Cloud und digitale Souveränität

Positionspapier der Open Source Business Alliance

Autoren: Dipl.-Wirt.Inform. Alfred Schröder,
Dipl.-Inform. Lothar K. Becker,
Dipl.-Ing. Ingo Wichmann

Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de

Vorwort zum Positionspapier „Cloud und Digitale Souveränität“ der OSB Alliance

Verfasser: Peter Ganten

Spätestens seit dem Digitalgipfel 2018 beherrscht das Schlagwort „Digitale Souveränität“ sowohl die digital- als auch die industriepolitische Diskussion. Viele Verantwortungsträger in Politik und Wirtschaft haben erkannt, dass nicht nur Individuen, sondern auch staatliche Institutionen und Unternehmen in Deutschland und Europa Gefahr laufen, die Kontrolle über die von ihnen generierten Daten zu verlieren oder diese schon verloren haben. Ein solcher Kontrollverlust hätte fatale Folgen für staatliches Handeln, für die Wettbewerbs- und Innovationsfähigkeit unserer Wirtschaft, aber vor allem auch für die Sicherung unserer humanistischen europäischen Werte und der darauf basierenden demokratischen Grundordnungen.

Der freie Zugriff auf die von Menschen und Organisationen durch Interaktion mit Informationstechnologie generierten Daten war auch bereits in früheren Jahren durch proprietäre Software und nicht-offene Schnittstellen immer wieder eingeschränkt. In den vergangenen Jahren ist dadurch jedoch eine massive Bedrohung in bisher ungeahnter Dimension geworden, denn geschlossene digitale Plattformen werden heute allgegenwärtig für Kommunikation, Ein- und Verkauf, Kollaboration und Datenablage genutzt.Diese Plattformen sind der wesentliche Teil dessen, was wir heute als „Cloud“ bezeichnen.

Deswegen ist dieses Papier so wichtig und den Autoren für ihre Arbeit daran sehr zu danken. Es zeigt, durch welche Mechanismen genau „die Cloud“ und digitale Plattformen die Kontrolle über Daten und damit die digitale Souveränität gefährden. Denn nur wenn diese Mechanismen klar benannt sind, lassen sich Strategien und Handlungsweisen bestimmen, mit der die mit vielen Cloud-Diensten unzweifelhaft verbundenen große Chancen etwa für Staat, Medizin oder Wirtschaft genutzt werden können. Und zwar so, dass digitale Souveränität und damit auch Innovationsfähigkeit nicht aufgegeben werden. Das wiederum ist auch Voraussetzung für die Schaffung besserer Cloud-Dienste, die unsere europäischen Werte schützen und in einer eher mittelständisch geprägten Wirtschaft Innovation und Wettbewerb fördern, um so auch im internationalen Vergleich erfolgreiche Angebote zu schaffen.

Im Namen der OSB Alliance bedanke ich mich ganz herzlich bei allen Autoren dieses Positionspapiers. Ohne Eure Geduld und Eure Bereitschaft, immer weiter „dran“ zu bleiben, wäre dieses wichtige Papier nicht möglich gewesen.

Bremen, Oktober 2019

Peter Ganten, Vorstandsvorsitzender

1 Kurzfassung

Die technologische Entwicklung der vergangenen Jahre ist von einer immer stärkeren Mobilität geprägt. Ein Nebeneffekt dieser Mobilität ist die umfassende Verlagerung von Diensten und Daten in die Cloud und damit an einen Ort, an dem diese Daten und Dienste jederzeit flexibel verfügbar sind. Mit dieser Verlagerung in „fremde“ Hände stellt sich zwangsläufig die Frage nach deren Sicherheit. Mit der stetig wachsenden Bedeutung von Diensten aus der Cloud rückt zudem die Frage nach der Abhängigkeit von diesen Diensten und – wichtiger noch – die nach der Abhängigkeit von einzelnen Anbietern in den Fokus. Am Ende geht es um die digitale Souveränität von Individuen aber auch von Unternehmen und von Staaten.

Die Hoheit über die eigenen Daten und Dienste und damit die Möglichkeit, exklusiv und uneingeschränkt über die Verwendung dieser Daten zu bestimmen, ist in einer vollständig vernetzen Welt ein Aspekt, den es bei der Festlegung von digitalen Strategien zu beachten gilt. Auch wenn es eine Anzahl von Gründen gibt, die zu unterschiedlichen Entscheidungen über Ausgestaltung und Ausprägung führen, sollte man diese Entscheidung immer vordringlich auch im Bewusstsein über das Thema digitale Souveränität treffen.

Dabei sollte es nicht um die Abschottung von Diensten und Daten, sondern um Transparenz und offene Schnittstellen gehen, um einseitige Abhängigkeit zu vermeiden.

Dem Staat kommt in diesem Prozess aus Sicht der Open Source Business Alliance eine wichtige Rolle auf verschiedenen Handlungsebenen zu. Diese Ebenen sind für uns:

1. Der Staat als Anwender ...
   … muss sensibel mit seinen Daten und den Daten seiner Bürger umgehen und sich der Implikationen einer Verlagerung zu Cloud-Diensten von proprietären Anbietern bewusst sein. Er muss zudem seine Handlungs- und Funktionsfähigkeit jederzeit sicherstellen.
2. Der Staat als Einkäufer und Förderer …
   … von Entwicklung und Aufbau von Software oder Diensten, die explizit den Anforderungen der digitalen Souveränität Rechnung tragen.

Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de

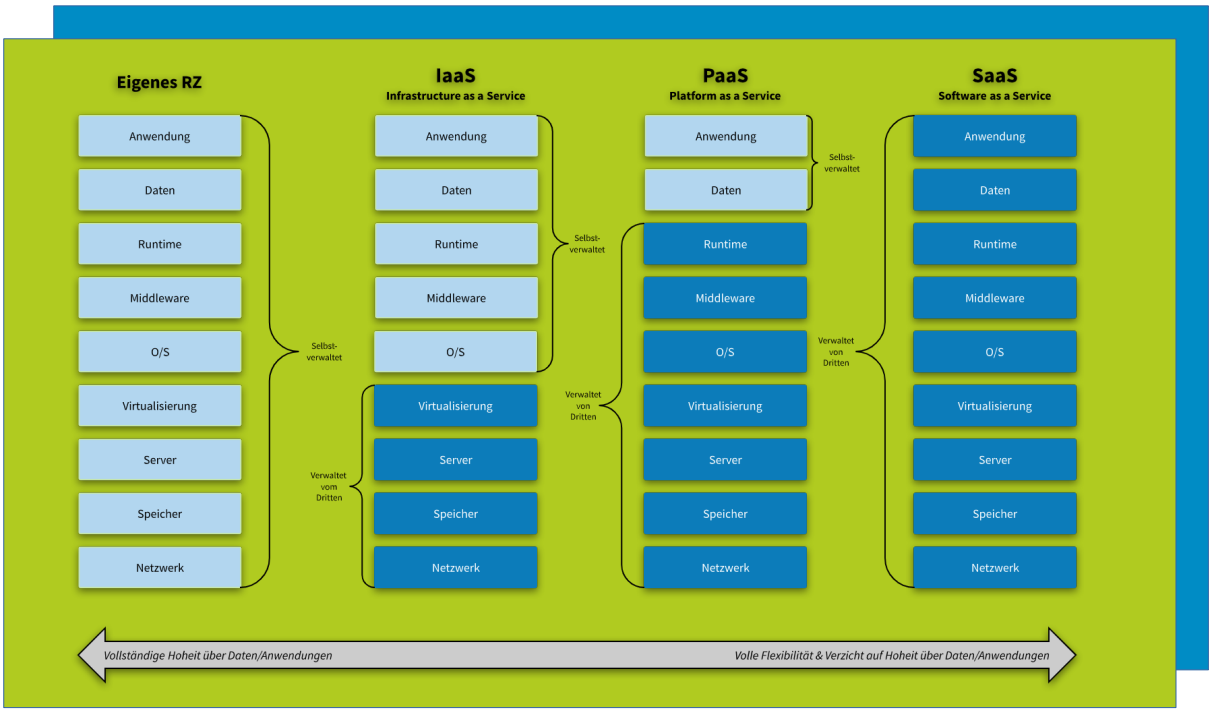
3. Der Staat als Vorbild …
   … für Bürger und Unternehmen bei der Verwendung von Informationstechnologien kann erheblich zur Sensibilisierung für das Thema beitragen.

Dabei ist ein möglicher und nachhaltiger Weg im Hinblick auf Unabhängigkeit, Flexibilität und Sicherheit bei der Digitalisierung eine konsequente Berücksichtigung von Open Source Software und offenen Standards bei der Umsetzung von Cloud-Strategien.

2 Ausgangslage

2.1 Cloud Computing

Die extrem schnelle und dynamische technologische Entwicklung hat zuletzt mit der ständig weiter wachsenden Bedeutung der Cloud einen weiteren Schwerpunkt gesetzt, der sich auf verschiedenen Ebenen und in verschiedenen Ausprägungen manifestiert.



Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de

Im Kern werden Daten und Anwendungen in unterschiedlichen Ausprägungsstufen aus der eigenen IT-Infrastruktur zu externen Dienstleistern verlagert. Die externen Dienstleister stellen einen Zugriff auf diese Daten und Anwendungen mobil und global zur Verfügung.

2.2 Digitale Souveränität

Im Zuge einer immer umfassenderen Durchdringung aller Lebens- und Arbeitsbereiche mit digitaler Technologie stellt sich die Frage nach der digitalen Selbstbestimmung. Wie abhängig sind Individuen, Unternehmen und Staat von einzelnen Technologien, bestimmten Produkten oder einzelnen Herstellern und Anbietern? Und ist diese Abhängigkeit für den Anwender ersichtlich bzw. kann bewusst zwischen Alternativen gewählt werden? Im Rahmen einer digitalen Souveränität muss der Anwender in der Lage sein, die Entscheidung über die Nutzung von Diensten und die Ablage und Verwendung seiner Daten bewusst und informiert zu treffen und diese Entscheidung auch jederzeit ändern zu können.

Zusammengefasst ist digitale Souveränität die Fähigkeit einer Organisation oder eines Individuums, selbst und sicher bestimmen zu können, wer unter welchen Bedingungen, mit welcher Software und für welchen Zweck auf die eigenen Daten zugreifen kann.

2.3 Cloud-Dienste und digitale Souveränität

Cloud und Cloud-Dienste – so wie man sie heute vornehmlich versteht – werden in großer Breite und mit großem Erfolg von Internetkonzernen angeboten.

Der Fokus dieser Unternehmen ist dabei die Sicherung und Verbesserung des eigenen Geschäfts. Dabei setzen die Unternehmen auf unterschiedliche Geschäftsmodelle. Der erste Ansatz wählt den Weg von expliziten Nutzungs- oder Transaktionsgebühren. Dementsprechend ist die Bindung von Kunden – wie bei jedem Unternehmen – fester Bestandteil der Unternehmensstrategie. Zur Erreichung dieses Ziels werden sehr unterschiedliche Ansätze gewählt. Dabei wird mitunter auch bewusst eine technologische oder vertragliche Abhängigkeit geschaffen, die unmittelbaren Einfluss auf die digitale Souveränität des Anwenders hat.[1]

Die zweite Dimension bei der Nutzung von Cloud-Diensten ist die Verwertung von Daten und Metadaten durch Anbieter. Diese nutzen die ihnen anvertrauten Daten bzw. die Zugriffe auf eben diese Daten, um weitere Geschäftsmodelle zu bedienen.[2] Eine

solche Nutzung hat ebenfalls unmittelbar Einfluss auf die beschriebene digitale Souveränität und angesichts des durchgängig hohen Datenschutzniveaus in Deutschland in Einzelfällen auch rechtliche Implikationen.

3 Auswirkungen

3.1 Abhängigkeiten

In Zeiten der „klassischen“ IT, bei der die Daten in lokalen Installationen weitestgehend unter der Kontrolle des Anwenders verblieben, war die Abhängigkeit von Softwareprodukten eines Herstellers bereits sehr ärgerlich[3], wurde aber nur von wenigen als ein schwerwiegendes und weitreichendes Problem erkannt. Mit der Verlagerung in die Cloud für einen flexiblen Zugriff verliert der Anwender nun aber die umfassende Kontrolle über diese Daten.

Je nach Art der Anwendung, welche in die Cloud verlagert wird, geht es soweit, dass diese Abhängigkeit von existentieller Bedeutung für den Anwender ist. D.h. ein Handeln ist ohne Zugriff auf Dienste und Daten in der Cloud nicht möglich.

Wenn der Cloud-Anbieter außerdem die Verlagerung zu anderen Anbietern und Cloud-Diensten erschwert oder verhindert, steht man in einem extremen Abhängigkeitsverhältnis zu diesem Anbieter. Hier muss man sich zum Beispiel die folgenden Fragen stellen:

Welche Auswirkungen entstehen, wenn ein Anbieter kurzfristig nicht mehr zur Verfügung steht? (Politische Entscheidung, Krisensituation, Insolvenz usw.)

- Kann ich den Anbieter kurzfristig mit geringem Aufwand wechseln?
- Kann ich sicherstellen, dass die Daten bei meinem bisherigen Anbieter zuverlässig gelöscht werden?
- Welche und wie viele Alternativen stehen mir für konkrete Dienste zur Verfügung?

3.2 Datensicherheit & Datenschutz

Neben rechtlichen Fragen in Bezug auf den Datenschutz, die mit der Nutzung von Cloud-Diensten verbunden sind[4], muss sich jedes Unternehmen und jede Behörde die Frage nach den Auswirkungen der Verlagerung kritischer Daten zu einem Cloud-Anbieter stellen. Dies gilt umso mehr, wenn die genutzten Dienste von Anbietern bereit gestellt werden, die entweder außerhalb der EU beheimatet sind oder die sich

gegenüber ausländischen Stellen (Dienste, Strafverfolgung) verantworten müssen. Hier sei der US-amerikanische CLOUD-Act genannt, der US-Behörden den Zugang zu Daten, die auf Servern von US-amerikanischen Anbietern gespeichert sind, erleichtert. Dieser Zugriff gilt selbst für Daten, die physisch in anderen Ländern gespeichert werden und ist unabhängig von einem Rechtshilfeabkommen oder davon, ob einem solchen Schritt jeweilige nationale Gesetzen entgegen stehen.[5] Anregungen für solche Fragen sind:

Was kann – im Falle eines Datenlecks oder der Weitergabe– mit diesen Daten passieren:

- Sind Persönlichkeitsrechte gefährdet?
- Sind Unternehmensgeheimnisse gefährdet?
- Sind generell vertrauliche Daten gefährdet?

3.3 Innovationsfähigkeit

Die digitale Wirtschaft steht für dynamische Entwicklung und auch für disruptive Innovationen. Um aber die Innovationsfähigeit, für die insbesondere junge und kleinere Unternehmen stehen, zu erhalten, braucht es Flexibilität und Unabhängigkeit. Eine Abhängigkeit von einzelnen Cloud-Providern und Einschränkung der digitalen Souveränität schränkt gleichzeitig auch Flexibilität und Experimentiermöglichkeiten ein und beeinträchtigt so die Fähigkeit, Innovation – insbesondere im eigenen Land – zu schaffen.

4 Grundprinzipien für eine Cloud mit Digitaler Souveränität

Cloud und digitale Souveränität schließen sich nicht gegenseitig aus – auch wenn durch die Cloud-Technologien neue Herausforderungen entstanden sind. Um das Maß an digitaler Souveränität bei der Verwendung von Cloud-Lösungen zu verbessern, gelten aus unserer Sicht einige Prinzipien, an denen man sich orientieren sollte.

1. Die Option der Verteiltheit und Offenheit
   Man sollte nicht gezwungen sein, die Cloud-Dienste und Daten exklusiv bei einem Anbieter / an einer Stelle nutzen zu müssen. Und es sollte möglich sein,

unterschiedliche Cloud-Angebote miteinander zu integrieren. Die Idee ist nicht Abschottung, sondern Öffnung. (Föderierte Multi-Cloud)

2. Geteiltes Wissen
   Das Wissen um die genutzten Cloud-Technologien muss für Viele verfügbar sein. Es muss die Möglichkeit bestehen, sich das nötige Wissen anzueignen, um informiert entscheiden zu können und technologische Lösungen nachvollziehbar zu machen.
3. Datenhoheit
   Der Erzeuger von Datensätzen muss entscheiden können, wo er seine Daten ablegen möchte und ob sowie zu welchem Zweck oder Mehrwert diese ausgewertet werden. Diese Entscheidung muss er jederzeit ändern können.
4. Transparente Umsetzung, Nutzung freier Standards und offener Schnittstellen
   Die Verwendung von Open-Source-basierten Cloud-Technologien, die auf offenen Standards aufbauen, bedeutet Transparenz für den Anwender und die Möglichkeit zu anderen Anbietern wechseln zu können, die auf die gleichen offenen Standards und offenen Technologien setzen.

5 Handlungsempfehlungen

Der Staat muss bei der Nutzung von Cloud-Technologien die digitale Souveränität von Staat und Bürgern in den Mittelpunkt stellen.

Das notwendige Umdenken muss dabei auf unterschiedlichen Handlungsebenen erfolgen. Diese Ebenen sollen auf den folgenden Seiten adressiert werden.

Der Staat als Anwender (Handlungsebene 1)

Den Daten von Staat, Behörden und Bürgern steht per se ein hohes Maß an Vertraulichkeit zu. Viele Daten und Dienste enthalten kritische Informationen, die in den falschen Händen erhebliches Potential für einen Missbrauch bergen. Und obwohl eine Vielzahl von Datenschützern die undifferenzierte Benutzung von Cloud-Diensten als rechtswidrig oder zumindest als problematisch bei personenbezogenen Daten ansehen, setzen Behörden und staatliche Einrichtung unter Hinweis auf pragmatische Erwägungen auf die Nutzung von Cloud-Diensten, die sich nicht-europäischer Rechtsprechung und Kontrolle unterwerfen müssen. So speichert die Bundespolizei

Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de

Aufnahmen der Bodycams von Beamten in der Amazon Cloud Infrastruktur und verweist pragmatisch auf technische Notwendigkeiten bis passende bundeseigene Cloud-Dienste zur Verfügung stehen.[6]

Hier muss der Aufbau eigener Lösungen auf Basis erprobter Open Source Technologien unter Einbindung europäischer oder eigener Rechenzentren zudem aus wirtschaftspolitischer Sicht Priorität genießen. Dabei erlaubt die Nutzung von offenen Standards den flexiblen Wechsel von Rechenzentrumsanbietern, sofern das Know-how über diese offenen Technologien beim Staat aufgebaut ist.

Der Staat oder die Behörde muss sich außerdem immer die Frage nach Ausweichmöglichkeiten für die Situation stellen, in der der ausgewählte Cloud Dienst vom Anbieter nicht zur Verfügung gestellt werden kann oder darf. Auch hier hilft die pragmatische Sicht auf die Dinge („Das ist der führende Anbieter, was soll da schon passieren?“) im Ernstfall nicht weiter. Die eigene Anwendung darf also niemals so abhängig von einem einzelnen Cloud-Anbieter werden, dass man sie nicht mit geringem Aufwand zu einem anderen Anbieter übertragen kann. Eine Herausforderung, die insbesondere dank Open Source und offener Standards gut zu adressieren ist – sofern man diese Herausforderung annimmt. Und gerade bei den eigenen Diensten und Daten sind Staat, Behörden und Bürger auf eine Verfügbarkeit angewiesen, um im Zweifel handlungsfähig zu bleiben.

Verantwortliche müssen für die Anforderungen einer digitalen Souveränität im Umgang mit Daten und Diensten sensibilisiert werden.

Eigenes Know-how zu offenen Cloud-Technologien muss aufgebaut oder regionales Know-how eingebunden werden.

Der Staat als Einkäufer und Förderer von Lösungen, die digitale Souveränität sicherstellen (Handlungsebene 2)

Allzu oft wird von staatlichen Stellen unter dem Hinweis auf Größe, Leistungsfähigkeit und einfacher Beschaffung der Schritt zu Branchengrößen gewählt. An vielen Stellen

Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de

und im Kern setzen die Lösungen dieser großen Anbieter oftmals unbemerkt oder unerwähnt aber auch auf Open Source Technologien. Insofern wäre es konsequent und naheliegend, direkt die weitere Entwicklung von diesen Technologien zu fördern und dabei das Ziel einer offenen, föderierten Cloud zu verfolgen.

Darüber hinaus stellt sich in den vergangenen Monaten das hohe Datenschutzniveau in Europa und Deutschland immer mehr als positiver Standortfaktor heraus, sodass nach und nach immer mehr heimische Rechenzentren entstehen, die den strengen Auflagen der DSGVO genügen.

Hier bietet sich für den Staat die Möglichkeit, bevorzugt auf Dienstleister und Rechenzentrumsbetreiber zu vertrauen, die auf Open Source Plattformen und offene Standards aufsetzen und einheitliche offene Schnittstellen für Installation und Betrieb von Cloud-Diensten und zugehörigen Daten bieten.

Durch eine Anpassung der Beschaffungskriterien, die bei Cloud-Diensten der Verwendung von Technologien Rechnung tragen, die eine digitale Souveränität ermöglichen, kann der Staat hier die Weiterentwicklung passender Angebote und Innovationen fördern.

Eine konsequente Förderung der Entwicklung von offenen Plattformen und passenden Cloud-Angeboten festigt die Möglichkeiten für eine digitale Souveränität in Bezug auf Infrastruktur und Daten und begünstigt Innovationssprünge gerade auch bei regionalen mittelständischen Anbietern.

Die Entwicklung von offenen Cloud-Plattformen und -Technologien und der Aufbau von passenden vertrauenswürdigen RZ-Angeboten muss durch direkte Förderung und Priorisierung von Vergabekriterien durch den Staat unterstützt und beschleunigt werden.

Ziel: Innovation beschleunigen und digitale Souveränität erlangen

Der Staat als Vorbild (Handlungsebene 3)

Auch wenn Deutschland in Bezug auf den Datenschutz ein hohes Niveau auszeichnet, so ist es auffällig, dass viele Unternehmen einigen strategischen Aspekten bei der

Auswahl von Cloud-Plattformen insbesondere auch für unternehmenskritische Dienste und Daten zu wenig Bedeutung beimessen.

Dabei gehen viele Unternehmen davon aus, dass die Daten und Dienste der öffentlichen Hand besonders schützenswert sind und orientieren sich nicht zuletzt deshalb auch an der Praxis der Nutzung von Cloud-Diensten der öffentlichen Verwaltung.

Der Staat sollte deshalb an der Sensibilisierung von Unternehmen und Bürgern für Themen der digitalen Souveränität und Nachhaltigkeit im Zusammenhang mit der verstärkten Nutzung von Cloud-Infrastrukturen mitwirken und die Vorteile einer offenen und standardisierten Architektur herausstellen.

Eine offene Cloud-Architektur vermeidet einseitige Abhängigkeiten und stärkt die Innovationskraft von Unternehmen und Wirtschaft. Dabei ist ein deutlicher Schub der Innovation in Bereich von Cloud und Digitalisierung erforderlich, um die Lücke zu US-amerikanischen oder chinesischen Unternehmen nicht noch größer werden zu lassen. Die Voraussetzungen dafür liegen in der Nutzung offener Ansätze auf Basis von Open Source Software und offener Standards und keinesfalls in regionalen Alleingängen und einer damit verbundenen Abschottung.

Der Staat sollte hier bei den eigenen Cloud-Diensten mit guten Beispiel vorangehen und Offenheit und digitale Souveränität in den Fokus seiner Bemühungen stellen. Dabei sollte er die strategischen Gründe für diese Entscheidung und für die Wahl eines offenen Weges deutlich kommunizieren und auf diese Weise die Sensibilisierung bei Unternehmen und Bürgern unterstützen.

Der Staat sollte bei der Sensibilisierung für die strategischen Implikationen einer Entscheidung für bestimmte Cloud-Technologien eine wichtige Rolle spielen.

Der Staat muss Vorbild beim Einsatz von Cloud-Technologien sein.

OSB Open Source Business ALLIANCE

Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de

Unsere Forderungen im Überblick:

- **Der Staat muss im Zuge seiner Cloud-Strategie bei der Auswahl von Lösungen und Anbietern den Fokus von pragmatischen auf strategische Fragestellung (wie die digitale Souveränität) lenken.**
- **Verantwortliche müssen für die datenschutzrechtlichen und die strategischen Implikationen einer Entscheidung für Cloud-Dienste sensibilisiert werden.**
- **In Entscheidungen zu Cloud-Strategien muss Know-how zu Open Source Technologie und offenen Standards einbezogen werden. Dieses Know-how sollte selbst aufgebaut oder über Experten aus der Region eingebunden werden.**
- **Der Staat sollte Lösungen bevorzugen, die vollständig transparent und mit offenen Schnittstellen implementiert sind.**
- **Der Staat sollte Anbieter und Rechenzentren bevorzugen, die auf vollständig transparente und offene Ansätze setzen.**
- **Der Staat sollte bei kritischen und sensiblen Daten ausschließlich auf Cloud-Plattformen setzen, die unter Verwendung von Open Source Technologien und offenen Standards aufgebaut sind und bei denen ein einfacher Anbieterwechsel möglich ist.**
- **Der Staat muss die Entwicklung von entsprechenden Technologien und Angeboten direkt und indirekt fördern.**
- **Der Staat muss sicherstellen, dass eigene Daten nur in einem Umfeld abgelegt werden, welches, gemessen an europäischen Datenschutzstandards, höchsten Ansprüchen genügt.**
- **Der Staat muss als Vorbild selbst strenge Kriterien beim Aufbau von Cloud-Lösungen anlegen und dabei die Unabhängigkeit von einzelnen Anbietern wahren.**

OSB Open Source Business ALLIANCE

Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de

Autoren: Alfred Schröder (GONICUS GmbH), Vorstand OSB Alliance
und stellv. Sprecher Working Group Public Affairs,
Lothar Becker (.riess applications gmbh), Vorstand OSB Alliance
und Sprecher Working Group Public Affairs,
Ingo Wichmann (Linuxhotel GmbH), Sprecher Lenkungsausschuß
Fokusprojekt Public Sector,
Oktober 2019

Linkliste:

[1] https://www.zdnet.com/article/game-of-clouds-lock-in-is-coming/
[2] https://www.zdf.de/nachrichten/heute/das-geschaeft-mit-den-daten-100.html
[3] Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern
https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.html?nn=4623908
[4] Cloud-Computing im Zeitalter von DSGVO und Cloud-Act (t3n):
https://t3n.de/news/cloud-computing-zeitalter-dsgvo-1126333/
[5] https://www.handelsblatt.com/politik/deutschland/cloud-act-bundesjustizministerium-warnt-unternehmen-vor-rechtsrisiken-bei-us-datenzugriff/24351610.html
[6] https://www.zeit.de/digital/datenschutz/2019-03/amazon-cloud-bundespolizei-speicherung-bilder

OSB Open Source Business ALLIANCE

Open Source Business Alliance e.V.
Büro Berlin, c/o RA Karl Krüger
Lehrter Str. 57 Haus 6
10557 Berlin

Tel.: +49 (30) 2353-1145
E-Mail: berlin@osb-alliance.de
Internet: http://www.osb-alliance.de