aus dem Fachbuch «*Beschaffung von Informatikmitteln: Submissionsverfahren - Pflichtenheft - Evaluation* (6. Auflage 2022, Haupt Verlag, Bern)» von J. Schreiber und R. Füllemann behandelt das *Pflichtenheft* als Kern von IT-Beschaffungen. Er zeigt die Struktur des Aufbaues von Pflichtenheften und geht auszugsweise auf wichtige Inhalte der einzelnen Hauptkapitel des Pflichtenheftes ein. Detailliertere Ausführungen dazu und zur Abwicklung des kompletten Evaluationsprozesses können dem aus drei Sektionen – Allgemeines über die Auswahl von Informatikmitteln, Vorgehensrahmen des Beschaffungsprozesses inkl. der wichtigsten Dokumente, Vermittlung von Praxisbeispielen – bestehenden Fachbuch entnommen werden.

INHALTSVERZEICHNIS

Die Schlüsselrolle des Pflichtenhefts in IT-Ausschreibungen 172
- Kapitel 1: Allgemeines zur Ausschreibung 174
- Kapitel 2: Ausgangslage 175
- Kapitel 3: Ist-Zustand 177
- Kapitel 4: Ziele 178
- Kapitel 5: Anforderungen (Anforderungsprofil) 180
- Kapitel 6: Mengengerüst, Häufigkeiten 185
- Kapitel 7: Aufbau und Inhalt des Angebotes 186
- Kapitel 8: Administratives und Bewertung der Angebote 188
- Kapitel 9: Anhänge zum Pflichtenheft 188

DIE SCHLÜSSELROLLE DES PFLICHTENHEFTS IN IT-AUSSCHREIBUNGEN

«Auswahlentscheide für die Beschaffung von Informatikmitteln und -dienstleistungen waren nie einfach und werden auch weiterhin in einem von Innovationen geprägten und hart umkämpften, unübersichtlichen Markt eine grosse Herausforderung darstellen. Gilt es doch einerseits, die Vorgaben des Beschaffungsrechts zu beachten, und andererseits, die vielfältigen, interessanten Möglichkeiten und Chancen komplexer Informations- und Kommunikationstechnologie in Kosteneinsparungen, Effizienzsteigerungen sowie in qualitative und strategische Vorteile für das jeweilige Unternehmen oder die Verwaltung umzumünzen»

Umschlagstext zu Schreiber, J. & Füllemann, R. (2022). *Beschaffung von Informatikmitteln: Submissionsverfahren - Pflichtenheft - Evaluation* (6. Auflage). Haupt Verlag, Bern.

Die Bedeutung des Pflichtenheftes

Das Pflichtenheft einer IT-Beschaffung bildet zusammen mit seinen verschiedenen Begleitdokumenten (zum Beispiel einem separaten Anforderungskatalog, Preiseingabeformular, Detailangaben zum Ist-Zustand) die *Ausschreibungsunterlagen* und es nimmt somit innerhalb des Beschaffungsvorhabens eine zentrale Stellung ein. Darin werden im Wesentlichen die Ziele, welche mit der Beschaffung zu erreichen sind, sowie die Anforderungen inkl. der Eignungs- bzw. KO-Kriterien und Wünsche an den Beschaffungsgegenstand formuliert. Damit wird das Pflichtenheft mit seinen Begleitdokumenten zur unentbehrlichen Grundlage für die Einladung möglicher Lieferanten bzw. Realisierungspartner zur Erarbeitung und Abgabe eines Angebotes.

Das Pflichtenheft mit seinen Begleitdokumenten bilden die Basis für den Aufbau und die Substanz der Offerten, für eine einfachere Bewertung der Angebote sowie für die Vertragsverhandlungen und die abzuschliessenden Verträge.

Ein Hinweis zur Begriffsdefinition:

In Deutschland wird an Stelle des Pflichtenhefts der Begriff «Lastenheft» verwendet. Inzwischen sprechen auch die Autoren der Schweizer Projektmethodik HERMES (aktuelle

Version 5.1) von «Lastenheft», räumen aber ein, dass in der Schweiz seit Jahrzehnten der Begriff «Pflichtenheft» üblich ist. Aus diesem Grund sprechen wir im vorliegenden Beitrag durchgängig vom Pflichtenheft.

Überblick zum Inhalt des Pflichtenheftes

Der Inhalt des Pflichtenheftes besteht im Wesentlichen aus den nachstehend aufgeführten Kapiteln, wobei die entsprechenden Daten und Fakten in der Regel bereits in früheren Projektphasen (Vorstudie, Konzeption) ermittelt und aufbereitet werden:

- Darstellung der für die Beschaffung relevanten Fakten der gegenwärtigen Situation, das heisst des *Ist- Zustandes* mit den betroffenen Prozessen, Applikationen und IT-Infrastruktur inkl. Angaben zum Betrieb sowie den Stärken und Schwächen, bezogen auf den Beschaffungsgegenstand;
- Formulierung der *Ziele*, die mit der Beschaffung erreicht werden sollen;
- Beschreibung der *Anforderungen* inkl. der Eignungs- bzw. KO-Kriterien (Anforderungsprofil) betreffend den Beschaffungsgegenstand;
- Aufstellung des *Mengengerüstes* und der *Häufigkeiten* (z. B. Anzahl und Häufigkeiten der Geschäftsfälle), Datenbewegungen und Datenbestände, Anzahl Benutzende;
- Vorgaben für den *Aufbau und Inhalt der Angebote*.

Ergänzt man diese Abschnitte mit weiteren Angaben zur Ausschreibung wie

- *Allgemeines* zur Ausschreibung,
- *Ausgangslage*,
- *Angaben zu administrativen Belangen und der Gewichtung der Zuschlagskriterien und*
- § verschiedenen *Anhängen*,

so erhält man das Gerüst des Pflichtenheftaufbaus (siehe Abbildung 1). Dieser Aufbau hat sich in der Praxis gut bewährt. Bei grösseren Beschaffungsvorhaben kann als Alternative zur Anforderungsdefinition im Pflichtenheft ein separates Dokument im Sinne eines eigenen *Anforderungskataloges* als Anhang zum Pflichtenheft erstellt werden. Das Pflichtenheft wird, abhängig vom Verfahren, durch weitere Anhänge ergänzt (z. B. ein Preiseingabeformular, eine Vorlage für die Selbstdeklaration, usw.)

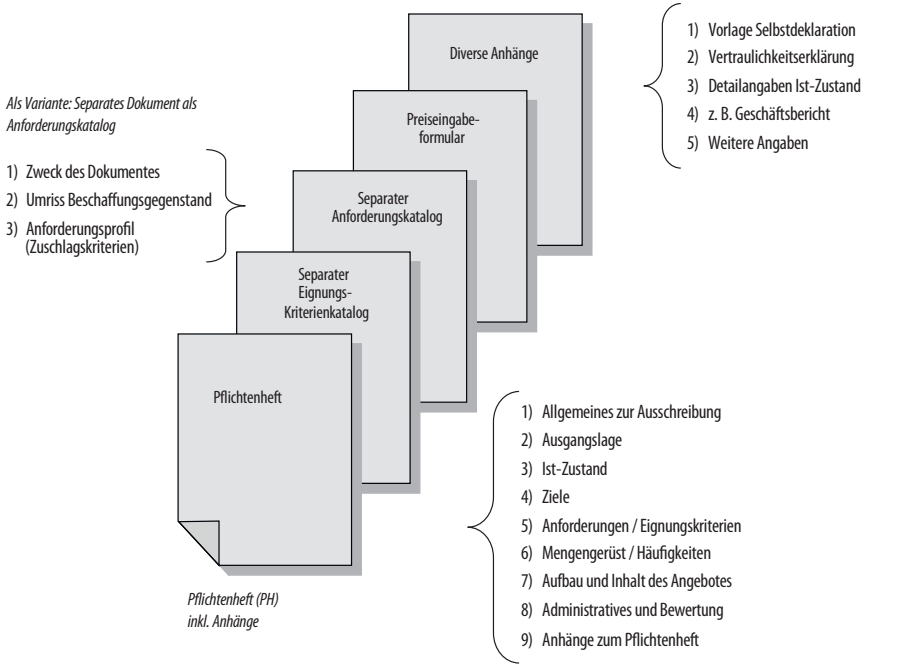

Abb. 1: Struktur des Pflichtenhefts und ergänzende Ausschreibungsunterlagen

Nachfolgend werden die Hauptkapitel des Pflichtenheftes detailliert aufgezeigt und erläutert.

KAPITEL 1: ALLGEMEINES ZUR AUSSCHREIBUNG

In diesem ersten Kapitel des Pflichtenheftes legt der Auftraggeber in kurzen Zügen den Zweck der Ausschreibung bzw. des Pflichtenheftes inkl. des Ausschreibungsgegenstandes dar und macht Angaben zur Bedarfs- / Vergabestelle und der Beschaffungsstelle (inkl. der Nennung der Kontaktdaten) und zum gewählten Verfahren.

Bemerkungen zu möglichen Vorbehalten

Auch Angaben zu möglichen Vorbehalten (Abbildung 2) im Zusammenhang mit der Ausschreibung, wichtige Abhängigkeiten zu anderen Vorhaben und dem Umgang mit

allfälligen Berichtigungen sollen in diesem Kapitel bekanntgegeben werden. Ausführungen zur Geheimhaltung und zur Einhaltung des Datenschutzes runden dieses erste Kapitel des Pflichtenheftes ab.

Vorbehalte

- Die ausschreibende Stelle übernimmt keine Haftung für Fehler oder Lücken in den Ausschreibungsunterlagen;
- Anbringen von Berichtigungen und Ergänzungen an den Ausschreibungsunterlagen, unter Wahrung der Gleichbehandlung aller Anbietenden, eventuell verbunden mit einer Fristerstreckung; die Anbietenden sind verpflichtet diese Ergänzungen in ihrer Offerte zu berücksichtigen;
- Der Auftrag kann nach dem Zuschlag ohne Kostenfolge für den Besteller widerrufen werden, wenn er nicht ausschreibungs- und vertragskonform ausgeführt wird; in diesem Fall kann der Besteller den Auftrag ohne neue Ausschreibung den an zweiter Stelle platzierten Anbieter vergeben;
- Der Zuschlag ist noch von Bedingungen abhängig (z. B. Genehmigung durch übergeordnete Gremien, Bewilligung des Kredites, Volksentscheiden, etc.);
- Der Besteller behält sich vor, Folgeaufträge, welche sich auf den Beschaffungsgegenstand beziehen, im freihändigen Verfahren zu vergeben;

Abb. 2: Vorbehalte (Auswahl)

KAPITEL 2: AUSGANGSLAGE

In diesem zweiten Kapitel des Pflichtenheftes stellt sich der Auftraggeber bzw. die Beschaffungsstelle (die von der Beschaffung betroffenen Organisationseinheiten) den Offertstellern mit seiner speziellen Ausgangssituation im Zusammenhang mit der geplanten Beschaffung vor. Auch im Zusammenhang mit dem Beschaffungsvorhaben bereits aus früheren Projektphasen vorhandene Grundlagen (Strategien, Leitplanken, Ergebnisse aus Analysen, etc.) sollen in diesem Unterkapitel des Pflichtenheftes ihren Niederschlag finden. Damit soll ein zusammenfassender Überblick über die Organisation sowie das Umfeld, das vom Beschaffungsvorhaben betroffen ist, vermittelt werden. Angaben zum Anstoss für die Beschaffung und zur vorgesehenen Projektorganisation runden die Angaben zur Ausgangslage ab.

Eine zweckmässige Gliederung für die möglichst knapp zu haltende Schilderung der Ausgangslage geht aus Abbildung 3 und den nachfolgenden Ausführungen hervor.

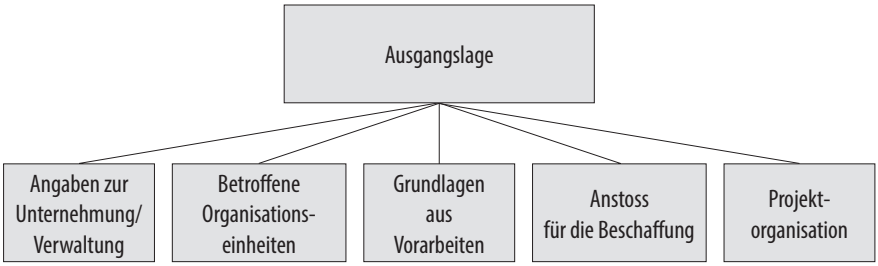

Abb. 3: Ausgangslage

Bemerkungen zu Grundlagen aus Vorarbeiten

In vielen Fällen wurden mit Blick auf die bevorstehende Beschaffung schon in früheren Phasen Vorarbeiten geleistet. Diese können sehr unterschiedlicher Natur sein, wie z. B.: Papiere betreffend strategische Änderungen (Restrukturierungen, Einsatzkonzept und Beschaffenheit für die IT-Endgeräte, Verlagerung von Arbeitsplätzen ins «Home Office», firmenübergreifende Digitalisierung von Fachprozessen, etc.), Auslagerung von Prozessen oder Systemen, Konzepte zur Optimierung von Fachprozessen und IT-Anwendungen, gesetzliche Änderungen und Vorgaben, Erschliessung neuer Eisatzfelder im Rahmen der Digitalisierung.

Bemerkungen zu Anstoss für die Beschaffung

Die Gründe für Beschaffungen von Informatikmitteln sind mannigfaltig. Für jede Beschaffung gibt es jedoch einen speziellen, meist zwingenden Grund, welcher ein Beschaffungsprojekt auslöst («Compelling Event»). Diesen Grund sollten die Anbietenden kennen. Deshalb soll an dieser Stelle im Pflichtenheft in wenigen Worten der Anstoss für die Beschaffung bekannt gegeben werden, damit die Anbieter die Gründe des Beschaffungsprojektes und den Beschaffungsgegenstand besser nachvollziehen können.

Bemerkungen zur Projektorganisation

Kurze Angaben zur Projektorganisation (für die Evaluationsphase), zum Beispiel in grafischer Form, können die Schilderung der Ausgangslage sinnvoll abrunden. Es werden damit auch die personellen Zuständigkeiten und die vorhandenen Skills nach aussen transparent gemacht.

Darüber hinaus können bei komplexeren und grossen Vorhaben hier auch die Projektstruktur und eine mögliche Einbettung des Beschaffungsvorhabens in ein übergeordnetes Projekt transparent gemacht werden.

KAPITEL 3: IST-ZUSTAND

Noch bevor man Ziele und Anforderungen formulieren kann, sind die für das jeweilige Beschaffungsvorhaben *relevanten Informationen* über den *Ist-Zustand* zu sammeln und festzuhalten. Diese Informationen sind insbesondere auch für die Anbieter von Interesse, können sie doch mit dem Wissen über die Stärken und Schwächen aber auch über unabänderliche Rahmenbedingungen der gegenwärtigen Situation ihre zu offerierende Lösung besser auf die Beseitigung der Probleme und auf die vorhandenen Systeme und Infrastrukturen hin abstimmen.

Zu diesem Zweck werden vor allem die vom Beschaffungsvorhaben betroffenen Prozesse (Arbeitsabläufe) mit ihren wichtigsten Aufgaben und Ausprägungen sowie die technischen Hilfsmittel (systemtechnische und Kommunikationsinfrastruktur) sowie Angaben zum Betrieb festgehalten.

Dabei ist es empfehlenswert, sich *auf das für die Beschaffung wirklich Wichtige des Ist-Zustandes zu konzentrieren, die so genannte 80 : 20-Regel anzuwenden* und sich auf die vom *Beschaffungsvorhaben betroffenen Bereiche* zu beschränken. Bei der Ist-Aufnahme kommt es also darauf an, das für den Beschaffungsgegenstand wirklich Relevante, sowie das richtige Mass zwischen genügendem Erkenntniswert und minimalem Aufwand zu finden. Dies setzt die Bereitschaft voraus, ein gewisses Mass an Unsicherheit zu ertragen und Mut zur Lücke zu haben. Eine umfassende, sehr detaillierte Wiedergabe des Ist-Zustandes kann schnell sehr aufwendig werden und ist im Hinblick auf die Beschaffung, auch nicht notwendig.

Eine zweckmässige Gliederung, zur Darstellung des Ist-Zustandes im Pflichtenheft geht aus Abbildung 4 hervor.

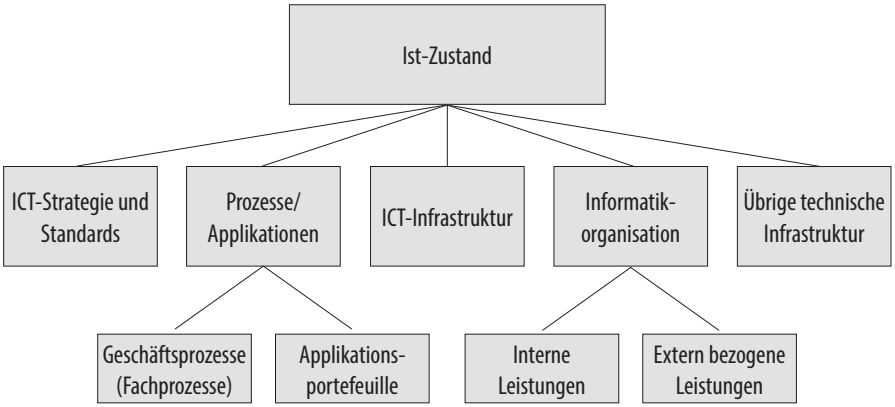

Abb. 4: Ist-Zustand

Als wichtigste Informationen bei der Schilderung des Ist-Zustandes haben sich in der Praxis die *ICT-Strategie und Standards* sowie eine konzise und knappe Darstellung der wichtigen *Geschäftsprozesse* im Umfeld des Beschaffungsgegenstandes erwiesen.

Eine weitere wichtige Informationsquelle ist das *Applikationsportefeuille* (auch Applikationsportfolio genannt). Hier sind diejenigen Applikationen aufzuführen, welche für den Beschaffungsgegenstand von Relevanz sind. Dies schliesst ein, dass auch all jene Applikationen bzw. Softwareprodukte, die in der zu beschaffenden ICT-Lösung weiterhin, zur Gewährleistung der Interoperabilität (Gewährleistung der Schnittstellen) über Applikations- und Systemgrenzen hinweg, benutzt werden, aufzuführen sind. Eine Darstellung als grafische Applikationsübersicht (mit Schnittstellen) hilft, den Beschaffungsumfang, die Abgrenzung des Beschaffungsgegenstandes sowie die Integration in die Applikationsumgebung aufzuzeigen.

KAPITEL 4: ZIELE

In diesem Abschnitt des Pflichtenheftes sind die Ziele, die mit der geplanten Beschaffung erreicht werden sollen, anzugeben. Die Ziele beziehen sich dabei gleichermassen auf

unternehmensstrategische und betriebswirtschaftliche, aber auch menschlich-soziale, also auf nutzenrelevante (wirkungsbezogene) wie auch auf lösungsspezifische (überwiegend funktionale) Aspekte.

Aus den nutzenrelevanten Zielen und Rahmenbedingungen (zum Beispiel Reduktion der Prozesskosten um x %, Leitplanken der Informatikstrategie, absolut einzuhaltende Termine wegen herrschender Sachzwänge) werden die Systemziele (lösungsspezifische Ziele) und die Vorgehensziele (zum Beispiel Etappen, Termine) abgeleitet (siehe Abbildung 5).

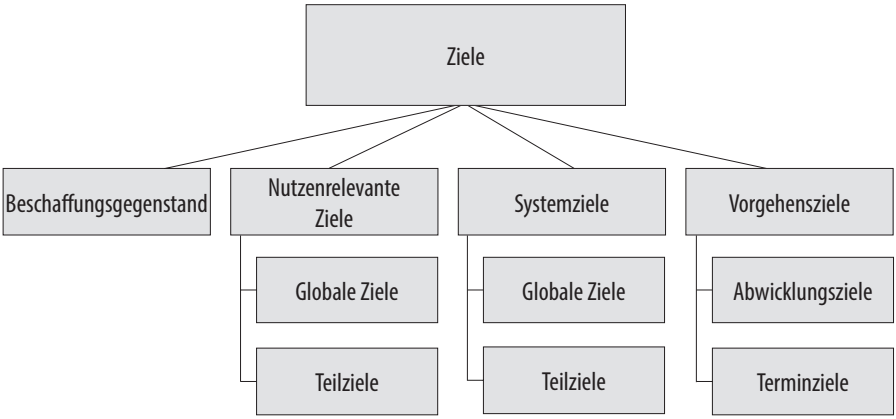

Abb. 5: Strukturierung der Ziele

Die nutzenrelevanten Ziele zeigen vor allem auf, was aus unternehmensstrategischer und betriebswirtschaftlicher Sicht mit der neuen Lösung zu erreichen ist. Die Systemziele beziehen sich auf die Eckpfeiler der neuen Lösung, das heisst sie definieren auf einer hohen Ebene, wie der Endzustand (Lösungsumriss) aussehen bzw. welche Eigenschaften er haben muss. Die Vorgehensziele beziehen sich auf die Umsetzung des Projektes (Etappen, Realisierungseinheiten, Termine usw.).

Damit handelt es sich um ein multiples Zielsystem, das heisst um mehrere Zielarten mit sehr unterschiedlichem Inhalt, die jedoch miteinander in einem direkten Zusammenhang stehen.

Der Formulierung der Ziele ist ein hoher Stellenwert beizumessen, verkörpern sie doch den eigentlichen Grund für die geplante Beschaffung und die Grundlage für die Formulierung der Eignungs- bzw. KO-Kriterien und der Anforderungen. Die Ziele sind zudem auch massgebend für die Gewichtung der Kriterienhierarchie (Zuschlagskriterien).

Ziele können auch zu wichtigen Vertragspunkten für das jeweilige Beschaffungsvorhaben werden (zum Beispiel Systemleistungen, Termine).

Bemerkungen zur Formulierung der Ziele

Bei der Formulierung der Ziele sind folgende Grundsätze zu beachten:

- Ziele müssen realistisch und erreichbar gesetzt werden,
- Ziele müssen quantifiziert (operational) vorgegeben werden, denn nur so kann der Grad der Zielerreichung der späteren Lösung festgestellt werden,
- Ziele müssen hersteller- bzw. anbieterneutral und strukturierbar sein,
- Ziele müssen von allen beteiligten Parteien und Stellen (Auftraggeber, Projektteam, betroffene Mitarbeitende) akzeptiert werden können,
- Ziele sollten nicht konkurrieren, das heisst einander gegenseitig ausschliessen;
- Zielkonflikte sind von Anfang an durch Mittel-/Zweckrelationen zu vermeiden. Wo dies nicht möglich ist, sollte der Widerspruch aufgezeigt und das Schwergewicht festgelegt werden.

KAPITEL 5: ANFORDERUNGEN (ANFORDERUNGSPROFIL)

Die Definition der Anforderungen an den Beschaffungsgegenstand (Applikationen, Systeme bzw. einzelne Systemkomponenten oder Dienstleistungen) stellt einen Schwerpunkt innerhalb des Pflichtenheftes dar. Die Offertsteller sollen sich auf eine präzise Formulierung der Anforderungen abstützen können. Das heisst jedoch nicht, dass bereits komplette Lösungen, insbesondere die Systemplattform mit ihren exakten Leistungsmerkmalen, vorzugeben sind; dies ist die Aufgabe der Offertsteller.

Hauptebenen zur Strukturierung der der Anforderungen

Die Anforderungen sind Grundlage für die im Rahmen der Evaluation definierten *Bewertungs- respektive Zuschlagskriterien* und sind als Konkretisierung der Ziele zu

verstehen. Sie beziehen sich auf alle Träger der künftigen Lösung, in den meisten Beschaffungsfällen auf die nachfolgend genannten drei Hauptebenen:

- die Applikationssoftware mit ihren Funktionen und Daten;
- die ICT-Infrastruktur, bestehend aus Hardware, Software und den Datennetzen inklusive Kommunikationsdiensten;
- die Dienstleistungen der Anbieter wie Hersteller, Lieferanten und Integrationshelfer sowie Dienstleister für den Betrieb und Support.

Diese drei Anforderungshauptebenen sind danach im Pflichtenheft tiefer zu strukturieren und zwar in die applikationsbezogenen und systemtechnischen Lösungsträger, die ICT-Infrastruktur und die zu erbringenden Dienstleistungen der Anbieter wie Hersteller.

Für die applikationsbezogenen und systemtechnischen Lösungsträger sind insbesondere die nachfolgend aufgeführten Kriterien (Anforderungen) von Bedeutung

- Funktionale Leistung, das heisst funktionale Richtigkeit und Vollständigkeit (fachliche Korrektheit, Konsistenz);
- Leistungsfähigkeit und Effizienz (Zeitverhalten, Ressourcenbedarf);
- Zuverlässigkeit (Integrität der Lösung, Verfügbarkeit der Systemleistung);
- Wartbarkeit (Anpassungsfähigkeit, Unterhalt);
- Datenschutz und Sicherheit;
- Systemunabhängigkeit (Portabilität, Skalierbarkeit, Interoperabilität);
- Benutzbarkeit (Benutzerfreundlichkeit, Einfachheit der Handhabung und des Betriebes der Lösung und Systeme).

Einen gleichermassen entscheidenden Einfluss auf das Gelingen des Beschaffungsvorhabens und die Einhaltung von Terminen und Kosten haben aber auch anbieter- und realisierungs- bzw. unterstützungsbezogene Leistungen sowie betriebliche (Outsourcing, Cloud-Computing) und Supportleistungen. Auf diese Anforderungen wird zu den Ausführungen zur Abbildung 6 noch näher eingegangen wie:

- Marktstellung, Solidität und fachliches Know-how der Hersteller bzw. Lieferanten und sonstigen Integrationshelfer;
- Realisierungskompetenz und die Unterstützungsleistungen vor, während und nach der Einführung;

- Erbringung betrieblicher Leistungen, sofern Outsourcing und Cloud-Computing ein Thema der Beschaffung sind;
- vertragliche Absicherung der Leistungen.

Detailangaben zu den Anbieterbezogene Anforderungen

Eine erfolgreiche Beschaffung und Implementierung von Informatikmitteln sowie deren spätere effiziente Nutzung hängt nicht nur von der Güte der Applikationssoftware und der Systemplattform, sondern ebenso von der Seriosität und der Fachkompetenz der Realisierungspartner, Hersteller, Lieferanten, Betreibern von Outsourcing- und Cloud-Lösungen und sonstigen Integrationshelfern ab. Deshalb hat der Pflichtenhefterstellerentsprechende anbieterbezogene Anforderungen an die Fachkompetenz der Anbieter und die zu erbringenden Dienstleitungen für Lieferung und Implementierung (projektbezogene Arbeiten) sowie für den Betrieb und Support zu formulieren (siehe Abbildung 6).

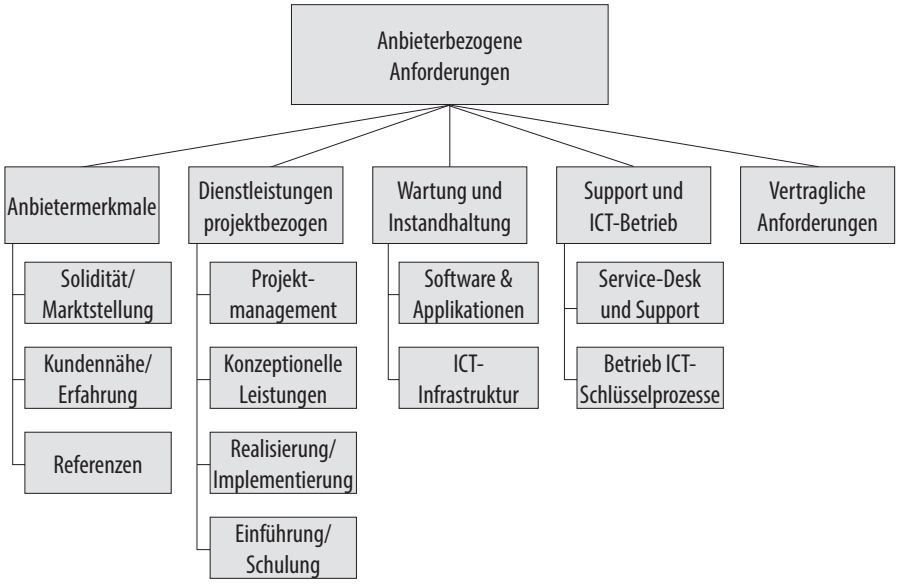

Abb. 6: Anbieterbezogene Anforderungen

Gerade auch wegen der meist mehrjährigen und oft nur schwer lösbaren Bindung an die Hersteller bzw. Lieferanten, insbesondere von Softwareprodukten oder an Outsourcing-Firmen, sind diese Art von Anforderungen besonders wichtig.

Bemerkungen zu den Anbietermerkmalen

In diesem Abschnitt des Pflichtenheftes geht es darum, durch entsprechende Anforderungen und Fragen sich ein Bild über die generelle Leistungsfähigkeit, Unternehmenskultur und Glaubwürdigkeit der Anbieterseite zu verschaffen. Anbietermerkmale, welche im Rahmen von IT-Beschaffungen geprüft werden, sind beispielsweise

- Solidität / Marktstellung
- Kundennähe / Erfahrung
- Referenzen
- Wirtschaftliches und technisches Leistungsvermögen

Bemerkungen zu den Eignungskriterien

Beim Vorgehen nach dem öffentlichen Beschaffungsrecht werden ausgewählte Anbietermerkmale in den Status von *Eignungkriterien* erhoben.

Dabei handelt es sich um Anforderungen, die unabdingbar zu 100% erfüllt sein müssen, damit der Teilnahmeantrag für eine Ausschreibung oder das Angebot selbst überhaupt im Evaluationsprozess weiter behandelt werden können. Wird die Hürde der Eignungskriterien von den anbietenden Firmen nicht übersprungen, so scheidet die betreffende Firma für den jeweiligen Beschaffungsfall aus. Deshalb werden die Eignungskriterien auch oft als KO-Kriterien bezeichnet.

Merkmale der Eignungskriterien

Gemäss den Bestimmungen des Beschaffungsrechtes (BöB und IVöB) haben sich die Eignungskriterien auf den Nachweis der finanziellen, wirtschaftlichen und technischen Leistungsfähigkeit der Anbieter zu beziehen. Sie sind somit also anbieterbezogen und fokussieren darauf, welche finanziellen oder wirtschaftlichen sowie spezifischen fach-

lichen, technischen und organisatorischen Voraussetzungen die Anbieter im Sinne eines Minimums erfüllen müssen.

Unter dem Begriff der Eignungs- oder KO-Kriterien definiert das Beschaffungsrecht auch «technische Spezifikationen» (IVöB Art. 30). In der Praxis lassen sich die auf den Anbieter bezogenen Eignungskriterien und technische Spezifikationen nicht immer klar trennen, beispielsweise wenn es um Betriebsleistungen wie Cloud-Hosting geht. Entscheidend ist, dass die Anzahl der Eignungskriterien und technischen Spezifikationen überschaubar bleibt. Zu vermeiden sind unnötig umfangreiche (technische) Vorgaben, die den Markt zu sehr einschränken und zum Ausschluss vieler Anbieter führen würden.

Formulierung der Eignungskriterien inkl. der technischen Spezifikationen

Die Eignungskriterien und technischen Spezifikationen sind äusserst sorgfältig zu bestimmen sowie sachgerecht und präzise zu formulieren. Dabei ist besonders auf die Nichtdiskriminierung und Gleichbehandlung der Anbietenden zu achten. In der Regel wird man sie von der Anzahl her auf ein Dutzend beschränken, mit dem Ziel, die für das jeweilige Beschaffungsvorhaben wirklich erfolgskritischen Punkte erfasst zu haben.

Bemerkungen zu den Dienstleistungen (Projektbezogen, Betrieb und Support)

Bei der Beschaffung von IT-Systemen ist der Fokus oft auf den komplexen Anforderungen, technischen Gegebenheiten und den damit verbundenen Investitionen in Hardware und Software. Darüber darf nicht vergessen werden, dass für eine erfolgreiche Lösungseinführung und einen effizienten Systembetrieb kompetent ausgeführte *Dienstleistungen* erbracht werden müssen.

Der Pflichtenhefter*steller* hat deshalb die für ihn relevanten Realisierungs- und Unterstützungsleistungen zu fordern. Sie beziehen sich auf die Projektorganisation und auf alle Träger der Lösung (Applikationen und Systemplattform) inklusive des Betriebes und Supports der Systeme sowie auf die in die Umsetzung der Lösung einbezogenen

Personen (Projektleitung, Informatikfachkräfte, Support- und Schulungspersonal). Zu nennen sind etwa:

- Wahrnehmung des Projektmanagements (Gesamtprojektleitung, Leitung von Teilprojekten)
- Konzeptionelle Leistungen (Fachkonzepte, Einführungs-Konzept, Datenmigrations-Konzept, Testkonzept, Schulungskonzept, usw.)
- Projektmitarbeit, insbesondere bei der Erstellung von Spezifikationen und Konzepten, der Konfigurierung und Parametrierung der Software, dem Aufbau der Daten und der Dokumentation sowie allfälligen Migrationsarbeiten
- Realisierungs- und Implementierungsleistungen wie die Installation von Hardware und Software, Softwareentwicklung und Realisierung von Schnittstellen sowie Systemtests
- Dienstleistungen zur Einführung und Schulung
- Erbringen von Wartungs-, Betriebs- und Supportleistungen über den Lebenszyklus der IT-Systeme

Im Rahmen einer IT-Beschaffung geht es immer darum, die Anforderungen – auch diejenigen an die Dienstleistungen – vollständig zu formulieren (damit die Anbieter diese in ihre Kalkulation einbeziehen können) um sodann im Rahmen der Evaluation sicherzustellen, dass die Anbieter die geforderten Leistungen auch erbringen können (Kompetenznachweis).

KAPITEL 6: MENGENGERÜST, HÄUFIGKEITEN

Das Mengengerüst und die Verarbeitungshäufigkeiten geben Auskunft, welche und wieviel Daten

- in die Systeme, bzw. Applikationen, in welchen Zeitperioden hineingehen (Input) und zu verarbeiten sind;
- permanent, das heisst zugriffsbereit zu verwalten sind (Datenbestände);
- aus den Systemen bzw. Applikationen in welchen Zeitperioden herauskommen (Output)
- und wie viele Arbeitsplatz- und Peripheriegeräte mit dem System bzw. der zu beschaffenden Anwendung unterstützt werden.

Damit bezieht sich das Mengengerüst gleichermassen auf Datenbewegungen und Datenbestände aber auch auf die Anzahl der zu unterstützenden Arbeitsplatzsysteme und der Anzahl der Benutzenden.

Die Angaben zu den Arbeitsplatzsystemen implizieren auch Angaben zur Anzahl der Benutzerinnen und Benutzer des Systems bzw. der einzelnen Applikationen. Diese Angaben sind nicht nur für die Systemleistung, sondern unter Umständen auch für die zu offerierenden Lizenzkosten – manche Softwareanbieter beziehen ihre Lizenzen auf die Anzahl «User» – relevant.

Wichtig ist es, bei diesen Angaben vom Ist-Zustand auszugehen (siehe Kapitel 3 «Ist-Zustand») jedoch auf den Soll-Zustand und zukünftige Entwicklungen (Tendenzen) während der Lebensdauer der Lösung (zum Beispiel fünf Jahre oder mehr) abzustellen. Unterliegen vor allem Datenbewegungen grösseren Schwankungen pro Zeiteinheit, so sind nicht nur die Durchschnittswerte pro Periode (Monat, Jahr), sondern auch die Spitzenwerte speziell zu vermerken (saisonale Schwankungen, Tages-, Monatsspitzen usw.).

KAPITEL 7: AUFBAU UND INHALT DES ANGEBOTES

In diesem Abschnitt des Pflichtenheftes werden die Vorgaben für den Offertaufbau inkl. allfälliger Beilagen festgelegt, dies im Interesse möglichst vollständiger und transparenter Offerten. Zudem wird damit die Informationsgewinnung und die Vergleichbarkeit der verschiedenen Angebote stark erleichtert. Der Aufbau der Offerte wurde so gewählt, dass er praktisch den Hauptpunkten der Anforderungen des Pflichtenheftes bzw. den Kriterien im Kriterienkatalog entspricht. Deshalb ist der Offertsteller anzuhalten, zwingend den vorgegebenen Offertaufbau zu beachten.

Eine zweckmässige Gliederung der Offerte geht aus Abbildung 7 hervor.

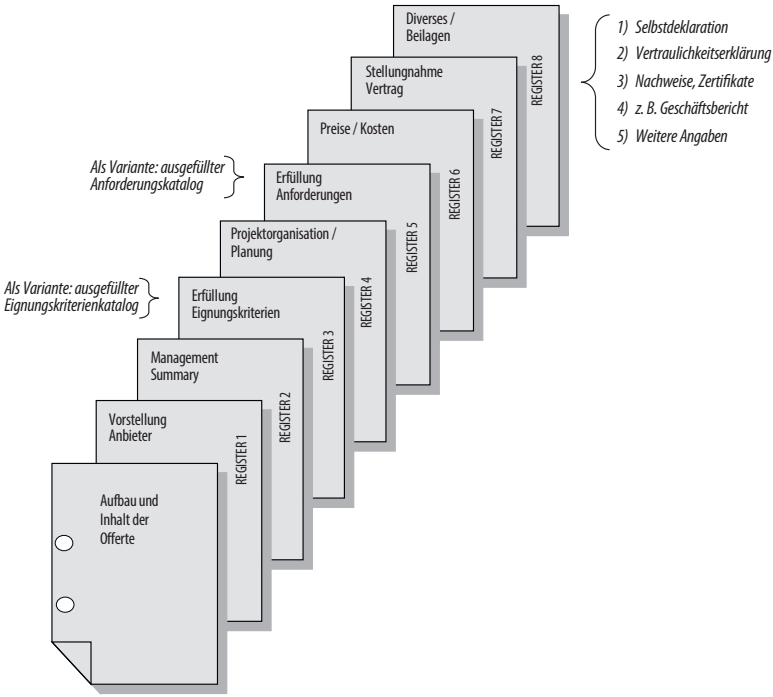

Abb. 7: Aufbau der Offerte

Zu den wichtigsten Vorgaben für die Offerte gehören

- Vorstellung des Anbieters (inkl. Partner bzw. Unterlieferanten)
- Nachweis der Erfüllung der Eignungskriterien
- Projektorganisation / Planung
- Erfüllung der Anforderungen
- Preis- und Kostenzusammenstellung (Einmalige Kosten wie Hard- und Software und Projektdienstleistungen sowie wiederkehrend Kosten für Lizenzen, Wartung, Outsourcing, Support)

Zur besseren Vergleichbarkeit der Offerten werden als Beilagen zum Pflichtenheft in der Regel standardisierte Formulare und Vorgaben verwendet, wie Anforderungskatalog, Preiseingabeschema und Vertragsentwürfe.

KAPITEL 8: ADMINISTRATIVES UND BEWERTUNG DER ANGEBOTE

In diesem Abschnitt des Pflichtenheftes werden die administrativen und terminlichen Vorgaben im Zusammenhang mit der Beschaffung aufgeführt, wie:

- Angaben zum Beschaffungsverfahren (z.B. Offenes Verfahren, Einladungsverfahren)
- Ablauf und Ecktermine der Beschaffung
- Einreichung des Angebots (Formvorschriften, Sprache, digitale und physische Kanäle)
- Angaben zu den Zuschlagskriterien und zur Bewertung (inkl. Methodik der Preisbewertung)
- Vertraulichkeit, Copyright, Rückgabe oder Vernichtung von Offerten

Da diese Angaben sich nicht auf fachliche oder technische Aspekte des Beschaffungsobjekts beziehen, gehören sie nach der Meinung einiger Beschaffungsstellen nicht zum «Pflichtenheft im engeren Sinne». Oft werden diese Angaben deshalb in ein separates Dokument (bspw. «Submissionsbedingungen» genannt) innerhalb der Ausschreibungsunterlagen ausgelagert.

KAPITEL 9: ANHÄNGE ZUM PFLICHTENHEFT

Den Abschluss des Pflichtenhefts bildet das Verzeichnis der Anhänge und Beilagen zum Pflichtenheft. Entweder sind sie vom Anbieter zu beantworten (auszufüllen) oder sie dienen ihm als präzisierende Angaben zur Ausschreibung. Die Anhänge verstehen sich damit als integraler Bestandteil des Pflichtenheftes. Dazu zählen in der Regel folgende Dokumente:

- Eignungskriterienkatalog,
- Anforderungskatalog,
- Preiseingabeformular,
- Vorlage für Selbstdeklaration,
- Vertraulichkeitserklärung,
- Vertragsentwürfe
- weitere Unterlagen zum Projekt, wie z.B. Vorstudien

ABKÜRZUNGSVERZEICHNIS

3TG	Zinn, Tantal, Wolfram, Gold
Abb.	Abbildungen
AGB	Allgemeine Geschäftsbedingungen
Amfori BSCI	amfori Business Social Compliance Initiative
Amt.Bull. S	Amtliches Bulletin des Ständerates
Art.	Artikel
Aufl.	Auflage
BAFU	Bundesamt für Umwelt
BBI	Bundesblatt
BBL	Bundesamt für Bauten und Logistik
BFH	Berner Fachhochschule
BGer	Bundesgericht
BGÖ	Öffentlichkeitsgesetz
BJ	Bundesamt für Justiz
BKB	Beschaffungskonferenz des Bundes
BöB	Bundesgesetz über das öffentliche Beschaffungswesen
Bst.	Buchstabe
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
bzw.	beziehungsweise
ChatGPT	(Chat)Generative Pre-trained Transformer
CLOUD-Act	Clarifying Lawful Overseas Use of Data Act

DSFA	Datenschutzfolgeabschätzung
DSG/KDSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DSV	Datenschutzverordnung
DVG	Gesetz über die Digitale Verwaltung des Kantons Bern
DR	Demokratische Republik
EfA	Einer-für-Alle-Ansatz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EFD	Eidgenössisches Finanzdepartement
EMBAG	Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben
EKG	Einkaufsgemeinschaft
ESG	Environmetal, Social and Corporate Governance
EW	Electronics Watch
ff.	fortfolgende
GPA	Government Procurement Agreement
GPL	General Public License
KI	Künstliche Intelligenz
Hrsg.	Herausgeber*innen
IaaS	Infrastructure as a Service
Ibid.	Ibidem, ebenda
IDG/ZH	Gesetz über die Information und den Datenschutz des Kantons Zürich
IKT	Informations- und Kommunikationstechnologien

ILO	International Labour Organization
ISB	Informatiksteuerorgan des Bundes
ISchV	Informationsschutzverordnung
ISG	Informationssicherheitsgesetz
ISMS	Informationssicherheits-Management-System
i.V.m.	in Verbindung mit
IVöB	Interkantonale Vereinbarung über das öffentliche Beschaffungswesen
Kap.	Kapitel
KG	Kartellgesetz
KI	Künstliche Intelligenz
KPIs	Key Performance Indicators
LGBTIQ	lesbian, gay, bisexual, transgender, intersexual, queer
LS	Loseblattsammlung
lit.	Littera (Buchstabe)
MetG	Bundesgesetz über die Meteorologie und Klimatologie
m.H.	mit Hinweisen
NCSC	Nationales Zentrum für Cybersicherheit
OECD	Organisation for Economic Co-operation and Development
OGD	Open Government Data
OHCHR	Office of the High Commissioner for Human Rights
Org-VöB	Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung
OR	Obligationenrecht

OS	Open Source
OSS	Open Source Software
PaaS	Platform as a Service
Para.	Paragraf
RBA	Responsible Business Alliance
revISG	Das neue Informationssicherheitsgesetz
RL 2014/24/EU	Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG Text von Bedeutung für den EWR
RMAP	Responsible Minerals Assurance Process
RVOV	Regierungs- und Verwaltungsorganisationsverordnung
rev.	revidiertes
Rz.	Randziffer
SaaS	Software as a Service
SECO	Staatssekretariat für Wirtschaft
sog.	sogenannte(e)
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch
TCO (Standard)	Tjänstemännens Centralorganisation
u.a.	unter anderem
UNDP	United Nations Development Programme
vgl.	vergleiche
vs.	versus
VGer	Verwaltungsgericht

VöB	Verordnung über das öffentliche Beschaffungswesen
WEED	World Economy, Ecology & Development
WTO	World Trade Organization
ZBDK	Zentralschweizer Baudirektorenkonferenz
Ziff.	Ziffer
Zit.	Zitiert als