Stellungnahmen der Arbeitsgemeinschaft Nachhaltige Digitalisierung (AGND)

zur Öffentliche Konsultation zur Transformation des Vergaberechts

("Vergabetransformationspaket") durch das Bundesministerium für Wirtschaft und Klimaschutz

von Caroline Krohn und Manuel ‚HonkHase' Atug

17.02.2023

Die Arbeitsgruppe Nachhaltige Digitalisierung (AGND) ist eine Gruppe von unabhängigen Fachleuten, die sich mit den Langzeitfolgen der Digitalisierung befasst. Kernforderung dieser Arbeitsgruppe ist es, technische Schulden an kommende Generationen zu vermeiden und Security by Design in allen Institutionen und Systemen durchzusetzen. Die digitale Transformation verantwortungsvoll anzugehen, ist gleichsam eine technische wie ethische Aufgabe.

Inhaltsverzeichnis

Aktionsfeld 1: Stärkung der umwelt- und klimafreundlichen Beschaffung

Wir wollen die öffentliche Beschaffung ökologisch ausrichten und die Verbindlichkeit von umwelt- und klimabezogenen Anforderungen stärken. Wir streben Mindestquoten für klimafreundliche Produkte in der öffentlichen Beschaffung an und wollen uns am Aufbau eines Systems zur Berechnung von Klima- und Umweltkosten beteiligen.

Grundsätzliche Anmerkung: Nachhaltigkeit beschränkt sich nicht auf ökologische Fragen. Im Hinblick auf eine echte Transformation – gerade auch im Zuge der Digitalisierung – ist die soziale Frage eine mindestens ebenso wichtige. Alles, was in diesem Papier steht, hat mittelbare oder unmittelbare Auswirkung auf die Unversehrtheit des Einzelnen und der Gesellschaft. Wenn Weichen falsch oder auch nur einseitig gestellt werden, finden wir uns zwar in einer Situation wieder, in der der Mensch sich dem Klimawandel noch anpassen und überleben kann. Aber mit dem rein ökologischen Blick findet er sich dann in einer Welt wieder, in der er nicht mehr in Freiheit und Selbstbestimmung, in Vielfalt und Teilhabe in der Gesellschaft, in Sicherheit und Unversehrtheit, Wohlstand und Bildung leben wird.

Frage 1: Auf welcher Stufe des Vergabeverfahrens können Sie sich eine (verpflichtende) Berücksichtigung von umwelt- oder klimabezogenen Aspekten am besten vorstellen? Eher in der Leistungsbeschreibung, bei den Eignungs- oder Zuschlagskriterien, in den Ausführungsbedingungen oder in einer Kombination davon?

In der Leistungsbeschreibung sollte darauf hingewiesen werden, dass es der vergebenden Behörde wichtig ist, ausschließlich datenschutzkonforme und sichere digitale Infrastruktur in Auftrag zu geben und zu betreiben. Rechtskonformität muss immer ein zwingender Bestandteil eines Angebots sein; alles andere ist absurd, denn der Gesetzgeber sollte bei der Gesetzesausübung immer als erster berücksichtigt sein. Oder anders: Was nützt es, ein Gesetz zu erlassen, wenn der Staat selbst auf die Einhaltung nicht besteht?

Insofern muss der Hinweis auch nochmal dringend in die Eignungs- und Zuschlagskriterien eingegeben werden: nur wer glaubhaft zeigt, security-by-design und privacy-by-design glaubhaft zu praktizieren, kann überhaupt nur für einen öffentlichen Auftrag in Betracht kommen. Die Ausführungsbedingungen könnten daher beispielsweise die nach EU-DSGVO § 32 ohnehin verpflichtende Aufstellung der Technischen und Organisationalen Maßnahmen (TOMs) mitsamt der entsprechenden bzw. relevanten Auftragsverarbeitungsvereinbarungen (AVV) einreichen. Dies

würde keinen weiteren bürokratischen Aufwand bedeuten, weil die good governance eines Unternehmens dies ohnehin gebietet und die Bedingung in einer öffentlichen Ausschreibung einen zusätzlichen Anreiz bietet, sich der Compliance zu widmen.

Frage 2: Existieren aus Ihrer Sicht bereits zielgerichtete und hinreichend praxistaugliche Vorbilder für die verbindliche Berücksichtigung von Nachhaltigkeitskriterien (welche?)?

Wenn TOMs (s.o.) als Nachhaltigkeitskriterien gelten können, dann dies. Digitale Nachhaltigkeit im Sinne der IT-Sicherheit zum Schutz des Menschen findet sich zudem im BSI-Grundschutz, in der ISO 27xxx-Normreihe, auch in den KRITIS-Gesetzen (u.a. § 8a,b BSI-Gesetz), weitergehend in Industrieprüfungsnormen TISAX, SWIFT, PCI DSS, MA-Risk, etc.. Letztlich geht es immer darum, Menschen davor zu schützen, durch digitale Maßnahmen, die schlecht, sprich: nachlässig/fahrlässig/opportunistisch/unverantwortlich/in reiner Gewinnerzielungs- und Kosteneinsparungsabsicht durchgeführt sind, gefährdet zu werden.

Frage 3: Welche rechtlichen oder praktischen Punkte könnten aus Ihrer Sicht am besten zu einer nachhaltigen öffentlichen Beschaffung beitragen? Wie hilfreich wären z.B. praktische Anleitungen, Begründungspflichten, Selbstverpflichtungen, Quoten, Ge- und Verbote oder Mindeststandards?

s.o.

Frage 4: In welchen Branchen sehen Sie besondere Chancen für die umwelt- und klimafreundliche Beschaffung? Gibt es Ihrer Ansicht nach Leistungen, die keine entsprechende Umwelt- oder Klimarelevanz haben könnten? Bitte erläutern Sie.

Sicherheit hat keine direkte Umwelt- und Klimarelevanz, muss aber mit demselben Stellenwert behandeln werden. Denn diese sichert nicht die Lebensgrundlagen in der physischen Welt, wohl aber die körperliche und geistige Unversehrtheit im Informationszeitalter. Die Vitalität – und damit die Notwendigkeit – der aus digitalem (Zusammen-)wirken verursachten Effekte für das Individuum und für die Gesellschaft werden weithin unterschätzt und müssen dringend in einer Vergabetransformationsinitiative möglichst frühzeitig integriert werden.

Aktionsfeld 2: Stärkung der sozial-nachhaltigen Beschaffung

Wir wollen die öffentliche Beschaffung sozial ausrichten und die Verbindlichkeit sozialer Anforderungen stärken.

Soziale Anforderungen sind aus Sicht der AGND gesellschaftliche Ziele, wie Freiheit, Selbstbestimmung, Teilhabe, Vielfalt, Schutz, Bildung, Gesundheit und Wohlstand – der Koalitionsvertrag zeichnet ein Gesellschaftsbild, das bei sämtlichen digitalisierbaren Beschaffungskomponenten zu berücksichtigen ist. Wirkungsmessungen, Monitorings, Prüfungen und Auditierungen müssen zu einer evidenzbasierten Auftragsvergabe führen. Es muss zudem ein Alignment stattfinden, damit nicht “versehentlich” negative (Neben-)Effekte erzeugt werden.

Frage 5: Welche Aspekte einer sozial verantwortlichen Beschaffung sollten über die Berücksichtigung von Tarifverträgen hinaus aus Ihrer Sicht prioritär bei der öffentlichen Beschaffung verfolgt oder intensiviert werden?

Wann immer an irgendeiner Stelle eines Projekts oder einer Maßnahme personenbezogene Daten involviert sind, ist eine besondere Schutzverpflichtung einzuhalten. Dies ist eigentlich auch bereits Rechtslage, findet nur in der öffentlichen Beschaffung weder implizit noch explizit irgendwo statt; weder auf Landes- noch auf Bundesebene.

Frage 6: Wie könnte dies aus Ihrer Sicht am besten im Vergabeverfahren und -recht integriert werden?

Technische und Organisatorische Maßnahmen (TOMs) sowie alle relevanten Auftragsverarbeitungsverträge (AVV) lt. EU-DSGVO sind bei einer Ausschreibung standardmäßig mit einzureichen und auf Seiten der Beschaffungsstelle zu überprüfen. Mindestens stichprobenhaft sollten dann jährlich Prüfungen erfolgen. Datenschutz- und Datensicherheitsvorfälle sind der auftraggebenden Behörde unmittelbar zu melden und Krisenbewältigungsschritte sind mit der auftraggebenden Behörde abzustimmen. In Vergabeprojekten ab einem Schwellenwert von 5 Mio Euro und/oder 50.000 zu verarbeitenden personenbezogenen Daten sollte zudem das BSI-Grundschutzzertifikat und/oder eine ISO-Zertifizierung vorgelegt werden.

Frage 7: Wie können soziale Innovationen wie. z.B. Sozialunternehmen durch die öffentliche Vergabe gestärkt werden?

Die Kosten für IT-Sicherheitsmaßnahmen im Vorfeld einer Vergabe könnte von der öffentlichen Hand getragen werden. Der Prozess sollte möglichst unkompliziert, aber – anders als bei "GoDigital" – seinerseits vollständig Datenschutz- und Datensicherheitskriterien genügen.

Aktionsfeld 3: Digitalisierung des Beschaffungswesens

Wir wollen die öffentlichen Vergabeverfahren digitalisieren, indem wir die rechtssichere Digitalisierung der Vergabe vorantreiben. Dazu wird unter anderem eine anwenderfreundliche zentrale Plattform geschaffen.

Anwenderfreundlichkeit ist mitnichten das einzige und noch nicht einmal das relevanteste Kriterium einer digitalen Plattform. Entscheidend ist: überall dort, wo Menschen ihre Daten hinterlegen müssen, muss für Sicherheit in Form von starken Authentifizierungs- und Authorisierungsprozessen, starker Verschlüsselung, rechtskonformer Verarbeitung und unter Hinzuziehung nachweislich integrer Dienstleister*innen im gesamten Wertschöpfungsprozess gesorgt sein. Eine Kompromittierung staatlich veranlasster digitaler Dienstleistung ist besonders katastrophal. Zudem dürfen sicherheitsaffine Menschen und Unternehmen nicht durch ein schlecht gesichertes Angebot diskriminiert werden.

Frage 8: Welche der folgenden Dienste kennen Sie und welche davon nutzen Sie? Zentraler Bekanntmachungsservice, Datenservice öffentlicher Einkauf, die neuen elektronischen Standardformulare, weitere Projekte zur Digitalisierung des öffentlichen Einkaufs (bitte benennen). Was fehlt aus Ihrer Sicht zur vollumfänglichen Digitalisierung der Vergabeverfahren?

Zur letzten Frage: konsequenter Datenschutz und konsequente Datensicherheit statt digitaler Populismus (Digitalisierung als Selbstzweck) und Glitzer (unnötige und unausgereifte „Hype-"Tools, wie KI oder Blockchain sowie eine einseitige Fokussierung auf Anwenderfreundlichkeit).

Frage 9: Spricht aus Ihrer Sicht etwas gegen die elektronische Einreichung von Nachprüfungsanträgen und virtuelle mündliche Verhandlungen in Nachprüfungsverfahren? Bitte erläutern Sie.

Identifizierungsnotwendigkeit und Datenvertraulichkeit bzw. Datenintegrität sind derzeit leider noch Zielkonflikte. Wenn Beantragungen die Möglichkeit bieten, digital Daten aller Art, vor allem aber Geschäftsgeheimnisse (zB Informationen über Dritte, wie zB Referenzen) und

personenbezogene Daten hochzuladen oder zu hinterlegen, muss die anfragende Instanz für die absolute Vertraulichkeit und Integrität sorgen.

Frage 10: Welche weiteren Schritte sind praktisch und rechtlich zur Digitalisierung der Nachprüfungsverfahren aus Ihrer Sicht insbesondere erforderlich?

Auch die öffentliche Hand hat eine inhärente Transparenz- und Offenlegungspflicht über die Schutzmaßnahmen eines Vergabeprozesses, der digitalisiert ist. So wie die Unternehmen und Organisationen, die sich um einen öffentlichen Auftrag bemühen, nachweisen müssen, dass sie alles dafür tun, den Staat durch digitale Nachlässigkeit/Fahrlässigkeit/Verantwortungslosigkeit in Verlegenheit zu bringen, muss der Staat seinerseits mit bestem Beispiel vorangehen.

Aktionsfeld 4: Vereinfachung und Beschleunigung der Vergabeverfahren

Wir wollen die öffentlichen Vergabeverfahren vereinfachen und beschleunigen sowie schnelle Entscheidungen bei Vergabeverfahren der öffentlichen Hand fördern.

Wenn ein digitaler Vorgang für Nutzer*innen einfach ist, ist er auch für Angreifer*innen einfach. Daten – insbesondere sensible Informationen – schaffen Begehren (bei ausländischen Nachrichtendiensten und weiteren staatlichen Akteuren, auf Überwachung und Spionage spezialisiere Unternehmen und in Organisierter Kriminalität wie Ransomware-Tätergruppierungen, die digital operieren).

Frage 11: Welche Vereinfachungs- und Beschleunigungspotentiale sehen Sie noch im Vergaberecht? Wo setzen aus Ihrer Sicht Rechtssicherheit, Wirtschaftlichkeit oder das europäische Vergaberecht wichtige Grenzen?

EU-DSGVO, BDSG und ggfs. KRITIS.

Frage 12: Inwieweit können Sie sich eine Flexibilisierung des Losgrundsatzes vorstellen, etwa für wichtige Transformationsvorhaben?

Es gibt im rein Digitalen keine Zufälle; das, was einem Zufall am nächsten kommt, ist eine Pseudo-Randomisierung.

Frage 13: Wie kann die Vergabepraxis einfacher und schneller gelingen? Wie könnten Ihrer Ansicht nach Vergabeverfahren z.B. noch weiter professionalisiert werden? Warum haben Sie oder Ihr Unternehmen sich zuletzt gegebenenfalls nicht mehr an öffentlichen Vergabeverfahren beteiligt?

Wenn über externe Projektträger die Datenschutz- und Datensicherheitsstandards mangelhaft sind, was leider die Regel ist.

Frage 14: Inwieweit können Sie sich auch eine weitere Vereinheitlichung des Vergaberechts vorstellen (formell in einem „Vergabegesetz“ oder materiell stärkere Angleichungen)?

Keine Beantwortung dieser Frage.

Aktionsfeld 5: Förderung von Mittelstand, Start-Ups und Innovationen

Die Zugangshürden für den Mittelstand sollen nicht erhöht werden. Wir wollen die öffentliche Beschaffung innovativ ausrichten. Öffentliche Ausschreibungen sollen zum Beispiel für Start-Ups einfacher gestaltet werden.

Der kleinere Mittelstand und Startups gehören zu den schwierigsten Playern im Bereich IT-Sicherheit. Es gibt sehr viele digital- bzw. datengetriebene neue Geschäftsmodelle. Sie alle eint, dass sie vor allem Opportunitäten im Blick haben und dass sie keine Ressourcen haben. Gerade dort muss aber Sicherheit angesetzt werden, nicht erst wenn sie irgendwann Zeit haben oder anderen Zwängen ausgesetzt sind, endlich einmal ihre digitalen Hausaufgaben zu machen. Hier spielt der Staat eine herausragende Rolle, die richtigen Anreize zu setzen, IT-Sicherheit und Datensicherheit nicht als optional zu betrachten, sondern als Notwendigkeit, die nicht in Frage gestellt werden kann. Fehlertoleranz kann überall dort praktiziert werden, wo Menschen nicht zu Schaden kommen. Daten, die geleakt werden, verschwinden allerdings niemals aus dem Internet – und damit aus dem Zugriff kriminell agierender Gruppen. Darum ist es unabdingbar, nicht an der Sicherheitshürde zu drehen, sondern die Förderung darin zu sehen, weitere Anreize für die Auseinandersetzung mit “security by design” und “privacy by design” anzusetzen: Der Staat kann für die erforderliche Beratung aufkommen, oder Ressourcen zur Verfügung stellen, die Programmcodes überprüfen, korrigieren oder dokumentieren. Aber gerade bei Startups und

gerade im Mittelstand ist ein Mindestmaß an Sicherheit zur Bedingung für staatliche Förderung unstrittig.

Frage 15: Welche rechtlichen und praktischen Stellschrauben sehen Sie für eine starke Einbeziehung von kleinen und mittelständischen Unternehmen in die öffentliche Beschaffung?

Durch die zunehmende Bedrohung in der Cybersicherheit, durch Skalierungs-, Beschleunigungs- und Netzwerkeffekte sowie durch das Phänomen der Supply Chain Attacken ist es unabdingbar, gerade kleinere Akteure, die nicht per se im Visier des Verbraucherschutzes und der Sicherheitsregulation sind, an dieser Stelle in die Pflicht zu nehmen. Gerade wenn sonst Kontrollhürden abgebaut werden sollen, ist es besonders wichtig, Sorgfaltspflichten bei den Unternehmen anzusetzen und verbindlich zu verankern.

Frage 16: Welche Rolle spielen für Sie zum Beispiel Unteraufträge oder Bietergemeinschaften, Eignungskriterien oder Ausführungsbedingungen? Welche rechtlichen und/oder praktischen Herausforderungen sehen Sie hier?

Speziell die sogenannten Supply Chain Attacks liefern eine erhebliche Flanke in der digitalen Sicherheit. Rechtskonformität durch Auftragsverarbeitungsverträge gemäß der EU-DSGVO sind festzuschreiben und als Beleg für die ernsthafte und gut durchdachte Auseinandersetzung mit dem Thema eine Grundvoraussetzung für das Beziehen öffentlicher Gelder. Doch nicht nur die rechtliche Absicherung ist für die staatliche Seite von Belang: gerade die technische Seite muss jedwedes Risiko ausschließen, sonst überträgt sich die Fahrlässigkeit eines auftragnehmenden Unternehmens auf den auftraggebenden Staat. Wir agieren alle global in komplexen Wertschöpfungsketten. Jede Komponente kann einen Sicherheitsvorfall im Netzwerk erzeugen und Menschen konkret physisch oder mental beschäftigen. Eine Gesellschaft ist nur so sicher wie ihr schwächstes Glied, darum muss der Staat Sorge tragen, dass in seinem Einflussbereich das schwächste Glied noch weniger vorkommt als irgendwo sonst, denn sonst ist der Staat selbst das schwächste Glied.

Frage 17: Wie stark nutzen Sie Markterkundungen oder funktionale Ausschreibungen bzw. innovative Vergabeverfahren, um Innovationen und Start-Ups im Design von Vergabeverfahren besser zu berücksichtigen? Welche praktischen oder rechtlichen Hürden sehen sie hier?

Keine Beantwortung dieser Frage.

Frage 18: Was hat Sie ggf. bisher gehindert, innovative Vergabeverfahren (wie zum Beispiel dynamische Beschaffungssysteme oder elektronische Auktionen) zu nutzen?

Innovative Vergabeverfahren können keine sein, die das Recht brechen. Alles, was bisher digital angeboten wird, reicht einem EU-DSGVO-konformen Level nicht. Generell ist entscheidend: Funktionen möglichst simpel zu halten und die simplen Funktionen auf diese Weise auf die Sicherheit in der Datenübermittlung zu konzentrieren. Es dürfen keine unnötigen Daten erhoben werden. Die Speicherung muss auf BSI-Grundschutz-zertifizierten europäischen Clouds erfolgen. Zugriffe müssen restriktiv und festgelegt sein. Das sind nur einige Beispiele – die ob ihrer weitgehenden Abwesenheit bisher für sicherheitsaffine Unternehmen eher abschreckend sind.

Sonstiges

Die Aktionsfelder und Lösungsmöglichkeiten ergänzen und verstärken sich in vielen Fällen, stehen teilweise aber auch im Zielkonflikte zueinander. Zudem gibt es womöglich weitere Herausforderungen für die öffentliche Beschaffung, die rechtlich oder praktisch angegangen werden könnten.

Frage 19: Wie priorisieren Sie die Aktionsfelder? Welche aufgeworfenen Fragen sind Ihnen besonders wichtig?

Nachhaltigkeit ist weit mehr als Ökologie und Klimaschutz. Auch wenn diese Felder wichtig sind und rechtmäßig erkannt wird, dass Digitalisierung einen wichtigen Beitrag zur Erreichung dieser Ziele leisten kann, ist augenscheinlich, dass die allgemeingesellschaftliche Naivität über die sorgsam durchdachte und umgesetzte Digitalisierung selbst sich staatlicherseits einfach fortsetzt. Da hier aber eine besondere Verantwortung Bürger*innen gegenüber besteht, muss gerade an der Schnittstelle zwischen dem öffentlichen und dem privaten Sektor ein besonderes Augenmerk auf Sicherheit von Daten und von IT-Infrastruktur gerichtet sein. Dies schafft weitreichende Anreize und hebt das Bewusstsein und die Gesamtqualität der Sicherheit in Deutschland und Europa. Ein Vergaberecht, dass Datenschutz und Datensicherheit in diesen Zeiten nicht berücksichtigt, kann nicht innovativ, transformiert oder gar modern genannt werden.

Frage 20: Sehen Sie Zielkonflikte und falls ja, wie sollten diese aus Ihrer Sicht aufgelöst werden?

Einfachheit, Unmittelbarkeit und Barrierefreiheit werden im Kontext des Bürokratieabbaus immer in den Vordergrund gestellt. Dass all das aber dazu führen kann, dass in der Sicherheit Abstriche gemacht werden, scheint kaum jemand auf dem Schirm zu haben. Dies fängt schon bei Beantragungstools und Verfahren über Projektträger oder unmittelbar an. Natürlich sind Sicherheitsmechanismen im Netz nicht einfach, unmittelbar und barrierefrei, aber sie sind unabdingbar. Dies ist ein Zielkonflikt, der heute auflösbar ist, aber man muss sich der Thematik eben mit der notwendigen Aufmerksamkeit widmen.

Frage 21: In welchen weiteren Bereichen sehen Sie rechtlichen Anpassungsbedarf der Vergabeverfahren? Welche praktischen Lösungen sehen Sie als besonders wichtig an?

Keine Beantwortung dieser Frage.

Für Rückfragen und Vertiefungen steht die AG Nachhaltige Digitalisierung zur Verfügung.