Stellungnahme

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023

Kriterien für Souveräne Clouds

Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023

Politische Strategien zur Digitalisierung der Europäischen Union sehen „Digitale Souveränität“ als erstrebenswertes politisches Entwicklungsziel an und souveräne Clouds als ein wichtiges Mittel dafür. Dazu hat der deutsche IT-Planungsrat die AG Cloud Computing und Digitale Souveränität gegründet. Der Begriff „Digitale Souveränität“ wird dabei in der öffentlichen Debatte mit unterschiedlichen Bedeutungen verwendet. Je nach Sichtweise – etwa aus dem Blickwinkel der Ökonomie, der Forschung, der Innovationskraft, der inneren und äußeren Sicherheit sowie der IT-Sicherheit – werden unterschiedliche Schwerpunkte der technologischen Unabhängigkeit betont. Nach der relativ neutralen Definition des Kompetenzzentrums Öffentliche IT ist „Digitale Souveränität“ in einem umfassenden Sinne „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.“[1] Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bringt hiermit ihre Expertise und ihre Erfahrungen in die politische Diskussion ein.

Dies ist insbesondere deshalb wichtig, weil es am Markt bereits einige Angebote gibt, die sich als „Souveräne Clouds“ bezeichnen. Ein einheitliches Verständnis dieses Begriffs gibt es aber bisher nicht. Weder „Digitale Souveränität“ noch „Souveräne Cloud“ sind Rechtsbegriffe. Sie werden in der DS-GVO nicht genannt. Sie sprechen jedoch ein Problem an, mit dem datenschutzrechtliche Aufsichtsbehörden täglich

[1] „Digitale Souveränität“, Kompetenzzentrum Öffentliche IT (ÖFIT), Nov. 2017 [1].

konfrontiert sind: Beispielsweise bereiten Clouds, die aus Ländern ohne gleichwertiges Datenschutzniveau oder von Unternehmen, die der Rechtsordnung solcher Länder unterworfen sind, angeboten werden, in der Umsetzung von Datenschutz besondere Schwierigkeiten. Verantwortliche, die solche Clouds nutzen, können vielfach ihren datenschutzrechtlichen Pflichten nicht nachkommen. Sie sind insbesondere nicht in der Lage nachzuweisen, dass sie unter Nutzung dieser Clouds die Anforderungen der DS-GVO erfüllen. Eine „Souveräne Cloud“ verdient diesen Namen aber nur, wenn sie es dem Verantwortlichen ermöglicht, seinen datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft nachzukommen.

Dieses Positionspapier zielt nicht auf eine abschließende datenschutzrechtliche Bewertung eines Cloud-Angebots und einer Cloud-Nutzung im Einzelfall. Es enthält vielmehr die Kriterien, die nach Meinung der DSK erfüllt sein sollten oder müssen, um von einer „Souveränen Cloud“ sprechen zu können. Im Mittelpunkt des Datenschutzes stehen dabei die Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung ihrer personenbezogenen Daten.

Die hier dargelegten Kriterien zielen dabei auf die digitale Souveränität aller Handelnden, losgelöst von ihrer datenschutzrechtlichen Stellung,[2] ab. Sie richten sich in erster Linie an Cloud-Anbietende (Anbietende)[3] und Cloud-Anwendende (Anwendende),[4] um die Einhaltung der Rechte und Freiheiten der betroffenen Personen zu unterstützen. Gleichwohl wird die konkrete Umsetzung in der Praxis an vielen Stellen den Anbietenden obliegen, da diese die technischen Grundlagen für die jeweilige Verarbeitung bereitstellen und damit deren Ausgestaltung in wesentlichen Teilen beeinflussen. Die digitale Souveränität eines Cloud-Angebots kann dabei nur dann gewährleistet werden, wenn alle durch die Anbietenden in der Kette des Cloud-Dienstes eingebundenen Auftragnehmenden bzw. die eingebundenen IT-Dienstleistungen und -produkte entsprechende Kriterien ebenfalls erfüllen.

Die Notwendigkeit der Einhaltung der Bestimmungen des geltenden Datenschutzrechts ist evident: Eine souveräne Cloud muss in der Lage sein, alle

[2] Betroffene Person, Verantwortlicher, Auftragsverarbeiter, Empfänger, Dritter, vgl. Art. 4 Ziffer 1, 7, 8, 9 und 10 und Kapitel 4 DS-GVO; *Europäischer Datenschutzausschuss (EDSA),* Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO des Europäischen Datenschutzausschusses, Version 2.0, 2021, [2].

[3] Anbietende sind natürliche oder juristische Personen, die Anwendenden IT-Dienstleistungen für Cloud-Services bereitstellen und dabei u. U. weitere Unter-Anbietende von Cloud-Services einbeziehen.

[4] Anwendende sind natürliche oder juristische Personen, die personenbezogene Daten Betroffener verarbeiten und hierfür von anderen Stellen angebotene IT-Dienstleistungen für Cloud-Services in Anspruch nehmen.

Bestimmungen des Datenschutzrechts – insbesondere die Vorgaben der Datenschutz-Grundverordnung (DS-GVO), aber auch die einschlägigen bundes- und landesrechtlichen Regelungen – einzuhalten. Wichtig ist zunächst, dass sich Anbietende und Anwendende ihrer datenschutzrechtlichen Rollen sowie der hiermit einhergehenden Rechte und Pflichten bewusst sind und gegebenenfalls notwendige vertragliche Vereinbarungen schließen.[5]

Für Verantwortliche im Sinne des Art. 4 Ziffer 7 DS-GVO sind die in Art. 5 DS-GVO normierten Datenschutzgrundsätze maßgebend:

- Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a DS-GVO),
- Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b DS-GVO),
- Datenminimierungsgrundsatz (Art. 5 Abs. 1 lit. c DS-GVO),
- Grundsatz der Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO),
- Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO),
- Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO),
- Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO).

Die Verarbeitungsgrundsätze des Art. 5 DS-GVO werden durch die weiteren Vorschriften der DS-GVO näher beschrieben.[6] Auf einzelne Aspekte dieser Grundsätze, denen im Zusammenhang mit einem souveränen Cloud-Angebot besondere Bedeutung zukommt, wird in der folgenden Betrachtung von Kriterien für souveräne Cloud-Angebote noch einmal konkretisierend eingegangen.[7]

Digitale Souveränität umfasst dabei mehr als die bloße Einhaltung der Datenschutzanforderungen. Digitale Souveränität ist nur erfüllt, wenn sie dazu beiträgt, das dargestellte Umsetzungsproblem grundlegend und nachhaltig zu lösen. Dementsprechend erfordert der Schritt von einer datenschutzkonformen Cloud hin zu einer souveränen Cloud auch die Erfüllung begleitender Kriterien, die die Einhaltung der datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft sicherstellen. Die Rechtsverbindlichkeit der Erfüllung dieser Kriterien muss dabei vielfach zwischen den beteiligten Handelnden erst hergestellt werden. Eine solche

[5] Siehe Fußnote 2.
[6] Vgl. etwa zum Grundsatz der Integrität und Vertraulichkeit die Vorgaben der Art. 25 und 32 DS-GVO oder die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO.
[7] Siehe z. B. zum Transparenzgrundsatz auch unter Nachvollziehbarkeit durch Transparenz (Abschnitt 1), zur Thematik des Drittstaatentransfers unter Datenhoheit und Kontrollierbarkeit (Abschnitt 2).

Bindungswirkung kann etwa durch eine vertragliche Regelung, eine Zertifizierung, einen Code of Conduct oder eine Kombination hieraus erreicht werden.

Die wesentlichen Kriterien, die in den folgenden Abschnitten betrachtet werden, lassen sich folgenden Themen zuordnen:

- Nachvollziehbarkeit durch Transparenz,
- Datenhoheit und Kontrollierbarkeit,
- Offenheit,
- Vorhersehbarkeit und Verlässlichkeit,
- Regelmäßige Prüfung der aufgestellten Kriterien.

Alle genannten Kriterien werden nachfolgend in die Kategorien **MUSS** und **SOLL** unterteilt. Die erste Kategorie beschreibt dabei die **Mindestkriterien**, die nach Ansicht der DSK zu erfüllen sind, damit ein Cloud-Angebot als souverän gelten kann. SOLL-Kriterien stellen hingegen zusätzliche **Empfehlungen** für den Betrieb einer souveränen Cloud dar.

1 Nachvollziehbarkeit durch Transparenz

Art. 5 Abs. 1 lit. a DS-GVO schreibt fest, dass jede Verarbeitung personenbezogener Daten in einer für die Betroffenen nachvollziehbaren Weise zu erfolgen hat (Transparenzgrundsatz). Dieser Grundsatz wird insbesondere durch die Informations- und Auskunftspflichten gemäß Artt. 12 ff. DS-GVO konkretisiert.

Verantwortliche, die Cloud-Dienste einsetzen, müssen nach Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO zudem sicherstellen, dass die mit diesen Diensten erfolgende Verarbeitung personenbezogener Daten gemäß den Vorgaben der DS-GVO erfolgt und hierfür den Nachweis erbringen können (Rechenschafts- und Compliancepflichten). Anwendende müssen ihrerseits über hinreichende Informationen verfügen, um ihren Rechenschafts- und Compliancepflichten nachkommen und ihre Pflichten gegenüber den Betroffenen umsetzen zu können. Damit eine datenschutzgerechte und selbstbestimmte Nutzung von Cloud-Diensten durch Anwendende möglich ist, können diese daher nur auf Anbietende zurückgreifen, die die erforderlichen Informationen bereitstellen.

Die DS-GVO definiert bereits ein breites Spektrum an Transparenzanforderungen, die gegenüber den Betroffenen zu erfüllen sind. Diese umfassen zum Beispiel die

Information über die Verarbeitungstätigkeiten.[8] Die Erfüllung dieser Anforderungen wird an dieser Stelle vorausgesetzt. Um sie verlässlich, effektiv, nachvollziehbar und dauerhaft sicherzustellen, setzt ein souveränes Cloud-Angebot nach Ansicht der DSK die Umsetzung der folgenden Kriterien voraus:

1.1 — Dokumentation vor Vertragsschluss (MUSS): Anbietende müssen die eingesetzten externen Komponenten und Dienstleistungen sowie die jeweiligen hierzu bestehenden (vertraglichen) Regelungen dokumentieren. Die Dokumentation muss den Nachweis ermöglichen, dass die vorgenommenen Verarbeitungen im Rahmen geeigneter (vertraglicher) Regelungen erfolgen und den gesetzlichen Anforderungen genügen. Dies kann insbesondere auch durch die Vorlage von Vereinbarungen erfolgen. Die Anbietenden stellen ihren Anwendenden diese Dokumentation bzw. den Teil der Dokumentation, der sich auf die in Anspruch genommenen Dienste bezieht, bereits vor Vertragsabschluss zur Verfügung, um eine informierte Entscheidung für bzw. gegen ein Angebot treffen zu können. Dabei müssen Anbietende auch die Vorlage der erforderlichen Dokumentation vor den Datenschutz-Aufsichtsbehörden zulassen.

1.2 — Schnittstellendokumentation (MUSS): Um eine Interoperabilität mit anderen Cloud-Systemen zu gewährleisten, müssen Anbietende eine Dokumentation der verfügbaren Schnittstellen anfertigen und ihren Anwendenden zur Verfügung stellen. Ferner müssen sie ihre Anwendenden über Möglichkeiten des Exports der in der Cloud verarbeiteten Daten informieren. Dies umfasst insbesondere die zur Verfügung stehenden Schnittstellen und Datenformate, um die Daten zu einem anderen Anbietenden übertragen zu können.[9]

1.3 — Transparenz hinsichtlich der Zukunftsfähigkeit (MUSS): Ein wichtiger Grundsatz von Souveränität ist die Zukunftsfähigkeit und die dauerhafte Erfüllung der Souveränitätsbedingungen. Anbietende souveräner Clouds müssen daher ihren Anwendenden darlegen, wie sie einen dauerhaften und unabhängigen Betrieb ihres Angebots voraussichtlich gewährleisten. Dies schließt etwaige Abhängigkeiten von Herstellenden, Dienstleistenden und weiteren Stellen mit ein.[10] Über absehbare oder eingetretene Veränderungen der mitgeteilten Tatsachen müssen Anbietende die

[8] *DSK,* Kurzpapier Nr. 6 – Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO, 2018 [3]; *DSK,* Kurzpapier Nr. 10 – Informationspflichten bei Dritt- und Direkterhebung, 2018 [4]; *Artikel 29-Datenschutzgruppe,* Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, 2018 [5]; *EDSA,* Guidelines 01/2022 on Data Subject Rights – Right of Access, Version 2.0, 2023 [6].

[9] Siehe auch Austauschbarkeit (3.1).

[10] Siehe auch Datenhoheit und Kontrollierbarkeit (Abschnitt1) sowie Vorhersehbarkeit und Verlässlichkeit (Abschnitt 4).

Anwendenden frühzeitig informieren. Optional können auch Nachweise über die wirtschaftliche Leistungsfähigkeit und daraus abgeleitete Prognosen über die Unabhängigkeit und zukünftige Geschäftsfähigkeit der Anbietenden dargelegt werden.

1.4 — Transparenz durch Open Source (SOLL): Durch den Einsatz von Open-Source-Software können Anbietende zusätzliche Transparenz für Anwendende schaffen. So können Anwendende selbst die eingesetzte Software prüfen oder von externer Stelle prüfen lassen. Um Anwendenden eine möglichst umfassende und tiefgehende Prüfung der Einhaltung der datenschutzrechtlichen Vorgaben zu ermöglichen, sollten Anbietende auf Open-Source-Software setzen und Code-Reviews ermöglichen.

1.5 — Transparenz durch offene Standards (SOLL): Die Verwendung von offenen Standards gewährleistet für Anwendende eine Vergleichbarkeit verschiedener Angebote und fördert die Interoperabilität zwischen verschiedenen Cloud-Diensten und weiteren von den Anwendenden eingesetzten Systemen und Diensten. Analog zur Verwendung von Open-Source-Software sollten Anbietende offene Standards für die Entwicklung ihrer Cloud-Dienste verwenden und dies transparent machen. Dies unterstützt Anwendende bei der Auswahl eines geeigneten Cloud-Dienstes.

2 Datenhoheit und Kontrollierbarkeit

Grundlegende Bedingung einer souveränen Cloud ist ihre Kontrollierbarkeit, d. h. Beherrschbarkeit und Nachprüfbarkeit, auch damit Betroffene ihre Datenhoheit wahren können. Mit Blick auf ein souveränes Cloud-Angebot ergeben sich daher folgende Kriterien:

2.1 — Verarbeitung durch Anbietende nur auf Weisung (MUSS): Die Verarbeitung von personenbezogenen Daten durch die Anbietenden darf ausschließlich im Rahmen von konkreten Weisungen des Anwendenden und zur Gewährleistung der Sicherheit der Verarbeitung erfolgen, z. B. im Rahmen einer Firewall.

2.2 — Trennung nach Verarbeitungen (MUSS): Im Rahmen der Kontrolle über die Verarbeitungstätigkeiten muss eine Trennung[11] erfolgen. Wenn eine physische Trennung nicht umsetzbar ist, müssen andere geeignete technische und organisatorische Maßnahmen implementiert und nachvollziehbar dokumentiert

[11] Siehe Standarddatenschutzmodell (SDM), Baustein 50 „Trennen“, [7]

werden. Für einen eventuell notwendigen Austausch zwischen Mandanten müssen sichere Kommunikationskanäle definiert werden.

2.3 — Einbindung von Unterauftragsverarbeitern (SOLL): Anwendende sollen auf die Inanspruchnahme einzelner Unterauftragsverarbeiter möglichst weitgehend gezielt einwirken und einzelne Unterauftragsverarbeiter abwählen können. Voraussetzung hierfür ist die Modularität (3.3) des Cloud-Angebotes.

2.4 — Kein Drittlandszugriffsrisiko auf Anbietende (MUSS): Anbietende könnten einem Risiko extraterritorialer Einwirkungen, Zugriffe oder Offenlegungsverpflichtungen durch bzw. gegenüber Drittland-Behörden unterliegen – etwa weil sie ihren Sitz in einem Drittland haben, Tochterunternehmen eines Konzerns sind, für den Herausgabepflichten bestehen können, oder weil sie entsprechende Auftragsverarbeiter einsetzen. Sie müssen dann zusätzliche Voraussetzungen für einen souveränen Betrieb erfüllen. So sind Maßnahmen durch Anbietende zu ergreifen, die ausschließlich nach EU-, EWR- bzw. nationalem Recht zulässige Zugriffe auf die personenbezogenen Daten ermöglichen. Rein vertragliche Maßnahmen genügen – auch wenn die Datenverarbeitung regelhaft ausschließlich in dem Europäischen Wirtschaftsraum (EWR) erfolgt – in der Regel nicht.

2.5 — Wirksame Rechtsdurchsetzbarkeit (MUSS): Souveränität setzt neben der Einhaltung datenschutzrechtlicher Vorgaben eine dauerhafte faktische Beherrschbarkeit der Datenverarbeitung durch den Verantwortlichen voraus. Eine Bedingung dafür sind vertraglich klar festgelegte Rechte, Pflichten und Sanktionen. Gerade für diese weitergehenden Aspekte mit Einfluss auf die Verarbeitung (z. B. Kündigungsfristen, Lebensdauer von Angeboten, Implementierung von offenen Schnittstellen und Zugriff auf deren Dokumentation o. Ä., siehe z. B. Abschnitt 3 und 4), die erst durch Verträge oder vergleichbare Instrumente zwischen den Beteiligten festgeschrieben werden, muss daher der gerichtlichen Durchsetzbarkeit besonderes Augenmerk geschenkt werden.

Anwendende müssen sich über eine transparente Anbieterstruktur (u. a. im Hinblick auf Sitzland, Konzernzugehörigkeit, Einsatz von weiteren Auftragsverarbeitern) davon überzeugen können, dass ihre Anbietenden ausschließlich dem Regelungsregime des Rechts der Europäischen Union bzw. des Europäischen Wirtschaftsraums unterliegen (siehe 2.6).

2.6 — Anbietersitz und Verarbeitung im Europäischen Wirtschaftsraum (MUSS): Während die DS-GVO einen Rechtsrahmen zur Übermittlung von personenbezogenen

Daten an Drittländer oder an internationale Organisationen[12] schafft, ist dieser für die weiteren hier dargelegten Aspekte der Souveränität eines Cloud-Angebots nicht ausreichend.[13] Eine effektive Kontrollierbarkeit von souveränen Cloud-Diensten durch Anwendende setzt daher voraus, dass die Verarbeitung aller Daten ausschließlich im EWR und durch in dem EWR ansässige Anbietende erfolgt, weil dort die Einhaltung und notfalls gerichtliche Durchsetzbarkeit des Datenschutzniveaus langfristig sichergestellt ist. Das bedeutet, dass sich sowohl der Unternehmenssitz des Anbietenden als auch der Standort der Rechenzentren sowie etwaiger Unterauftragnehmer mit Zugriff auf personenbezogene Daten im EWR befinden.

3 Offenheit

Offenheit im Sinne digitaler Souveränität bedeutet, dass den Anwendenden ein breites Spektrum an Wahlmöglichkeiten zwischen unterschiedlichen Anbietenden für die Ausgestaltung ihrer Verarbeitungstätigkeiten zur Verfügung steht. So können beispielsweise mehrere Cloud-Angebote in Kombination eingesetzt werden, um eine oder mehrere Verarbeitungstätigkeiten umzusetzen. Weiterhin sollten die mit der Auswahl einer konkreten Ausgestaltung einhergehenden Abhängigkeiten, wie z.B. Lock-In-Effekte, auf ein möglichst geringes Maß reduziert werden. Anwendende sollten in die Lage versetzt werden, getroffene Entscheidungen für den Einsatz eines Angebotes mit möglichst geringen Wechselbarrieren zu revidieren. Daraus lassen sich folgende Kriterien für ein souveränes Cloud-Angebot ableiten:

3.1 — Austauschbarkeit (MUSS): Souveräne Cloud-Angebote müssen ihren Anwendenden einen einfachen Ersatz ermöglichen. Hierzu müssen Anbietende geeignete Möglichkeiten zum Export aller betrieblich relevanten Daten bereitstellen. Je nach Cloud-Angebot sollten auch weitere Objekte einfach in eine neue Umgebung überführbar sein, in einem Platform-as-a-Service-Betriebsmodell, also z. B. virtuelle Rechner, Konfigurationen virtueller Umgebungen oder Eigenentwicklungen.

3.2 — Kombinierbarkeit (SOLL): Anbietende souveräner Clouds sollen ein hohes Maß an Kombinierbarkeit ihrer Lösungen gewährleisten. Hierzu sollten sie auf der einen Seite Möglichkeiten zur Einbindung externer IT-Systeme und -Dienste bieten, etwa on-premise betriebene Authentifizierungssysteme oder andere Cloud-Angebote. Auf der anderen Seite sollten souveräne Cloud-Lösungen ihrerseits eine Integration in

[12] Siehe Kapitel V DS-GVO.

[13] Siehe hierzu auch das zuvor genannte Kriterium Wirksame Rechtsdurchsetzbarkeit (2.5), für dessen Erfüllung zumeist ein gemeinsamer Rechtsraum vorteilhaft ist.

andere Lösungen ermöglichen, etwa über die Bereitstellung geeigneter technischer Schnittstellen. In beiden Fällen müssen Anwendenden angemessene Dokumentationen und Hilfsmittel zur Nutzung bereitgestellter und genutzter Integrationsmöglichkeiten zur Verfügung gestellt werden.[14]

3.3 — Modularität (SOLL): Bei souveränen Cloud-Angeboten sollte die Möglichkeit bestehen, auch Teilkomponenten und -funktionen zu nutzen und Anwendenden so zusätzliche Optionen zur Umsetzung von Verarbeitungstätigkeiten zu bieten. Zur Nutzung von Teilkomponenten und -funktionen müssen angemessene Dokumentationen und Hilfsmittel bereitgestellt werden.[15]

3.4 — Unterstützung offener Standards (SOLL): Die Nutzung einer souveränen Cloud sollte für Anwendende auf Basis offener Standards möglich sein. Dies sollte nicht auf Datenformate beschränkt sein, sondern z.B. auch etwaige Schnittstellen einschließen. Die Unterstützung offener Standards sollte sich auf alle Bereiche einer souveränen Cloud erstrecken und sich nicht nur auf Kernfunktionalitäten beschränken. So sollte z.B. eine etwaige Protokollierung ebenfalls auf offenen Standards basieren.[16] Die Nutzung einer souveränen Cloud sollte auch ohne spezifische Erweiterungen von Standards möglich sein bzw. auf angebotsspezifische Erweiterungen der Standards verzichten. Mit wachsender Verbreitung eines Standards steigen auch dessen Vorteile für Anwendende. Daher sollten sich Anbietende aktiv in die Weiterentwicklung und Verbreitung offener Standards einbringen.

3.5 — Offenheit durch Open Source (SOLL): Über die Unterstützung offener Standards hinaus sollten souveräne Clouds vollständig auf Open-Source-Software basieren.[17] Anwendende werden so in die Lage versetzt, bei Bedarf Einblick in die Umsetzung der zugrundeliegenden Cloud-Plattform zu nehmen und hierdurch hilfreiche Informationen zu erhalten, etwa für den Fall eines Wechsels der Cloud-Plattform. Steht die eingesetzte Cloud-Plattform auch unter einer freien Lizenz, besteht zusätzlich die Möglichkeit, Teile der Umsetzung beim Wechsel zu übernehmen.

[14] Siehe hierzu auch die zuvor genannten Kriterien Nachvollziehbarkeit durch Transparenz (Abschnitt 1) und Datenhoheit und Kontrollierbarkeit (Abschnitt 2).
[15] Eine geeignete Modularität ergibt sich aus dem Dreiklang der Kriterien Dokumentation vor Vertragsschluss (1.1), Einbindung von Unterauftragsverarbeitern (2.3) und Modularität (3.3). Siehe zudem Einfluss- und Wahlmöglichkeiten auf die Angebotsausgestaltung (4.2).
[16] Siehe hierzu auch das zuvor genannte Kriterium Transparenz durch offene Standards (1.5).
[17] Siehe hierzu auch das zuvor genannte Kriterium Transparenz durch Open Source (1.4).

4 Vorhersehbarkeit und Verlässlichkeit

Souveränität ist kein Zustand, der, einmal erreicht, von selbst fortwährt. Die Souveränitätseigenschaft einer Cloud ist vielmehr ein kontinuierlicher Prozess, an dem Anbietende und Anwendende beteiligt sind. Dazu gehört, dass relevante Änderungen frühzeitig angekündigt werden. Der Verlässlichkeit eines Cloud-Angebots, das dem Gedanken der digitalen Souveränität Rechnung tragen will, kommt daher besondere Bedeutung zu. Für souveräne Cloud-Angebote folgt hieraus:

4.1 — Unterrichtung bei Souveränitätsgefährdung (MUSS): Anbietende müssen über Änderungen in ihrer Struktur, die die Souveränität gefährden,[18] rechtzeitig die Anwendenden unterrichten, um ihnen eine Migration zu einem souveränitätswahrenden Anbietenden zu ermöglichen.

4.2 — Einfluss- und Wahlmöglichkeiten auf die Angebotsausgestaltung (MUSS): Die Prinzipien von Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DS-GVO) und durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) müssen vom Verantwortlichen eingehalten werden. Durch Anbietende stillschweigend eingeführte Änderungen können bewirken, dass ein Cloud-Dienst personenbezogene Daten neuen oder geänderten Verarbeitungen unterwirft, bevor Anwendende überhaupt die Möglichkeit haben, dem entgegenzuwirken. Anbietende müssen daher Voreinstellungen stets datenschutzfreundlich wählen und Wechselwirkungen mit bestehenden Einstellungen transparent machen. Das Einbringen von Weiterentwicklungen muss möglichst modular erfolgen und durch die Anwendenden möglichst auch abwählbar sein. Dies gilt insbesondere in den Fällen, in denen sich aus den Änderungen neue oder geänderte datenschutzrechtliche Risiken ergeben könnten.

4.3 — Transparenter Produktlebenszyklus (MUSS): Anbietende müssen die Weiterentwicklung, Änderung und Abkündigung von Eigenschaften in transparent dargelegten und planbaren Zyklen vornehmen, damit sich Anwendende auf die Kontinuität des Betriebs verlassen können. Nur so wird ihnen die Möglichkeit gegeben, ihre Maßnahmen und Prozesse zur Datenschutzkonformität, insbesondere zur Gewährleistung der Betroffenenrechte, schritthaltend fortzuentwickeln.

4.4 — Prüffähige Qualität (MUSS): Nur qualitativ hochwertige Software kann Vertrauen darin bestärken, dass technische Maßnahmen greifen und organisatorische

[18] Siehe hierzu auch das zuvor genannte Kriterium Kein Drittlandszugriffsrisiko auf Anbietende (2.4).

Maßnahmen durchsetzbar sind. Damit Anwendende die Qualität des Angebotes überprüfen können, müssen Anbietende ihre Angebote daher von vornherein prüffähig gestalten, z. B. indem sie die in Offenheit durch Open Source (3.5) definierten Kriterien umsetzen.

4.5 — Featureparität zu nicht souveränen Cloud-Angeboten (SOLL): Anbietende, die ihre Public Clouds auch in einer souveränen Ausgestaltung anbieten, sollten sicherstellen, dass mittelfristig Featureparität zwischen beiden Varianten hergestellt wird, um keinen schleichenden Druck zum Verzicht auf das souveräne Angebot zu erzeugen. In Fällen, in denen dies nicht möglich ist oder in denen Featureparität bewusst nicht angestrebt wird, sollte transparent und neutral über die hieraus erwachsenden Unterschiede der Angebote informiert werden. Featureparität ist dabei nicht auf funktionale Aspekte beschränkt, sondern umfasst auch weitergehende Aspekte des Angebots wie z. B. Aktualisierung, Qualität und Service.

4.6 — Transparentes Finanzierungsmodell des Angebots (SOLL): Das Geschäfts- und Finanzierungsmodell des Anbietenden sollte so transparent sein, dass sich anhand dieses Modells sowohl die Seriosität und Rechtmäßigkeit des Modells überprüfen lässt, als auch die Frage, inwiefern die Nutzenden mit ihren personenbezogenen Daten bezahlen. Hierbei reicht es nicht, nur das gegenwärtige Finanzierungsmodell zu betrachten. Eine unilaterale Änderung der Geschäftsbedingungen, die die eigene Datennutzung durch Anbietende z. B. zu Monetarisierungszwecken ermöglicht, steht der Souveränität der Anwendenden und der Betroffenen entgegen.[19]

5 Regelmäßige Prüfung der aufgestellten Kriterien

Ob Anbietende alle oder Teile der oben dargestellten Kriterien für eine souveräne Cloud erfüllen, muss für Anwendende prüf- und nachvollziehbar sein. Für datenschutzrechtliche Anforderungen ergibt sich dies aus den Artikeln 5, 24 und 32 DS-GVO.

Die Überprüfung kann u. a. erfolgen durch

- von Anwendenden selbst durchgeführte Prüfungen,

[19] Siehe hierzu auch *EDSA,* Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, 2019, Rn. 54 [8] sowie *EDSA,* Erklärung 05/2021 zum Daten-Governance-Gesetz angesichts der gesetzgeberischen Entwicklungen, 2021, Seite 4 [9].

- externe Überprüfungen, die von einzelnen oder Gruppen von Anwendenden spezifisch beauftragt wurden, oder
- Prüfnachweise des Anbietenden, insbesondere Zertifikate, Siegel oder Auditierungen unabhängiger und vertrauenswürdiger Dritter.

5.1 — Überprüfung der eingesetzten Software (MUSS): Zur Verwirklichung der Souveränität gehört nicht nur die Möglichkeit Software zu prüfen, sondern auch die tatsächliche Prüfung. Eine souveräne Cloud ist nur so lange souverän, wie Softwarekomponenten auf Schwachstellen und Integrität geprüft werden. Zu den Softwarekomponenten gehören z. B. auch Software zum Betrieb der Plattform und Plugins der Cloud-Anwendung.

Diese Überprüfung muss regelmäßig durchgeführt werden, spätestens jedoch dann, wenn sich die mit den Verarbeitungsvorgängen verbundenen Risiken geändert haben.

5.2 — Unterstützung bei Überprüfungen (MUSS): Für eine wirkungsvolle Überprüfung bedarf es der grundsätzlichen Bereitschaft der Anbietenden, an einer solchen Überprüfung aktiv mitzuwirken (vgl. Art. 28 Abs. 3 lit. h DS-GVO). Dies beinhaltet die Bereitstellung von detaillierten, strukturierten und aussagekräftigen Dokumentationen sowie die Bereitschaft, auch detaillierte Nachfragen zu beantworten und bei Inaugenscheinnahmen und Vor-Ort-Überprüfungen aktiv mitzuwirken. Diese Unterstützung umfasst nicht nur die Überprüfung der Einhaltung der DS-GVO, sondern auch die weiteren Kriterien an eine souveräne Cloud, die in diesem Papier identifiziert wurden, muss sich in Bezug auf die Datenschutz-Anforderungen aber auch auf die Mitwirkung bei Prüfungen der Aufsichtsbehörden beziehen.

5.3 — Zertifizierung (SOLL): Anbietende sollten bestenfalls relevante Zertifizierungsverfahren nutzen, mit denen neben der Datenschutzkonformität[20] auch die Einhaltung der hier genannten zusätzlichen Kriterien für souveräne Clouds nachgewiesen wird.

[20] Z. B. über eine Zertifizierung nach Art. 42 DS-GVO.

Online-Referenzen

[1] https://www.oeffentliche-it.de/publikationen?doc=71579&title=Digitale+Souveränität

[2] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_de

[3] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf

[4] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf

[5] https://ec.europa.eu/newsroom/article29/items/622227/de

[6] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_de

[7] https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Trennen_V1.0.pdf

[8] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_de

[9] https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-052021-data-governance-act-light-legislative_de