IONOS

White Paper



Cloud mit Zukunft

Wie digitale Souveränität die Auftragsvergabe im öffentlichen Dienst beeinflusst

© IONOS 2023

IONOS

Inhaltsverzeichnis

1 Einleitung 3

2 Begriffsbestimmung: Digitale Souveränität 3

2.1 Rechtliche Souveränität 4
2.2 Organisatorische Souveränität 5

3 Datenschutzrechtliche Vorgaben 6

3.1 Anwendbares Recht 6
3.2 Schwierigkeiten bei der Cloud-Nutzung 8
3.2.1 Cloud-Betreiber als Auftragsverarbeiter im Sinne von Art. 28 DSGVO 8
3.2.2 Risiko Drittlandtransfer 9
3.2.3 TOM und der Anforderungskatalog C5 des BSI 11
3.3 Lösungsansätze 12
3.3.1 Projekte der US-Hyperscaler 12
3.3.2 Open-Source-Lösungen 15
3.3.3 Wann ist die Cloud wirklich souverän? 16

4 Vergaberechtliche Vorgaben 18

4.1 Besonderheiten im Ausschreibungsverfahren 18
4.1.1 Grundsatz 18
4.1.2 Ausnahme für reine Open-Source-Leistungen 18
4.1.3 Digitale Souveränität und öffentlich-öffentliche Zusammenarbeit 19
4.1.4 Gestaltungsmöglichkeiten in Vergabeverfahren 20
4.1.5 Zwingende datenschutzrechtliche Vorgaben können um Ausschuss von Drittstaatenanbietern führen 22
4.1.6 Direktbeauftragung privater Cloud-Anbieter möglich? 25
4.2 Rolle der neuen EVB-IT Cloud 26
4.3 Die Vergabeentscheidung 28

5 Fazit und Checkliste 29

Über IONOS 32

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

IONOS

1 Einleitung

Bereits 2019 hat sich die Bundesregierung „Digitale Souveränität" zum Ziel gesetzt.[1] Anwendungen wie Microsoft Office betreibt die Regierung längst auf eigenen Servern, doch auf kommunaler Ebene, wenn auch nicht nur dort, handelt es sich allem Anschein nach immer noch um ein (zu) großes Ziel. Vielfach wird nach wie vor auf Angebote von US-Anbietern zurückgegriffen und die unterschiedlichen Einrichtungen nutzen trotz verschiedener Zusammenschlüsse auf kommunaler Ebene noch viele unterschiedliche Systeme – digitale Souveränität scheint da weit entfernt.

Aber was verbirgt sich hinter dem Begriff digitale Souveränität? Warum ist sie gerade im öffentlichen Bereich erstrebenswert und wie kann sie erreicht werden? Genau hier setzt dieses White Paper an und vermittelt aus rechtlicher Sicht einen ersten Überblick über das Verhältnis von Cloud-Nutzung und digitaler Souveränität im öffentlichen Bereich. Auch wenn sich viele öffentliche Einrichtungen noch dafür entscheiden, Software lokal oder auf eigenen Servern zu hosten, gewinnen Clouds an Bedeutung und werden durch ihre Flexibilität und hohe Skalierbarkeit auch im öffentlichen Bereich immer wichtiger.

Dieses White Paper vermittelt zunächst einen Überblick über datenschutzrechtliche Aspekte und Fallstricke bei der Cloud-Nutzung durch die öffentliche Hand. Im Anschluss daran sollen die Besonderheiten im Vergabeverfahren unter besonderer Berücksichtigung der neuen ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT Cloud) beleuchtet werden.

2 Begriffsbestimmung: Digitale Souveränität

Der Begriff ist nicht klar definiert, entfernt sich aber vom historischen Begriff der staatlichen Souveränität, der etwa von Hobbes, Locke und Rousseau geprägt wurde, und die ein vorläufiges Ende mit dem demokratischen Verfassungsstaat als Souverän fand.[2]

Grundsätzlich geht es bei digitaler Souveränität darum, die Kontrolle über die eigenen Daten und die Anwendungen, die sie verarbeiten, zu behalten. Vollständige Autarkie des Dateninhabers wird hingegen nicht verlangt. Ein Fokus liegt in der Debatte häufig bei der Beauftragung von Cloud-Anbietern mit Servern oder Unternehmenssitz im Ausland bzw. außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraumes (EWR), welche die digitale Souveränität gefährden soll.

1. S. etwa https://www.it-planungsrat.de/beschluss/beschluss-2019-38, zuletzt abgerufen am 11.01.2023.

2. Hobbes: Leviathan oder Stoff, Form und Gewalt eines kirchlichen und bürgerlichen Staates, 17. Auflage 2020; Locke/Siep: Zweite Abhandlung über die Regierung, 4. Auflage 2020; Rousseau: Vom Gesellschaftsvertrag oder Grundsätze des Staatsrechts, 1762.

Zum Teil wird der Begriff auch in Datensouveränität und technologische Souveränität aufgeteilt. Dabei erlaubt Datensouveränität die selbstbestimmte Kontrolle über Erhebung, Speicherung, Nutzung und Verarbeitung der eigenen Daten, während die technologische Souveränität die freie Wählbarkeit von datenverarbeitenden Technologien und ihnen zugrundeliegenden Rahmenbedingungen bedeuten soll. Zusätzlich sind Systeme nur dann souverän, wenn sie in der Lage sind, ihr Funktionieren im Inneren zu sichern und gleichzeitig ihre Integrität nach außen zu schützen.[3] Um sowohl Datensouveränität als auch technologische Souveränität zu gewährleisten, muss sich der Datenbesitzer also in die Lage versetzen, autonom zu entscheiden, wo die Daten gespeichert und von wem sie zu welchem Zweck verarbeitet werden dürfen, und unter welchen technischen Bedingungen dies geschieht.[4]

2.1 Rechtliche Souveränität

Rechtlich souverän ist die Cloud, wenn ein anderer als der Verantwortliche, also der Kunde des Cloud-Anbieters, ohne dessen Erlaubnis nicht auf die in der Cloud verarbeiteten Daten zugreifen darf. Gemeint ist hier grundsätzlich, dass die Behörden in Drittländern, die nicht zur EU oder dem EWR gehören, keine rechtlich zulässige Möglichkeit haben dürfen, Zugriff auf die oder Herausgabe der betreffenden Daten zu verlangen. Ergänzt wird dies durch technische Maßnahmen, die in der Lage sind, den Zugriff auch faktisch zu verhindern.

Um vollständige Datensouveränität zu erreichen, muss die verwendete Cloud zudem rechtlich und organisatorisch souverän sein.

Rechtlicher Hintergrund hierfür sind die Artikel 44 ff. der EU-Datenschutz-Grundverordnung (DSGVO), die für den Drittlandtransfer personenbezogener Daten ein angemessenes Datenschutzniveau im Empfängerland voraussetzen. Hierauf basierend ist bereits 2020 das Urteil ***Schrems II***[5] des Europäischen Gerichtshofs (EuGH) ergangen, welches den bis dahin bestehenden EU-US-Privacy-Shield als Angemessenheitsbeschluss der EU-Kommission für unwirksam erklärte, der bis dahin in der Regel nach vorheriger Unterwerfung der entsprechenden US-Unternehmen als Rechtsgrundlage für Datentransfers an US-Unternehmen diente.[6] Begründet hat der EuGH dies unter anderem damit, dass US-Behörden auf Daten von EU-Bürgerinnen und -Bürgern auf Grundlage des US CLOUD Act[7] selbst dann ohne förmlichen richterlichen Beschluss zugreifen können, wenn die Daten ausschließlich auf den europäischen Servern eines US-Unternehmens gespeichert werden.

EU-Unternehmen und -Behörden müssen daher obige Regeln und obige Rechtsprechung zur Inanspruchnahme von Cloud-Anbietern mit Hauptsitz in Drittstaaten beachten, um rechtliche Souveränität zu erreichen.

---

3. Bitkom – Digitale Souveränität – Positionsbestimmungen und erste Handlungsempfehlungen für Deutschland und Europa, 2015, https://www.bitkom.org/sites/main/files/file/import/BITKOM-Position-Digitale-Souveraenitaet.pdf, S. 7, zuletzt abgerufen am 11.01.2023.
4. Vgl. Tiedeke: Die (notwendige) Relativität digitaler Souveränität, MMR 2021, 624.
5. EuGH, Urteil vom 16. Juli 2020, C-311/18, abrufbar unter https://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&doclang=DE, zuletzt abgerufen am 11.01.2023.
6. Mehr dazu unter https://www.baden-wuerttemberg.datenschutz.de/ueberblick-eu-u-s-privacy-shield/, zuletzt abgerufen am 11.01.2023.
7. Clarifying Lawful Overseas Use of Data Act, 2018, US-Congress H.R.4943.

2.2 Organisatorische Souveränität

Organisatorische Souveränität soll hingegen sicherstellen, dass auch im Hardware- und Infrastrukturbereich keine Abhängigkeiten entstehen. Neben den datenschutzrechtlichen Risiken durch behördliche Zugriffe (s.o.) oder unzureichende Datenschutzgesetze in Drittländern besteht insbesondere die Sorge, dass die Verfügbarkeit der Dienste im Falle diplomatischer Verwerfungen mit der Regierung des Herkunftslandes eines Cloud-Anbieters nicht mehr gesichert ist (vgl. etwa a) das aktuelle Verbot von Huawei-Geräten in den USA,[8] an dem zu sehen ist, dass erhebliche Risiken durch Regierungsentscheidungen anderer Staaten entstehen können[9] sowie b) die parallele Debatte in der EU). Abhängigkeiten von EU-Anbietern werden in der öffentlichen Debatte hingegen kaum als Problem gesehen, obwohl die eigene Souveränität auch durch die Abhängigkeit von einem dieser Anbieter eingeschränkt sein kann. Zudem kann die Abhängigkeit von technischen Komponenten von Drittlandanbietern, etwa Mikrochips, einer organisatorischen Souveränität entgegenstehen.



Um organisatorische Souveränität zu gewährleisten, ist es folglich wichtig, dass Behörden und Einrichtungen sich nicht von lediglich einem Anbieter abhängig machen. Dies gilt insbesondere dann, wenn diese ihren Hauptsitz in einem Drittland haben, also außerhalb der EU oder des EWR. **Darüber hinaus müssen öffentliche Einrichtungen sicherstellen, dass Interoperabilität zwischen den verwendeten Komponenten besteht (etwa Hardwarekomponenten, Rechenzentren oder die in der Cloud gehostete Software), wodurch Lock-In-Effekte einfacher vermieden werden können.**

Um all dies sicherzustellen, zielt die öffentliche Verwaltung derzeit auf eine **Multi-Cloud-Infrastruktur**, bei der die Cloud-Angebote unterschiedlicher Anbieter je nach Bedarf nebeneinander verwendet und miteinander verbunden werden. Ergänzt wird dies bspw. durch die **Open-Source-Strategie** des Bundesfinanzministeriums,[10] wonach gemeinsame Standards und offene Schnittstellen für Cloud-Lösungen (möglichst unter Verwendung von Open-Source-Technologie) eingesetzt werden sollen (mehr dazu unten).

8. S. etwa https://www.zeit.de/wirtschaft/unternehmen/2022-11/spionageverdacht-usa-huawei-smartphones-nationale-sicherheit-verbot, zuletzt abgerufen am 11.01.2023.

9. Vgl. Bitkom: Eckpunktepapier – Eckpunkte für eine souveräne Cloud- und Infrastruktur, 2019, https://www.bitkom.org/sites/main/files/2019-10/20191022-bitkom_eckpunkte_souverane-cloudinfrastruktur_final.pdf, zuletzt abgerufen am 11.01.2023.

10. S. auch BT-Drucks. 20/2150.

3 Datenschutzrechtliche Vorgaben

Die Nutzung von Clouds, um Speicherplatz flexibel erweitern zu können oder gleich ganze Softwareanwendungen auf fremden Servern laufen zu lassen, ist attraktiv und heute vielerorts Standard. Kein Wunder also, dass Unternehmen und Behörden heute immer stärker auf die Cloud setzen. Dabei ist die Cloud-Nutzung nicht immer genauso sicher wie einfach: Werden große Mengen häufig personenbezogener Daten einem Dritten anvertraut, müssen höchste Sicherheitsstandards eingehalten werden. Und auch rechtlich gibt es hier Besonderheiten. Vor und während des Einsatzes von Cloud-Anbietern muss deshalb regelmäßig geprüft werden, ob alle notwendigen Vorkehrungen getroffen wurden und alle Verträge in der aktuellen Version vorliegen.

3.1 Anwendbares Recht

Anders als für Unternehmen sind für Behörden und die öffentliche Verwaltung (***öffentliche Stellen***[11] im Sinne von § 2 BDSG) das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze maßgeblich, für die zum Teil von den Öffnungsklauseln der DSGVO Gebrauch gemacht wurde (z.B. Art. 6 Abs. 2 DSGVO). Dabei sind die Landesdatenschutzgesetze für die öffentlichen Stellen der Länder vorrangig anzuwenden. Im Übrigen finden die Regelungen der DSGVO Anwendung. Zudem gibt es bspw. für Behörden häufig spezielle Gesetze, die ergänzend anzuwenden sind.

Im Ergebnis ähnelt der Rechtsrahmen für den Datenschutz dem für privatwirtschaftliche Unternehmen. Besonders herauszuheben ist jedoch, dass die Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO für öffentliche Einrichtungen keine Anwendung findet; diese Einrichtungen die Verarbeitung personenbezogener Daten also nicht alleine auf das Vorliegen überwiegender berechtigter Interessen stützen dürfen. Ausnahmen gibt es hingegen etwa für die Verarbeitung personenbezogener Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, also auch für die Strafvollstreckung und Gefahrenabwehr.

Sonderfall Kirchen

Für Kirchen ist die Rechtslage noch einmal anders. Diese dürfen nach Art. 91 DSGVO weiterhin eigene Datenschutzregeln anwenden, sofern sie dies auch schon vor Inkrafttreten der DSGVO taten. Ist das der Fall, sind diese Regeln vorrangig anwendbar, ansonsten gilt die DSGVO auch für Kirchen und religiöse Einrichtungen.

11. Öffentliche Stellen im Sinne des BDSG sind ungeachtet der Rechtsform neben den Behörden die Organe der Rechtspflege sowie andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts und deren Vereinigungen sowie Gerichte, s. etwa Helfrich in Sydow-Marsch DS-GVO/BDSG § 5 Rn. 9-10.



Zumindest die beiden großen Kirchen in Deutschland sowie einige kleinere Religionsgemeinschaften haben von dieser Möglichkeit Gebrauch gemacht.[12] Diese Gesetze folgen in weiten Teilen jedoch ebenfalls der DSGVO. Besonderheiten sind etwa die Rechtsgrundlage der „Datenverarbeitung im kirchlichen Interesse“ oder ein Schriftlichkeitserfordernis für Einwilligungen in der katholischen Kirche. Zudem haben die großen Kirchen ihre eigenen Aufsichtsbehörden, die katholische Kirche hat sogar eigene Datenschutzgerichte geschaffen.

Zudem haben die Kirchen eigene datenschutzrechtliche Aufsichtsstellen: Für die Evangelische Kirche hat etwa der Beauftragte für den Datenschutz der Evangelischen Kirche Deutschland schon im Jahr 2019 festgelegt, unter welchen Bedingungen Microsoft-Cloud-Dienste genutzt werden dürfen.[13] Neben der inzwischen üblichen Verschlüsselung der übermittelten Daten, dem Abschluss eines Auftragsverarbeitungsvertrages und der Unterbindung des Transfers von personenbezogenen Telemetriedaten[14] müssen Kirchen bei Beauftragung von Cloud-Anbietern aus Drittländern eine **Zusatzvereinbarung**[15] abschließen, mit denen die Provider sich der kirchlichen Datenschutzaufsicht unterstellen. Diese Zusatzvereinbarung stellt allerdings lediglich sicher, dass die kirchliche Aufsichtsbehörde im Falle einer unrechtmäßigen Datenverarbeitung informiert wird. Auch eine derartige Zusatzvereinbarung ist daher alleine nicht in der Lage, einen ausreichenden Schutz der verarbeiteten Daten sicherzustellen – selbst der BfD EKD empfiehlt aufgrund der mehrdeutigen Formulierungen zusätzlich ein Begleitschreiben zur Zusatzvereinbarung.[16] Ohne die enthaltenen Konkretisierungen sei eine Verwendung der obigen Zusatzvereinbarung nicht datenschutzkonform. Eine in den Dokumenten zum Teil vorgesehene Verschlüsselung, zu der nur die Kirche selbst den Schlüssel hat, ist häufig nicht praktikabel, etwa wenn die Cloud für mehr als nur die bloße Speicherung von Daten genutzt werden soll (z.B. bei Software as a Service, SaaS).

Diese eigenen Datenschutzregeln sind deshalb so wichtig, weil Kirchen als Trägerinnen von Kindergärten, Schulen, Pflegeeinrichtungen, Krankenhäusern etc. große Mengen teilweiser sensibler Daten verarbeiten und datenschutzkonform verwalten müssen.

12. Etwa mit dem Gesetz über den Kirchlichen Datenschutz (KDG) der Katholischen Kirche und dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).

13. https://datenschutz.ekd.de/2020/02/14/nutzung-von-microsoft-cloud-diensten/, zuletzt abgerufen am 11.01.2023.

14. Telemetriedaten sind Daten, die über Fernmessung erfasst werden und etwa Diagnose- und Funktionsdaten von Geräten, Anwendungen oder sogar Dateien umfassen können, aber auch personenbezogene Daten des Anwenders. In vielen Anwendungen kann deren Übermittlung deaktiviert werden.

15. https://datenschutz.ekd.de/wp-content/uploads/2020/03/20191127-MS-Muster-Zusatzvereinbarung.pdf, zuletzt abgerufen am 11.01.2023.

16. https://datenschutz.ekd.de/wp-content/uploads/2020/03/MicrosoftCloudHinweise.pdf, zuletzt abgerufen am 11.01.2023

In jedem Fall muss auch aus Sicht der Kirche vor Einführung von Cloud-Diensten wie Microsoft 365 eine **Datenschutzfolgenabschätzung** durchgeführt werden.

3.2 Schwierigkeiten bei der Cloud-Nutzung

3.2.1 Cloud-Betreiber als Auftragsverarbeiter im Sinne von Art. 28 DSGVO

Cloud-Anbieter werden in der Regel als Auftragsverarbeiter im Sinne von Art. 28 DSGVO tätig.

Cloud-Anbieter werden nach herrschender Auffassung in der Regel als Auftragsverarbeiter im Sinne von Art. 28 DSGVO tätig, da sie die Daten, die sie von ihren Kunden erhalten, ausschließlich in deren Auftrag und auf deren Weisung hin verarbeiten, nicht aber zu eigenen Zwecken.

Zusammen mit dem Cloud-Vertrag muss also (fast) immer auch ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, der alle Pflicht-Inhalte des Art. 28 DSGVO enthält. Viele Cloud-Anbieter bieten ihrerseits bereits Vertragsvorlagen an, die diesen Anforderungen entsprechen. Seit 2021 gibt es zudem einen Mustervertrag der EU-Kommission (Standardvertragsklauseln) zur Auftragsverarbeitung.[17] Wird dieser Vertrag verwendet und durch den Cloud-Anbieter (aus der EU/dem EWR) eingehalten, ist man aktuell auf der sicheren Seite. Diese Vertragsklauseln können allerdings nur dann eine sichere Verarbeitung gewährleisten, wenn sie mit einem europäischen Anbieter vereinbart werden. Bei Anbietern, die ihren Sitz nicht in der EU oder dem EWR haben, gibt es weitere Voraussetzungen, die erfüllt werden müssen (dazu unten mehr).

Wichtig für eine Auftragsverarbeitung ist, dass die Cloud-Unternehmen die vom Auftraggeber übermittelten Daten auf keinen Fall **zu eigenen Zwecken verarbeiten** dürfen. Dies steht nicht nur im Widerspruch zur Auftragsverarbeitung, bei der die Verarbeitung durch den Auftragnehmer ausschließlich auf **Weisung** des Auftraggebers erfolgen soll, sondern kann auch ein erhebliches Haftungsrisiko darstellen, wenn es für die Verarbeitung durch den Auftragnehmer keine geeignete Rechtsgrundlage gibt (in der Regel Art. 6 Abs. 1 DSGVO). Behält sich ein Cloud-Anbieter vertraglich die Verarbeitung zu anderen Zwecken als denen des Auftraggebers vor, bräuchte es hierzu also eine Rechtsgrundlage. Rechtsgrundlage der Datenverarbeitung durch öffentliche Stellen ist häufig die Erfüllung ihrer Aufgaben im öffentlichen Interesse.

Eine Aufgabenerfüllung des öffentlichen Auftraggebers liegt bei einer eigenen Verarbeitung durch den Cloud-Anbieter meist allerdings nicht mehr vor. Eine Verarbeitung auf Grundlage berechtigter Interessen entfällt bei öffentlichen Stellen regelmäßig. **Insofern ist eine Verarbeitung personenbezogener Daten zu eigenen Zwecken des Cloud-Anbieters in der Regel allenfalls auf Grundlage der informierten Einwilligung der Betroffenen möglich.** Die Betroffenen werden diese Einwilligung jedoch oft nicht erteilen und können sie zudem jederzeit widerrufen. Zudem fehlt den Auftraggebern in diesen Fällen

17. Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32021D0915.

häufig selbst das erforderliche Wissen, um den Betroffenen eine informierte Einwilligung zu ermöglichen. Insofern sollte es selbstverständlich sein, dass Cloud-Anbieter die Daten ausschließlich für den Auftraggeber verarbeiten. Trotzdem finden sich in der Praxis immer wieder solche Klauseln, in denen sich Cloud-Anbieter (teils verklausuliert) die Verwendung der Daten für die Produktentwicklung, eigene Geschäftstätigkeiten oder ähnliches vorbehalten oder eine Offenlegung der Daten auf Grundlage nicht-europäischer Rechtsordnungen nicht ausschließen.

Solche Klauseln sind unzulässig, führen dazu, dass die Privilegierung als Auftragsverarbeitung entfällt und betroffene Personen nicht ausreichend informiert werden können und sollten nicht nur, aber insbesondere von öffentlichen Stellen auf keinen Fall akzeptiert werden. Dies gilt aktuell in den meisten Fällen selbst dann, wenn die Daten nur in aggregierter Form verwendet werden.

3.2.2 Risiko Drittlandtransfer

Deutlich komplizierter wird die Rechtslage, wenn der gewählte Cloud-Anbieter seinen Sitz außerhalb von EU und EWR in einem so genannten Drittland hat. **In diesem Fall muss durch zusätzliche Maßnahmen sichergestellt werden, dass die betroffenen personenbezogenen Daten bei der Verarbeitung in dem Drittland genauso gut geschützt sind wie in der EU. Besonders tückisch ist dabei, dass bereits ein möglicher Zugriff auf Daten, die auf Servern in der EU verarbeitet werden, aus einem Drittland eine Drittlandsverarbeitung darstellen kann, die den erhöhten Anforderungen der Art. 44 ff. DSGVO unterliegt.**

Für einige Länder hat die Europäische Kommission Angemessenheitsbeschlüsse nach Art. 45 DSGVO erlassen. Diese bescheinigen dem jeweiligen Drittland ein Datenschutzniveau, das dem in der EU entspricht, sodass für diese keine weiteren Maßnahmen notwendig sind.[18] Bei der Datenverarbeitung in allen anderen Drittländern sind weitere Maßnahmen erforderlich, sogenannte ***geeignete Garantien*** im Sinne von Art. 45 DSGVO, etwa genehmigte interne Datenschutzvorschriften oder der Abschluss von Standarddatenschutzklauseln (***Standard Contractual Clauses***, kurz SCC).

Nachdem der EuGH im Jahr 2020 den Angemessenheitsbeschluss für die USA (den EU-US-Privacy-Shield) für unwirksam erklärt hatte, wurde für Datentransfers in die USA in der Regel auf Standarddatenschutzklauseln ausgewichen, also auf Musterverträge der EU-Kommission. Allerdings hatte der EuGH im Rahmen des Schrems-II-Urteils auch für die alte Version der Standarddatenschutzklauseln (damals noch Standardvertragsklauseln) festgestellt, dass diese heute angesichts der umfassenden Überwachungspraxis durch US-Behörden zumindest im Hinblick auf einen US-Datentransfer nicht mehr ausreichend seien, um einen angemessenen Datenschutz sicherzustellen.

Insbesondere rund um die SCC gab es seit dem Erlass der DSGVO viele Diskussionen und Änderungen.

[18] Aktuell gibt es Angemessenheitsbeschlüsse für die folgenden Länder: Andorra, Argentinien, Kanada, Färöer, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Schweiz, Südkorea, Uruguay und Vereinigtes Königreich.

In der Folge veröffentlichten die Behörden verschiedene Empfehlungen mit weiteren, ergänzend umzusetzenden technischen, organisatorischen und vertraglichen Schutzmaßnahmen, bis die EU-Kommission schließlich vollständig überarbeitete Standarddatenschutzklauseln für den Drittland-Transfer veröffentlichte, die seit dem 27. Dezember 2022 auch für alle Altverträge verpflichtend umzusetzen sind.[19]

Dennoch besteht auch bei Verwendung der neuen SCC keine uneingeschränkte Rechtssicherheit. Auftraggeber einer Auftragsverarbeitung sind nun dazu verpflichtet, selbständig zu überprüfen, ob in dem Drittland ein angemessenes Datenschutzniveau herrscht (sog. ***Data Transfer Impact Assessment – DTIA***; vgl. Klausel 14 der SCC Drittland). Auf Grundlage dieses Ergebnisses müssen sie dann unter Umständen weitere Verpflichtungen in den Vertrag aufnehmen oder sogar ganz von der Beauftragung absehen, wenn ein angemessenes Datenschutzniveau nicht hergestellt werden kann. Dies bürdet Auftraggebern einer Cloud-Verarbeitung erhebliche Verantwortung auf und im Zweifel sogar die umfassende Prüfung einer unbekannten Rechtsordnung.

Dabei bestehen aktuell insbesondere bei der Beauftragung von US-Unternehmen erhebliche Zweifel daran, dass diese rechtlich in der Lage sind, die Daten ihrer Kunden ausreichend zu schützen. Denn selbst wenn die Cloud auf den deutschen Rechenzentren eines US-Anbieters betrieben wird, sind US-Behörden auf Grundlage des Cloud Act jedenfalls rechtlich in der Lage, die Herausgabe dieser Daten zu verlangen. Zwar weisen die Statistiken der US-Cloud-Anbieter darauf hin, dass ein solcher Zugriff die Ausnahme darstellt. Das Risiko ist allerdings angesichts eindeutiger Ermächtigungsgrundlagen in der US-Gesetzgebung existent.

Aufgrund dieser Unsicherheiten befinden sich EU und USA aktuell in den Verhandlungen über ein ***EU-US Data Privacy Framework***, also einen neuen Angemessenheitsbeschluss („EU-US-Privacy-Shield 2.0“), der einen sicheren Datentransfer an US-Unternehmen in Zukunft wieder möglich machen soll. So sollen europäische Datensubjekte in Zukunft effektive Rechtsschutzmöglichkeiten gegen behördlichen Datenzugriff in den USA haben. Den ersten großen Schritt haben die USA mit der Einführung einer entsprechenden Durchführungsverordnung (***executive order***) bereits gemacht.[20] **Allerdings wird auch hier Kritik laut, wonach gerichtlicher Rechtsschutz in den USA weiterhin nicht gewährt werde – stattdessen sei der neue „Data Protection Review Court“ ein Organ der Exekutive – und vor allem sei eine executive order gerade kein Gesetz, sondern könne als interne Dienstanweisung jederzeit wieder geändert werden und der Schutz von EU-Bürgerinnen und -Bürgern überraschend auslaufen.**[21]

---

19. Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=DE.

20. Executive Order 14086, 7. Oktober 2022, abrufbar unter: https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.

21. S. z.B. https://www.handelsblatt.com/politik/deutschland/eu-datenschutz-datenabkommen-mit-den-usa-droht-zu-scheitern-weil-ein-klaeger-aus-oesterreich-wohl-wieder-vor-gericht-zieht/28881394.html, zuletzt abgerufen am 11.01.2023.

Dennoch hat die EU-Kommission im Dezember 2022 ihren Vorschlag für den neuen Angemessenheitsbeschluss präsentiert, der für alle Unternehmen gelten soll, die sich dem Data Privacy Framework unterwerfen.[22] Der Entwurf der EU wird nun noch weiter beraten. Zunächst haben die Mitgliedsstaaten und Datenschutzbehörden die Möglichkeit, Stellungnahmen abzugeben. **Auch wenn die Kommission plant, das Verfahren in den kommenden Monaten (Stand dieser Einschätzung ist Januar 2023)** abzuschließen, bleibt die Rechtslage bei der Übermittlung von Daten in die USA derzeit weiter unsicher. Zudem ist unklar, wie lange das neue Data Privacy Framework tatsächlich in Kraft sein wird – hat doch der Datenschützer Schrems bereits angedeutet, auch gegen diesen Angemessenheitsbeschluss klagen zu wollen.[23]

Es bleibt also dabei, dass die Übermittlung personenbezogener Daten in die USA mit Vorsicht zu genießen ist.

3.2.3 TOM und der Anforderungskatalog C5 des BSI

Auftragsverarbeiter, also auch die meisten Cloud-Anbieter, sind nach Art. 28 Abs. 2 S. 2 lit. c und Art. 32 DSGVO dazu verpflichtet, ***technische und organisatorische Maßnahmen*** (**TOM**) zu ergreifen, die den Schutz der verarbeiteten personenbezogenen Daten sicherstellen. Wirkung und Umsetzung der TOM sind für Auftraggeber häufig schwierig zu überprüfen.

Zur Unterstützung des Nachweises angemessener TOM ist die Vorlage eines Testats über die Einhaltung des C5-Kataloges des BSI gut geeignet. Mit dem C5 Kriterienkatalog[24] hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Unternehmen und der öffentlichen Verwaltung einen ersten Leitfaden mit Mindestanforderungen für die Nutzung externer Cloud-Dienste zur Verfügung gestellt, die bei der Auftragsvergabe durch die Bundes- und Landesverwaltung bindend zu beachten sind (vgl. § 8 Abs. 1 BSIG). Mit der Vorlage eines Testats kann der Cloud-Anbieter nachweisen, dass er effektive Schutzmaßnahmen ergriffen hat, um den Mindeststandard des C5-Kataloges zu erreichen. Die Zertifizierung kann etwa durch einen Wirtschaftsprüfer erfolgen.

Gerade in Verbindung mit dem IT-Grundschutz25 ist ein BSI-C5-Zertifikat ein geeigneter Ausweis für das Vorliegen der Standardkonformität zu Art. 32 DSGVO.

Inzwischen sind die C5-Anforderungen Teil der neuen EVB-IT Cloud zur Beauftragung von Cloud-Anbietern durch die öffentliche Verwaltung und werden so in Zukunft voraussichtlich regelmäßiger Bestandteil öffentlicher Ausschreibungen.

Allerdings bleibt es selbst bei Vorliegen eines Testats dem Auftraggeber überlassen, zu entscheiden, ob die Mindeststandards des C5-Anforderungskataloges in der Lage sind, dem konkreten Schutzbedarf gerecht zu werden.

---

22. Abrufbar unter https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf, zuletzt abgerufen am 11.01.2023.

23. https://noyb.eu/en/new-us-executive-order-unlikely-satisfy-eu-law, zuletzt abgerufen am 11.01.2023.

24. Cloud Computing Compliance Criteria Catalogue – C5:2020, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html, zuletzt abgerufen am 11.01.2023.

25. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, zuletzt abgerufen am 11.01.2023.

26. https://news.microsoft.com/de-de/microsoft-eu-datengrenze-cloud-2023/, zuletzt abgerufen am 11.01.2023.

Gerade bei sensiblen Daten oder großen Datenmengen müssen die von der Behörde festgelegten Anforderungen unter Umständen über die Mindeststandards hinausgehen und weitere TOM ergriffen werden. **Die Prüfpflicht und die Verantwortlichkeit hinsichtlich des Datenschutzniveaus bleiben also bei dem Auftraggeber. Auch im Rahmen von US-Transfers bzw. der Beauftragung von US-Unternehmen bleibt es Aufgabe des Auftraggebers, sicherzustellen, dass diese nicht zu unannehmbaren Risiken führen.** Der BSI-C5-Katalog stellt für die Cloud-Nutzung durch öffentliche Stellen aber in jedem Fall eine gute Orientierung dar (weitere Informationen zu den EVB-IT Cloud finden sich in der zweiten Hälfte dieses White Papers).

3.3 Lösungsansätze

Auch wenn der Einsatz von US-Unternehmen aktuell mit Rechtsunsicherheiten verbunden ist, suchen die öffentliche Verwaltung und die US-Cloud-Anbieter nach Wegen, um die Nutzung im Einklang mit EU-Recht zu ermöglichen. Neben neuen Lösungsansätzen der US-Cloud-Anbieter werden in der öffentlichen Verwaltung auch Multi-Cloud- und Cloud-Computing-Ansätze verfolgt.

3.3.1 Projekte der US-Hyperscaler

a) Microsoft und die Data Boundary

Am 1. Januar 2023 hat etwa Microsoft mit der Einführung der ***Data Boundary*** begonnen, mit dem Ziel, europäischen Nutzern Unabhängigkeit von US-Servern und möglichem Zugriff der US-Behörden auf (personenbezogene) Daten zu gewährleisten.[26] Die Kunden von Microsoft 365, Azure, Power Platform und Dynamics 365 sollen die Möglichkeit erhalten, Kundendaten ausschließlich innerhalb der EU zu speichern und zu verarbeiten – also innerhalb der „Datengrenze“. In Verbindung mit dem neuen Data Privacy Framework sollen so auch Microsoft-Kunden souverän werden, indem der Schutz vor dem Zugriff durch US-Behörden erhöht wird.

Dass Microsoft seine neue Datengrenze schon in der Einführungsphase so intensiv bewirbt, ist nicht überraschend: Erst Ende letzten Jahres endeten Verhandlungen zwischen Microsoft und den deutschen Datenschutzbehörden (Datenschutzkonferenz – DSK) mit einem überarbeiteten **Data Protection Addendum (DPA)**[27] – dem die DSK immer noch ein unzureichendes Schutzniveau und nur „geringfügige Verbesserungen“ attestierte.[28] Dieses Urteil begründet die DSK damit, dass Microsoft sich vorbehält, Daten der Kunden auch zu eigenen Zwecken zu verarbeiten und Daten an Behörden offenzulegen, die nicht dem Recht der Union oder der Mitgliedsstaaten unterliegen.

---

27. Abrufbar unter: https://104654.seu2.cleverreach.com/c/78084869/d188ac9f21b-rm7yts, zuletzt abgerufen am 11.01.2023.

28. DSK: Festlegung vom 24.11.2022, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf; s. auch https://www.heuking.de/de/news-events/newsletter-fachbeitraege/artikel/microsoft-365-und-der-datenschutz-us-datenuebermittlung-unzulaessig-einwilligungen-unwirksam.html, zuletzt abgerufen am 11.01.2023.

Zudem mache das Unternehmen keine ausreichenden Angaben dazu, wessen Daten zu eigenen Zwecken verarbeitet werden. Die DSK kommt deshalb zu dem Ergebnis, dass ein Einsatz der Microsoft-Cloud-Anwendungen in Behörden unter diesen Umständen auf keinen Fall möglich sei.

Aber auch neben der Kritik der Datenschutzbehörden sieht es aktuell nicht aus, als würde die Data Boundary in absehbarer Zeit halten, was sie verspricht. So soll die Umstellung auf die ausschließliche Speicherung und Verarbeitung in der EU schrittweise erfolgen, sodass es eine mit weiterer Rechtsunsicherheit verbundene Übergangsphase geben wird. Darüber hinaus sieht es so aus, als wolle Microsoft auch in Zukunft Unterauftragsverarbeiter und eigene Mitarbeiter außerhalb der EU einsetzen, um Daten innerhalb der Data Boundary zu verarbeiten. Dazu kommt, dass Microsoft davon ausgeht, dass einzelne Dienste weiterhin „begrenzte Übertragungen von Kundendaten außerhalb der EU“ durchführen werden. So schneidet sich Microsoft aber einen wichtigen Weg ab, um vollständige Undurchlässigkeit der Datengrenze sicherzustellen. Weitere Verzögerungen dürften dadurch entstehen, dass Microsoft die ergänzenden „Transparenzdokumente“ für die Data Boundary zunächst nur auf Englisch veröffentlichen wird. Die letzte Phase des Data-Boundary-Rollouts soll erst 2024 abgeschlossen sein.[29]

Somit ist die Data Boundary nach jetzigem Planungsstand nicht in der Lage, einen Zugriff durch US-Behörden vollständig rechtlich auszuschließen, auch wenn die Risiken durch den Verbleib der Daten in der EU deutlich reduziert werden. Trotzdem ist es noch ein weiter Weg zu einer rechtssicheren Nutzung der Standard-Programme.



29. https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098, zuletzt abgerufen am 11.01.2023.

b) T-Systems und Google – klappt es dieses Mal mit der Datentreuhand?

Nachdem ein gemeinsames Datentreuhandmodell des Telekom-Unternehmens T-Systems und Microsoft im Jahr 2018 scheiterte,[30] versucht es die Telekom nun mit US-Cloud-Anbieter Google: Mitte 2022 ist die ***T-Systems Sovereign Cloud powered by Google Cloud live*** gegangen. In dieser werden außer den Office-Anwendungen alle Google-Cloud-Dienste angeboten, Zielgruppe sind nicht nur Unternehmen, sondern auch der öffentliche Sektor.[31] Das Angebot soll allerdings etwas teurer sein als die Public Cloud von Google.[32]

Auch wenn Google und T-Systems umfassende Maßnahmen ergriffen haben, verbleibt das Risiko, dass die eingesetzten Server Google gehören und dort personenbezogene Daten von EU-Unternehmen gespeichert werden (wenn auch verschlüsselt). Dieses Risiko wäre vermeidbar, würden stattdessen eigene Server der T-Systems verwendet. Theoretisch wäre es zudem möglich, dass Google Hintertüren in die Software einbauen und den US-Behörden so doch eine Zugriffsmöglichkeit verschafft. Für eine solche Vorgehensweise gibt es aktuell jedoch keine Anhaltspunkte.

c) Microsoft for Sovereignty: Zusammenarbeit mit SAP und Delos

Neben der Data Boundary arbeitet Microsoft auch noch an einem neuen Angebot, das sich ausdrücklich an Behörden und öffentliche Einrichtungen richten soll. Im Rahmen des Projektes Microsoft for Sovereignty sollen zusammen mit Unternehmen aus den jeweiligen EU-Staaten Cloud-Lösungen entwickelt werden, die von Microsofts US-Angeboten unabhängig sind und den hohen Datenschutzstandards in der EU gerecht werden.[33]

Im Rahmen des Projektes Microsoft for Sovereignty sollen Cloud-Lösungen entwickelt werden, die von Microsofts US-Angeboten unabhängig sind.

Bereits 2021 hatte sich Microsoft mit den französischen Unternehmen Orange und Capgemini zusammengeschlossen, um auf deren Servern strikt getrennt von der globalen Microsoft-Infrastruktur die Microsoft-Cloud-Angebote für französische Behörden zu betreiben.[34] Vergangenes Jahr wurde ein ähnlicher Zusammenschluss auch für Deutschland öffentlich gemacht. Zunächst hatte sich Microsoft mit SAP und Arvato zusammengetan, um eine „souveräne" Verwaltungscloud aufzubauen, betrieben durch Arvato Systems bzw. eine neu zu gründende Tochterfirma. Anders als bei dem Angebot von T-Systems war geplant, diese Lösung auf eigenen Servern der deutschen Betreiberfirma zu hosten und so die Zugriffsmöglichkeiten von Microsoft zu minimieren.

30. S. z.B. https://www.computerwoche.de/a/aus-fuer-microsoft-cloud-deutschland,3545727, zuletzt abgerufen am 11.01.2023.

31. S. z.B. https://www.heise.de/news/Souveraene-Cloud-fuer-Deutschland-6194879.html, zuletzt abgerufen am 11.01.2023.

32. https://www.tagesspiegel.de/berlin/wir-halten-an-unserem-plan-fest-6853897.html, zuletzt abgerufen am 11.01.2023.

33. https://www.microsoft.com/en-us/industry/sovereignty/cloud, zuletzt abgerufen am 11.01.2023.

34. S. z.B. https://www.heise.de/select/ct/2021/14/2111909443963380865, zuletzt abgerufen am 11.01.2023.

Aktuell wird nun doch ein Projekt ohne Unterstützung von Arvato verfolgt. Die SAP-Tochter Delos Cloud soll als Betreiberin nunmehr gemieteter Rechenzentren bis 2024 eine Cloud-Struktur auf Grundlage von Microsoft-Software aufbauen, auf der auch die Cloud-Dienste vieler anderer Anbieter verfügbar sein sollen.[35] Während sich Microsoft und SAP einer souveränen Cloud rühmen, bleiben kritische Stimmen nicht aus. Hierbei wird angeführt, dass es auch bei Verwendung der Delos-Server dabei bliebe, dass sich der Staat von Microsoft abhängig mache.

Wenn allerdings tatsächlich nur Delos Zugriff auf die Server hätte, so wäre von einem angemessenen Datenschutzniveau wohl auszugehen und Microsoft müsste aktiv Hintertüren in die bereitgestellte Software einbauen, damit US-Behörden Zugriff auf die Daten erhalten. Zudem könnte Microsoft die fremden Server auch nicht ohne Weiteres abstellen. Erst wenn die US-Regierung Microsoft dazu bringen würde, die Belieferung mit Sicherheitsupdates einzustellen, entstünden hier ernstzunehmende Sicherheitsrisken. Beide Szenarien scheint die Bundesregierung aktuell allerdings für unwahrscheinlich zu halten. Schließlich verwendet die Bundesregierung auch jetzt Microsoft-Programme – gehostet auf den eigenen Servern.

Nach ihrer Fertigstellung soll die geplante Microsoft-Cloud voraussichtlich auch für Länder und Kommunen freigegeben werden.[36] Ein Angebot an private Unternehmen ist nach jetzigem Kenntnisstand hingegen nicht geplant, was Fragen zu Skaleneffekten und deren Auswirkung auf die Betriebskosten aufwürfe. Aktuell soll eine Abnahme der Delos-Cloud durch das BSI 2024 erfolgen, gerade die Anmietung bestehender Server dürfte den Aufbau der Infrastruktur beschleunigen. Wann die neue Cloud dann auch für die kommunale Ebene freigegeben wird, ist hingegen noch nicht bekannt, auch hier entsteht also keine kurzfristige Lösung für Einrichtungen auf kommunaler Ebene. Zudem wäre nach Live-Gang zunächst eine Einschätzung der Datenschutzbehörden abzuwarten.

3.3.2 Open-Source-Lösungen

Auch der Einsatz von Open-Source-Lösungen wird sowohl bei lokal installierter Software als auch in der Cloud immer beliebter. Dadurch, dass der Quellcode von Open-Source-Software frei einsehbar ist und in der Regel beliebig verändert, angepasst oder kopiert werden kann, können Sicherheitslücken durch die beteiligte Community schneller behoben werden und der absichtliche Einbau von Hintertüren durch den Softwarehersteller wird erschwert. Deswegen überrascht es nicht, dass sowohl auf Bundesebene als auch auf Landesebene Open-Source-Strategien verfolgt werden[37] und die Software kommerziellen Programmen häufig in nichts nachsteht.

Open-Source-Lösungen werden immer beliebter.

35. S. z.B. https://www.heise.de/news/Digitale-Souveraenitaet-Microsoft-Cloud-soll-2024-starten-7338725.html, zuletzt abgerufen am 11.01.2023.

36. S. z.B. https://www.heise.de/news/Souveraene-Cloud-Microsoft-lockt-Bundesregierung-mit-kostenloser-Testplattform-6030508.html, zuletzt abgerufen am 11.01.2023.

37. Etwa die Open-Source-Strategie des Bundesfinanzministeriums; s. etwa https://www.zeit.de/news/2022-02/03/sap-und-arvato-bauen-verwaltungs-cloud-mit-microsoft-technik, zuletzt abgerufen am 11.01.2023.

Doch obwohl der Einsatz von Open Source grundsätzlich erstrebenswert ist, muss aus rechtlicher Sicht keinesfalls konsequent und um jeden Preis ausschließlich auf Open Source gesetzt werden. Es gibt in der Praxis immer wieder Anwendungsfälle, in denen aus Sicht der öffentlichen Hand (noch) nicht auf die kommerziellen Angebote, etwa von Microsoft, verzichtet werden kann. Da ein Aufbau der von der Bundesregierung angestrebten Open-Source-Programme häufig noch Jahre dauern dürfte, gewinnen Multi-Cloud-Angebote an Bedeutung. Dadurch, dass bei der Multi Cloud die Cloud-Angebote mehrerer Anbieter über nur eine Infrastruktur zur Verfügung gestellt werden, können diese flexibel miteinander kombiniert werden, sodass eine parallele Nutzung von Open-Source- und anderen Angeboten möglich ist. Der Aufbau einer Multi Cloud ist jedoch kompliziert und verlangt bestenfalls vorherige Erfahrungen mit dem Aufbau einer eigenen IT-Infrastruktur; ein entsprechendes Projekt der Bundesregierung ist aber hierbei bereits recht weit vorangeschritten. Alternativ ist es denkbar, auf die Cloud-Infrastruktur nur eines Anbieters zu setzen, der dennoch die Möglichkeit bietet, die Cloud Server, sowie die darauf angebotenen Funktionen und Anwendungen flexibel zusammenzustellen.

Wichtig ist dabei in erster Linie, dass der Cloud-Anbieter technologieoffen ist, bestenfalls bekannte sowie noch unbekannte Open-Source-Lösungen unterstützt und bereits eigene Open Source Partner hat, deren Angebote einfach in Anspruch genommen werden können.

3.3.3 Wann ist die Cloud wirklich souverän?

Entscheidet sich eine Behörde, Daten und Software nicht auf eigenen Servern zu hosten, beginnt die Suche nach einem passenden Anbieter. Da die Lösungen der US-Cloud-Anbieter genauso wie durchaus auch ausschließlich auf Open-Source setzenden Angebote nicht immer marktreif sind oder das notwendige Schutzniveau nicht erreichen, suchen öffentliche Einrichtungen nach Alternativen. Dabei haben sie genau wie Unternehmen vielfältige Anforderungen an Funktionalitäten und Datenschutz zu beachten. Ist die ausschließliche Nutzung von Open-Source-Komponenten nicht mit dem angestrebten Zweck vereinbar, müssen Kriterien festgelegt werden, die der künftige Vertragspartner erfüllen sollte. Auch wenn sich diese Kriterien je nach Einsatzgebiet erheblich unterscheiden können, ist folgendes zu beachten, um rechtliche und technische Souveränität zu gewährleisten:

Mindestanforderungen sind hier in der Regel eigene Rechenzentren und eine tatsächliche physische Trennung der Server mittels eines Air Gaps. Besonders sicher ist es, wenn ein europäischer Cloud-Anbieter die Rechenzentren selbst betreibt oder diese durch eine europäische Partnerfirma innerhalb der EU betrieben werden.

38. Vgl. etwa Hermann Pünder/Anika Klafki, in: Pünder/Schellenberg, Vergaberecht, 3. Auflage 2019, § 108 GWB Rn. 1.

Auch die Energieversorgung oder der Schutz vor Naturkatastrophen und Angriffen der Rechenzentren ist für die Bewertung der Souveränität von Bedeutung. Um Souveränität zu erreichen, ist es zudem wichtig, dass eine einfache Datenmigration auf die oder von den Servern des Cloud-Anbieters möglich ist und dass der Anbieter eine hohe Flexibilität bei der Auswahl der gehosteten Software und Partner bietet. Bestenfalls sollte der Cloud-Anbieter technologieoffen sein und viele Anbieter sowie Open-Source-Anwendungen unterstützen. Indizien für einen sicheren und souveränen Cloud-Anbieter sind Zertifizierungen über den IT-Grundschutz, ISO 27001 und die C5-Kriterien.

Besonders attraktiv sind Anbieter, die nicht nur BSI C5-zertifiziert sind, sondern auch in der Lage sind, höchste Schutzstandards einzuhalten.

Besonders hohe Flexibilität und geringe Abhängigkeit von einzelnen Anbietern wird durch Multi-Cloud-Ansätze oder Anbieter, welche die flexible Kombination mit weiteren Diensten ermöglichen, erreicht. Diese erlauben es, einzelne Angebote der US-Cloud-Anbieter zu nutzen, während an anderer Stelle die Angebote anderer Anbieter oder sogar eigene Open-Source-Lösungen eingebunden werden, und finden so einen Kompromiss zwischen maximaler Datensicherheit und Praktikabilität.



Die öffentliche Hand hat bei der Verhandlung von Rahmenbedingungen durch ihr erhebliches Verhandlungsgewicht im Vergleich zu individuellen Verhandlungen durch die einzelnen Einrichtungen darüber hinaus die Möglichkeit, auch bei großen Anbietern gewisse Zugeständnisse zu erwirken, etwa im Hinblick auf die Datensicherheit. Auch das Patch-Management kann bei höherer Einheitlichkeit besser und schneller werden.

Dies braucht jedoch Zeit, wie man etwa an der Entwicklung der Delos-Cloud sieht. Gerade wenn eine schnelle Lösung benötigt wird, ist es deshalb sinnvoll, auf bestehende Lösungen zurückzugreifen und auf (Multi-)Cloud-Anbieter zu setzen, die schon jetzt das europäische Datenschutzrecht und die C5-Kriterien umsetzen. Wenn die Cloud darüber hinaus eine hohe Kompatibilität gewährleistet, bleibt auch die sukzessive Einbindung der Anwendungen weiterer Anbieter möglich.

4 Vergaberechtliche Vorgaben

Nach der obigen Darstellung der datenschutzrechtlichen Vorgaben im Hinblick auf die Inanspruchnahme von Cloud-Diensten soll nun nachfolgend eine Bewertung aus vergaberechtlicher Sicht erfolgen.

4.1 Besonderheiten im Ausschreibungsverfahren

Besonderheiten ergeben sich insbesondere, wenn Bund, Länder oder Kommunen, deren Verbände oder von ihnen finanzierte oder kontrollierte juristische Personen (vgl. § 99 GWB) Cloud-Leistungen entgeltlich am Markt beschaffen (vgl. § 103 Abs. 1, 4 GWB). In diesen Fällen müssen sie das Vergaberecht beachten. Dies hat zur Folge, dass der Einkauf in der Regel nach bestimmten gesetzlichen Vorgaben in wettbewerblichen Vergabeverfahren erfolgen muss (vgl. §§ 97, 119 GWB; §§ 1, 14 VgV).

4.1.1 Grundsatz

Erreicht oder überschreitet der Gesamtauftragswert (inkl. sämtlicher Implementierungs-, Lizenz-, Schulungs-, Service- (Hosting, Betrieb, Wartung, Pflege) und optionalen Leistungen; vgl. § 3 VgV) die EU-Schwellenwerte in Höhe von EUR 215.000 EUR netto (bei obersten Bundesbehörden sowie allen oberen Bundesbehörden und vergleichbaren Bundeseinrichtungen sind es EUR 140.000 EUR netto), können Konkurrenzunternehmen im konkreten Vergabeverfahren gerichtlich durchsetzen, dass der öffentliche Auftraggeber die Vorgaben des Vergaberechts einhält (vgl. §§ 97 Abs. 6, 155, 160, 168, 171, 178 GWB).

4.1.2 Ausnahme für reine Open-Source-Leistungen

Vergaberecht findet keine Anwendung, wenn der Staat Leistungen unentgeltlich erhält. **Deswegen können Behörden Software ohne Vergaberecht beschaffen, die ihnen lizenzkostenfrei überlassen wird. Dies kann etwa bei reiner Open Source Software der Fall sein. Sind zu deren Einsatz allerdings entgeltliche Dienstleistungen erforderlich (für die Implementierung, Schulung, das Hosting usw.), unterliegen diese wiederum dem Vergaberecht.** Bei der Vergabe der entsprechenden Dienstleistungen kann der öffentliche Auftraggeber gehalten sein, wettbewerbsverzerrende Vorteile eines bei der Software-Überlassung und damit vorbefassten Unternehmens auszugleichen (vgl. § 7 Abs. 1, 2 VgV sowie OLG Düsseldorf, Beschl. v. 03.02.2021 – VII-Verg 25/18 = NZBau 2021, 344 und EuGH, Urt. v. 28.5.2020 – C-796/18 (Informatikgesellschaft für Software-Entwicklung mbH [ISE]/Stadt Köln)).

Unentgeltliche Beschaffungen erfüllen nicht den Tatbestand des „öffentlichen Auftrags“ im Sinne von § 103 Abs. 1 GWB.

4.1.3 Digitale Souveränität und öffentlich-öffentliche Zusammenarbeit

Auch bei öffentlich-öffentlicher Zusammenarbeit darf ein privater Dritter nicht in ungerechtfertigter Weise profitieren: Überlässt etwa Bundesland A Bundesland B eine Software gegen das Versprechen, sich später gegenseitig Weiterentwicklungen dieser Software zu überlassen, kann dies ein gem. § 108 Abs. 6 GWB vergaberechtsfreier Vorgang sein. Allerdings darf sich daraus auf dem nachgelagerten Markt kein ungerechtfertigter Vorteil für einzelne private IT-Dienstleister ergeben (vgl. OLG Düsseldorf, Beschl. v. 03.02.2021 – VII-Verg 25/18 = NZBau 2021, 344) und EuGH (Urt. v. 28.5.2020 – C-796/18)).

Insgesamt sind zahlreiche öffentlich-öffentliche Transaktionen vom Vergaberecht freigestellt. Zentralnorm ist hier § 108 GWB: Außer der sog. „horizontalen" öffentlich-öffentlichen Zusammenarbeit im Sinne von § 108 Abs. 6 GWB sind vor allem sog. „Inhouse"-Geschäfte in zahlreichen Konstellationen (Mutter-an-Tochtergesellschaft, Tochter-an-Muttergesellschaft, Beauftragung zwischen Schwestergesellschaften usw.) vom Vergaberecht freigestellt. Der Staat soll nicht gezwungen sein, Leistungen an den Markt zu bringen, die den Staatsbereich nicht verlassen.[38] Nach § 120 Abs. 4 GWB darf der Staat zentrale Beschaffungsstellen einsetzen, die für diesen oder mehrere öffentliche Auftraggeber in eigenen oder in fremdem Namen Leistungen am Markt einkaufen. §§ 108, 120 Abs. 4 GWB sind für einen föderalen und kommunal organisierten Staat wie Deutschland von großer Bedeutung. In Deutschland wird jüngst verstärkt von den sich daraus ergebenden Möglichkeiten Gebrauch gemacht.

§§ 108, 120 Abs. 4 GWB ermöglichen es einem öffentlichen Anbieter wie Dataport AöR aus Altenholz, zentraler IT-Dienstleister für mehrere Bundesländer und Kommunen zu sein. Dataport ist auch Teil des Projekts „Deutsche Verwaltungscloud"[39]. Andere wichtige öffentliche „Player" im Bereich IT-Versorgung der öffentlichen Verwaltung sind etwa die AKDB Anstalt für Kommunale Datenverarbeitung in Bayern mit Sitz in München[40], die Bundesdruckerei Gruppe GmbH[41] in Berlin oder die govdigital eG, eine bundesweite Genossenschaft zur Integration innovativer IT-Lösungen im öffentlichen Sektor.[42] Software-, Server-, Rechenzentrums- und Cloud-Leistungen, die von der öffentlichen Hand selbst bereitgestellt werden, entwickeln sich zu einer wichtigen Säule der digitalen Souveränität in Deutschland.

39. S. z. B. https://www.dataport.de/was-wir-bewegen/thema/deutsche-verwaltungscloud/ , zuletzt abgerufen am 06.01.2023.

40. S. z. B. https://www.akdb.de/ueber-die-akdb/unternehmensleitung-und-gremien/ , zuletzt abgerufen am 06.01.2023.

41. S. etwa https://www.bundesdruckerei.de/de/loesungen, zuletzt abgerufen am 06.01.2023.

42. S. etwa https://www.govdigital.de/govdigital/ueber-uns, zuletzt abgerufen am 06.01.2023.

Einer der Vorreiter ist die Freie und Hansestadt Hamburg. Das Bundesland hat das Prinzip der digitalen Souveränität durch rein öffentlich-öffentliche Beschaffung in einem neuen Gesetz umgesetzt. Im September 2022 hat die Bürgerschaft das sog. „IT-Souveränitätsgesetz“ beschlossen.[43] Danach dürfen Aufträge der Behörden und Ämter der Freien und Hansestadt Hamburg über bestimmte Software-Leistungen, deren Einsatz für die Ausübung hoheitlicher Aufgaben unverzichtbar ist, künftig ausschließlich „inhouse“ (vgl. § 108 Abs. 1-5 GWB) oder im Rahmen öffentlich-öffentlicher Kooperationen (vgl. § 108 Abs. 6 GWB) vergeben werden, soweit die entsprechenden Fachverfahren/-anwendungen nicht ohnehin von staatlichen Stellen selbst betrieben werden.



4.1.4 Gestaltungsmöglichkeiten in Vergabeverfahren

Entscheidet sich die öffentliche Hand hingegen, Cloud- oder andere IT-Leistungen am Markt zu beschaffen, hat sie umfangreiche Gestaltungsmöglichkeiten.

So folgt aus dem sog. „Leistungsbestimmungsrecht“ öffentlicher Auftraggeber (analog § 311 Abs. 1 BGB), dass sie den genauen Leistungszuschnitt selbst bestimmen darf. **Voraussetzung ist, dass sich die Leistungsvorgaben diskriminierungsfrei aus dem konkreten Beschaffungsbedarf ergeben** (grundlegend zum Leistungsbestimmungsrecht etwa OLG Düsseldorf, Beschl. v. 13.04.2016 – VII-Verg 47/15). **Offene oder verdeckte produkt- oder herstellerspezifische Vorgaben sind nur ausnahmsweise und bei hinreichender sachlicher Begründung zulässig** (vgl. zum sog. „Verbot produktspezifischer Ausschreibung“ § 31 Abs. 6 VgV).[44]

43. S. etwa https://www.hamburg.de/pressearchiv-fhh/16473474/2022-09-06-bjv-mehr-sicherheit-in-der-it/, zuletzt abgerufen am 06.01.2023.

44. Vgl. etwa Trutzel, in: Ziekow/Völlink, Vergaberecht, 4. Auflage 2020, § 31 VgV Rn. 51.

Im Hinblick auf Software-Beschaffungen gilt: Es bleibt Sache der jeweiligen Bundes-, Landes- oder kommunalen Einrichtung, ob sie eine Software als Service oder lieber „on premise“ beschaffen möchten. Jeweils können Bedarfsträger und Vergabestelle frei entscheiden, ob sie die Lösung auf eigenen oder fremden Servern hosten und betreiben (lassen) möchten. Es gibt keine Pflicht, Software stets auf eigenen Servern oder gar lokal auf dem einzelnen PC zu installieren und zu betreiben. Der jeweilige öffentliche Auftraggeber kann sich auch für das Hosting auf fremden Servern oder in der Cloud entscheiden. Für letzteren Fall hat der Bund die sog. „EVB-IT Cloud“ als „AGB der öffentlichen Hand“ entwickelt und im Frühjahr 2022 erstmals veröffentlicht (dazu unten mehr).

Das Vergaberecht hindert öffentliche Auftraggeber auch nicht daran, im Rahmen der Leistungsbeschreibung i. S. v. § 121 GWB i. V. m. § 31 VgV oder in den sonstigen Ausführungsbedingungen i. S. v. § 128 GWB Mindestvorgaben für die Vertragsausführung zu machen. So können sie Unternehmen (auch solche aus Drittstaaten) verpflichten, die angebotene Software für den konkreten Auftrag z. B. auf einem bestimmten Server an einem bestimmten Ort in Deutschland zu hosten bzw. hosten zu lassen. Ebenso zulässig wäre, vorzuschreiben, dass sämtliche Cloud-Server innerhalb der EU stehen müssen (Vorgaben für den Leistungsort sind also zulässig; nicht aber solche bezogen auf Herkunft oder Standort des Unternehmens). Solche Vorgaben müssen aus dem konkreten Bedarf abgeleitet werden und sachlich gerechtfertigt sein. Öffentliche Auftraggeber müssen die Gründe gem. § 8 Abs. 1 VgV dokumentieren, um die Nachprüfung zu ermöglichen.

Selbstverständlich stellen gesetzliche Vorgaben sachliche Gründe dar. Lassen sich aus dem Datenschutzrecht bestimmte Vorgaben für die Leistungsbestimmung ableiten, so müssen öffentliche Auftraggeber diese beachten bzw. gewährleisten, dass (potenzielle) Auftragnehmer diese einhalten. So liefert das Datenschutzrecht den sachlichen Grund, vorzugeben, dass sich die Cloud-Server innerhalb der EU befinden müssen. Nach unserer Auffassung ist zudem nicht völlig ausgeschlossen, dass im konkreten Einzelfall über den EU-Datenschutz hinausgehende nationale Sicherheitsinteressen (z. B. Sicherungsmöglichkeit der physikalischen Zugriffsmöglichkeiten durch nationale Sicherheitsbehörden) auch den verpflichtenden Serverstandort in Deutschland rechtfertigen können. Ein entsprechender Fall ist, soweit ersichtlich, in der höchstrichterlichen Rechtsprechung aber noch nicht entschieden.

Sachlich gerechtfertigt und folglich vergaberechtlich zulässig sind etwa folgende Vorgaben:

- Vorgabe des Betriebsmodells (zum Beispiel: „im eigenen Rechenzentrum“)
- Einhaltung deutschen und europäischen Datenschutzrechts als Mindestanforderung in Leistungsbeschreibung oder Ausführungsbedingungen
- Definition weiterer datenschutzrechtlicher Vorgaben in Leistungsbeschreibung oder Ausführungsbedingungen

- Festlegung des gewünschten Schutz-/Sicherheitsniveaus in Leistungsbeschreibung oder Ausführungsbedingungen, z. B. Sicherheitsmanagement nach ISO 27001; IT-Grundschutz des BSI
- Regelungen zum Vertragsende: Übertragbarkeit / Weiterbetrieb der Leistungen

Schließlich haben öffentliche Auftraggeber einen großer Ermessensspielraum bei der Gestaltung der Zuschlagskriterien für die Zuschlagsentscheidung i. S. v. § 127 GWB i. V. m. § 58 VgV. Soweit nicht ohnehin zwingend, können bestimmte optionale Merkmale mit Bezug zu Datenschutz und Ortsansässigkeit mit einer besseren Bewertung und damit besseren Chancen auf den Vertrag mit dem öffentlichen Auftraggeber versehen werden.

4.1.5 Zwingende datenschutzrechtliche Vorgaben können zum Ausschluss von Drittstaatenanbietern führen

Zwar erlaubt das Vergaberecht regelmäßig nicht, (potenzielle) Bieter oder (potenzielle) Unterauftragnehmer (vgl. § 36 Abs. 5 VgV i. V. m. §§ 123, 124 GBW) allein auf Grund ihrer Herkunft oder Ortsansässigkeit auszuschließen (vgl. den Gleichbehandlungsgrundsatz in § 97 Abs. 2 GWB; vgl. jüngst wieder der EuGH, Urt. vom 14. Juli 2022 – Rs. C-436/20).

Es gibt aber gesetzliche Ausnahmen. Auch aus dem Datenschutzrecht können sich mittelbar Ausschlussgründe ergeben, wenn Unternehmen aus Drittstaaten nicht die Gewähr für das erforderliche Schutzniveau bieten. Vergaberechtliche Anknüpfungspunkte für den Ausschluss von Angeboten bestimmter Unternehmen ergeben sich dabei aus besonderen und allgemeinen gesetzlichen Regelungen über das Vergabeverfahren:

Zu den etablierten Spezialregelungen gehört § 55 SektVO. Diese Ausschlussnorm gilt allerdings nur für sog. „Sektorentätigkeiten“ i. S. v. § 102 GWB, d.h. im Bereich der Wasser-, Strom-, Gas-, Wärme, Verkehrs-, Brennstoffversorgung, also netzbasierter kritischer Versorgungsleistungen. § 55 SektVO erlaubt unter bestimmten Voraussetzungen den Ausschluss von Angeboten mit Erzeugnissen aus außerhalb des Europäischen Wirtschaftsraums liegenden Staaten, mit denen auch sonst keine entsprechenden Handelsabkommen bestehen (s. hier auch Abs. 3 für Software für die Ausstattung von Telekommunikationsnetzen). So durften öffentliche Auftraggeber ein Angebot mit chinesischen Straßenbahnfahrzeugen ausschließen (vgl. OLG Brandenburg, Beschluss vom 02.06.2020, 19 Verg 1 / 20). Bei verteidigungs- und sicherheitsspezifischen öffentlichen Aufträgen iSv § 1 VSVgV und § 104 Abs. 1 GWB gab es bisher schon die Möglichkeit, bestimmte Anforderungen an die Person des (potenziellen) Bieters und (potenzieller) Unterauftragnehmer zu stellen (etwa bei Verschlusssachenaufträgen iSv § 7 VSVgV und mit Blick auf die Versorgungssicherheit iSv § 8 VSVgV). Dies gilt selbstverständlich auch für IT- und Serverleistungen mit entsprechendem Sicherheitsbezug.

Die geopolitischen Entwicklungen der jüngsten Zeit haben weitere Spezialregelungen hervorgebracht. Mit diesen können öffentliche Auftraggeber insbesondere Unternehmen aus Nicht-EU-Staaten den Zugang zu öffentlichen Aufträgen verwehren:

- **Bundeswehr:** Das bis zum 31.12.2026 befristete Bundeswehrbeschaffungsbeschleunigungsgesetz erlaubt nun in § 7 Abs. 2-4 den Ausschluss von Bewerbern, Bietern oder (potenziellen) Unterauftragnehmern, wenn diese in einem Staat außerhalb der Europäischen Union ansässig sind, der nicht die notwendige Gewähr für die Wahrung der Sicherheitsinteressen der Bundesrepublik Deutschland bietet. Nach Abs. 5 gilt dies allerdings nicht in Bezug auf Auftragnehmer und Unterauftragnehmer, die in einem Staat ansässig sind, der Vertragspartei des Abkommens über den Europäischen Wirtschaftsraum ist. Sie gelten ferner nicht in Bezug auf Auftragnehmer und Unterauftragnehmer, die in einem Drittstaat ansässig sind, der dem Übereinkommen über das öffentliche Beschaffungswesen von 1994 (ABl. C 256 vom 3.9.1996, S. 1), geändert durch das Protokoll zur Änderung des Übereinkommens über das öffentliche Beschaffungswesen (ABl. L 68 vom 7.3.2014, S. 2) oder anderen, für die Europäische Union bindenden internationalen Übereinkommen beigetreten ist, wenn der öffentliche Auftrag in den Anwendungsbereich des jeweiligen Übereinkommens fällt.
- **Russland-Sanktionen:** Gemäß Artikel 5k Absatz 1 der VO (EU) Nr. 833/2014 ist es verboten, einen öffentlichen Auftrag oder eine Konzession an ein Unternehmen zu vergeben, dass einen „Bezug zu Russland“ im Sinne von Artikel 5k VO(EU) Nr. 833/2014 aufweist (sog. Zuschlagsverbot). Bis zum 11.10.2022 durften Altverträge mit Unternehmen im o.g. Sinne noch erfüllt werden. Dies ist nun ebenso verboten (sog. Vertragserfüllungsverbot).
- **„Instrument betreffend das internationale Beschaffungswesen der EU (IPI)“:** Auf EU-Ebene wurde außerdem mit Wirkung vom 23.06.2022 die VO (EU) 2022/1031 verabschiedet „über den Zugang von Wirtschaftsteilnehmern, Waren und Dienstleistungen aus Drittländern zum Unionsmarkt für öffentliche Aufträge und Konzessionen und über die Verfahren zur Unterstützung von Verhandlungen über den Zugang von Wirtschaftsteilnehmern, Waren und Dienstleistungen aus der Union zu den Märkten für öffentliche Aufträge und Konzessionen von Drittländern (Instrument betreffend das internationale Beschaffungswesen — IPI)“. Ziel der Verordnung ist es ausweislich ihres Art. 1 Abs. 1, den Zugang von Wirtschaftsteilnehmern, Waren und Dienstleistungen aus der Union zu den Märkten für öffentliche Aufträge und Konzessionen in Drittländern zu verbessern. Um dies zu erreichen, kann die EU-Kommission bestimmte Maßnahmen ergreifen, um Unternehmen aus den betreffenden Drittländern zu sanktionieren, wenn diese Drittländer ihrerseits Unternehmen aus der EU den Marktzugang erschweren. Die Verordnung legt im Falle von IPI-Maßnahmen auch öffentlichen Auftraggebern Pflichten gegenüber Bietern aus

Drittstaaten auf (vgl. Art. 8 der VO (EU) 2022/1031).

Zwar zielen diese Sonderregelungen primär auf Unternehmen aus „unfreundlichen" Drittstaaten wie Russland oder China. Allerdings können öffentliche Auftraggeber auch aus allgemeinen vergaberechtlichen Regelungen verpflichtet sein, Angebote von Unternehmen aus Drittstaaten – auch solchen aus den USA – auszuschließen:

Dies ist dann der Fall, wenn sich herausstellt, dass diese Unternehmen bestimmte Vorgaben in den Vergabeunterlagen nicht erfüllen können oder wollen. Fehlende Erklärungen oder Abweichungen zu den Mindestvorgaben oder Ausführungsbestimmungen (vgl. §§ 121, 128 GWB) verpflichten öffentliche Auftraggeber dann ohne Ermessensspielraum, die betreffenden Angebote vom weiteren Verfahren auszuschließen (vgl. § 57 Abs. 1 Nr. 2 und 4 VgV).

Dies ist zum Beispiel dann der Fall, wenn der öffentliche Auftraggeber in den Vergabeunterlagen vertraglich vorschreibt (vgl. zu diesen § 29 Abs. 1 VgV), dass Bieter über die Vertragslaufzeit bestimmte datenschutzrechtliche Mindestanforderungen erfüllen oder ein bestimmtes Schutzniveau gewährleisten müssen. Können sie ein entsprechendes Leistungsversprechen nicht abgeben oder es objektiv nicht erfüllen, muss die ausschreibende Stelle die entsprechenden Angebote unberücksichtigt lassen.

Zwar hat das OLG Karlsruhe (Beschluss vom 07.09.2022 – 15 Verg 8/22 = NZBau 2022, 615, 619, m.w.N.) erst jüngst entschieden, dass es primär auf das Leistungsversprechen der Bieter ankommt:

- „Der öffentliche Auftraggeber darf [...] grundsätzlich davon ausgehen, dass ein Bieter seine vertraglichen Zusagen erfüllen wird."

Das bedeutet: Sichert ein Anbieter mit seinem Angebot verbindlich zu, dass er im Leistungszeitraum alle datenschutzrechtlichen Vorgaben aus den Vergabeunterlagen erfüllen wird, kann sich ein öffentlicher Auftraggeber im Ausgangspunkt auf dieses Leistungsversprechen verlassen. Allerdings gibt es Grenzen:

Gibt es begründete Zweifel, dass der potenzielle Auftragnehmer das Leistungsversprechen einhalten kann, wird oder ist es sogar objektiv unmöglich, darf der öffentliche Auftraggeber das Angebot nicht berücksichtigen. Es liegt ein zwingender Ausschlussgrund vor, wenn das Angebot nicht die geforderten Unterlagen enthält oder – hier: in datenschutzrechtlicher Hinsicht –

von den Vergabeunterlagen, d.h. den vertraglichen Vorgaben des öffentlichen Auftraggebers, abweicht (vgl. § 57 Abs. 1 Nr. 2 und 4 VgV).

Dem widerspricht auch die Entscheidung des OLG Karlsruhe nicht: Das Gericht hielt einen Angebotsausschluss nur deshalb nicht für angezeigt, weil es im konkreten Fall die Zweifel an der datenschutzrechtlichen Leistungsfähigkeit des betroffenen Tochterunternehmens eines US-amerikanischen Cloud-Anbieters nicht teilte (vgl. OLG Karlsruhe, Beschluss vom 07.09.2022 – 15 Verg 8/22, m.w.N = NZBau 2022, 615, 619 f.). **Lässt sich hingegen etwa nachweisen, dass ein betreffendes Unternehmen personenbezogene Daten aus**



dem Auftragsverhältnis im Zweifel auch vertragswidrig an US- oder anderer Drittstaaten-Behörden herausgeben muss, kommt sein Angebot für den Zuschlag nicht mehr in Betracht.

4.1.6 Direktbeauftragung privater Cloud-Anbieter möglich?

Nicht in jedem Fall ausgeschlossen ist, dass die öffentliche Hand private Software- oder Cloud-Anbieter direkt beauftragen darf. Es handelt sich aber um Ausnahmefälle.

Voraussetzung ist in der Regel ein technisches Alleinstellungsmerkmal (vgl. § 14 Abs. 4 Nr. 2 Buchst. b) VgV). Die Leistungsanforderung, auf die sich dieses technische Alleinstellungsmerkmal bezieht, muss der öffentliche Auftraggeber im Sinne von § 31 Abs. 6 VgV diskriminierungsfrei aus seinem konkreten Beschaffungsbedarf abgeleitet und dies gem. § 8 Abs. 1 VgV dokumentiert haben. Die Rechtsprechung prüft sodann gem. § 14 Abs. 6 VgV, ob es zur vermeintlich technisch einmaligen Lösung keine vernünftige Alternative oder Ersatzlösung gibt und der mangelnde Wettbewerb nicht das Ergebnis einer künstlichen Einschränkung der Auftragsvergabe-Parameter ist. Diese Betrach-

tung bezieht sich für Auftragsvolumina, die die EU-Schwellenwerte erreichen, auf den gesamten EU-Binnenmarkt. Eine solche objektive Monopolstellung im EU-Markt wird häufig nicht ganz einfach zu begründen sein.

Unterhalb der EU-Schwellenwerte (also bis EUR 140.000 EUR netto für die obersten Bundeseinrichtungen; bis EUR 215.000 EUR netto für alle anderen öffentlichen Auftraggeber; dazu bereits oben), genügt es, zu begründen, dass die Leistung nur von einem bestimmten Unternehmen erbracht oder bereitgestellt werden kann (vgl. § 8 Abs. 4 Nr. 10 UVgO). Gem. § 106 Abs. 1 S. 1 GWB finden die Vorschriften über Nachprüfungsverfahren in den §§ 155 ff. GWB auf öffentliche Aufträge unterhalb der EU-Schwellenwerte keine Anwendung.

Unterschwellige Vergabeentscheidungen können vergaberechtlich nicht angegriffen werden.

4.2 Rolle der neuen EVB-IT Cloud

Am 1. März 2022 hat das Bundesministerium des Inneren (BMI) die Ergänzenden Vertragsbedingungen für Cloudleistungen (EVB-IT Cloud) veröffentlicht,[45] die geeignet sind, für höhere Sicherheit bei der Beauftragung von Cloud-Anbietern zu sorgen. Es gibt nun also ein Vertragswerk, das die öffentliche Hand der Ausschreibung von Cloud-Leistungen zugrundelegen kann. Neben dem EVB-IT Cloud Hauptvertrag gehören zum Vertragswerk die entsprechenden AGB, ein Kriterienkatalog, Nutzungshinweise und die Möglichkeit zur Einbindung der AGB des Auftragnehmers.

Die EVB-IT Cloud beruhen maßgeblich auf dem C5-Katalog des BSI, können also gerade von Cloud-Anbietern, die sich schon bisher an den BSI-Standard gehalten haben, leicht umgesetzt werden. Die Einhaltung wird dann durch einen BSI-C5-Prüfbericht nachgewiesen.

Zwar sind, anders als bisher, neben den Bundesbehörden auch die Landesbehörden und viele kommunale Behörden gehalten, die EVB-IT Cloud zu nutzen und nur Cloud-Anbieter zu beauftragen, die den BSI-C5-Standard einhalten und nachweisen können. Aus Sicht der öffentlichen Auftraggeber ist es i. d. R. auch zweckmäßig, die vertraglichen Regelungen an die EVB-IT anzuknüpfen.

Allerdings sind die meisten öffentlichen Auftraggeber nur durch binnenwirksame Verwaltungsvorschriften zum Bundes- oder jeweiligen Landeshaushaltsrecht gebunden und auch die EVB-IT Cloud selbst enthalten Öffnungsklauseln. **Diese erlauben es sogar, die AGB der Cloud-Anbieter punktuell vorrangig einzubinden (Ziff. 1.5 und Anlage II EVB-IT Cloud). Cloud-Anbieter können sich also keinesfalls darauf verlassen, dass Ausschreibungen für Cloud-Angebote in Zukunft immer exakt auf dem neuen Vertragswerk fußen werden.**

Dennoch ist wohl damit zu rechnen, dass sich beide Seiten – also Cloud-Anbieter sowie öffentliche Auftraggeber – künftig an den Anforderungen und

45. Abrufbar unter https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-und-bvb/evb-it/evb-it-node.html#, zuletzt abgerufen am 11.01.2023.

Vertragsinhalten orientieren werden. Erhebliche Abweichungen bleiben aber möglich und gerade in Verhandlungsverfahren kann es bei der Vergabe öffentlicher Aufträge zu weiteren Modifikationen kommen.

Wichtige Inhalte der EVB-IT Cloud:

- Enthalten sind für die typischen Cloud-Leistungen Anforderungen an deren Art und Umfang (EVB-IT Cloud AGB) sowie die transparente Aufgabenteilung.
- Cloud-Anbieter werden zum monatlichen KPI-Reporting, zur Meldung von Störungen und Überschreitungen von Reaktions- und Wiederherstellungszeiten sowie zum transparenten Umgang mit Störungsfällen verpflichtet (Ziff. 9-11 EVB-IT Cloud AGB).
- Pflicht zur Unterstützung bei der Datenmigration (Ziff. 13 EVB-IT Cloud AGB).
- Die EVB-IT Cloud enthalten neben dem Kriterienkatalog weitere Anforderungen an **IT-Sicherheit und Datenschutz:** Die Daten dürfen ausdrücklich nur **im Einklang mit der DSGVO** verarbeitet werden. Weiterhin sind die Benennung eines IT-Sicherheitsbeauftragten und ein Informationssicherheitsmanagementsystem nach ISO 27001 vorgeschrieben (Ziff. 6 EVB-IT Cloud AGB). Die Datenverarbeitung darf grundsätzlich nur in der EU, dem EWR und der Schweiz stattfinden (Ziff. 4 EVB-IT Cloud AGB). **Es gibt jedoch eine Ausnahme für Metadaten und auch die Steuerung der Cloud aus Drittländern bleibt möglich.** Zudem schließt jedenfalls der Bitkom die bekannten Hyperscaler auch als Subunternehmer nicht aus.

Für Auftraggeber haben die EVB-IT Cloud den Vorteil, dass ihnen nun ein einseitiges Kündigungsrecht gewährt wird, wenn der Cloud-Anbieter seinen Pflichten bezüglich Datenschutzes und IT-Sicherheit auch nach Setzung einer angemessenen Frist nicht nachkommt (Ziff. 6.5 EVB-IT Cloud AGB).

- Auf Grundlage der Prüfberichte nach BSI C5 kann der Auftraggeber **Prüfungen** durchführen. Vor-Ort-Prüfungen sind jedoch nur bei Zweifeln an der Umsetzung möglich (Ziff. 6.4 EVB-IT Cloud AGB).
- **„Technische no-spy Klausel“:** Die Software darf gemäß Ziff. 1.4 EVB-IT Cloud AGB keine Funktionen haben, die die Integrität, Vertraulichkeit und Verfügbarkeit von Software, Hardware oder Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen. **„Hintertüren“, die den Zugriff durch den Auftragnehmer oder Dritte ermöglichen, sind also ausdrücklich vertraglich ausgeschlossen.**
- **AGB des Auftragnehmers** können **nachrangig** (Ziff. 1.2.4 EVB-IT Cloud, Ziff. 1.5 EVB-IT Cloud AGB / Anlange I) oder **punktuell vorrangig** einbezogen werden (Ziff. 1.5 und Anlage II EVB-IT Cloud).

Auch wenn diese Vorgaben eine einheitliche Entscheidungspraxis der Behörden zum Ziel haben, müssen öffentliche Auftraggeber bei der Ausschreibung stets selbst prüfen, ob die EVB-IT Cloud für den Auftrag geeignet sind oder es gegebenenfalls umfassender Modifikationen, Streichungen oder Ergänzungen

bedarf. Schließlich macht auch die Verwendung der EVB-IT Cloud die in der Regel notwendige Erstellung weiterer Datenschutz-Dokumente, wie etwa den Vertrag zur Auftragsverarbeitung, nicht entbehrlich.

4.3 Die Vergabeentscheidung

Nach § 127 Abs. 1 S. 1 GWB müssen öffentliche Auftraggeber stets dem im jeweiligen Vergabeverfahren wirtschaftlichsten wertungsfähigen Angebot den Zuschlag erteilen. Dies gilt nach § 43 Abs. 1 UVgO auch für unterschwellige Vergabeverfahren. Wertungsfähig ist ein Angebot nur, wenn es die von der ausschreibenden Stelle in den Vergabeunterlagen im Sinne von § 29 VgV vorgegebenen Mindestanforderungen einhält. Dazu gehören die Mindestvorgaben aus der Leistungsbeschreibung (vgl. § 29 Abs. 1 S. 2 Nr. 3 VgV), aus „A"- oder „Ausschlusskriterien" u.ä. (vgl. § 29 Abs. 1 S. 2 Nr. 1 und 2 VgV), aber auch sämtliche Vertragsunterlagen und -bedingungen (vgl. § 29 Abs. 1 S. 2 Nr. 3 VgV). Zu den Vertragsbedingungen gehören auch AGB wie die EVB-IT Cloud, soweit der jeweilige Auftraggeber sie den Vergabeunterlagen beigefügt hat.

Angebote von Bietern, welche von den gem. § 41 Abs. 1 VgV bereitgestellten Vergabeunterlagen abweichen, werden durch den öffentlichen Auftraggeber ausgeschlossen (vgl. § 57 Abs. 1 Nr. 2, 4 VgV). Sofern die Vergabeunterlagen keine entsprechende Öffnungsklausel enthalten, führen auch bieterseitige, den Vergabeunterlagen widersprechende AGB zum Ausschluss des betreffenden Angebots.[46] In den Vergabeverfahrensarten, die Verhandlungen verbieten (vgl. § 119 Abs. 1-4 GWB i. V. m. §§ 15 Abs. 5 S. 2, 16 Abs. 9 VgV; §§ 9 Abs. 2 S. 2, 10 Abs. 3, 11 Abs. 3 UVgO), ist dieser Ausschluss regelmäßig zwingend. Aus diesem Grund enthalten alle EVB-IT-Vertragsformulare Öffnungsklauseln für auftragnehmerseitige AGB, wie etwa Ziff. 1.2.4 im EVB-IT-Cloud-Vertrag. Allerdings schreiben öffentliche Auftraggeber IT-Leistungen häufig in Form von Verhandlungsverfahren aus. Diese Verfahrensart (vgl. § 119 Abs. 5 GWB i. V. m. § 17 VgV; ebenso: § 12 UVgO) erlaubt es, über Vertragsklauseln zu verhandeln.

In welchem Umfang sich auftraggeberseitige AGB (also etwa die Klauseln der EVB-IT Cloud) oder auftragnehmerseitige AGB durchsetzen, ist dann Frage der konkreten Verhandlungssituation. So wurden etwa zwischen Microsoft und dem Bund spezielle, übergreifende Konditionen für die Beschaffung von Bund, Ländern und Kommunen vereinbart.[47] In wettbewerblichen Vergabeverfahren sind solche Verhandlungssituationen allerdings eher die Ausnahme, denn der öffentliche Auftraggeber kann sich darauf zurückziehen, wegen § 97 Abs. 2 GWB allen Bietern dieselben Vertragsbedingungen stellen zu müssen.

- Unter den wertungsfähigen Angeboten entscheidet dann die Wirtschaftlichkeit. Diese ergibt sich gem. § 127 Abs. 1 S. 2 GWB daraus, ob und inwieweit die jeweiligen Angebote die in den Vergabeunterlagen vorgegebenen preis-/kosten- und/oder leistungsbezogenen Zuschlagskriterien erfüllen. Hier steht den öffentlichen Auftraggebern häufig ein Beurtei-

46. Vgl. etwa Ulf-Dieter Pape, in: Pünder/Schellenberg, Vergaberecht, 3. Auflage 2019, § 57 VgV Rn. 32).

47. Vgl. https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/it-beschaffung/microsoft-konditionenvertraege/microsoft-konditionenvertraege-node.html; zuletzt abgerufen am 06.01.2023. Vgl. etwa Ulf-Dieter Pape, in: Pünder/Schellenberg, Vergaberecht, 3. Auflage 2019, § 57 VgV Rn. 32).

lungsspielraum zu. Dies gilt insbesondere bei Zuschlagsentscheidungen, die auf Konzeptwertungen oder der Bewertung von Teststellungen oder Präsentationen beruhen.

5 Fazit und Checkliste

Wenn sich öffentliche Einrichtungen entscheiden, Software und Daten nicht lokal, sondern in der Cloud zu hosten, gibt es **vergaberechtlich** viel zu beachten. Der oftmals hohe Schutzbedarf der Daten macht konkrete vertragliche und technische Schutzmaßnahmen erforderlich und im Rahmen von Ausschreibungen ist zu beachten, dass im Regelfall der Einsatz von Servern mit Standort innerhalb der Europäischen Union zwingend ist. Teilweise liegen die regulatorischen Vorgaben zur öffentlichen Ausschreibung deutlich höher, insbesondere im Bereich der Sektorentätigkeiten, was dazu führen kann, dass Cloud-Anbieter mit Hauptsitz in Drittstaaten unberücksichtigt bleiben müssen. Jedem Ausschreibungsverfahren mit Cloud-Bezug muss daher im Hinblick auf die Einhaltung obige gesetzlicher Vorgaben eine rechtliche Prüfung vorausgehen unter besonderer Berücksichtigung eines möglichen Datentransfers in Drittstaaten. Erleichterungen gibt es im anschließenden Vergabeverfahren dadurch, dass öffentliche Auftraggeber sich grundsätzlich auf die Zusagen ihrer Bieter verlassen dürfen und ohne entsprechende Anhaltspunkte nicht verpflichtet sind, die Angaben zu überprüfen.

Im Hinblick auf den **Datenschutz** sind pauschale Vorgaben nur bedingt möglich. Das passende Cloud-Modell, die Anforderungen an Datenschutz- und Datensicherheit sowie die vertragliche Ausgestaltung hängen eng mit dem Schutzbedarf der betroffenen Daten zusammen. Bevor im Rahmen der Ausschreibung Sicherheitskriterien festgelegt werden, muss deshalb immer erst einmal definiert werden, welche Daten von dem Auftrag betroffen sein werden und ob die Verarbeitung mit einem besonderen Risiko für die betroffenen Personen verbunden ist. Letzteres ist insbesondere der Fall, wenn es sich um besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO handelt, also beispielsweise um Daten, aus denen politische Meinungen oder religiöse Überzeugungen hervorgehen, Gesundheitsdaten, genetische oder biometrische Daten. Danach muss bestimmt werden, welchem Risiko die betroffenen Daten ausgesetzt werden. Je nachdem, welche und wie viele Daten betroffen sind, steigen auch die Anforderungen an die erforderlichen Datenschutzmaßnahmen.

Checkliste für die Datenschutzmaßnahmen

Es sollte in der Regel auf folgende Punkte geachtet werden:

- Cloud-Anbieter haben ihre Server ausschließlich in einem Land der EU oder des EWR und treffen effektive Maßnahmen, um den Zugriff durch Behörden in Drittländern zu verhindern.
- Deutsches und europäisches Datenschutzrecht wird eingehalten und der Cloud-Anbieter sichert zu, dass ein unzulässiger Datenzugriff ausgeschlossen ist.
- Bei Zweifeln an der Einhaltung des Datenschutzrechts bleibt eine Prüfung des konkreten Anbieters erforderlich.
- **Cloud-Anbieter müssen jedenfalls die BSI C5-Mindestanforderungen umsetzen und in geeigneter Weise nachweisen. Hierauf sollten sich auch Cloud-Anbieter vorbereiten, die für die Zukunft planen, an öffentlichen Ausschreibungen teilzunehmen.**
- Darüber hinaus ist das konkrete Schutz-/Sicherheitsniveau zu bestimmen.
- Die EVB-IT Cloud sowie der Kriterienkatalog sollten vor der Verwendung ebenfalls dahingehend geprüft werden, ob diese in der Lage sind, ein ausreichendes Schutzniveau sicherzustellen.

Aus **Bietersicht** ist gerade der Leistungszuschnitt entscheidender Hebel für die in einem Vergabeverfahren zu erwartende Konkurrenzsituation.

Öffentliche Auftraggeber sondieren im Vorfeld von Vergabeverfahren den Markt (sog. „Markterkundung“, vgl. § 28 VgV). Teilweise finden Interessenbekundungsverfahren statt (vgl. § 7 Abs. 2 S. 3 BHO) oder werden Vorinformationen veröffentlicht (vgl. § 38 Abs. 1 VgV). Die öffentliche Hand ist gerade bei der Vorbereitung von Vergabeverfahren im IT-Bereich auf das Knowhow der Marktteilnehmer angewiesen. Diese sind daher gut beraten, schon im Vorfeld von Vergabeverfahren auf die Leistungsbestimmung der öffentlichen Hand einzuwirken. Es ist dann Sache der öffentlichen Auftraggeber mögliche Informationsunterschiede über die Vergabeunterlagen auszugleichen (vgl. § 7 Abs. 1, 2 VgV).

Checkliste zur Vorbereitung von Vergabeverfahren

Mit Blick auf die EVB-IT Cloud empfiehlt sich Folgendes:

- Marktteilnehmer sollten sich grundsätzlich mit diesen auseinandersetzen und zu den einzelnen Klauseln positionieren, ggf. Alternativen entwickeln und vorbereiten.
- In jedem Vergabeverfahren sollten Marketteilnehmer prüfen, ob ein Verhandlungsverfahren vorliegt und ob die ausschreibende Stelle die Öffnungsklausel für bieterseitige AGB in Ziff. 1.2.4. EVB-IT Cloud aktiviert hat. Andernfalls droht der Ausschluss ihres Angebots, wenn sie eigene Klauseln oder AGB zugrunde legen.
- Im Rahmen von Verhandlungen sollte versucht werden, eigene Klauseln/AGB durchzusetzen.

IONOS

Autor:

Dr. Hans Markus Wulf
Partner bei HEUKING KÜHN LÜER WOJTEK
Fachanwalt für IT-Recht und Datenschutzauditor (TÜV)

Über HEUKING KÜHN LÜER WOJTEK

Mit über 400 Rechtsanwälten, Steuerberatern und Notaren an acht Standorten in Deutschland und einem Büro in Zürich ist Heuking Kühn Lüer Wojtek eine der großen wirtschaftsberatenden deutschen Sozietäten. Vor über 50 Jahren gegründet, gehört sie laut Branchenverlag JUVE zu den TOP 20 der umsatzstärksten Kanzleien in Deutschland.

Über IONOS

IONOS ist der führende europäische Digitalisierungs-Partner für kleine und mittlere Unternehmen (KMU). IONOS hat mehr als sechs Millionen Kundinnen und Kunden und ist mit einer weltweit verfügbaren Plattform in 18 Märkten in Europa und Nordamerika aktiv. Mit seinen Web Presence & Productivity-Angeboten agiert das Unternehmen als “One-Stop-Shop“ für alle Digitalisierungs-Bedürfnisse - von Domains und Webhosting über klassische Website-Builder und Do-It-Yourself-Lösungen, von E-Commerce bis zu Online-Marketing-Tools. Darüber hinaus bietet IONOS Cloud-Lösungen für Firmen, die im Zuge der Weiterentwicklung ihres Geschäfts in die Cloud wechseln möchten.

Mehr Informationen verfügbar unter https://cloud.ionos.de/

Impressum

IONOS SE
Berlin Office
Revaler Straße 30
10245 Berlin, Germany

IONOS Cloud Kontakt

Telefon +49 30 57700 840
Telefax +49 30 57700 8598
E-Mail produkt@cloud.ionos.de
Website https://cloud.ionos.de

Vorstand

Hüseyin Dogan, Dr. Martin Endreß, Claudia Frese, Dr. Markus Noga,
Arthur Mai, Britta Schmidt, Achim Weiß

Aufsichtsratsvorsitzender

Sven Fritz

Handelsregister

IONOS SE: Amtsgericht Montabaur / HRB 24498

Umsatzsteuer-IdentNummer

IONOS SE: DE815563912

Copyright

Die Inhalte des White Papers wurden mit größter Sorgfalt erstellt. Für Richtigkeit, Vollständigkeit und Aktualität keine Gewähr.

Alle Informationen in diesem White Paper dienen allein der allgemeinen Information. Sie stellen keinesfalls eine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen.

© Dr. Hans Markus Wulf, Kanzlei: Heuking Kühn Lüer Wojtek, Georg-Glock-Straße 4, 40474 Düsseldorf, www.heuking.de

Alle Rechte vorbehalten – einschließlich der, welche die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung der Inhalte dieses Dokumentes oder Teile davon außerhalb der Grenzen des Urheberrechtes betreffen. Handlungen in diesem Sinne bedürfen der schriftlichen Zustimmung durch IONOS. IONOS behält sich das Recht vor, Aktualisierungen und Änderungen der Inhalte vorzunehmen.