IT-PLANUNGSRAT

Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung

Anforderungen an Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität

– Version vom 6. Februar 2024 –

Impressum

Herausgeber
Arbeitsgruppe Cloud Computing und digitale Souveränität
des IT-Planungsrats

Ansprechpartner
Referat DG II 2 „Digitale Souveränität für die IT der öffentlichen Verwaltung“
Bundesministerium des Innern und für Heimat
Postanschrift: Alt-Moabit 140, 10557 Berlin
Hausanschrift: Salzufer 1 (Zugang Englische Straße), 10587 Berlin
E-Mail: DGII2@bmi.bund.de
www.cio.bund.de

Stand
Februar 2024

Nachdruck, auch auszugsweise, ist genehmigungspflichtig.

Inhalt

1. Ausgangslage und Motivation 3

2. Ziel des Dokuments 4

3. Anforderungen 4

I. Selbstständigkeit 9

II. Selbstbestimmtheit 13

III. Sicherheit 15

4. Anlagen 20

Glossar 20

Abkürzungsverzeichnis 21

1. Ausgangslage und Motivation

Bund, Länder und Kommunen haben sich zum Ziel gesetzt, die Digitale Souveränität der Öffentlichen Verwaltung in Deutschland gemeinsam zu stärken. Grundlage dieses Vorgehens bildet das erarbeitete und beschlossene Eckpunktepapier[1], welches auf den Erkenntnissen einer durchgeführten strategischen Marktanalyse[2] zur Untersuchung von Abhängigkeiten von Softwareanbietern in der Bundesverwaltung basiert. Das vorliegende Papier ist Teil des im Eckpunktepapier definierten Handlungsfeldes 2 „strategische Lösungskonzeption" und gibt wichtige Hinweise und Empfehlungen im Bereich IT-Beschaffung.

Digitale Souveränität wird gemäß Eckpunktepapier zur Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung definiert als *„die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können"*. Dazu muss die Verarbeitung der für die Verwaltung notwendigen Daten durch zeitgemäße funktionale und vertrauenswürdige Informationstechnik gewährleistet werden. Dafür bedarf es einer Transformation der Informationstechnik der Öffentlichen Verwaltung, mit dem Ziel sie unabhängiger von einzelnen Anbietern und Produkten zu machen und ihre Resilienz zu erhöhen, insbesondere auch durch die Austauschbarkeit von Komponenten. Digitale Souveränität heißt also auch, Alternativen zu schaffen und einen offenen, wettbewerbsfähigen Markt zu unterstützen. Dies begünstigt Innovation sowie Flexibilität in der IT der Öffentlichen Verwaltung – zwei wichtige Treiber in der Digitalisierung in der Verwaltung. Digitale Souveränität hat somit das Potential, die Verwaltungsdigitalisierung zu beschleunigen.[3,4]

Digitale Souveränität ist insbesondere für die Öffentliche Verwaltung zur Erfüllung ihrer hoheitlichen Aufgaben durch digitale Verwaltungsprozesse wichtig. Sofern sie nicht ausreichend gewahrt ist, kann die Handlungsfähigkeit der entsprechenden Individuen und Institutionen negativ beeinflusst werden. Sie ist daher für die Öffentliche Verwaltung zentral und fortlaufend zu evaluieren.

Ein wesentlicher Aspekt Digitaler Souveränität im Hinblick auf Informations- und Kommunikationstechnik ist die Reduzierung von kritischen Abhängigkeiten von einzelnen Anbietern. Die nachfolgenden Punkte sollen dementsprechend Wechselmöglichkeiten fördern, die Gestaltungsfähigkeit der IT der Öffentlichen Hand sicherstellen und durch entsprechend gestaltete Vergabeverfahren auch Einfluss auf Angebote von Anbietern[5] haben. Unabhängig davon ist die Verwaltung auf allen föderalen Ebenen in Deutschland angehalten, ihre IT-Architektur im Sinne der Digitalen Souveränität zu gestalten.

---

[1] „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung; Eckpunkte – Ziel und Handlungsfelder" (Beschluss in 31. Sitzung IT-PLR, Entscheidung 2020/07 sowie Beschluss im IT-Rat Nr. 2020/01)

[2] Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern; Studie im Auftrag des Bundesministeriums des Innern, für Bau und Heimat, August 2019.

[3] Vgl. CIO Bund, Digitale Souveränität, https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html

[4] Landesgesetze (z.B. § 1 Gesetz zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen oder Art. 3 Gesetz über die Digitalisierung im Freistaat Bayern) definieren Digitale Souveränität abweichend.

[5] Vgl. Konzept: Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung – Strategische Ziele und Umsetzung.

Dieses Dokument gibt einen Überblick über für die Digitale Souveränität relevante Regelungsbereiche im Rahmen von Beschaffungsvorgängen, sowie eine initiale Übersicht über denkbare grundsätzliche Anforderungen und deren jeweilige Anwendungsbereiche. Diese Anforderungen wurden gemeinsam von Bund, Ländern, Kommunen sowie weiteren relevanten Stellen (z. B. Bundesamt für Sicherheit in der Informationstechnik, Beschaffungsamt des BMI) entwickelt.

2. Ziel des Dokuments

Ziel dieses Dokuments ist es, Empfehlungen für die Beschaffung von Informations- und Kommunikationstechnik durch bzw. für die Öffentliche Verwaltung[6] und deren bedarfs- und risikogerechte Anwendung zu geben. Diese Anforderungen sollen die Digitale Souveränität stärken, indem sie einen Rahmen für die Beschaffung von IT-Leistungen für die Öffentliche Verwaltung bietet. Im Ergebnis soll dies die Abhängigkeit von einzelnen Anbietern reduzieren und dadurch die Digitale Souveränität der Öffentlichen Verwaltung in ihrer Rolle als Auftraggeber, Nutzer und Bereitsteller von IT stärken. Relevante Zielgruppen hierbei sind in erster Linie die Beschaffungsstellen der Öffentlichen Verwaltung von Bund, Ländern und Kommunen. Mittelbar soll dieses Dokument auch Einfluss auf die entsprechenden Anbieter von Informations- und Kommunikationstechnik haben, indem es wesentliche Anforderungen darstellt, mit denen Anbieter in Vergabeverfahren künftig verstärkt rechnen können und müssen.

Dieses Dokument berührt die Anwendungsempfehlung des IT-Planungsrats zu den EVB-IT nicht. Die Empfehlungen aus diesem Dokument sollen die EVB-IT ergänzen. Unabhängig davon ist geplant, die wesentlichen Empfehlungen dieses Dokumentes im etablierten Prozess, im Austausch mit der IT-Wirtschaft, in die EVB-IT einzubringen bzw. diese entsprechend weiterzuentwickeln.

3. Anforderungen

Zur Erreichung des beschriebenen Ziels der Digitalen Souveränität formuliert die Öffentliche Verwaltung von Bund, Ländern und Kommunen hiermit gemeinsame Anforderungen an IT-Leistungen und die Auswahl der Anbieter.
Die Anforderungen werden zunächst entlang von 3 wesentlichen Aspekten Digitaler Souveränität - **Selbstständigkeit, Selbstbestimmtheit und Sicherheit** - definiert (vgl. Abbildung 1):

I. **Selbständigkeit** bedeutet, dass die Öffentliche Verwaltung die Nutzung der eingesetzten Digitalen Technologien kontrolliert und im Rahmen der vergabe- und vertragsrechtlich zulässigen Gestaltungsmöglichkeiten und im haushaltsrechtlich zulässigen, d. h. insbesondere wirtschaftlich sinnvollen Umfang Einfluss auf deren Gestaltung nimmt. Um dies zu erreichen, sollten entsprechende Anforderungen die Transparenz hinsichtlich der Rahmenbedingungen der

[6] Regelmäßige Fortschreibung vorgesehen.

Leistungserbringung, sowie den eigenständigen Betrieb durch die Öffentliche Verwaltung fördern.

II. **Selbstbestimmtheit** bedeutet, dass die Öffentliche Verwaltung eine wirkliche Wahlfreiheit bei den eingesetzten Technologien und Software hat und in sensiblen Bereichen und anderen besonders gelagerten Fällen auch deren Weiterentwicklung bestimmen oder wenigstens entscheidend mitbestimmen kann. Um dies zu erreichen, sollten entsprechende Anforderungen die Interoperabilität und Diversität fördern und so die Austauschbarkeit von Daten zwischen Software unterschiedlicher Anbieter bzw. die Austauschbarkeit von Software bei vollständiger Beibehaltung des Datenbestands gewährleisten, um Lock-In Effekte zu verhindern. Ebenso sollte sichergestellt werden, dass die vereinbarte Nutzung durch einen Anbieter oder Hersteller nicht einschränkbar ist. Weiterentwicklungen und Anpassungen durch Anbieter, die zu Einschränkungen bei der oder Auswirkungen auf die Nutzung durch die Öffentliche Verwaltung führen können, z. B. aufgrund vorhandener Restriktionen bestehender Infrastrukturen bei der öffentlichen Verwaltung, müssen für diese planbar sein und dementsprechend mit einer angemessenen Vorlaufzeit angekündigt werden.

III. **Sicherheit** bedeutet insbesondere, dass die in der Öffentlichen Verwaltung eingesetzten Technologien und aus deren Einsatz resultierenden Prozesse die Schutzziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) sowie die datenschutzrechtlichen Anforderungen (insbesondere solche der Datenschutzgrundverordnung) und die Anforderungen des Geheimschutzes, in dessen Anwendungsbereich, erfüllen. Entsprechend des erforderlichen Schutzniveaus ist zwischen unterschiedlichen Schutzbedarfen im Normalbetrieb nach BSI IT-Grundschutz (IT-GS), dem datenschutzrechtlichen Schutzbedarf und Anforderungen, die sich aus den verschiedenen Geheimhaltungsgraden laut Verschlusssachenanweisung (VSA) von Bund, Ländern und Kommunen ergeben, zu trennen. Geheimschutzrelevante Aspekte von Hardware und Software (VS-IT) sind VSA-konform umzusetzen.

Abbildung 1: Übersicht Aspekte der Digitalen Souveränität

Die folgenden Empfehlungen ergänzen sowohl die Anforderungen aus anderen einschlägigen Regelungen (z. B. IT-Grundschutz, VSA von Bund, Ländern und Kommunen, Mindeststandards zur Nutzung externer Cloud-Dienste des BSI oder C5) als auch die von der ausschreibenden Behörde selbst festzustellenden eigenen funktionalen und nichtfunktionalen Anforderungen. Sie betreffen primär die Beschaffung von IT-Dienst-/ Werkleistungen, Software und Hardware – unter Anwendung ggf. passender EVB-IT Verträge (z. B. EVB-IT Cloud).
Die in diesem Dokument gegebenen Hinweise, beispielsweise im Bereich IT-Sicherheit, ergänzen daher die Vorgaben an anderer Stelle bzw. in anderen Dokumenten, ersetzen oder reduzieren diese jedoch nicht.

Risikoorientierte Anwendung der Empfehlungen
Die Empfehlungen sind vor dem Hintergrund des Beschaffungsbedarfs und der Marktlage risikoorientiert anzuwenden. Die zur Anwendung durch den IT-Planungsrat empfohlenen und von der Verwaltung in Bund, Ländern und Kommunen aufgrund verschiedener Verwaltungsvorschriften verbindlich anzuwendenden EVB-IT stellen weiterhin eine geeignete Grundlage für die Beschaffung von IT-Leistungen dar. Diese bilden ein ausgewogenes Verhältnis von Aspekten der digitalen Souveränität, der Wirtschaftlichkeit und der Durchführbarkeit von Vergaben ab.
Das bedeutet, dass der Umfang, in dem die nachfolgenden Empfehlungen in Beschaffungen eingefordert werden, im Wesentlichen davon abhängen, ob unter einzelnen Gesichtspunkten erhöhte Anforderungen bestehen.

Dies kann z. B. hinsichtlich des Schutzbedarfs der betroffenen Daten bzw. Informationen (z. B. abhängig von dem Risiko für die Rechte und Freiheiten der betroffenen Personen) und den in einer Risikoanalyse festgestellten Risiken für die Digitale Souveränität der Fall sein. Das Ergebnis der Risikoanalyse ist auch unter Durchführbarkeits- und Wirtschaftlichkeitsgesichtspunkten sowie der Notwendigkeit der Aufgabenerfüllung zu bewerten.

Die entsprechenden Risikoanalysen (z. B. analog zu BSI Standard 200-3, ISO 27005 oder ISO 31000) sollten insbesondere die folgenden Kriterien berücksichtigen:

- Art und Umfang der durch die erbrachte Leistung unterstützten Verwaltungsaktivitäten
- Anforderungen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit der Daten (unter Beachtung von BSI IT-Grundschutz, etc.)
- Einschätzungen zur Zuverlässigkeit der Lieferkette bezüglich Leistungsinhalt[7]

[7] Rechtsgrundlage für die Prüfung des Lieferkettenmanagement- und Lieferkettenüberwachungssystems in einem Vergabeverfahren kann dafür z. B. § 46 Abs. 3 Nr. 4 Vergabeverordnung (VgV) sein. Verbindliche Regelungen zu den unternehmerischen Sorgfaltspflichten in Lieferketten enthält außerdem das ab 2023 geltende Lieferkettensorgfaltspflichtengesetz.

- Abhängigkeiten von einem oder mehreren Anbietern (z. B. Vendor-Lock-In), Möglichkeiten zur Rückmigration einschließlich Portierung von Daten
- Einhaltung der einschlägigen Vorschriften, insbesondere der datenschutzrechtlichen Vorschriften z. B. DSGVO, ePrivacy-Richtlinie[8] aber auch aller weiteren gesetzlichen Anforderungen, die zwingend sind.

Auf dieser Basis kann im Einzelfall und für wiederholt gleichartige Vorgänge eine vereinfachte Risikoanalyse begründet werden (z. B. in Form eines Vermerks), wenn evident ist, dass keine oder nur geringe zusätzliche Risiken für die Digitale Souveränität bestehen (z. B. bei Beschaffungen zusätzlicher Standardkomponenten bspw. zusätzliche Lizenzen), jedoch unter Berücksichtigung der gesamten eignen IT-Landschaft.[9]
Der vorstehend dargestellte risikobasierte Ansatz setzt jedoch voraus, dass dieser im Hinblick auf die jeweiligen Anforderungen rechtlich zulässig ist.[10]
Vielfach diskutiert wird auch der Aspekt der Datensouveränität. Für den Begriff der Datensouveränität besteht gegenwärtig noch keine feststehende, allgemein akzeptierte Definition. Grundsätzlich existieren zwei unterschiedliche Definitionsansätze. Einerseits kann Datensouveränität auf ein Individuum bezogen werden und meint dann die Kontrolle einer Person über die Erhebung, Speicherung und Verarbeitung der sie selbst betreffenden oder ihr zustehenden Daten. Ebenfalls möglich ist jedoch auch ein überindividuelles Verständnis des Konzepts „Datensouveränität", welches dann gleichbedeutend mit „digitaler Souveränität" gesetzt werden kann und auf Staatsebene die Freiheit eines Staates bei der Gestaltung und dem Einsatz digitaler Technologien auf seinem Staatsgebiet beschreibt. Datensouveränität unterscheidet sich dabei von Datenschutz dadurch, dass nicht nur personenbezogene Daten insbesondere vor ungerechtfertigter Erhebung, Speicherung, Verarbeitung und Weitergabe geschützt werden sollen, sondern alle Daten. Außerdem erfassen die Konzepte „Datensouveränität" und „digitale Souveränität" auch die im Umgang mit den Daten eingesetzten Technologien.[11]
Im Rahmen dieses Papiers wird, aufgrund der fehlenden Definitionsfestlegung, beiden Aspekten Rechnung getragen und beide Aspekte an den relevanten nachfolgenden Stellen für die IT der Öffentlichen Verwaltung als Ganzes betrachtet.

[8] Vgl. Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Amtsblatt Nr. L 201 vom 31/07/2002 S. 0037 – 0047.

[9] Dies bedeutet, dass beispielsweise viele an sich geringe Abhängigkeiten von einem Anbieter in Summe wieder zu einer erheblichen Abhängigkeit der gesamten eigenen IT-Landschaft von diesem Anbieter führen können.

[10] Beispielsweise darf die Anwendung dieses Ansatzes nicht dazu führen, dass personenbezogene Daten ohne eine Rechtsgrundlage verarbeitet werden, nur weil das Risiko für die Betroffenen bei einer unrechtmäßigen Verarbeitung als gering eingestuft wird. Auch in diesem Fall müssen die zwingenden gesetzlichen Anforderungen an die Verarbeitung erfüllt werden.

[11] Vgl. Bayrisches Forschungsinstitut für Digitale Transformation, Glossar, https://www.bidt.digital/glossar-datensouveraenitaet/

Datensouveränität wird jedoch nicht verstanden als eigentumsähnliche Verwertungshoheit und kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.[12] Zusätzlich schränkt Datensouveränität keinesfalls die Vorgaben des Datenschutzes ein.

Unabhängig von den unter I. bis III. dargestellten Anforderungen, bzw. ergänzend zu dem Aspekt der Datensouveränität sind die gesetzlichen Anforderungen zum Schutz personenbezogener Daten zu erfüllen. Diese unterliegen nur soweit einem risikobasierten Ansatz, als die einschlägigen datenschutzrechtlichen Regelungen dies zulassen. So bedarf es z. B. für die Verarbeitung jeder Art von personenbezogenen Daten, auch wenn es sich dabei nicht um Datenkategorien im Sinne des Art. 9 DSGVO handelt, einer Rechtsgrundlage. Hingegen kommt der risikobasierte Ansatz z. B. in Art. 32 DSGVO bei der Akzeptanz bzw. Wahl der vorzunehmenden technischen und organisatorischen Maßnahmen zum Datenschutz zur Anwendung. Obwohl auch unter Ziffer I. bis III. zum Teil auf konkrete datenschutzrechtliche Anforderungen eingegangen wird, gilt daneben stets die Anforderung einer unbedingten Einhaltung der anwendbaren Datenschutzvorschriften. Die Risikoanalyse für den Datenschutz ist (soweit ein risikobasierter Ansatz nach dem Vorstehenden zulässig ist) unter Berücksichtigung der datenschutzrechtlichen Gewährleistungsziele (Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit) durchzuführen. Bei Auftragnehmern (und Unterauftragnehmern) außerhalb der EU sind unter anderem die Anforderungen des Positionspapiers der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023 „Kriterien für Souveräne Clouds“ zu berücksichtigen. Entsprechendes gilt auch für die formalen gesetzlichen Anforderungen zum Schutz der Vertraulichkeit, insbesondere zum Schutz von anvertrauten Geheimnissen, der Verpflichtung nach Verpflichtungsgesetz, dem Meldegeheimnis oder dem Fernmeldegeheimnis sowie geheimschutzrechtliche Anforderungen, die nicht durch technologische Lösungen wie Verschlüsselung erfüllt werden.

Umsetzung der Empfehlungen

Die Empfehlungen sind im Kontext der zu beschaffenden Leistung, des adressierten Marktes und der Sicherstellung der Aufgabenerfüllung des öffentlichen Auftraggebers hinsichtlich ihrer Durchsetzbarkeit zu bewerten.

- Handelt es sich um Standardprodukte bzw. Standardleistungen, die für eine Vielzahl von Kunden identisch oder im Wesentlichen gleich angeboten werden, dann sind individuelle Anforderungen bzw. spezielle Anforderungen der Öffentlichen Verwaltung tendenziell schwerer durchzusetzen.
- Handelt es sich um Standardprodukte oder Standardleistungen für die Öffentliche Verwaltung, sind spezielle Anforderungen der Öffentlichen Verwaltung deutlich leichter durchsetzbar, weil die Anbieter in diesem Fall tendenziell eher bereit sind, auf die Bedürfnisse der Öffentlichen Verwaltung einzugehen oder weil die Produkte und Leistungen bereits darauf ausgerichtet sind.

[12] Vgl. Göttingen, 30.03.2017, Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Göttinger Erklärung: Vom Wert des Datenschutzes in der digitalen Gesellschaft

- Handelt es sich um individuelle Lösungen oder um Lösungen, die ohnehin für einzelne Kunden angepasst werden müssen, sind tendenziell sehr viele Anforderungen umsetzbar.

Grundsätzlich sollte das Ziel darin bestehen alle Anforderungen umzusetzen.
Dabei gilt außerdem, dass Anforderungen, die Auswirkungen auf die Gestaltung von Standardprodukten selbst haben, schwerer durchzusetzen sind, als Anforderungen, die das Umfeld der Produkte betreffen, z. B. deren Dokumentationen und ähnliche Themen.
Naturgemäß gibt es Ausnahmen von diesen Regeln. Beispielsweise kann es erforderlich sein, dass auch bei Standardprodukten einzelne Öffentliche Auftraggeber, z. B. Behörden wie das BSI, weitergehende Informationen wünschen und davon auch die Beschaffung abhängig machen. Zudem existieren Produktgruppen von Standardsoftware und auch von Hardware, die für Einsatzzwecke entwickelt wurden, deren Kunden stets hohen Wert auf Sicherheit legen. Hier werden die Anbieter eher bereit sein, Informationen und z. B. auch Quellcodes zur Verfügung zu stellen als bei anderen Standardprodukten.
Die empfohlenen Anforderungen sehen teilweise besondere Informationspflichten durch die Anbieter vor. Solche Pflichten sind stets auch vor dem Hintergrund zu betrachten, dass diese bei dem öffentlichen Auftraggeber Ressourcen für die Auswertung etc. erfordern können. (Beherrschbarkeit des Umgangs mit Informationen, Wahrung der Vertraulichkeit sensibler Informationen).
Zudem ist der Umfang der zu erteilenden Informationen und der Umgang damit vor dem Hintergrund des berechtigten Interesses der Wahrung von Betriebs- und Geschäftsgeheimnissen durch Anbieter, insbesondere der mittelständischen Wirtschaft und auch einer etwaigen Sicherheitsrelevanz zu bewerten.
Diejenigen Empfehlungen, die im konkreten Einzelfall berücksichtigt werden soll, müssen bereits im Vergabeverfahren als Anforderungen oder in den Vertragsbestandteilen vom Auftraggeber formuliert werden. Dies kann sowohl im jeweiligen EVB-IT Vertrag als auch in der Leistungsbeschreibung bzw. im Anforderungskatalog für die Leistung geschehen.

I. Selbstständigkeit

I.1 Zugang zu Dokumentation

Soweit nicht durch die jeweiligen Regelungen in den EVB-IT AGB abgedeckt, sollte in den Vergabeunterlagen festgelegt werden, welche weitergehenden Informationen auf welche Art und Weise dem Auftraggeber vom Auftragnehmer bei Bedarf zur Verfügung gestellt werden müssen. Sofern erforderlich, kann es sich dabei auch um über das allgemein offen zugängliche Maß hinausgehende Details der Implementierung oder auch Konfigurationsmöglichkeiten/Parametrisierung/Customizing handeln (z. B. vergleichbar zu den Vorgaben des C5:2020 PSS-01). Soweit es dabei nicht um spezifisch beauftragte Anwendungen, sondern um Standardprodukte geht, ist jedoch zu beachten, dass Auftragnehmern solche Informationen nicht immer zugänglich sind (z. B. wenn sie nur Händler der Produkte sind) und Hersteller solche Informationen ggf. weder an Händler

noch an Kunden herausgeben. Falls notwendig ist hierbei die vertrauliche Behandlung der Informationen durch den Auftraggeber zu regeln und vertraglich zu fixieren.[13]

I.2 Geschäftsmodelle und Arbeitsweisen der Anbieter transparent machen

Der Auftraggeber sollte sich im Vorfeld einer geplanten Beschaffung einen Überblick über Geschäftspraktiken und Geschäftsmodelle von Anbietern verschaffen und die daraus gewonnenen Erkenntnisse z. B. hinsichtlich der Seriosität von Geschäftsmodellen bei den Anforderungen an die Leistung und an die Eignung der potentiellen Bieter berücksichtigen.[14]. Zudem sollte sich der öffentliche Auftraggeber, z.B. durch vertraglich vereinbarte Statusgespräche mit dem Auftragnehmer, einen Überblick hinsichtlich anstehender relevanter Änderungen am Geschäftsmodell (z. B. Lizenzmodell, Vertriebsmodell, Abkündigung von Produkten) verschaffen.

I.3 Weitergabe von Anforderungen an Unterauftragnehmer

Alle Zusicherungen des Auftragnehmers, insbesondere die Einhaltung der technischen und organisatorischen Maßnahmen zum Datenschutz (insbesondere im Rahmen der Auftragsverarbeitung), Transparenz (Informationsbereitstellung, Knowhow-Transfer, etc.), sind von Unterauftragnehmern ebenfalls zu gewährleisten.[15] Sämtliche im Rahmen dieses Papieres erhobenen bzw. definierten Anforderungen sind auch an Unterauftragnehmer weiterzugeben. Dies sollte grundsätzlich vertraglich fixiert werden.

I.4 Zustimmung zum Einsatz von Unterauftragnehmern

Soweit nicht im Vergabeverfahren erfolgt, hat der Auftragnehmer unmittelbar nach Vertragsschluss bzw. im Zuge des Vertragsschlusses eine Übersicht über alle Unterauftragnehmer und deren Auftragsanteile an den Auftraggeber zu übermitteln.[16] Der Einsatz von Unterauftragnehmern und deren Wechsel sollte grundsätzlich der Zustimmung des öffentlichen Auftraggebers bedürfen oder diesem zumindest ein Widerspruchsrecht zustehen. Dies ist jeweils in den relevanten EVB-IT Vertragstypen abgebildet. Die Vorlaufzeit für diese Information sollte vom Auftraggeber in Abhängigkeit von

[13] Bei Open Source Software entfällt dies üblicherweise.

[14] Derzeit sieht lediglich § 55 Sektorenverordnung (SektVO) nur für den Sektorenbereich vor, dass Angebote mit Erzeugnissen aus Drittländern unter bestimmten Voraussetzungen zurückgewiesen werden können oder bei der Wertung benachteiligt werden können. Eine analoge Übernahme in das klassische Vergaberecht ist derzeit nicht möglich (vgl. OLG Düsseldorf, B. v. 1.12.2021, Verg. 54/20), solange nicht auf EU-Ebene, etwa mit ergänzenden Drittlandsklauseln, nachgesteuert wurde. Gesetzliche Grundlage für die Prüfung und ggf. Ausschluss des Unternehmens von der Teilnahme an einem Vergabeverfahren bieten in diesem Zusammenhang unter anderem § 123, 124 Abs. 1 Gesetz gegen Wettbewerbsbeschränkungen (GWB) und § 46 Abs. 2 VgV.

[15] Selbstverständlich muss der Unterauftragnehmer in seinem Verantwortungsbereich auch sonstige Verpflichtungen einhalten, die an den Auftragnehmer zu stellen sind.

[16] Vgl. § 4 Nr. 4 VOL/B bzw.§ 9 VSVgV, insbesondere § 9 Abs. 1 S. 2 VSVgV (Änderungen bei Unterauftragnehmern sind mitzuteilen).

den erwarteten Folgen eines solchen Widerspruchs individuell festgelegt werden.[17] Idealerweise führt ein Widerspruch dazu, dass der neue Unterauftragnehmer nicht eingesetzt, die Leistung aber dennoch vereinbarungsgemäß erbracht wird.[18]

I.5 Einblick in Datenströme / Verhindern von Datenabfluss

Der Auftragnehmer legt dem Auftraggeber auf Anfrage lückenlos offen, welche Daten er von ihm verarbeitet und welche zur Erbringung der vertraglichen Leistung zwingend verarbeitet werden müssen. Dies schließt die Information über Daten, die von seinen IT-Systemen zu externen IT-Systemen übertragen werden, sowie im Sinne der Transparenz die Nachvollziehbarkeit der Datenverarbeitung insbesondere die Verarbeitung, Ablageorte und Transportwege der Daten, ein. Die Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form übermittelt werden. Von Seiten des Auftraggebers kann ansonsten eine Nachbesserung der übermittelten Informationen verlangt werden. Hierfür notwendig sind organisatorische und sofern sinnvoll möglich technische Maßnahmen. Der Auftragnehmer schafft die Voraussetzungen dafür, dass für den Auftraggeber die notwendigen Informationen leicht zugänglich sind. Zusätzlich muss der Auftragnehmer frühzeitig prüfen und den Auftraggeber informieren, ob durch neue Features und geänderte Konfigurationen neue oder veränderte Datenabflüsse entstehen.

Diese Vorgaben schränken die Vorgaben der Free-Flow-Verordnung nicht ein, diese sind uneingeschränkt zu beachten.

I.6 Informationen über Neuerungen

Im Rahmen beispielsweise regelmäßiger Statusgespräche (siehe dazu I.2) soll der Auftragnehmer, den Auftraggeber auch über neuartige Produkte, Technologien (z.B. APIs, Schnittstellen) und weitere Produktlinien informieren. Soweit die vertraglichen Leistungen betroffen sind, z. B. durch neue Programmstände, sollte dies mit einem hinreichenden zeitlichen Vorlauf geschehen, damit ggf. notwendige Sicherheitsanalysen durchgeführt werden können.

Zusätzlich sind Änderungen der Datenverarbeitung, Speicherorte, Datenübertragungen und Transportwege etc., insbesondere wenn sie Änderungen an eingesetzten Software-Komponenten betreffen, in diesem Rahmen mitzuteilen.

I.7 Informationen über Risiken

Es sollte geregelt werden, dass der Auftragnehmer Informationen, welche Einfluss auf die Bewertung von Risiken für die Informationssicherheit oder den Betrieb oder den

[17] Dies kann zum Beispiel bedeuten, dass der Auftragnehmer über Änderungen bezüglich der Unterauftragnehmer mit einer Vorlaufzeit zu informieren hat, die dem Auftraggeber eine Neuausschreibung der betreffenden Leistung ermöglicht., wenn der Widerspruch zu einem Sonderkündigungsrecht (und nicht zum Verzicht auf den Einsatz des neuen Unterauftragnehmers) führt. Vergaberechtliche Regelungen zu Auftragsänderungen während der Vertragslaufzeit (vgl. § 132 GWB) sind zu beachten.

[18] Siehe z.B. §4 Nr. 4 VOL B

Schutz personenbezogener Daten haben, unverzüglich dem Auftraggeber mitteilt, es sei denn, die vom Auftragnehmer vorzunehmende Abwägung ergibt, dass ein Bekanntwerden einer Schwachstelle vor Vorliegen einer wirksamen Gegenmaßnahme nicht vertretbar ist. Zu jeder entsprechenden Schwachstelle ist anzugeben, ob und bis wann für diese entsprechend neue Programmstände (z. B. Patches, Updates) verfügbar sind.

Cloud-Anbieter betreiben oder verweisen auf ein tagesaktuell gepflegtes Online-Register bekannter Schwachstellen, die den bereitgestellten Cloud-Dienst sowie vom Cloud-Anbieter bereitgestellte Assets betreffen, die Cloud-Kunden in ihrem Verantwortungsbereich selbst installieren, bereitstellen oder betreiben müssen (vgl. C5 PSS-02 i. V. m. PSS-03).

Zusätzlich sind Informationen zur Einleitung von Sofortmaßnahmen, wie Empfehlungen für eine sichere Nutzung, wenn Sicherheits-Patches oder Sicherheits-Updates noch nicht vorliegen (Workaround-Maßnahmen-Empfehlungen), bis hin zur Empfehlung der Außerbetriebnahme der Komponenten zur Verfügung zu stellen.

I.8 Transparenz über gesetzliche Informationsweitergabeverpflichtungen des Auftragnehmers und Möglichkeiten zur Unterbindung nicht gewünschter Informationsweitergaben

Aufgrund verschiedener gesetzlicher Regelungen anderer Staaten bestehen für den Auftragnehmer ggf. Pflichten zur Weitergabe von Informationen an deren Regierungsstellen. Daher ist bereits im Vorfeld des Vergabeverfahrens, spätestens jedoch in dessen Rahmen zu klären, welche solcher Pflichten für die jeweiligen Bieter bestehen, damit der Auftraggeber diese Informationen ggf. bewerten und Konsequenzen daraus hinsichtlich des Umgangs mit seinen, ggf. sensiblen Daten ziehen kann. Der Auftraggeber berücksichtigt diese Informationen in seiner Risikoanalyse. Im Extremfall kann dies zum Ausschluss des Angebots oder nach Vertragsschluss zur Inanspruchnahme eines Sonderkündigungsrechts führen.

I.9 Keine unberechtigte Übermittlung an Dritte

Eine unberechtigte Übermittlung von Informationen an Dritte ist untersagt.

Dies umfasst auch jegliche sonstige Verarbeitung von Informationen außerhalb des vertraglich vereinbarten Rahmens, insbesondere von personenbezogenen Daten (z. B. auch Übermittlung an Nachrichtendienste und Sicherheitsbehörden, sofern eine Rechtsgrundlage hierfür nicht vorliegt).

Zusätzlich kann mit dem Auftragnehmer vertraglich vereinbart werden, dass bei Anfragen zur Herausgabe von Informationen im Rahmen ausländischer Gesetze der Auftragnehmer dazu verpflichtet ist für den Schutz der Daten zu streiten und den Auftraggeber unverzüglich und unaufgefordert über entsprechende Anfragen zur Herausgabe von Informationen zu informieren.

I.10 Zugänglichmachung von Quellcodes, Prozess- und Entwurfsdokumentation

Soweit nicht ohnehin die Übergabe von Quellcodes, Entwicklungsdokumentationen etc. vereinbart ist, wie z. B in Verträgen auf Basis der EVB-IT System, EVB-IT Erstellung und EVB-IT Dienstleistung, kann vorgesehen werden, dass der Auftragnehmer im Bedarfsfalle, z. B. bei einer Einstellung des Geschäftsbetriebes die Herausgabe von (bzw. notfalls nur die Einsicht in) Quellcodes, sowie Prozess- und Entwicklungsdokumentationen, gemäß eines gemeinsam vereinbarten Prozesses und zu vorab vereinbarten finanziellen Konditionen ermöglicht, z. B. auf Basis eines ESCROW-Agreements[19]. Einzelheiten bezüglich der Herausgabe und entsprechende Bedarfsfälle sind zu definieren. Der Auftraggeber sollte zur Prüfung auch Dritte beauftragen können.

I.11 Rechtmäßigkeit

Daten müssen auf rechts- und vertragskonforme Weise verarbeitet werden. Um dies prüfen zu können, sollte der öffentliche Auftraggeber berechtigt werden, dies regelmäßig mit geeigneten Maßnahmen, zu überprüfen. Die EVB-IT Cloud-AGB sehen entsprechende Regelungen vor, die sinngemäß ggf. auch in nicht Cloud-Anwendungsfällen Anwendung finden können. Bei Nichteinhaltung sind unverzüglich Gegenmaßnahmen einzuleiten (z. B. Vertragskündigung, etc.). Welche Gegenmaßnahmen geeignet sind, ist jeweils im Einzelfall vom Auftraggeber individuell zu entscheiden

I.12 Transparenz, Zweckbindung und Datenminimierung

Schützenswerte Daten - gemäß DSGVO - dürfen nur für die vertraglich festgelegten Zwecke erhoben werden und die Erhebung und Speicherung muss auf das für die Zwecke der Verarbeitung notwendige und jeweils zulässige Maß beschränkt sein. Ferner hat die Verarbeitung in einer für den Auftraggeber nachvollziehbaren Weise zu erfolgen. Unberührt bleibt die Verpflichtung des Auftragnehmers zur Einhaltung auch der darüber hinaus gehenden Gewährleistungsziele des Datenschutzes, der Informationssicherheit und des Geheimschutzes.

II. Selbstbestimmtheit

II.1 Funktionale neue Programmstände

Neue Programmstände für den genutzten Dienst bzw. Service sind zu dokumentieren und zu protokollieren. Grundsätzlich dürfen neue Programmstände (funktional oder sicherheitsrelevant) nicht die Konfiguration (z. B Sicherheitseinstellungen) der zu aktualisierenden Software ändern; ist dies ausnahmsweise doch der Fall, ist der Auftraggeber in der Dokumentation explizit darauf hinzuweisen und es muss beschrieben werden, ob und wenn ja wie Änderungen an der Konfigurationseinstellung rückgängig gemacht

[19] Dabei ist zu beachten, dass ESCROW-Agreements nach einigen Auffassungen für nicht „insolvenzfest“ gehalten werden.

werden können. Neue Programmstände dürfen nur qualitätsgesichert und von einer vertrauenswürdigen Quelle,[20] zur Verfügung gestellt werden.

II.2 Insolvenz / Ausfall des Herstellers/Auftragnehmers

Für den Fall einer Insolvenz des Herstellers/Auftragnehmers oder eines anderen Ereignisses, welches den Ausfall des Herstellers/Auftragnehmers bzw. seiner Fähigkeit zur Erbringung der vereinbarten Leistung verursacht, werden von dem Auftraggeber bereits bei der Vertragsgestaltung – soweit unter Risikogesichtspunkten erforderlich – Regelungen getroffen, die einen autarken Betrieb und eine autarke, zumindest übergangsweise Weiterentwicklung beschaffter Software durch verwaltungseigenes oder von der Verwaltung beauftragtes Personal ermöglichen (siehe dazu u.a. I.10).

II.3 Standardisierte und offene Schnittstellen

Die Lösungen bieten dokumentierte, standardisierte und offene Schnittstellen, um Austauschbarkeit und Erweiterbarkeit zu ermöglichen. Soweit ausnahmsweise proprietäre Schnittstellen nicht vermeidbar sind, etwa aus zwingenden technischen Gründen, sind diese vollständig, einschließlich der Kommunikationsprotokolle etc. zu dokumentieren.

II.4 Offene Dokumentenstandards und etablierte Industriestandards

Die Lösungen nutzen zum Datenaustausch grundsätzlich etablierte offene Standards (z.B. Dokumentenstandards, Dateistandards, Geodatenstandards, etc.)[21] oder ersatzweise etablierte Industriestandards (z. B. allgemein verbreitete Dokumentendateiformate). Soweit ausnahmsweise nicht offene Standards verwendet werden, sind diese vollständig zu dokumentieren.

II.5 Modulare und erweiterbare Architektur

Die Lösungen ermöglichen ihre Nutzung in modularen Architekturen und die lose Kopplung von Komponenten durch klar definierte, dokumentierte, standardisierte, offene Schnittstellen. Als Grundsatz gilt: Schnittstellen können erweitert, nicht aber in ihrer Funktionalität nachträglich, ohne Einverständnis des Auftraggebers, modifiziert werden, außer es handelt sich um die Abschaltung einer Funktionalität die erhebliche Sicherheitsrisiken mit sich bringt. („Open for extension, closed for modification"). Änderungen von Schnittstellen werden mit einem vertraglich zu vereinbarendem Vorlauf avisiert, mindestens jedoch so rechtzeitig, dass der Auftraggeber die Anpassung von angeschlossenen Systemen vornehmen bzw. veranlassen kann, ohne dass es zu einer Unterbrechung der Nutzung kommt.

---

[20] Dies ist im Allgemeinen der Fall, wenn eine Gesellschaft oder Organisation dem europäischen Rechtsrahmen im Hinblick auf Datenschutz und IT-Sicherheit unterliegt.

[21] Strengere Vorschriften sind zum Teil im Landesgesetzten bereits festgelegt z.B. Art. 3 Abs. 4 BayDiG

II.6 Leistungseinschränkung beim Auftragnehmer

In Bezug auf für die öffentliche Verwaltung besonders wichtige Systeme, beispielsweise Systeme mit einer hohen Bedeutung für die Aufgabenwahrnehmung der jeweiligen Behörde, müssen Behörden bzw. Auftraggeber ihre eigenen Anforderungen an Betrieb und Wartbarkeit konkretisieren und entsprechende Rechteinräumungen durch den Auftragnehmer vorsehen, um im Falle von langfristigen oder dauerhaften Leistungseinschränkungen des Auftragnehmers beschaffte Produkte und Lösungen im Bedarfsfall auch auf einer eigenen Infrastruktur betreiben zu können. Dazu müssen die organisationseigenen Software- und Hardware-Komponenten identifiziert und analysiert werden (z.B. Architektur Verteilungsdiagramm, textuelle Beschreibung, Helm/Terraform Scripts).

Der Auftragnehmer hat die Lösungen so zu gestalten und seine Leistungen so zu erbringen, dass die oben genannten Anforderungen der Öffentlichen Hand umgesetzt werden können. Beispielsweise sind entsprechende Nutzungsrechte an der Software zu erteilen, damit die Software auch auf der eigenen Infrastruktur der Öffentlichen Hand betrieben werden kann und entsprechende Migrationsprozesse festzulegen, sofern sinnvoll bzw. vom Auftraggeber gewünscht. Zusätzlich sind gesicherte Unterstützungszeiträume und -Kanäle mit entsprechenden Ressourcen zur Gewährleistung eines sicheren und robusten Betriebs vertraglich zu definieren.

III. Sicherheit

III.1 Gewährleistung von Integrität, Vertraulichkeit und Verfügbarkeit

Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Durch geeignete technische und organisatorische Maßnahmen muss sichergestellt werden, dass die Daten vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Veränderung geschützt werden.

Dies bedeutet insbesondere, dass Informationen über gewählte Konfigurationen, IT-Probleme oder IT-Sicherheitsvorfälle vertraulich behandelt werden und in den dafür vorgesehenen Fällen die nach Landes- oder Bundesrecht zuständige Stelle für IT-Sicherheitsvorfälle zur Bewertung und Unterstützung hinzugezogen wird. Für den Bund ist dies gemäß BSIG das BSI. Ebenso ist sicherzustellen, dass Daten, die über unsichere Netze (wie das Internet) übertragen werden, angemessen kryptographisch gesichert werden. Zudem sind im Hinblick auf Cloud Services u. a. durch Stellen der Bundesverwaltung die Anforderungen des BSI-Mindeststandards zur Nutzung externer Cloud-Dienste in der Bundesverwaltung. einzuhalten. Auf Landes- und Kommunalebene gelten ggf. entsprechende Landes- und Kommunalregelungen.

Auf gemeinsam genutzten virtuellen und physischen Ressourcen in der Cloud gespeicherte und verarbeitete Daten von Cloud-Kunden sind gemäß eines dokumentierten

Konzepts, auf Basis einer Risikoanalyse gemäß OIS-07, sicher und strikt von Daten anderer Kunden zu separieren, auch von anderen Kunden aus der öffentlichen Verwaltung (Mandantentrennung), um die Vertraulichkeit und Integrität dieser Daten zu gewährleisten.

Integrität, Vertraulichkeit und Verfügbarkeit sind sowohl aus der Sicht der Informationssicherheit als auch des Datenschutzes zu gewährleisten. Weitere Gewährleistungsziele (s. o.) bleiben unberührt und sind ebenfalls zu erfüllen.

Zusätzlich ist vertraglich zu vereinbaren, dass die Verfügbarkeit von dringend benötigten Kernfunktionalitäten und Schnittstellen für wichtige Dienste gewährleistet wird bzw. diese über einen ausreichend langen Zeitraum zur Verfügung stehen.

III.2 Kontrollierte Informationsübermittlung

Grundsätzlich findet keine Übermittlung von Informationen an nicht entsprechend berechtigte Empfänger (siehe I.9) bzw. kein unberechtigter Datenabfluss (siehe I.5) statt. Dies gilt auch für Telemetriedaten. In vertraglich fixierten Fällen kann einer Verarbeitung durch den Auftragnehmer zugestimmt werden, soweit dies rechtlich zulässig ist.

III.3 Kontrollierbare Datenhaltung

Daten werden nur in Ländern verarbeitet, die der DSGVO und der Verordnung (EU) 2018/1807 – sog. Free-Flow- Verordnung oder einer als gleichwertig anerkannten Regelung unterliegen.

Die EVB-IT Cloud-AGB sehen folgende Regelung vor: Die Speicherung und sonstige Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer erfolgt ausschließlich innerhalb der EU und des EWR sowie in Ländern für welche ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht, es sei denn, der Auftraggeber hat ausdrücklich zusätzlich weitere Regionen für die Leistungen zugelassen. Zusätzlich sind die Anforderungen des Positionspapieres der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023 „Kriterien Souveräne Clouds“ zu berücksichtigen.

Der potentielle Auftragnehmer ist im Vergabeverfahren aufzufordern, nachvollziehbare und transparente Angaben zur Lokation der Daten des Auftraggebers, einschließlich Meta- und Paradaten, bei der Verarbeitung, Sicherung und Speicherung auf Systemkomponenten zur Bereitstellung des Cloud-Dienstes im Verantwortungsbereich des Auftragnehmers, einschließlich seiner Unterauftragnehmer zur Verfügung zu stellen.

Soweit vertraglich Optionen dafür vorgesehen werden, muss der Auftraggeber auch tatsächlich in die Lage versetzt werden, die Lokationen (Ort/Land) der Datenverarbeitung und Speicherung einschließlich der Datensicherungen entsprechend festzulegen. Dies muss z.B. durch die Cloud-Architektur sichergestellt sein.

III.4 Vertrauenswürdigkeit der Lieferkette (Supply-Chain)

Als Maßnahmen zur Stärkung der Vertrauenswürdigkeit der Lieferkette sind Offenlegungspflichten, Herkunftsnachweise, Vertraulichkeitserklärungen oder Kontroll- und Prüfrechte einzufordern. Ein Grundvertrauen in den Auftragnehmer kann zudem durch Anforderungen an nachhaltige- und klimafreundliche Produkte und Dienste sowie die Einhaltung der ILO-Kernarbeitsnormen (z. B. Lieferkettensorgfaltspflichtengesetz, BITKOM-Verpflichtungserklärung) gestärkt werden, wenn diese Pflichten sich auch auf die Zulieferer erstecken.

III.5 Prüfnachweise

Bereits im Vergabeverfahren sollte der öffentliche Auftraggeber festlegen, welche Belege mit Relevanz für digitale Souveränität (z. B. Audit- und Prüfungsberichte, Zertifizierungen, geheimschutzrechtliche Zulassung sowie zugrundeliegende Evidenzen) und ggf. erfolgte Testverfahren der Software im Rahmen der Eignungsprüfung bzw. zum Nachweis der Qualität der Leistungen vom Bieter vorzulegen sind.

Zusätzlich sind bei Bedarf, abhängig von den identifizierten Schutzbedarfen, eigene Prüfrechte des Auftraggebers bzw. der Bedarfsträger mit dem Auftragnehmer zu vereinbaren. Siehe dazu beispielhaft auch Ziffer 6.4 der EVB-IT Cloud-AGB.

III.6 Sicherheitsanalysen

Im Bedarfsfall sollte der Auftraggeber mit dem Auftragnehmer vereinbaren, dass der Auftragnehmer dafür sorgt, dass Sicherheitsanalysen mit einer Relevanz für digitale Souveränität (bspw. Penetrationstests, Audits im Rahmen von ISO 27001, etc.) an den vereinbarten Produkten und Leistungen bei Bedarf jederzeit, auch durch vom Auftraggeber beauftragte Dritte, durchgeführt werden können.

Die Durchführung von Sicherheitsanalysen wird in angemessenem Umfang vom Auftragnehmer unterstützt. Soweit planbar, ist der Umfang vorab im Vertrag zu definieren. Ergeben sich aus der Sicherheitsanalyse Softwareschwachstellen, sind diese gemäß III.9 zu behandeln. Für Hardwareschwachstellen gelten die Anforderungen analog. Hierfür sind bereits bei Vertragsschluss mit dem Auftragnehmer Reaktionszeiten und ggf. Erledigungszeiten zu definieren.

III.7 Produkte frei von undokumentierten Funktionalitäten

Der Auftraggeber sollte mit dem Auftragnehmer vereinbaren, dass dieser für die bereitgestellten Produkte und Leistungen gewährleistet, dass keine Funktionalitäten integriert sind bzw. werden, die nicht in der dem Auftraggeber zur Verfügung gestellten Dokumentation beschrieben sind. In den EVB-IT, die ab 2015 veröffentlicht wurden, ist dies durch die sogenannte technische No-Spy Klausel bereits geregelt (siehe beispielhaft Ziffer 2.3 der EVB-IT Überlassung AGB Typ A). Für ältere EVB-IT, z. B. EVB-IT System und EVB-IT Erstellung und andere Verträge empfiehlt sich die sinngemäße Übernahme der Klausel.

III.9 Sicherheitsrelevante neue Programmstände

Der Auftraggeber sollte mit dem Auftragnehmer vereinbaren, dass dieser kritische Schwachstellen unverzüglich und unaufgefordert schließt und entsprechende neue Programmstände zur Verfügung stellt. Hierfür sind vertraglich Reaktionszeiten zu definieren. Bei neuen Programmständen muss der Auftragnehmer Sicherheitsfunktionalitäten beachten, wie bspw. Versionierung, Identitätsprüfung des Updateservers, Sicherstellung der Authentizität und Integrität der neuen Programmstände etc. Wann eine Sicherheitslücke als kritisch oder hoch anzusehen ist, ist dabei individuell zu regeln (z. B. durch die Festlegung eines entsprechenden CVSS Schwellenwertes im Vertrag). Im Cloud-Kontext gelten die Anforderungen des C5 OPS-18 ff. zum Umgang mit Schwachstellen, Störungen und Fehlern.

III.10 Produktpflege

Im Bedarfsfall sollte der Auftraggeber mit dem Auftragnehmer vereinbaren, dass die Produkte durch diesen kontinuierlich daraufhin überprüft werden, ob sie gegen aktuelle Angriffstechniken bzw. -Methoden geschützt sind (z. B. durch Penetrationstests) und bei Bedarf entsprechend aktualisiert werden, es sei denn, dies ist technisch nicht möglich.

Die durchgeführten Prüfungen, deren Ergebnisse und ebenso durchgeführte Aktualisierungen sind zu dokumentieren und dem Auftraggeber zur Verfügung zu stellen. Zusätzlich sollte der Auftragnehmer bei Bedarf darauf verpflichtet werden den Auftraggeber oder durch ihn beauftragte Dritte bei der Durchführung eigener Tests zu unterstützen.

III.11 Beendigung des Vertragsverhältnisses und Datenrückgabe

In den Vergabeunterlagen ist durch den Auftraggeber verbindlich zu regeln, wie verarbeitete Daten nach Vertragsbeendigung an den Auftraggeber übergeben werden sollen (z. B. Fristen, Datenformat, Datenträger, Protokolle usw.).

Ergänzend dazu sind die Daten beim Auftragnehmer vollständig und rückstandsfrei zu löschen. Dabei ist darauf zu achten, Backups, Caches usw. ebenfalls sicher zu löschen. Dabei muss sichergestellt werden, dass die Maßnahmen dem zuvor ermittelten Schutzbedarf entsprechen. Soweit der Löschung gesetzliche Aufbewahrungsfristen entgegenstehen, sind die Daten dem Schutzbedarf entsprechend gesichert aufzubewahren und nach Ablauf der Aufbewahrungsfristen ebenfalls in vorgenanntem Sinne sicher zu löschen.

III.12 Ausschluss von Leistungsverweigerungs- und Zurückbehaltungsrechten

Leistungsverweigerungs- und Zurückbehaltungsrechte an den vertraglich vereinbarten Leistungen zu Lasten der öffentlichen Verwaltung, insbesondere Zurückhaltungsrechte an Daten des Auftraggebers sind, auszuschließen. In den EVB-IT Vertragsmustern ist

dies bereits geregelt. Entsprechende Formulierungen sollten bei individuellen Verträgen übernommen werden.

III.13 Anwendbares Recht und Gerichtsstand

Es sollten ausschließlich Verträge nach deutschem Recht (unter Ausschluss des United Nations Convention on Contracts for the International Sale of Goods (CISG)) und deutschem Gerichtsstand abgeschlossen werden.[22] In den EVB-IT ist dies bereits geregelt und entsprechende Formulierungen sollten bei individuellen Verträgen übernommen werden. Ist dies nicht möglich, ist darauf zu achten, dass vertraglich klare Regelungen zum Gerichtsstand und anwendbarem Recht getroffen werden.

[22] Vgl. §19 Nr. 2 VOL B und MST Cloud NCD.2.2.03. Sollte kein Vertrag nach deutschen Recht und deutscher Gerichtsbarkeit abgeschlossen werden können, sind die im MST NCD unter NCD.2.2.03 b) und c) aufgeführten Kriterien anzuwenden.

4. Anlagen

Glossar

- Öffentliche Rolle „Auftraggeber“: Als Auftraggeber verantwortet die Öffentliche Verwaltung die Beschaffung neuer IT-Lösungen. Auftraggeber sind beispielsweise der Bund, das Land, die Kommune, gegebenenfalls vertreten durch die jeweiligen zuständigen IT-Dienstleister oder Beschaffungsstellen der entsprechenden Öffentlichen Verwaltung.
- Öffentliche Rolle „Nutzer“: Als Nutzer verantwortet die Öffentliche Verwaltung den Einsatz von IT-Lösungen zur Unterstützung der Arbeit der Behörde. „Nutzer“ versteht sich im Sinne der einsetzenden Institution, nicht im Sinne des Endnutzers. Nutzer sind beispielsweise einzelne Behörden von Bund, Ländern und Kommunen. Als Nutzer/ Kommunikationspartner kommen auch Bürger (G2C) und Unternehmen (G2B) in Frage, die entsprechende Dienste und Services nutzen.
- Öffentliche Rolle „Bereitsteller“: Als Bereitsteller verantwortet die Öffentliche Verwaltung die Entwicklung, Inbetriebnahme und den Betrieb von IT-Lösungen. Bereitsteller sind beispielsweise IT-Dienstleister der Öffentlichen Verwaltung.
- Öffentliche Rolle „Bedarfsträger“: Bedarfsträger sind Behörden oder sonstige Institutionen, die einen entsprechenden Bedarf an dem beschafften Service bzw. der Dienstleistung haben.
- Öffentliche Veraltung: Die Öffentliche Verwaltung im Sinne dieses Papiers umfasst sowohl Behörden von Bund, Ländern und Kommunen als auch verwaltungseigene Gesellschaften, Stiftungen, Vereine, etc.
- Anbieter: Anbieter im Kontext dieses Dokuments sind Wirtschaftsteilnehmer, die sich an einem entsprechenden Vergabeverfahren beteiligen und Angebote abgeben.
- Auftragnehmer: Auftragnehmer sind ein oder mehrere Unternehmen, die einen Auftrag zur Erbringung von Leistungen erhalten haben.
- Hersteller: Hersteller im Kontext dieses Dokumentes ist, wer das Endprodukt, einen Grundstoff oder ein Teilprodukt (bei Software Teil des Codes) hergestellt hat. Als Hersteller gilt auch jeder, der sich durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgibt. (§4 Abs.1 ProdHaftG).
- Produkte: Unter dem im Text genannten Begriff „Produkte“ sind sowohl Produkte als auch Services und Dienstleistungen subsumiert.

Abkürzungsverzeichnis

Abkürzung	Bedeutung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CVSS	Common Vulnerability Scoring System
DSGVO	Datenschutz-Grundverordnung
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen
ILO	International Labour Organization
VgV	Vergabeverordnung
VSA	Verschlusssachenanweisung
VSVgV	Vergabeverordnung Verteidigung und Sicherheit