Simon Lang, Ralf Kneuper

Datenschutz und Informationssicherheit in Gaia-X

Gaia-X ist ein Projekt zum Aufbau eines europäischen Cloud-Ökosystems, das die besonderen Anforderungen von EU-Organisationen berücksichtigen soll. Insbesondere soll dabei eine Datensouveränität der EU-Staaten auf Basis einer sicheren und vertrauenswürdigen Infrastruktur erreicht werden. Wesentliche von Gaia-X umzusetzende Anforderungen sind die Unterstützung eines Datenschutzes auf EU-Niveau sowie einer angemessenen Informationssicherheit. In diesem Beitrag wird daher die Umsetzung dieser Anforderungen analysiert, wobei sich zeigt, dass gerade in Bezug auf den Datenschutz Gaia-X den Nutzern nur wenig Unterstützung bietet.

1 Einführung

1.1 Cloud Computing und Gaia-X

Cloud-Computing spielt für die Digitalisierung von Industrie und Verwaltung eine wichtige Rolle, denn Digitalisierungsprojekte sind ressourcenhungrig. Hier bedarf es gut skalierbarer Lösungen, die große Datenmengen innerhalb kürzester Zeit verarbeiten können. Gerade hier hängt Europa allerdings weit hinter den großen Cloud-Anbietern außerhalb der EU, vorrangig aus den USA und dem asiatischen Raum, her. Je mehr jedoch auf diese Anbieter statt auf eigene europäische Lösungen gesetzt wird, desto mehr begeben sich die europäischen Unternehmen in Abhängigkeit der großen Konzerne. Neben Lock-In-Effekten, die Unternehmen dazu zwingen, bei einem (Cloud-)Anbieter zu bleiben, und damit einen ökonomischen Faktor bilden, ist dieser Umstand auch aus dem Blickwinkel des Datenschutzes und der Informationssicherheit kritisch zu betrachten. Denn die Daten, ob personenbezogen oder nicht, liegen physisch bei einem kommerziellen Anbieter. Die Datensouveränität ist gefährdet, auch wenn aus ökonomischer Sicht kein generelles Interesse der großen Cloud-Anbieter an den Inhalten der Daten bestehen dürfte.

Mit der Initiative Gaia-X soll daher ein ganzheitliches europäisches Ökosystem aus Infrastruktur (IaaS), Plattform (PaaS) und Software-Lösungen (SaaS) geschaffen werden, in dem vertrauenswürdige und sichere Anbieter ihre Dienste anbieten und insbesondere Unternehmen ihre Unternehmenswerte sicher übermitteln, speichern und verarbeiten können.

Dieses Ökosystem wurde vom deutschen Bundeswirtschaftsministerium gemeinsam mit dem Bundesforschungsministerium initiiert [1], mittlerweile sind auch Organisationen und Anbieter aus vielen anderen EU-Ländern und darüber hinaus beteiligt. Dies ist ein häufig genannter Kritikpunkt, da es sich in vielen Fällen um Unternehmen handelt, die bisher eher als Blockierer der hier geplanten offenen Systeme und einer europäischen Datensouveränität und als Sammler und Nutzer personenbezogener Daten deutlich über das europäische Datenschutzverständnis hinaus gesehen werden (z.B. Google, Microsoft, Amazon, Palantir).

Gaia-X ist nicht als Cloud-Dienst im herkömmlichen Sinne konzipiert, sondern als föderaler Dienst zu verstehen, der Cloud-Dienste kommerzieller Anbieter auf Basis eines einheitlichen Frameworks zu einem komplexen Ökosystem zusammenschließt.

Dabei unterscheidet Gaia-X verschiedene Rollen der Teilnehmer (Participants) wie folgt [2, Kap. 3.1]:

- Provider (Anbieter) stellen Cloud-Resourcen bereit.
- Federator stellen föderale Dienste (Federation services) auf Basis der Cloud-Resourcen bereit.
- Consumer nutzen diese Cloud-Dienste, um Endnutzern die gewünschten digitalen Angebote zu machen

Simon Lang

General Management (M.A.), Zertifizierter Datenschutzbeauftragter. Produktmanager bei der Althammer & Kill GmbH & Co. KG

E-Mail: sl@althammer-kill.de

Prof. Dr. Ralf Kneuper

Dipl.-Mathematiker, Promotion in Informatik. Professor für Datenschutz und IT-Sicherheit an der IU Internationale Hochschule.

E-Mail: ralf.kneuper@iu.org

Hier ist zu beachten, dass „Consumer“ also das Unternehmen oder die Organisation beschreibt, das bzw. die die Cloud-Dienste einsetzt, und nicht den einzelnen Endnutzer. Der Verantwortliche im Sinne des Datenschutzes ist also üblicherweise der „Consumer“, während Provider und Federator typischerweise die Rolle von Auftragsverarbeitern innehaben.

Daraus ergeben sich viele Herausforderungen an die Umsetzung von Datenschutz und Informationssicherheit, die im Folgenden näher analysiert werden sollen. Insbesondere geht es um die Frage, inwieweit Gaia-X selbst diese Umsetzung unterstützt, um den Nutzerorganisationen die Einhaltung der relevanten Anforderungen einfach zu machen.

1.2 Relevante Anforderungen an Datenschutz und Informationssicherheit

Für die Verarbeitung von personenbezogenen Daten innerhalb des Gaia-X-Ökosystems gelten die allgemeinen Grundsätze der Datenschutz-Grundverordnung (DSGVO) und anderer Datenschutzgesetze (z. B. Bundesdatenschutzgesetz, bereichsspezifische Datenschutzgesetze), sofern der räumliche und sachliche Anwendungsbereich eröffnet ist (siehe hierzu 2.). Daraus folgt, dass bei Nutzung von Gaia-X die Anforderungen dieser Gesetze eingehalten werden müssen. Die weitere Betrachtung beschränkt sich auf die DSGVO, da diese im Gegensatz zu den anderen relevanten Gesetzen unabhängig von Land und Branche praktisch immer anwendbar ist und auch alle Kernanforderungen enthält.

Insbesondere sind geeignete technische und organisatorische Maßnahmen erforderlich, um gemäß dem gegenwärtigen Stand der Technik den Schutz der personenbezogenen Daten, aber auch anderer kritischer Unternehmenswerte wie bspw. Patente, zu gewährleisten.

Für die Informationssicherheit gibt es keine der DSGVO vergleichbaren allgemeingültigen Vorgaben als Referenz. Hierfür nutzt Gaia-X Selbstbeschreibungen und Gütesiegel mit mehreren Anforderungsstufen, mit denen die Provider zeigen können, dass ihre angebotenen Dienstleistungen die relevanten Anforderungen erfüllen.

2 Datenschutz in Gaia-X

Dieses Kapitel gibt einen Überblick über die Besonderheiten des Datenschutzes nach DSGVO bei Cloud-Lösungen mit Gaia-X.

2.1 Sachlicher und räumlicher Anwendungsbereich

Soweit personenbezogene Daten verarbeitet werden, ist der sachliche Anwendungsbereich der DSGVO nach Art. 2 in Cloud-Lösungen mit Gaia-X aufgrund der automatisierten Verarbeitung eröffnet.

Auch der räumliche Anwendungsbereich (Art. 3 DSGVO) dürfte für die meisten Verarbeitungsvorgänge innerhalb des Gaia-X-Ökosystems eröffnet sein, denn die Mehrzahl aller heutigen Mitglieder von Gaia-X operieren aus Niederlassungen innerhalb der Europäischen Union und sind als Verantwortliche oder Auftragsverarbeiter anzusehen (Art. 3 Abs. 1 DSGVO).

2.2 Grundsätze des Datenschutzes

Artikel 5 DSGVO regelt die Grundsätze für die Verarbeitung von personenbezogenen Daten, die gleichermaßen für alle Rollen im Gaia-X-Ökosystem (Provider, Federator und Consumer) gelten. Neben der Rechtmäßigkeit der Verarbeitung, insbesondere bei der Einbindung von Anbietern aus Drittländern oder deren EU-Tochtergesellschaften, stellen die Transparenz der Verarbeitung sowie die Datenminimierung wichtige Aspekte dar, die im Rahmen dieser Ausarbeitung näher untersucht werden. Gleichermaßen werden in diesem Artikel auch angemessene technische und organisatorische Maßnahmen aufgeführt.

Der Verantwortliche, somit also in den meisten Fällen der Consumer oder Nachfrager von Angeboten im Gaia-X-Ökosystem, muss für die Rechtmäßigkeit der Verarbeitung entsprechend Art. 6 bzw. 9 DSGVO Sorge tragen. Im Umkehrschluss muss und darf der Anbieter von Cloud-Ressourcen, in diesem Sinne also der Auftragsverarbeiter, darauf vertrauen, dass der Verantwortliche seiner Pflicht zur Herstellung der rechtmäßigen Verarbeitung nachgekommen ist. Diese Frage der Rechtmäßigkeit der Verarbeitung ist weitgehend unabhängig davon, ob die Verarbeitung im Gaia-X-Ökosystem oder außerhalb stattfindet.

2.3 Betroffenenrechte

Es obliegt zunächst dem Verantwortlichen, die Rechte der betroffenen Personen (Art. 13-20 DSGVO) stets zu wahren, insbesondere auch dann, wenn die Verarbeitung personenbezogener Daten auf einen Auftragsverarbeiter (siehe unten) ausgelagert wird.

Das Gaia-X-Ökosystem zeichnet sich dadurch aus, dass Dienste (IaaS, PaaS, SaaS) zahlreicher Anbieter europäischer und nichteuropäischer Herkunft miteinander auf Basis eines einheitlichen technischen Frameworks verknüpft werden können. Den Nutzern des Ökosystems, also den datenschutzrechtlich Verantwortlichen, soll es möglich sein, Dienste oder Ressourcen unterschiedlichster Anbieter miteinander verknüpfen und bei Bedarf wechseln zu können. Im Hinblick auf die Betroffenenrechte, insbesondere die Informationspflichten nach Art. 13 f. DSGVO kann dies eine Herausforderung darstellen. Schlussendlich muss der Verantwortliche die eingesetzten Dienste und die dahinterstehenden Anbieter jederzeit kennen und bei Erhebung von personenbezogen Daten, ob direkt oder indirekt, die betroffenen Personen auf das Hinzuziehen der Anbieter hinweisen und über Änderungen informieren. Nur so lässt sich gewährleisten, dass die weiteren Betroffenenrechte, insbesondere Art. 15-19, wahrgenommen werden können. Dies kann dazu führen, dass ein Verantwortlicher eine Konfiguration von Diensten vorab definiert und aufgrund der datenschutzrechtlichen Komplexität im Anschluss nicht verändert, auch wenn dies ökonomisch geboten und aufgrund des einheitlichen Frameworks technisch leicht umzusetzen wäre.

2.4 Verantwortliche und Auftragsverarbeiter

Sofern nur eine Partei die Zwecke und Mittel einer Verarbeitung festlegt, für die Erfüllung jedoch eine weitere Organisation (Auftragsverarbeiter) einbindet, handelt es sich um eine Auftragsverarbeitung. Der Verantwortliche, also derjenige, der Zwecke und Mittel einer Verarbeitung festlegt, hat dafür Sorge zu tragen, dass er nur mit Auftragsverarbeitern zusammenarbeitet, die hinreichende Garantien bieten, um den Schutz der Rechte der betroffenen Person zu gewährleisten. Die Nutzung von IaaS-, PaaS- oder SaaS-Lösungen stellt eine klassische Auftragsverarbeitung dar und unterscheidet sich im Gaia-X-Ökosystem nicht von der Inanspruchnahme klassischer Cloud-Anbieter. Von der Gaia-X European Association for Data and Cloud AISBL wird daher auf die Notwendigkeit zum Schließen von Verträgen zur Auftragsverarbeitung hingewiesen. Zwar dürfte diese Aufgabe nach mehr als vier Jahren DSGVO für die allermeisten Unternehmen grundsätzlich keine große Herausforderung mehr darstellen. Im Kontext von Gaia-X entsteht aber eine komplexe Rollenverteilung von einzeln oder gemeinsam Verantwortlichen sowie einer Vielzahl von Auftragsverarbeitern, die durch die Einbeziehung von Cloud-Anbietern in Drittländern noch an Komplexität zunimmt (s. 2.5). Das Vertragswesen, und damit auch das Verwalten von Verträgen zur Auftragsverarbeitung oder zur gemeinsamen Verantwortlichkeit, wurde aber, bis auf die genannten Hinweise, aus dem Gaia-X-Ökosystem ausgeklammert. Hier obliegt es den Verantwortlichen und den Auftragsverarbeitern, datenschutzkonforme Verträge zu formulieren, zu prüfen und schlussendlich abzuschließen. Dafür wäre ein in das Ökosystem eingebettetes Regelwerk wünschenswert, das die Einhaltung insbesondere von Art. 26 und 28 (gemeinsame Verantwortlichkeit, Auftragsverarbeitung) unterstützt.

2.5 Übermittlung in Drittländer

Zusätzliche Herausforderungen entstehen bei der Nutzung von Anbietern, die aus Drittländern wie bspw. den USA oder Asien stammen und ihre Dienste direkt oder über EU-Tochtergesellschaften in das Ökosystem einbringen. Spätestens mit dem EuGH-Urteil *Rechtssache C-311/18* („Schrems II“) ist die Einbindung von Unternehmen aus (unsicheren) Drittstaaten in Frage gestellt. Dies betrifft US-Unternehmen und deren EU-Tochtergesellschaften im besonderen Maße, da US-Gesetze laut Urteil des EuGH die Herausgabe von personenbezogenen Daten erzwingen können (z. B. FISA, E.O. 12333). Vor allem betrifft das Urteil auch das Gaia-X-Ökosystem und seine Teilnehmer, da sich unter diesen sowohl Tochtergesellschaften von US-Unternehmen als auch Anbieter aus weiteren Drittländern befinden. Daher bedarf es in den meisten Fällen einer ausführlichen Prüfung der im Herkunftsland des Anbieters geltenden gesetzlichen Strukturen und besonders im Hinblick auf die Befugnisse der Geheim- und Nachrichtendienste und einer damit verbundenen Risikoanalyse bzgl. einer möglicherweise rechtswidrigen Offenlegung von Daten (Transfer Impact Assessments, TIA). Ausgenommen von einem TIA sind diejenigen Drittländer, für die es einen Angemessenheitsbeschluss [3] der EU-Kommission gibt. Für alle anderen Anbieter aus Drittländern bedarf es jedoch konkreter Lösungsvorschläge seitens der Gaia-X-Verantwortlichen, wie solche Anbieter datenschutzkonform eingebunden werden können. Denn auch mehr als zwei Jahre nach dem oben aufgeführten Urteil wird das Hinzuziehen von Cloud-Anbietern aus unsicheren Drittländern in die Verarbeitung personenbezogener Daten von den Aufsichtsbehörden trotz zahlreicher Anpassungen an Verträgen (insb. Verträge zur Auftragsverarbeitung und Standarddatenschutzklauseln) kritisch beurteilt und in einigen Branchen sogar (insb. Bildung und Schulwesen) teilweise untersagt.

3 Informationssicherheit in Gaia-X

Neben dem Datenschutz spielt die Informationssicherheit in einem digitalen Ökosystem eine entscheidende Rolle. Die Gewährleistung der Informationssicherheit schützt die Daten natürlicher Personen sowie alle weiteren Unternehmenswerte gleichermaßen. Gaia-X verspricht die Möglichkeit eines schnellen Wechsels von einem Anbieter zum anderen (Portabilität und Interoperabilität). Insofern müssen Consumer darauf vertrauen können, dass Anbieter von Cloud-Leistungen eine hinreichende Informationssicherheit gewährleisten können, ohne diese durch Vorortkontrollen oder mühsames Durcharbeiten von Informationen zu technischen und organisatorischen Maßnahmen für jeden einzelnen Anbieter selbst kontrollieren zu müssen. Um dies zu erreichen, fordert Gaia-X von allen Teilnehmern die Erstellung einer Selbstbeschreibung.

- **Selbstbeschreibungen**
  sind maschinenlesbare Darstellungen, die in einem vom W3C definierten Format die beteiligten Entitäten beschreiben. Somit soll es für alle Rollen bzw. alle Angebote der Teilnehmer eine Selbstbeschreibung geben (z. B. Consumer, Federator, Provider, Ressourcen- und Dienstleistungsangebote). Jede Gaia-X-Entität stellt schlussendlich Selbstbeschreibungen bereit, die von Dritten (innerhalb des Ökosystems) validiert und signiert werden [2, Kap. 4].

Darüber hinaus sollen Gaia-X-Gütesiegel an Dienstangebote vergeben werden und als Hilfsmittel für Nachfrager dienen, um datenschutz- und informationssicherheitskonforme Dienstangebote auswählen zu können.

- **Gütesiegel**
  sind ein Mittel, um ein gewünschtes Maß an Vertrauen und Sicherheit zu erreichen, ohne die angegebenen und geprüften Selbstbeschreibungen der Dienstangebote selbst überprüfen zu müssen. Gütesiegel fassen alle überprüfbaren Nachweise eines Dienstanbieters zusammen. Anschließend kann das Dienstangebot in einen der drei definierten Level (Gütesiegel Level 1-3) eingruppiert werden. Ausschlaggebend für die Eingruppierung ist die Einhaltung datenschutzrechtlicher und informationssicherheitstechnischer Anforderungen. Technisch gesehen handelt es sich bei Gaia-X-Gütesiegeln um einen verifizierbaren W3C-Berechtigungsnachweis, ähnlich wie die Berechtigungsnachweise von Selbstbeschreibungen. Damit das GAIA-X-Ökosystem in den ersten Monaten seine Arbeit aufnehmen kann, wird sich die Gaia-X European Association for Data and Cloud AISBL selbst als Gütesiegel-Emittenten und Vertrauensdienstanbieter ernennen. Hierbei handelt es sich jedoch nur um eine kurzfristige, vorübergehende Lösung, die den Zweck verfolgt, das Betriebsmodell zu demonstrieren und zu validieren. Auch soll dadurch unterbunden werden, dass unseriöse Dritte das Vertrauensmodell ins Wanken bringen.

Anfangs verlangten alle Stufen der Gütesiegel die Erfüllung des ENISA European Cybersecurity Scheme (Basic-, Substantial oder High-Level). Dieser Umstand war seinerzeit besonders kritisch zu bewerten, da die Zertifizierungsmechanismen dafür noch im Entstehen sind, während andere, bewährte Testierungs- und Zertifizierungsverfahren nicht berücksichtigt wurden. Zwischenzeitlich wurden jedoch weitere Verfahren ergänzt, wie bspw. C5 oder die ISO/IEC 270xx-Reihe. Dies ist zu begrüßen, da es sich hierbei um weltweit akzeptierte und etablierte Standards handeln. Dies dürfte die Akzeptanz für das Gaia-X-Gütesiegel-Modell steigern.

Aufgrund der oben aufgeführten datenschutzrechtlichen Problematik bzgl. etwaiger Drittlandstransfers gehen die Gütesiegel jedoch nicht weit genug. Level 1 sieht keinen zwingenden Standort innerhalb der EU vor, Level 2 verlangt lediglich, dass den Consumern ein Dienststandort innerhalb Europas angeboten werden muss.

4 Zusammenfassung und Ausblick

Grundsätzlich muss festgehalten werden, dass, trotz der Komplexität des Vorhabens, ein europäisches Daten-Ökosystem zu schaffen, nur spärliche Informationen dazu existieren und diese zumeist von den Projektverantwortlichen selbst publiziert wurden. Insofern ist eine neutrale Bewertung von Datenschutz und Informationssicherheit bei Gaia-X derzeit sehr schwierig. Das Projekt befindet sich jedoch noch im Aufbau, sodass in Zukunft unvollständige oder fehlende Informationen, auch von Dritten, ergänzt werden können.

Es lässt sich jedoch bereits feststellen, dass datenschutzrechtlich Nachholbedarf besteht. Die Projektverantwortlichen haben es verpasst, viele äußerst relevante datenschutzrechtliche Fragestellungen transparent und plausibel zu beantworten. Hier scheint es, dass die Möglichkeit vertan wird, Datenschutz durch Technikgestaltung („Data Protection by Design", Art. 25 DSGVO) von vornherein zu berücksichtigten und damit Wettbewerbsvorteile zu generieren.

Allerdings scheint es, als liege der Fokus von Gaia-X in der Verarbeitung nicht-personenbezogener Daten, bspw. bei der Analyse von Sensordaten. Jedoch würde ein europäisches Cloud-Projekt gerade im Bereich der personenbezogenen Daten überaus Sinn ergeben und einen echten Mehrwert, z.B. durch den Abbau (datenschutz-)rechtlicher Problemstellungen, bieten. Die datenschutzrechtlichen Regularien lassen Verarbeitungstätigkeiten in Cloud-Lösungen außereuropäischer Anbieter nur begrenzt zu. Verantwortliche müssen aktuell bei der Auslagerung von Verarbeitungstätigkeiten in Cloud-Lösungen datenschutzrechtliche Risiken und ökonomischen Nutzen, z.B. durch Effizienzgewinne, abwägen. Dabei bleibt ein datenschutzrechtliches Restrisikos für Verantwortliche, mit der Gefahr, mit Bußgeldern oder Schadensersatzforderungen belangt zu werden. Gerade bei einem Ansatz wie Gaia-X ist das Ausbleiben von lösungsorientierten Antworten verwunderlich und wird durch die Einbeziehung außereuropäischer Mitglieder noch verschärft.

Aus dem Blickwinkel der Informationssicherheit scheint das Ökosystem auf einem guten Weg zu sein. Durch eine Selbstbeschreibung werden alle Teilnehmer und insbesondere die Anbieter von Cloud-Lösungen zur Herstellung einer nachweisbaren Transparenz gezwungen. Diese Selbstbeschreibungen werden von anderen Dritten verifiziert, die wiederum von weiteren Dritten verifiziert wurden. Diese Verkettung hilft schlussendlich Nachfragern dabei, geeignete Dienstleister ausfindig zu machen, die das gewünschte Sicherheitsniveaus ermöglichen. Dieses Konstrukt bleibt jedoch nur stabil, sofern sich alle Teilnehmer an die Regelungen halten. Unseriöse Dritte könnten das Konstrukt ins Wanken bringen. Hier gilt es frühzeitig Vorsorge zu betreiben, was durch die Ernennung der Gaia-X European Association for Data and Cloud AISBL als temporär primären Vertrauensdienstanbieter geschehen soll. Grundsätzlich erscheint das Modell des nachweisbaren Vertrauens jedoch geeignet zu sein, um Vertrauen und Sicherheit ins Ökosystem zu bringen.

Die oben aufgeführten Gütesiegel können ebenfalls einen erheblichen Mehrwert für Nachfrager und Anbieter darstellen, da sie einen erheblichen Informationswert aufweisen. Zum einen können „hohe" Gütesiegel einen Wettbewerbsvorteil für Anbieter darstellen und weniger gut bewertete Anbieter dazu bringen, ebenfalls ein höheres Gütesiegel anzustreben. Zum anderen dienen die Gütesiegel den Nachfragern von Cloud-Leistungen als Signal dafür, ob ein Leistungsangebot den Sicherheitsbedürfnissen der eigenen Unternehmenswerten gerecht wird. Gleichzeitig beantworten Gütesiegel auch, zumindest zum Teil, wie es um die datenschutzrechtliche Gestaltung des Leistungsangebots bestimmt ist. Doch auch hier besteht vor dem Hintergrund der aktuellen datenschutzrechtlichen Debatte eindeutig Nachholbedarf.

Ob Gaia-X unter diesen Rahmenbedingungen ein europäischer Erfolg werden kann, bleibt abzuwarten. Das *offene* Design verspricht einen deutlichen Mehrwert gegenüber gegenwärtigen *geschlossenen* Cloud-Lösungen, indem es deren Herausforderungen, z. B. Lock-In-Effekte oder fehlende Portabilität und Interoperabilität, adressiert. Um jedoch die ambitionierten Ziele zu erreichen, wird noch einige Zeit verstreichen. Die hierfür notwendigen Fördermittel wurden allerdings, Berichten zufolge, vom Bundeswirtschaftsministerium gestrichen [4]. Zudem gilt es kritische Fragestellungen hinsichtlich des Datenschutzes zu beantworten. Sofern hier kein deutlicher Fortschritt erzielt werden kann, wird Gaia-X für die Verarbeitung von personenbezogenen Daten keinen Mehrwert bieten und der Erfolg bleibt sehr fraglich.

Open Access

Funding

Open Access funding enabled and organized by Projekt DEAL.

Literatur

[1] Weiss, A. Gaia-X. Grundlagen für den Aufbau föderierter, digitaler Ökosysteme nach europäischen Regeln. DuD 46, 227–232 (2022).

[2] Gaia-X European Association for Data and Cloud AISBL Gaia-X Architecture Document: 22.04 Release (2022) https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf

[3] European Commission: Adequacy decisions. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, zuletzt abgerufen am 18.07.2022

[4] Ross, U. Förderprojekt Gaia-X Rescue bekommt von der Bundesregierung kein Geld mehr (2022). https://www.heise.de/news/Kein-Geld-fuer-Gaia-X-Projekte-6655227.html