EUROPEAN DATA PROTECTION SUPERVISOR

Leitlinien zur Nutzung von Cloud-Computing-Diensten durch die Organe und Einrichtungen der EU

16. März 2018

INHALT

Zweck und Anwendungsbereich

Die Organe, Einrichtungen und Agenturen der EU (im Folgenden „EU-Institutionen“) ziehen die Nutzung von Cloud-Computing-Diensten aufgrund von Vorteilen, wie Kosteneinsparungen und größerer Flexibilität, in Betracht. Sie sehen sich jedoch mit den Herausforderungen der besonderen Risiken des Cloud-Computing konfrontiert und sind weiterhin in vollem Umfang für die Einhaltung ihrer Datenschutzverpflichtungen verantwortlich. Für die Nutzung von Cloud-Diensten müssen die EU-Institutionen ein gleichwertiges Schutzniveau für personenbezogene und andere Daten vorsehen wie bei jedem anderen IT-Infrastrukturmodell.

Mit den vorliegenden Leitlinien soll den EU-Institutionen eine **praktische Anleitung und Anweisungen** an die Hand gegeben werden, um die Anforderungen der Verordnung (EG) Nr. 45/2001 zu erfüllen. Da derzeit ein Gesetzgebungsverfahren läuft, in dem die Grundsätze der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, im Folgenden „Datenschutz-Grundverordnung“) in die Datenschutzbestimmungen für die EU-Institutionen integriert werden sollen, werden die neuen Konzepte in diesen Leitlinien berücksichtigt, und es wird auf die relevanten Vorschriften der Datenschutz-Grundverordnung Bezug genommen. Nach Annahme der neuen Datenschutzverordnung für EU-Institutionen wird eine aktualisierte Version veröffentlicht.

Die vorliegenden Leitlinien enthalten Empfehlungen und bewährte Praktiken zur Umsetzung der Rechenschaftspflicht für den Schutz personenbezogener Daten, indem sie **helfen, die Risiken für den Schutz der Daten, die Privatsphäre und andere Grundrechte natürlicher Personen, deren personenbezogene Daten mithilfe von Cloud-Diensten verarbeitet werden, zu bewerten und zu bewältigen.** Die Ratschläge, die der Europäische Datenschutzbeauftragte (EDSB) den EU-Institutionen in den letzten Jahren gegeben hat, z. B. hinsichtlich der ersten interinstitutionellen Ausschreibung, wurden gesammelt und zusammengefasst.

Diese Leitlinien beschreiben den Ansatz, den die EU-Institutionen annehmen sollten, um personenbezogene Daten zu schützen, wenn sie die Nutzung von Cloud-Computing-Diensten für ihre IT-Systeme prüfen. Das besondere Risiko, das Cloud-Computing mit sich bringt und das die Risiken der externen Auftragsvergabe einschließt und häufig verstärkt, muss festgestellt und bewältigt werden und es müssen relevante Sicherheitsgarantien eingerichtet werden.

Der EDSB sieht die nachfolgend aufgeführten bewährten Praktiken als **Richtwerte** zur Prüfung der Einhaltung der Verordnung. Die EU-Institutionen können sich unter Berücksichtigung ihres spezifischen Bedarfs auch für andere, gleichermaßen wirksame Maßnahmen entscheiden, die in diesem Dokument nicht dargestellt werden. In diesem Fall müssen sie darlegen, wie diese Maßnahmen zu einem gleichwertigen Schutz der personenbezogenen Daten beitragen.

Auch wenn sich diese Leitlinien vor allem an die behördlichen Datenschutzbeauftragten, Datenschutzkoordinatoren, das IT- und IT-Sicherheitspersonal und andere Verwaltungsdienste der EU-Institutionen richten, die sich mit der Entwicklung, Planung und Vergabe von Cloud-Computing-Diensten befassen, können sie auch für andere am Datenschutz und Cloud-Computing interessierte Organisationen hilfreich sein.

Die EU-Institutionen sollten die Auswirkungen der geplanten Cloud-Dienste auf die zu verarbeitenden Daten prüfen. Ergibt diese Prüfung, dass die EU-Institutionen im Prinzip Sicherheitsgarantien annehmen können, um das Risiko in annehmbaren Grenzen zu halten, dann sollten die EU-Institutionen die sich ergebenden Anforderungen berücksichtigen und sie für die Vergabespezifikationen nutzen. Fällt die Prüfung negativ aus, so sollten die EU-Institutionen ihre Pläne ändern und entweder weniger risikoreiche Cloud-Computing-Dienste in Betracht ziehen oder die Nutzung von Cloud-Computing insgesamt verwerfen.

Der Schwerpunkt der Leitlinien liegt auf folgenden Aspekten:

- der Prüfung der Eignung der Cloud-Computing-Option;
- wie Datenschutzanforderungen bei der Festlegung und Auswahl der Cloud-Computing-Option im Vergabeverfahren berücksichtigt werden sollten;

- einer Grundlage relevanter organisatorischer und technischer Sicherheitsgarantien, mit Schwerpunkt auf Vertragsklauseln.

Die Feststellung und Bewertung allgemeiner Cloud-spezifischer Risiken findet sich im Anhang.

Hier liegt der Schwerpunkt auf den Verträgen für die Bereitstellung von Cloud-Computing-Diensten. Auch zum Betrieb von Cloud-Diensten und zu Dienstleistungsvereinbarungen, in denen ebenfalls die IT-Sicherheitsanforderungen beschrieben werden können, werden Anleitungen gegeben. Die vertraglichen Vereinbarungen sollten auch die Anforderungen bei einer Kündigung des Dienstes, einschließlich der sicheren Rückübertragung der Daten oder der Datenübertragung zu einem anderen Dienstanbieter, beinhalten.

1. Einleitung

1 Die Organe, Einrichtungen und Agenturen der Europäischen Union (im Folgenden „EU-Institutionen“) ziehen die Nutzung von Cloud-Computing-Diensten in Betracht, da sie Vorteile bieten, wie Kosteneinsparungen für Vorab- und Verwaltungsressourcen und die teilweise oder vollständige Auslagerung von Software-Anwendungen, IT[1]-Infrastruktur und Datenspeicherung. So könnten interne IT-Verwaltungsaufgaben und -arbeiten reduziert oder vermieden sowie neue Möglichkeiten geschaffen werden und gegebenenfalls eine Reihe möglicher Vorteile, wie ein höheres Niveau der IT-Sicherheit, genutzt werden. Sie sehen sich jedoch mit den Herausforderungen der besonderen Risiken des Cloud-Computing konfrontiert und sind weiterhin in vollem Umfang für die Einhaltung ihrer Datenschutzverpflichtungen verantwortlich.

2 Mit den vorliegenden Leitlinien sollen den EU-Institutionen praktischer Rat und Anleitungen zur Einhaltung der Verordnung (EG) Nr. 45/2001[2] und der vorgeschlagenen geänderten Rechtsvorschriften (im Folgenden „Verordnungsvorschlag“)[3] an die Hand gegeben werden; sie sollen helfen, die Risiken für den Schutz der Daten, die Privatsphäre und andere Grundrechte natürlicher Personen, deren personenbezogene Daten mithilfe von Cloud-Diensten verarbeitet werden, zu bewerten und zu bewältigen. Die Empfehlungen, die der Europäische Datenschutzbeauftragte den EU-Institutionen in den letzten Jahren gegeben hat, wurden gesammelt und zusammengefasst.

3 Die Grundsätze des Verordnungsvorschlags sollen mit den der neuen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, im Folgenden „Datenschutz-Grundverordnung“)[4] übereinstimmen und in den EU- und den EWR-Mitgliedstaaten angewendet werden. Da der Verordnungsvorschlag noch nicht angenommen wurde, wird **in diesen Leitlinien bei der Nennung spezifischer Artikel auf die Vorschriften der Datenschutz-Grundverordnung verwiesen. Der Text wird aktualisiert, sobald der Verordnungsvorschlag verabschiedet und veröffentlicht ist.**

4 Als unabhängige Aufsichtsbehörde mit Zuständigkeit für die Verarbeitung personenbezogener Daten durch die EU-Institutionen kann der EDSB unter anderem Leitlinien zu bestimmten Aspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten herausgeben. Die vorliegenden Leitlinien sind das Ergebnis eines

---

[1] Der Begriff IT bezieht sich auf Informations- und Kommunikationstechnologien.

[2] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

[3] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, COM(2017) 8 final vom 10.1.2017, abrufbar unter: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0008:FIN.

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); ABl. L 119 vom 4.5.2016, S. 1, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL.

Prozesses, in dessen Rahmen die EU-Institutionen konsultiert wurden und dazu Stellung nahmen[5].

5 Die vorliegenden Leitlinien richten sich an behördliche Datenschutzbeauftragte und Datenschutzkoordinatoren in den EU-Institutionen sowie an das IT- und IT-Sicherheitspersonal und andere Verwaltungsdienste, die sich mit der Entwicklung, Planung und Vergabe von Cloud-Computing-Diensten befassen.

6 Die Leitlinien sollen den EU-Institutionen helfen, ihre Verpflichtungen zu erfüllen. Letztere sind jedoch weiterhin verantwortlich für die Einhaltung der sich aus dem Grundsatz der Rechenschaftspflicht ergebenden Verpflichtungen. Die in diesen Leitlinien empfohlenen Maßnahmen erlauben es den EU-Institutionen, den erwarteten Prozess der Rechenschaftspflicht zu starten und sind zukunftsorientiert, da die zu erwartenden Gesetzesänderungen berücksichtigt wurden. Die EU-Institutionen können sich unter Berücksichtigung ihres spezifischen Bedarfs auch für andere, gleichermaßen wirksame Maßnahmen entscheiden, die in diesem Dokument nicht dargestellt werden. In diesem Fall müssen sie darlegen, wie diese alternativen Maßnahmen zu einem gleichwertigen Schutz der personenbezogenen Daten führen.

[5] 2017 verteilte der EDSB einen Entwurf dieser Leitlinien an die Datenschutzbeauftragten, IT-Manager und IT-Sicherheitsbeamten der Organe, Einrichtungen und Agenturen der EU. Es gingen mehr als 400 Stellungnahmen ein, die in der endgültigen Version berücksichtigt wurden.

2. Geltungsbereich und Gliederung der Leitlinien

7 Mit dem vorliegenden Dokument werden den EU-Institutionen Leitlinien an die Hand gegeben, wie sie bei der Planung und Nutzung von Cloud-Computing-Diensten zur Unterstützung ihrer Aufgaben personenbezogene Daten und die Privatsphäre schützen und den Verordnungsvorschlag einhalten können; dabei sollen sie ihren operativen Anforderungen entsprechen, was sich auch aus den Konsultationsersuchen und den Vorabprüfungen durch den EDSB ergeben hat.

8 Der Schwerpunkt dieses Dokuments liegt auf der Nutzung von Cloud-Computing-Diensten, die von kommerziellen Einrichtungen angeboten werden. Somit befasst es sich natürlich auch mit den Problemen, die durch die externe Vergabe von IT-Diensten, die personenbezogene Daten verarbeiten, entstehen.

9 Die Leitlinien gehen insbesondere auf folgende Punkte ein:

- **Rollen und Verantwortlichkeiten im Bereich Datenschutz** bei EU-Institutionen und dem Anbieter von Cloud-Diensten (im Folgenden „Cloud-Anbieter“) und die damit zusammenhängen Rechenschaftspflichten (Abschnitt 3).
- Faktoren, die bei der **Prüfung** und **Auswahl** eines Cloud-Computing-Dienstes über eine öffentliche Auftragsvergabe zu berücksichtigen sind, einschließlich des anzunehmenden **Ansatzes**, und der relevanten **Sicherheitsgarantien** (Abschnitte 4.1 und 4.2).
- Nutzung der Cloud-Computing-Dienste und Vorschriften/Sicherheitsgarantien für die Zeit nach „Beendigung des Vertrags“ (Abschnitt 4.3).
- Beispiele für **Sicherheitskontrollen** zur Minderung der besonderen Risiken des Cloud-Computing (Abschnitt 4.4) und Verweise zu einigen externen Quellen (siehe Anhang 5) für weitere Informationen.

10 Folgende Informationen sind im Anhang der Leitlinien enthalten:

- Weitere rechtliche Leitlinien zu spezifischen Themen (Anhang 2).
- Grundlegende Konzepte des Cloud-Computing, spezifische Aspekte des Dienstleistungsmodells (IaaS/PaaS/SaaS) und des Bereitstellungsmodells (öffentlich, privat, Community oder hybrid) für Cloud-Umgebungen (Anhang 3).
- Eine Beschreibung besonderer Datenschutzrisiken, die durch die Nutzung von Cloud-Computing-Diensten entstehen oder verstärkt werden (Anhang 4).
- Verweise auf andere nützliche Dokumente (Stellungnahmen, technische Normen, bewährte Praktiken usw.) (Anhang 5).

11 Nicht Gegenstand dieses Dokuments sind:

- Risiken für die EU-Institutionen durch Cloud-Computing, die nicht die Einhaltung des Verordnungsvorschlags betreffen, wie finanzielle Risiken in Verbindung mit der Vergabe von Cloud-Diensten oder in Verbindung mit Verschlusssachen.
- IT-Sicherheitsrisiken, die nicht speziell durch die Nutzung von Cloud-Computing-Diensten entstehen oder verstärkt werden.
- Eine umfassende Abdeckung relevanter IT-Sicherheitsmaßnahmen.
- Die technischen und funktionalen Merkmale der bereitgestellten IT-Infrastruktur, wie Art der Server, Software-Plattformen und Anwendungen, Netzgeräte usw.

- Die grundlegenden Datenschutz-Grundsätze und -pflichten, sofern sie nicht speziell von der Nutzung von Cloud-Computing-Diensten betroffen sind. Entsprechende Leitlinien hierzu finden sich in anderen bestehenden und geplanten Dokumenten des EDSB.

3. Ansatz zur Cloud-Computing-Option

3.1. Gewährleistung eines gleichwertigen Schutzniveaus für personenbezogene Daten wie bei jedem anderen Computing-Modell.

12 Die Nutzung von Cloud-Computing kann unter bestimmten Umständen Vorteile bringen, einschließlich einer Erhöhung des Schutzniveaus für die verarbeiteten Informationen. Das Cloud-Computing-Modell birgt jedoch auch neue Risiken[6] für den Schutz personenbezogener Daten und verändert bestehende Risiken. Zu den wichtigsten Risiken gehören: Organisationen und natürliche Personen haben im Allgemeinen beim Cloud-Computing weniger Kontrolle über die Art und Weise, wie Daten verarbeitet und ausgewertet werden; viele dritte Parteien könnten zu dem Dienst beitragen und es könnten sich so Unsicherheiten über Zuständigkeiten ergeben; die Nutzung des öffentlichen Internets birgt ein weiteres Risiko und durch das dynamische Zusammenspiel vieler Rechenzentren ist nicht immer gewährleistet, dass der physische Speicherort der Daten bekannt ist.

13 Der wesentliche zugrundeliegende Grundsatz dieser Leitlinien besagt, dass Cloud-Computing das Schutzniveau für personenbezogene Daten im Vergleich zur Datenverarbeitung über andere IT-Infrastrukturmodelle nicht mindern darf[7].

> *Durch die Verarbeitung personenbezogener Daten über einen Cloud-Dienst dürfen beispielsweise keine anderen Datenaufbewahrungsfristen als bei einer „nicht cloudbasierten" Verarbeitung, die in den relevanten thematischen Leitlinien des EDSB festgelegt sind, gelten.[8]*

14 Daher sind **spezifische Sicherheitsgarantien[9] erforderlich, um die neuen Risiken zu bewältigen**, damit das Schutzniveau gleich sein kann. Sollten keine angemessenen Sicherheitsgarantien verfügbar sein, so sollten die EU-Institutionen ihre Pläne ändern und

---

[6] Siehe Anhang 4, in dem hohe datenschutzbezogene Risiken, die durch die Nutzung von Cloud-Computing-Diensten entstehen, beschrieben werden.

[7] „Sopot Memorandum", angenommen im April 2012 von der Berliner Internationalen Arbeitsgruppe für den Datenschutz in der Telekommunikation (IWGDPT), abrufbar unter:

https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2012/2012-WP-Sopot_Memorandum-de.pdf.

Siehe die Entschließung des Europäischen Parlaments vom 10. Dezember 2013 zur Freisetzung des Cloud-Computing-Potenzials in Europa, Empfehlung 63: „weist erneut darauf hin, dass **das Niveau des Datenschutzes in einer Cloud-Computing-Umgebung grundsätzlich nicht niedriger sein darf als in jedem anderen Datenverarbeitungsprozess**". Ebenso in der Entschließung des Europäischen Parlaments vom 12. März 2014: „in der Erwägung, dass das Niveau des Datenschutzes in einer Cloud-Computing-Umgebung grundsätzlich nicht niedriger sein darf als in jedem anderen Datenverarbeitungsprozess; in der Erwägung, dass das Datenschutzrecht der Union aufgrund seiner technologischen Neutralität bei Cloud-Computing-Diensten innerhalb der EU schon heute uneingeschränkt Anwendung findet;".

[8] Zum Beispiel in den Leitlinien des EDSB für die Verarbeitung personenbezogener Daten in den Bereichen Urlaub und Gleitzeit, abrufbar auf der EDSB-Website unter:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-12-20_Guidelines_Leave_Flexitime_DE.pdf; die Datenaufbewahrungsfristen werden auf Seite 9-11 angegeben.

[9] Der Begriff „Sicherheitsgarantie", der häufiger im Bereich Datenschutz benutzt wird, und der Begriff „Kontrolle", der häufiger im Bereich IT-Sicherheit benutzt wird, beziehen sich beide auf Maßnahmen zur Bewältigung von Risiken.

entweder weniger risikoreiche Cloud-Computing-Dienste in Betracht ziehen oder die Cloud-Computing-Option insgesamt verwerfen.

15 Die politische Beratung durch den EDSB und die Artikel-29-Datenschutzgruppe (WP29)[10] können für die Untersuchung der Herausforderungen des Cloud-Computing und für die Planung geeigneter Sicherheitsgarantien nützlich sein.

3.2. Politische Steuerung und Verantwortlichkeit: Kontrolle der Datenverarbeitung im Rahmen von Cloud-Diensten

16 Auch wenn die EU-Institution der **für die Verarbeitung Verantwortliche** und der Cloud-Anbieter nur der **Auftragsverarbeiter**[11] ist, müssen die **Rollen und Verantwortlichkeiten** aller Parteien klar definiert werden. Bei vielen Cloud-Computing-Diensten auf dem Markt ist die Rolle des Dienstanbieters nicht immer klar. In manchen Fällen ist der Cloud-Anbieter zu einem gewissen Grad verantwortlich für die Verarbeitung, was die Rolle des Auftragsverarbeiters übersteigt, indem er Vorgänge mit den personenbezogenen Daten durchführt, die nicht vom Kunden beauftragt wurden, oder er dem Kunden keine Wahl lässt, mit welchen Mitteln oder Verfahren die Daten verarbeitet werden. Die EU-Institutionen müssen dies durch Aushandeln geeigneter Verträge und Sicherheitsgarantien oder durch Wahl eines anderen Cloud-Anbieters vermeiden.

17 Die EU-Institution muss aufgrund ihrer rechtlichen Verpflichtung über die Verarbeitung personenbezogener Daten mittels eines Cloud-Dienstes [12]**verantwortlich bleiben** (und die **Zwecke** und **Mittel** bestimmen). In den vertraglichen Rechtsrahmen zwischen den EU-Institutionen und dem Cloud-Anbieter (im Folgenden „Vertrag“) müssen zu diesem Zweck spezifische Anforderungen aufgenommen werden.

---

[10] Zu den Herausforderungen des Cloud-Computing im Bereich Datenschutz siehe die Stellungnahme des Europäischen Datenschutzbeauftragen zur Mitteilung der Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa“, abrufbar unter:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_DE.pdf.

und die Stellungnahme 05/2012 der Artikel-29-Datenschutzgruppe zum Cloud-Computing, abrufbar unter:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf

[11] Nach Artikel 2 der Verordnung (EG) Nr. 45/2001 und nach Artikel 4 (Nr. 8) der Datenschutz-Grundverordnung.

[12]Nach Artikel 14 der Verordnung (EG) Nr. 45/2001 hat die betroffene Person beispielsweise das Recht, *von dem für die Verarbeitung Verantwortlichen* [der in Artikel 2 Buchstabe d der Verordnung als „das Organ oder die Einrichtung der Gemeinschaft, die Generaldirektion, das Referat oder jede andere Verwaltungseinheit“ definiert wird] zu verlangen, dass unrichtige oder unvollständige personenbezogene Daten unverzüglich berichtigt werden.

Siehe auch die Spezifikation in Artikel 23 Absatz 2 Buchstabe a der Verordnung, dass der „Auftragsverarbeiter [...] nur auf Weisung des für die Verarbeitung Verantwortlichen [handelt]“.

Artikel 16 der Datenschutz-Grundverordnung besagt außerdem: „Die betroffene Person hat das Recht, *von dem Verantwortlichen* unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.“ Ähnlich wie in der Verordnung (EG) Nr. 45/2001 ist in der Datenschutz-Grundverordnung in Artikel 28 Absatz 3 festgelegt, „dass der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen [...] verarbeitet“.

18 Kurz gesagt, die EU-Institutionen müssen, um die **Verantwortung zu behalten** und die Anforderungen des Verordnungsvorschlags[13] und ihre Rechenschaftspflicht zu erfüllen:

- **Einen Cloud-Anbieter auswählen, der ausreichende Sicherheitsgarantien bietet**, sowohl in Bezug auf die technischen als auch die nicht technischen Maßnahmen, die er durchführen kann, um die EU-Institution bei der Einhaltung und Wahrung der Datenschutzrechte natürlicher Personen, deren Daten verarbeitet werden, zu unterstützen.
- **Einen rechtsverbindlichen Vertrag [14] (im Folgenden „Vertrag") zwischen dem Cloud-Anbieter und der EU-Institution abschließen** und neben anderen Geschäftsbedingungen festlegen, dass der „Cloud-Kunde" (die EU-Institution) **allein für die Verarbeitung verantwortlich** ist und der Auftragsverarbeiter nur Daten auf Weisung des Verantwortlichen verarbeiten darf.
- Wenn der Vertrag läuft, aktiv die **Umsetzung** der erforderlichen Sicherheitsgarantien und der anderen Vertragsbestimmungen **sicherstellen und überwachen**.

19 Wir weisen darauf hin, dass ein **Auftragsverarbeiter**, der Cloud-Anbieter, rechtlich den **spezifischen Verpflichtungen** unterliegt (Artikel 28, 29 und 30 der Datenschutz-Grundverordnung[15]).

20 Der Cloud-Anbieter muss die EU-Institution dabei **unterstützen**, die Einhaltung der Datenschutzpflichten sicherzustellen, insbesondere hinsichtlich der Pflicht, unverzüglich auf Anfragen von betroffenen Personen, die ihre **Datenschutzrechte ausüben[16]**, in Bezug auf den Zugang zu und die Sperrung, Berichtigung und das Löschen von Daten zu reagieren. Es muss im Vertrag geregelt sein, dass entweder der für die Verarbeitung Verantwortliche die Verarbeitung direkt durchführen kann, die notwendig ist, um die Rechte der betroffenen Personen zu erfüllen oder dass der Cloud-Anbieter unverzüglich auf Anweisung der EU-Institution reagiert und die Anfrage einer betroffenen Person bearbeitet (Zugang zu, Berichtigung, Sperrung, Löschen von personenbezogenen Daten). In jedem Fall muss klar festgelegt werden, dass die endgültige Antwort an die betroffene Person von der EU-Institution oder auf deren Anweisung erfolgen muss.

---

[13] Wir weisen darauf hin, dass spezifische Vorschriften der Datenschutz-Grundverordnung für die Verarbeitung personenbezogener Daten im Auftrag der EU-Institution (nach Artikel 28) in diesem Fall gelten.

[14] Der Begriff „Vertrag" bezieht sich **sowohl** auf den Vertrag *als auch* auf die „Dienstleistungsvereinbarung" sowie auf alle Anhänge, die zusammen den vertraglichen Rahmen bilden, der von der EU-Institution mit dem Cloud-Anbieter vereinbart wurde.

Was der Cloud-Anbieter tun muss, um den für die Verarbeitung Verantwortlichen bei der Erfüllung seiner Aufgaben zu unterstützen, wird in schriftlichen Verträgen geregelt. Diese Verträge sind in der Regel so strukturiert, dass die operativen Bedingungen des Dienstes, der vom Cloud-Anbieter erbracht wird, definiert sind und in einem Vertragsabschnitt oder einem anderen Dokument, das eine Erweiterung des Vertrags darstellt und als Dienstleistungsvereinbarung bezeichnet wird, vereinbart werden. Auch wenn in diesen Leitlinien zwischen diesen beiden Dokumenten, wie es üblich ist, unterschieden wird, so steht es den EU-Institutionen frei, den Vertrag nach ihren Wünschen zu strukturieren.

[15] Siehe Artikel 28 bis 30 der Datenschutz-Grundverordnung

[16] Gemäß Artikel 12 bis 23 der Datenschutz-Grundverordnung.

3.3. Planung der Vergabe von Cloud-Computing-Diensten

21 Unter Berücksichtigung der oben aufgeführten Aspekte und der Rechtsnatur, der institutionellen Aufgaben und Verantwortlichkeiten (die Ausübung einer öffentlichen Funktion, Auslösen spezieller Vorkehrungen) der EU-Institutionen[17] sollten letztere folgendes Verfahren für die Planung von Cloud-Computing-Diensten anwenden:

- **Rat von Experten** einholen und relevante **bewährte Praktiken** suchen und annehmen. Sich mit anderen EU-Institutionen verbinden, um beispielsweise Erfahrungen über relevante frühere Auftragsvergaben zu erhalten.
- Entscheidungsträger, Unternehmer, Vertragsmanager und IT-Personal über die sich aus der Nutzung von Cloud-Computing-Diensten ergebenden Risiken **schulen** und Vertragspartner anweisen, sich weiterzubilden.
- Eine **Bewertung der Datenschutzrisiken** durchführen, um festzustellen, ob es möglich ist, Cloud-Dienste zu vergeben, um die Datenverarbeitung im vorgesehenen Anwendungsbereich zu unterstützen und einen geeigneten Cloud-Anbieter auszuwählen, der ein geeignetes Schutzniveau für personenbezogene Daten im Hinblick auf die Minderung der Auswirkungen auf die Grundrechte und Grundfreiheiten natürlicher Personen und die Einhaltung des Verordnungsvorschlags bieten kann.

  Das Maß an Formalität und Einblick der Bewertung kann von Faktoren abhängen, die in Abschnitt 4.1 beschrieben werden.

22 Wir empfehlen, dass die EU-Institutionen möglichst damit beginnen, Fachkenntnisse und Erfahrungen im Bereich der Verarbeitung personenbezogener Daten mithilfe von Cloud-Diensten mit Operationen, die mit **geringeren Datenschutzrisiken**[18] verbunden sind, zu sammeln und nur sensiblere Operationen in Betracht zu ziehen, wenn sichergestellt ist, dass sie eine effektive Kontrolle über diese Dienste haben.

23 Falls die geplante Cloud-Option machbar ist (auf der Grundlage der Bewertung), müssen die EU-Institutionen:

---

[17] EU-Institutionen sind besondere öffentliche Verwaltungen auf supranationaler Ebene, deren Rechtsrahmen im Bereich Datenschutz in der Verordnung (EG) Nr. 45/2001 und in naher Zukunft in der vorgeschlagenen Verordnung geregelt ist. In rechtlicher Hinsicht muss darauf hingewiesen werden, dass das vorgenannte Datenschutzrecht **in Verbindung mit** anderen Rechtstexten, die die Aktivitäten der EU-Institutionen regeln, wie das **Protokoll über die Vorrechte und Befreiungen der Europäischen Union**, anzuwenden ist.

Protokoll (Nr. 36) über die Vorrechte und Befreiungen der Europäischen Union (1965) Amtsblatt Nr. C 321 E vom 29.12.2006, S. 0318 - 0324, abrufbar unter:

http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12012E/PRO/07&from=DE.

In den **Verordnungen der Agenturen der EU**, z. B. der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde) wird auch auf das Protokoll über die Vorrechte und Befreiungen Bezug genommen und Folgendes festgelegt: „Artikel 67 - Vorrechte und Befreiungen: Das dem Vertrag über die Europäische Union und dem AEUV beigefügte Protokoll (Nr. 7) über die Vorrechte und Befreiungen der Europäischen Union findet auf die Behörde und ihr Personal Anwendung."

[18] Im Prinzip ohne die in Artikel 9 der Datenschutz-Grundverordnung aufgeführten besonderen Kategorien personenbezogener Daten.

- Notwendige Rollen festlegen, relevante Aufgaben und Ressourcen zuweisen und interne politische Maßnahmen, Prozesse und Verfahren zur Verwaltung der zukünftigen Cloud-Dienste festlegen.
- Sicherstellen, dass Verträge und Dienstleistungsvereinbarungen mit dem Cloud-Anbieter alle erforderlichen Sicherheitsgarantien enthalten, einschließlich:
    - einer klaren Anweisung, dass der Cloud-Anbieter die ihm von der EU-Institution anvertrauten personenbezogenen Daten **nur auf dokumentierte Weisung der EU-Institution** verarbeiten darf;
    - gewährleisten, dass sich die zur Verarbeitung personenbezogener Daten befugten Personen zur **Vertraulichkeit** verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
    - die klare Angabe und Definition der **Zuständigkeiten und der Haftung** der verschiedenen Parteien (einschließlich Unterauftragnehmern, falls vorhanden);
    - klare Definition und Angabe, insbesondere wie der Cloud-Anbieter die EU-Institution dabei unterstützen soll, ihre Verpflichtungen als für die Verarbeitung Verantwortlicher gegenüber den betroffenen Personen und dem EDSB zu erfüllen;
    - Vorschriften, die es der EU-Institution erlauben, selbst oder über einen externen (dritten) Prüfer, der von der EU-Institution beauftragt wird, **Prüfungen** des Cloud-Anbieters durchzuführen;
    - klare Angabe des **Standorts** des Cloud-Anbieters und gegebenenfalls anderer vom Cloud-Anbieter beauftragter Auftragsverarbeiter (Unterauftragnehmer) und deren Datenverarbeitung, einschließlich Backups;
    - klare Angabe, dass der Auftragsverarbeiter keine **weiteren Auftragsverarbeiter** ohne vorherige schriftliche Genehmigung der EU-Institution in Anspruch nimmt. Diese Genehmigung kann spezifisch (für einen bestimmten Unterauftragnehmer) oder allgemein gelten. Bei einer allgemeinen Genehmigung muss der Cloud-Anbieter den für die Verarbeitung Verantwortlichen über jeden neuen oder ersetzten Unterauftragnehmer informieren und die EU-Institution hat das Recht, dieser Änderung zu widersprechen;
    - **keine Offenlegung** gegenüber Strafverfolgungsbehörden von EU-Mitgliedstaaten oder Nicht-EU-Staaten (im Folgenden „LEA“) der dem Cloud-Anbieter (sowie gegebenenfalls Unterauftragnehmern) von der EU-Institution anvertrauten personenbezogenen Daten, *sofern dies nicht ausdrücklich dem EU-Recht unterliegt.* Als Einrichtung der EU unterliegt die EU-Institution den **Vorrechten und Befreiungen der Europäischen Gemeinschaften**[19], insbesondere hinsichtlich der Unverletzlichkeit der Archive (einschließlich des physischen Standorts der Dienste) und der Informationssicherheit;
    - Verfahren zur Datenübertragung / Wiederherstellung / Löschung;
    - **Löschen oder Rückgabe**, nach Wahl der EU-Institution, aller der dem Cloud-Anbieter von der EU-Institution anvertrauten personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen;
    - klare Angabe der vom Cloud-Anbieter und möglichen Unterauftragnehmern zu gewährleistenden **IT-Sicherheitsmaßnahmen**.

[19]Siehe Fußnote 17.

- Verwaltung, Ausführung und Beendigung des Vertrags und Überwachung der Verarbeitungsleistungen durch den Cloud-Anbieter in Bezug auf die ihm von der EU-Institution „anvertrauten“ personenbezogenen Daten.

24 Das Ergebnis der Bewertung der Datenschutzrisiken kann auch ergeben, dass der geplante Cloud-Dienst **Datenschutzrisiken erzeugt, die nicht ausreichend und angemessen bewältigt werden können.** Dann sollte die EU-Institution **in Betracht ziehen, einen oder mehrere andere Cloud-Dienste mit Risiken, die angemessen bewältigt werden können, zu vergeben** oder **die gesamte Cloud-Option zu verwerfen**.

25 Das allgemein empfohlene **Verfahren** zur Vergabe von Cloud-Diensten wird in Kapitel 4 detailliert beschrieben.

4. Bewertung der Cloud-Computing-Option, der Vergabe und der Durchführung der Cloud-Dienste

4.1. Prüfung der Angemessenheit des Datenschutzes eines Cloud-Dienstes

26 Die Vergabe von Cloud-Computing-Diensten zur Verarbeitung personenbezogener Daten kann unterschiedlich sein, je nachdem, ob die EU-Institution

- (Szenario I) Cloud-Dienste zur Unterstützung ***spezifischer*** **Verfahren** (z. B. zur Verwaltung der Organisation von Gruppen- und Expertensitzungen) vergeben möchte oder
- (Szenario II) das Portfolio an künftigen zu unterstützenden Prozessen relativ weit fasst, was **eine Reihe von Diensten** und Bereitstellungsmodellen erfordert.

Die beiden Szenarien werden separat beschrieben, auch wenn sie viele gemeinsame Merkmale haben.

Bewertung der Datenschutzrisiken der Cloud-Dienst-Option

27 Die EU-Institution muss prüfen, ob die **Anforderungen für die Einhaltung** des Verordnungsvorschlags erfüllt werden können.

28 Die EU-Institution muss die Datenschutzrisiken auch hinsichtlich der Grundrechte und Grundfreiheiten natürlicher Personen bewerten und dabei die ihr zu diesem Punkt zur Verfügung stehenden Informationen berücksichtigen:

- Die **Art der** zu verarbeitenden **personenbezogenen Daten**.

  Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind[20], verdienen besonderen Schutz.

- Die **Art der** durchzuführenden **Verarbeitung**.

  „Profiling" ist beispielsweise eine Art der Verarbeitung, die mögliche hohe Risiken für natürliche Personen birgt[21].

- Der **Umfang** und **Kontext** der Verarbeitung.

  Die Verarbeitung von Daten einer großen Zahl natürlicher Personen kann das Risiko erhöhen.

---

[20] Dies sind insbesondere Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person und Daten über strafrechtliche Verurteilungen und Straftaten. Dies ist jedoch nicht der einzige Faktor, der die Höhe des Risikos bestimmt. Personenbezogene Daten, die nicht unter die genannten Kategorien fallen, können unter Umständen zu hohen Risiken für die Rechte und Freiheiten natürlicher Personen führen, insbesondere wenn die Verarbeitung eine Bewertung der natürlichen Personen vorsieht, die Folgen für ihr Leben, beispielsweise im beruflichen oder finanziellen Kontext, hat oder eine automatische Entscheidung mit rechtlichen Folgen oder eine systematische Überwachung, z. B. per Videoüberwachung umfasst. (Siehe auch die *Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt"* der Arkikel-29-Datenschutzgruppe, WP 248 Rev.01 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236).

[21] Siehe auch die Leitlinien der Artikel-29-Datenschutzgruppe zur automatisierten Einzelentscheidung und Profiling für die Zwecke der Verordnung 2016/679 „*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)*".http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Der Kontext der Verarbeitung, wie Kategorie der betroffenen Personen (z. B. EU-Bedienstete oder nicht; Arbeitsplatz der natürlichen Personen, Rolle und Aufgaben; Einbeziehung von Kindern); mögliche Folgen für die Umgebung (z. B. mögliche Vorurteile gegenüber natürlichen Personen aufgrund ihrer besonderen Kultur) usw.

- Der **Zweck** der Verarbeitung.

  Beispiele sind: Verwaltung der E-Mail-Kommunikation, Bewertung der Mitarbeiterleistung, speichern und verarbeiten von Bildern und Videos aus der Videoüberwachung usw.

29 Bei der Bewertung müssen folgende Aspekte berücksichtigt werden:

- Die **allgemeinen Risiken im Zusammenhang mit Cloud-Computing** (wie in Anhang 4 beschrieben) und die **Risiken in Verbindung mit der spezifischen Cloud-Dienst-Option** und die spezifischen personenbezogenen Daten und die Verarbeitung fallen in den Anwendungsbereich der Ausschreibung.
- Die **derzeitige Marktrealität** und **die Dauer des Einsatzes des künftigen Cloud-Anbieters** im Hinblick auf dessen Fähigkeit, die Anforderungen für die Einhaltung des Verordnungsvorschlags zu erfüllen und die Risiken in einer annehmbaren Höhe zu halten. Dies kann durch Sammeln einiger Vorabinformationen (öffentlich oder auf Anfrage verfügbare Informationen), erreicht werden, einschließlich möglicher Sicherheitsinstrumente, wie sie in Abschnitt 4.2.1 aufgeführt sind.

30 In der Datenschutz-Grundverordnung werden Bedingungen festgelegt, unter denen eine Bewertung der Risiken für natürliche Personen verpflichtend ist, sowie der Mindestinhalt einer solchen Bewertung, die als **Datenschutz-Folgenabschätzung (DSFA)** bezeichnet wird[22]. Die Artikel-29-Datenschutzgruppe hat Leitlinien zu den Bedingungen, Modalitäten und dem Inhalt der DSFA herausgegeben[23].

31 Die vorliegenden Leitlinien liefern keine weiteren Anleitungen dazu, wie eine DSFA durchzuführen ist. Der EDSB entwirft derzeit relevante Leitlinien für die EU-Institutionen, auf die in dieser Hinsicht verwiesen werden kann. Der behördliche Datenschutzbeauftragte der EU-Institutionen übernimmt eine wichtige Rolle, wenn es darum geht, letztere zu beraten, ob eine DSFA verpflichtend und wie diese durchzuführen ist.

32 Ist eine DSFA gemäß den zukünftigen Leitlinien des EDSB erforderlich, dann müssen die Ergebnisse auch hinsichtlich der möglichen Nutzung des Cloud-Computing-Dienstes durch die EU-Institution berücksichtigt werden. Ist eine DSFA **nicht** erforderlich, so kann die EU-Institution dennoch die entsprechende DSFA-Methodik anwenden, um eine Bewertung der Datenschutzrisiken durchzuführen.

33 Mögliche Maßnahmen zur Einhaltung des Verordnungsvorschlags und zur Minderung dieser Risiken sind Teil dieser Leitlinien und werden in den Abschnitten 4.2, 4.3 und 4.4 beschrieben. Diese Verpflichtungen und Empfehlungen können als **Grundlage der für alle Cloud-Computing-Dienste einzuführenden Sicherheitsgarantien** betrachtet werden.

34 Diese Grundlage schließt nicht die Pflicht aus,

[22] Siehe Artikel 35 der Datenschutz-Grundverordnung.

[23] Abrufbar unter: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

- die Restrisiken und die Risiken in Zusammenhang mit dem geplanten spezifischen Kontext und der Verarbeitung durch den Cloud-Dienst zu bewerten (siehe auch Anhang 4)
- und letztendlich mögliche notwendige Maßnahmen festzulegen, um diese Risiken zu bewältigen.

Daher ist ein **dokumentiertes Risikomanagement** der EU-Institution in jedem Fall verpflichtend[24].

35 Sollte die EU-Institution aufgrund ihrer Risikobewertung entscheiden, keine der in diesem Dokument vorgeschlagenen Maßnahmen als Grundlage zu ergreifen, so muss sie dies in verantwortungsvoller Weise tun und die Gründe für diese Entscheidung dokumentieren.

36 Die EU-Institution muss in jedem Fall notwendige Maßnahmen zur Erfüllung der Pflichten aus dem Verordnungsvorschlag umsetzen.

Die EU-Institution muss letztendlich prüfen, ob die festgestellten Risiken bewältigt werden können, so dass deren Folgen gemindert werden und die Verordnung eingehalten werden kann, und entscheiden, **ob ein Cloud-Dienst eine geeignete Option ist oder nicht**.

Szenario I: Öffentliche Vergabe von Cloud-Computing-Diensten für eine spezifische Verarbeitung personenbezogener Daten

37 Ergibt die Bewertung, dass die EU-Institution grundsätzlich in der Lage ist, die Sicherheitsgarantien zur Minderung der Risiken von Cloud-Computing-Diensten für die spezifische Verarbeitung zu gewähren oder irgendwie die Risiken in angemessener Weise zu bewältigen, und somit positiv entscheidet, müssen die Datenschutzanforderungen (einschließlich der Sicherheitsanforderungen), die in einer Risikobewertung festgelegt werden, in Kriterien in den Vergabespezifikationen umgewandelt werden.

38 Können die Anforderungen von den verfügbaren Cloud-Diensten **nicht** erfüllt werden, so darf die Verarbeitung **nicht** in der bewerteten Cloud-Dienst-Umgebung durchgeführt werden (**negative Entscheidung**).

39 In diesem Fall können die Anforderungen durch Einschränkung der Verarbeitung durch Cloud-Dienste auf weniger risikobehaftete Dienste geändert, oder gegebenenfalls und sinnvollerweise, durch eine Beschränkung der zu verarbeitenden Daten auf weniger sensible Kategorien oder nicht personenbezogene Daten begrenzt werden. Alternativ kann ein anderes Bereitstellungs-/Dienstmodell mit geringeren Risiken bewertet werden. Möchte die EU-Institution die personenbezogenen Daten weiterhin verarbeiten, muss eine neue Bewertung der Anforderungen und Risiken durchgeführt werden.

[24] Siehe Artikel 24 Absatz 1 der Datenschutz-Grundverordnung: „Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.“

Szenario II: Öffentliche Vergabe von Rahmenverträgen für Cloud-Computing-Dienste zur Verarbeitung personenbezogener Daten in umfangreichen Anwendungsfällen

40 Ein Verfahren zur öffentlichen Vergabe von Rahmenverträgen für Cloud-Computing-Dienste zur Verarbeitung personenbezogener Daten in umfangreichen Anwendungsfällen (z. B. vollständige IT-Infrastruktur der EU-Institutionen, IT-Ressourcen zur Entwicklung und zum Betreiben institutioneller Webseiten, IT-Umgebungen für Entwickler usw.), die häufig auf IaaS- und PaaS-Dienste abzielen, könnten die Datenschutzanforderungen in den folgenden drei Hauptphasen berücksichtigen.

Phase 1: Dienstgruppen für einen Rahmenvertrag

41 Die oben beschriebene Bewertung muss für **eine Gruppe von möglichen Verarbeitungen/Anwendungen** durchgeführt werden, für die die Cloud-Dienste, die auf der Grundlage eines Rahmenvertrags vergeben werden, genutzt werden können.

42 Die bei der Risikobewertung festgestellten Datenschutzanforderungen und die Sicherheitsgarantien müssen **in Kriterien** in den Vergabespezifikationen umgewandelt werden.

43 Die EU-Institutionen bewerten, welche Cloud-Dienstangebote geeignet sind und wählen nur Dienstanbieter aus, die diese Anforderungen erfüllen können. Gibt es kein geeignetes Angebot, so kommt kein Vertrag zustande.

Phase 2: Geeignetheit einer spezifischen Verarbeitung für Cloud-Dienste

44 Sobald ein Rahmenvertrag existiert, kann die EU-Institution möglicherweise entscheiden, ob eine spezifische Verarbeitung/Anwendung durch einen der Cloud-Dienste, die von dem/den Auftragnehmer(n) angeboten wird, durchgeführt werden kann.

45 Für eine spezifische Anwendung, die mithilfe eines Cloud-Dienstes durchgeführt werden soll, gilt:

Die EU-Institution muss **prüfen, ob einer der im Rahmenvertrag verfügbaren Cloud-Dienste** den Datenschutzanforderungen der durchzuführenden spezifischen Verarbeitung **entspricht**.

46 Können die Anforderungen von den verfügbaren Cloud-Diensten **nicht** erfüllt werden, so darf die Verarbeitung **nicht** in der bewerteten Cloud-Dienst-Umgebung durchgeführt werden (**negative Entscheidung**).

47 In diesem Fall können die Anforderungen durch Einschränkung der Verarbeitung durch Cloud-Dienste auf weniger risikobehaftete Dienste geändert, oder gegebenenfalls und sinnvollerweise, durch eine Beschränkung der zu verarbeitenden Daten auf weniger sensible Kategorien oder nicht personenbezogene Daten begrenzt werden. Alternativ kann ein anderes Bereitstellungs-/Dienstmodell mit geringeren Risiken bewertet werden. Möchte die EU-Institution die personenbezogenen Daten weiterhin verarbeiten, muss eine neue Bewertung der Anforderungen und Risiken durchgeführt werden.

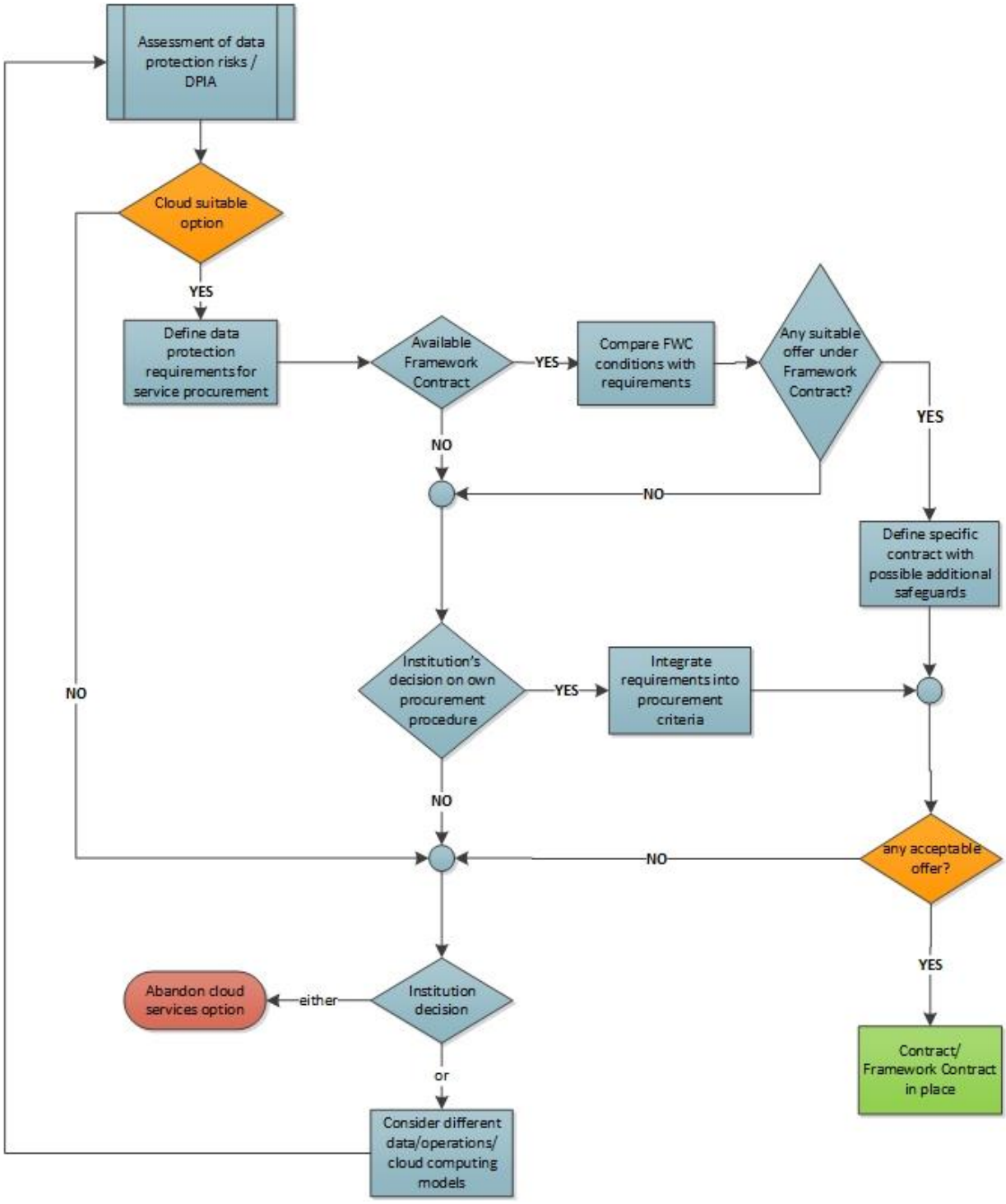
Phase 3: Verträge für spezifische Verarbeitungen

48 Zeigt das Ergebnis von Phase 2, dass ein oder mehrere Verarbeitungen im Prinzip für die verfügbaren Cloud-Dienste geeignet sind, muss die EU-Institution möglicherweise, sofern rechtlich zulässig, mögliche neue Anforderungen in einem spezifischen Vertrag,

verhandeln, um sicherzustellen, dass alle erforderlichen Sicherheitsgarantien und Maßnahmen vorhanden sind.

49 Da eine weitere Integration aufgrund von Beschränkungen der öffentlichen Vergabe nicht möglich ist, ist es in jedem Fall äußerst wichtig, dass die EU-Institution die gesamte geplante Nutzung der geplanten Dienste seit der ursprünglichen Bewertung in Phase 1 so genau wie möglich berücksichtigt und festlegt.

Das gesamte Verfahren kann in folgendem Ablaufdiagramm zusammengefasst werden:



Assessment of data protection risks / DPIA	Bewertung der Datenschutzrisiken / DSFA

Cloud suitable option	Geeignete Cloud-Option
Define data protection requirements for service procurement	Festlegung von Datenschutzanforderungen für den zu vergebenden Dienst
Available Framework Contract	Verfügbarer Rahmenvertrag
Compare FWC conditions with requirements	Vergleich der Bedingungen des Rahmenvertrags mit den Anforderungen
Any suitable offer under Framework Contract?	Geeignetes Angebot im Rahmenvertrag?
Define specific contract with possible additional safeguards	Festlegung eines spezifischen Vertrags mit möglichen Sicherheitsgarantien
Institution's decision on own procurement procedure	Entscheidung der Institution über ein eigenes Vergabeverfahren
Integrate requirements into procurement criteria	Integration der Anforderungen in die Vergabekriterien
any acceptable offer?	Akzeptables Angebot?
Abandon cloud service option	Verwerfen der Cloud-Dienst-Option
Institution decision	Entscheidung der Institution
Consider different data/operations/cloud computing models	Berücksichtigung verschiedener Daten/Verarbeitungen/Cloud-Computing-Modelle
Contract/Framework Contract in place	Vertrag/Rahmenvertrag vorhanden
YES	JA
NO	NEIN
either	entweder
or	oder

4.2. Kriterien und Anforderungen für die Vergabe von Cloud-Diensten

50 Wenn die Entscheidung zugunsten des Cloud-Dienstes getroffen wird, müssen **Kriterien und Anforderungen** für die öffentliche Vergabe und das sich daraus ergebende Servicemanagement (Betrieb, Wartung, Kündigung) festgelegt werden.

51 Hinsichtlich des **Ausschreibungsverfahrens im Allgemeinen** wird dringend empfohlen, dass die EU-Institutionen Maßnahmen ergreifen, um eine **gemeinsame Strategie**[25] für das Cloud-Computing festzulegen. Diese sollte die **Planung** der Vergabe von Cloud-Diensten umfassen, auch um die Verhandlungsposition gegenüber den Cloud-Anbietern zu stärken,

[25] Siehe die Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa", auf Seite 27: „118. Im Zusammenhang mit der Europäischen Cloud-Partnerschaft wird die Kommission an konkreten Vorgaben für die Auftragsvergabe im öffentlichen Sektor arbeiten und **gemeinsame Anforderungen für die Auftragsvergabe im Bereich von Cloud-Computing-Diensten** festlegen. Der EDSB weist darauf hin, dass diese gemeinsamen Anforderungen für die Auftragsvergabe auch Datenschutzanforderungen einschließlich angemessener Sicherheitsvorkehrungen **enthalten müssen**, die auf eine den konkreten Risiken der Verarbeitung von Daten des öffentlichen Sektors in einer Cloud-Computing-Umgebung angemessenen Weise festgelegt werden sollten. Geschehen sollte dies nach einer sorgfältigen und auf die Art und Sensibilität der Verarbeitung abgestimmten **Datenschutz-Folgenabschätzung** (z. B. Differenzierung zwischen der Verarbeitung von Gesundheitsdaten, Daten über Straftaten, vertrauliche Daten usw. durch den öffentlichen Sektor). Im Ergebnis werden die Anforderungen in den Vergabebedingungen je nach Sensibilität der verarbeiteten Daten differenziert werden müssen, was zu unterschiedlichen Reihen gemeinsamer Anforderungen führen sollte." Siehe in dieser Hinsicht auch die Entschließung des Europäischen Parlaments vom 12. März 2014.

sowie andere Elemente enthalten, wie z. B einen Rahmen für Dienstleistungsvereinbarungen mit Datenschutzanforderungen, einschließlich insbesondere Managementverträge und Vermittlungsgebühren[26].

52 Dies könnte mögliche Schwierigkeiten kleinerer Einrichtungen der EU, die ihr eigenes Vergabeverfahren haben, lösen, wenn es darum geht, vertragliche Anforderungen festzulegen und spezifische Sicherheitsgarantien in den Rahmenvertrag/die Ausschreibung aufzunehmen.

4.2.1. Gebührende Sorgfalt bei der Wahl des zukünftigen Cloud-Anbieters

53 Die EU-Institution muss einen Cloud-Anbieter auswählen, **der ausreichende Garantien bietet, um im Namen der EU-Institution zu handeln und die notwendigen technischen und organisatorischen Datenschutzmaßnahmen umzusetzen**; außerdem muss die Wirksamkeit dieser Maßnahmen überprüft werden.

54 Als Nachweis für diese Garantien kann die EU-Institution Folgendes nutzen:

- **Von akkreditierten Dritten ausgestellte Zertifikate** für den Datenschutz und die IT-Sicherheit im Rahmen der relevanten Zertifizierungen[27]. Hierzu gehören Cloud-bezogene Datenschutz- und IT-Sicherheitszertifizierungen für die festgestellten Risiken[28]. Im Allgemeinen gelten Selbsteinschätzungen nicht als ausreichende Garantien.
- Einhaltung von **Verhaltensregeln im Bereich Cloud-Computing**, die einen Mehrwert in Bezug auf Maßnahmen zum Schutz personenbezogener Daten liefern und dazu beitragen, die Einhaltung der Verordnung in einer Cloud-Umgebung nachzuweisen[29].
- **Frühere Erfahrungen mit Projekten** mit ähnlichen (oder höheren) Risiken für analoge Kategorien personenbezogener Daten. Weitere Sicherheit kann durch nachweisbare Erfahrung mit öffentlichen nationalen oder europäischen Verwaltungen belegt werden.
- **Bereits vorhandene Praktiken der Rechenschaftspflicht**, wie einen Datenschutzbeauftragten im Unternehmen; vorhandene Datenschutzvorschriften und

[26] Durchgeführt von der Europäischen Kommission im Namen anderer EU-Institutionen im Zusammenhang mit dem interinstitutionellen Rahmenvertrag Cloud I. Ein ähnlicher Ansatz wird von den Agenturen der EU im Zusammenhang mit einem Rahmenvertrag angewendet, der von der Europäischen Behörde für Lebensmittelsicherheit (EFSA) verwaltet wird.

[27] Die Artikel-29-Datenschutzgruppe bietet Leitlinien für die Regelung von **Zertifizierungen**, die dazu beitragen können, die Einhaltung nach den Bedingungen der Datenschutz-Grundverordnung zu belegen. Eine Liste dieser Zertifizierungen wird von den nationalen Datenschutzbehörden oder dem zukünftigen Datenschutzausschuss bereitgestellt werden.

[28] In Artikel 28 Absatz 5 der Datenschutz-Grundverordnung ist festgelegt, dass Auftragsverarbeiter (in diesem Fall Cloud-Anbieter) **Zertifizierungen** (die in Artikel 42 der Datenschutz-Grundverordnung beschrieben werden) als Faktor heranziehen können, um Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen nachzuweisen.

[29] Die Artikel-29-Datenschutzgruppe wird Leitlinien zu den **Verhaltensregeln** bereitstellen, die dazu beitragen können, die Einhaltung nach den Bedingungen der Datenschutz-Grundverordnung nachzuweisen. Eine Liste dieser Verhaltensregeln wird von den nationalen Datenschutzbehörden oder dem zukünftigen Datenschutzausschuss bereitgestellt werden.

-verfahren; Beitrag zur Durchführung einer DSFA oder Vorhandensein einer anderen Methode zur Bewertung der Datenschutzrisiken; (gegebenenfalls) Nutzung von Standardvertragsklauseln[30]; ein etablierter IT-Risikomanagementrahmen; bereits vorhandene IT-Sicherheitsvorschriften, Verfahren und Sicherheitsgarantien.

4.2.2. Vertragsgestaltung: die richtigen Geschäftsbedingungen für den zukünftigen Cloud-Anbieter[31]

(i) Einleitung und allgemeine Anmerkungen

55 Um sicherzustellen, dass die EU-Institution überwachen kann, wie der Cloud-Anbieter die beauftragten Dienste bereitstellt, müssen **im Vertrag mit dem Cloud-Anbieter geeignete Geschäftsbedingungen ausgehandelt und erreicht werden**. Einige dieser Geschäftsbedingungen werden nachfolgend (als „Musterklauseln“) spezifiziert.

56 Es muss betont werden, dass solche Geschäftsbedingungen **angepasst** werden müssen, so dass die für die EU-Institutionen geltenden rechtlichen Beschränkungen berücksichtigt werden (insbesondere die Anwendbarkeit des Protokolls über die Vorrechte und Befreiungen der Europäischen Gemeinschaften[32]) und gemäß den Anforderungen zur Bewältigung der Risiken durch die Datenverarbeitung **abgeändert** werden müssen (nach dem risikobasierten Ansatz).

(ii) Gesamtbewertung der vertraglichen Vereinbarungen

57 Die für die Verarbeitung Verantwortlichen müssen sich der Bedeutung der **Gesamtbewertung des Vertragsrahmens**, der für die Bereitstellung des Cloud-Dienstes gilt, bewusst sein[33].

---

[30] In Artikel 29 Absätze 6 bis 8 der Datenschutz-Grundverordnung wird auf Standardvertragsklauseln Bezug genommen.

[31] Siehe allgemein zu diesem Thema die Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa“, Seite 26 und 27, Absatz 117.

[32] Siehe Fußnote 17.

[33] Eine **schnelle Checkliste** findet sich in der Stellungnahme 05/2012 zum Cloud-Computing, Abschnitt 3.4.2 **Vertragliche Absicherungsklauseln der Beziehung(en) „für die Verarbeitung Verantwortlicher“ - „Auftragsverarbeiter“**, Seite 15 bis 17; es sind 14 Punkte aufgeführt, von denen wir Folgende hervorheben möchten:

Punkt 5 – „Einschluss einer **Vertraulichkeitsklausel**, die sowohl für den Cloud-Anbieter als auch für alle seine Angestellten verbindlich ist, die Zugang zu den Daten haben. Ausschließlich autorisierte Personen dürfen Zugang zu den Daten haben.“

Punkt 7 – „In dem Vertrag sollte ausdrücklich festgelegt werden, dass **der Cloud-Anbieter die Daten keinem Dritten mitteilen darf** – auch nicht zu Zwecken der Aufbewahrung – sofern die Hinzuziehung von Unterauftragnehmern nicht vertraglich geregelt ist. Der Vertrag sollte festlegen, dass Unterauftragsverarbeiter ausschließlich auf der Grundlage einer Einwilligung beauftragt werden dürfen, die der für die Verarbeitung Verantwortliche generell erteilen kann. Der Auftragsverarbeiter ist eindeutig dazu verpflichtet, den für die Verarbeitung Verantwortlichen über beabsichtigte diesbezügliche Änderungen zu informieren. Der für die Verarbeitung Verantwortliche hat dabei jederzeit die Möglichkeit, solchen Änderungen zu widersprechen oder den Vertrag zu beenden. Der Cloud-Anbieter sollte eindeutig dazu verpflichtet sein, **alle beauftragten Unterauftragnehmer zu nennen** (z. B. in einem öffentlichen digitalen Register). Es muss sichergestellt werden, dass Verträge zwischen dem Cloud-Anbieter und dem Unterauftragnehmer die Bestimmungen des Vertrags zwischen dem Cloud-Anwender und dem Cloud-Anbieter widerspiegeln (d. h., dass Unterauftragsverarbeiter denselben vertraglichen Verpflichtungen unterliegen wie der Cloud-Anbieter). Es muss insbesondere garantiert werden, dass sowohl der Cloud-Anbieter als auch alle Unterauftragnehmer ausschließlich auf Weisung des Cloud-

- Das bedeutet, dass die EU-Institution **alle Bestandteile** der Vertragsunterlagen des Cloud-Anbieters (einschließlich der Anhänge) prüfen muss, die insbesondere die in der Vereinbarung festgelegte Verarbeitung beschreiben (z. B. Kategorien der verarbeiteten Daten, vom Cloud-Anbieter eingeführte Sicherheits- und Vertraulichkeitsmaßnahmen usw.). Die EU-Institution muss **im Einzelfall** prüfen, wie der Vertrag, die Dienstleistungsvereinbarung und die Anhänge (d. h. der gesamte Vertragsrahmen) die spezifischen Datenschutzpflichten und rechtlichen Anforderungen erfüllen.
- Es ist insbesondere wichtig, die sogenannten „**sonstigen** Vertragsklauseln" (d. h. Klauseln, die **nicht direkt mit dem Datenschutz zusammenhängen, jedoch für die Einhaltung der Rechenschaftspflicht wichtig sind**) zu prüfen, einschließlich der Klauseln über das **für den Vertag selbst anwendbare Recht** („geltendes Recht") und die **gerichtliche Zuständigkeit**; über das **Recht der Parteien, Abweichungen vom Vertrag einzuführen**; über die **Verpflichtungen des Cloud-Anbieters nach Beendigung des von der EU-Institution „extern vergebenen" Datenverarbeitungsdienstes**.

58 Weitere Klauseln, die in dem Vertrag über die Cloud-Dienste festgelegt werden müssen, sind Klauseln zur **Verfügbarkeit und Qualität des Dienstes** (in denen der Zeitrahmen festgelegt wird, in dem der Dienst verfügbar ist, sowie technische Eigenschaften, Effektivität und Effizienz und relevante Kennzahlen definiert werden). Häufig werden solche Anforderungen in einer Dienstleistungsvereinbarung zusammengefasst.

59 Wir möchten allgemein darauf hinweisen, dass alle Cloud-Anbieter, die Kunden, die dem EU-Recht unterliegen, Dienste anbieten, verpflichtet sind, die Übereinstimmung ihrer vertraglichen Vereinbarungen mit den Datenschutzanforderungen der EU auf der Grundlage des Verordnungsvorschlags zu prüfen und dabei die Herausforderungen des Cloud-Computing für die Datenverarbeitung, wie in der Stellungnahme 05/2012 der Artikel-29-Datenschutzgruppe zum Cloud-Computing sowie in der entsprechenden Stellungnahme des ESDB beschrieben werden, zu berücksichtigen[34].

(iii) Zu bestimmten „zentralen" Datenschutzthemen, die in den vertraglichen Geschäftsbedingungen geregelt werden müssen

60 In die Vertragsbedingungen muss unbedingt aufgenommen werden, dass es dem Cloud-Anbieter **verboten ist**, gegenüber **einer Strafverfolgungsbehörde („LEA")** eines EU-Mitgliedstaates oder eines Drittlandes die dem Cloud-Anbieter von der EU-Institution anvertrauten personenbezogenen Daten offenzulegen, *sofern dies nicht ausdrücklich im EU-*

Anwenders handeln. Wie in dem Abschnitt über die Vergabe von Unteraufträgen erklärt wurde, sollte die **Haftungskette** in dem Vertrag klar festgelegt werden. Der Vertrag sollte den Auftragsverarbeiter verpflichten, internationalen Übermittlungen einen Rahmen zu geben, beispielsweise durch die Unterzeichnung von Verträgen mit den Unterauftragsverarbeitern, die auf den Standardvertragsklauseln aus 2010/87/EU basieren."

Punkt 11 – „Es sollte vertraglich festgelegt werden, dass der Cloud-Anbieter dazu verpflichtet ist, den **Anwender** über einschlägige Änderungen bei den jeweiligen Cloud-Diensten **zu informieren**, wie beispielsweise über die Implementierung zusätzlicher Funktionen."

Punkt 12 – „Der Vertrag sollte die **Protokollierung und Prüfung** der relevanten Verarbeitungstätigkeiten an personenbezogenen Daten festlegen, die durch den Cloud-Anbieter oder die Unterauftragnehmer durchgeführt werden."

[34]Siehe Fußnote 10.

Recht oder dem Recht eines Mitgliedstaates erlaubt ist, so dass die im EU-Recht festgelegten Bedingungen für eine solche Offenlegung erfüllt sind[35].

61 **Transparenz** ist in der Beziehung zwischen der EU-Institution und dem Cloud-Anbieter wichtig, da sie **direkte Auswirkungen auf die Einhaltung der Verpflichtungen der EU-Institution nach dem Verordnungsvorschlag hat**. Daher muss der Cloud-Anbieter relevante Änderungen in der zugrundeliegenden Infrastruktur, den Verfahren und den Ergebnissen der relevanten Sicherheitsaudits der EU-Institution unverzüglich und unter Wahrung der Vertraulichkeit **mitteilen**. Hierzu gehören auch Informationen hinsichtlich Aktivitäten im Rahmen von Geschäftskontinuitätsmaßnahmen, Tests oder Operationen mit potenziellen Folgen für den Kundendienst.

62 Da die EU-Institution für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist, hat sie das Recht, zu verlangen, dass der Cloud-Anbieter sie **unverzüglich informiert**, wenn der Cloud-Anbieter die Einhaltung der Vertragsverpflichtungen nicht mehr gewährleisten kann. Hinsichtlich der Transparenz sind – in der Dienstleistungsvereinbarung oder im Vertrag – **alle Unterauftragsverarbeiter**, die an der Bereitstellung des Cloud-Dienstes mitwirken, sowie **alle Orte**, an denen die personenbezogenen Daten verarbeitet werden, aufzuführen.

63 Der **Standort** des Unternehmens, das den Cloud-Dienst anbietet, seiner Rechenzentren, in denen die Server und andere Geräte stehen, in denen Daten gespeichert oder verarbeitet werden (einschließlich Backup, Geschäftskontinuitätsmaßnahmen und Übertragungen sowie Standorte, von denen aus Fernzugriffe durchgeführt werden) ist ebenfalls ein wichtiger Faktor, der berücksichtigt werden muss.

- In dieser Hinsicht **empfiehlt der EDSB, dass die Verarbeitung der dem Cloud-Anbieter von der EU-Institution anvertrauten personenbezogenen Daten sowie jede untergeordnete Verarbeitung *generell* im Hoheitsgebiet der EU stattfinden muss**[36].

  Der Grund für diese Empfehlung ist, – auch in der „Cloud-Umgebung" – die Anwendbarkeit der Vorrechte und Befreiungen der EU-Institutionen im Hoheitsgebiet

[35]Dieses Verbot ergibt sich – als obligatorische rechtliche Verpflichtung – aus dem **Protokoll über die Vorrechte und Befreiungen der Europäischen Gemeinschaften**. Eine Erinnerung in den Geschäftsbedingungen des Cloud-Dienstvertrags wäre für den Cloud-Anbieter sehr nützlich. Artikel 1 des zuvor genannten Protokolls besagt Folgendes: [...] „*Die Vermögensgegenstände und Guthaben der Union dürfen ohne Ermächtigung des Gerichtshofs nicht Gegenstand von Zwangsmaßnahmen der Verwaltungsbehörden oder Gerichte sein.*". Hinsichtlich dieser Vorschrift stellen wir fest, dass dies auch die Cloud-Computing-Dienste abdeckt, für die den EU-Institutionen eine Nutzungslizenz gewährt wurde; Artikel 2 legt fest: „*Die Archive der Union sind unverletzlich.*" In Artikel 6 heißt es: „*Den Organen der Union steht für ihre amtliche Nachrichtenübermittlung und die Übermittlung aller ihrer Schriftstücke im Hoheitsgebiet jedes Mitgliedstaats die gleiche Behandlung wie den diplomatischen Vertretungen zu.*"

[36] Die EFSA stellte beispielsweise sicher, dass folgende Klausel von der EU-Agentur in den Dienstleistungsvertrag für Cloud-Computing aufgenommen wird: „*die Cloud-Computing-Dienste dürfen nur im Hoheitsgebiet des Europäischen Wirtschaftsraums gehostet werden. Der Cloud-Dienstanbieter, seine Tochtergesellschaften und alle Unterauftragsverarbeiter werden die Daten (der EU-Agentur), einschließlich aller Backup-Daten auf Speichermedien und in Datenzentren hosten, die sich in folgenden **Mitgliedstaaten** befinden*".

ihrer Mitgliedstaaten nach dem **Protokoll über die Vorrechte und Befreiungen der Europäischen Gemeinschaften**[37] sicherzustellen.

Artikel 1 des Protokolls besagt: „Die Räumlichkeiten und Gebäude der Union sind unverletzlich. Sie dürfen nicht durchsucht, beschlagnahmt, eingezogen oder enteignet werden. Die Vermögensgegenstände und Guthaben der Union dürfen ohne Ermächtigung des Gerichtshofs nicht Gegenstand von Zwangsmaßnahmen der Verwaltungsbehörden oder Gerichte sein." Artikel 2 legt fest: „Die Archive der Union sind unverletzlich." Und Artikel 5 besagt schließlich: „Den Organen der Union steht für ihre amtliche Nachrichtenübermittlung und die Übermittlung aller ihrer Schriftstücke im Hoheitsgebiet jedes Mitgliedstaats die gleiche Behandlung wie den diplomatischen Vertretungen zu."

Neben den obigen Ausführungen berücksichtigen wir auch, dass bei einer Speicherung der Daten im Hoheitsgebiet eines Nicht-EU-Staates die Möglichkeit besteht, dass eine Strafverfolgungsbehörde in diesem Gebiet im Rahmen einer Zwangsmaßnahme Zugriff auf die Daten **unter Anwendung des dort geltenden öffentlichen Rechts** (z. B. Strafrecht, Verfahrensrecht, Gesetze über Vorratsdatenspeicherung *usw.*) verlangen kann. Dieses Risiko muss von den EU-Institutionen sorgfältig geprüft werden.

Es muss auch angemerkt werden, dass es im Falle eines Hostings der Cloud-Infrastruktur in einem **Nicht-EU-Staat für den EDSB problematischer sein wird, Kontrollen** mit den zuständigen Aufsichtsbehörden **durchzuführen und zu koordinieren** und so die Durchsetzung der Vorschriften der Verordnung sicherzustellen.[38].

(iv) Musterklauseln (was zu prüfen ist, was im Vertrag festgelegt/enthalten sein muss)

64 Einige Inhalte dieses Abschnitts können auch in Form einer Dienstleistungsvereinbarung vorliegen (siehe Abschnitt 4.3.2), wie beispielsweise die Sicherheitsvorschriften. Die Dienstleistungsvereinbarung muss Teil der verbindlichen Vertragsvereinbarung sein (die

---

[37] Zum anerkannten Schutz der EU-Institutionen durch die EU-Mitgliedstaaten gemäß dem Protokoll siehe insbesondere die Artikel 1, 2 und 5 des Protokolls, das in seiner konsolidierten Fassung abrufbar ist unter: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12012E/PRO/07&from=DE.

[38] Wir weisen darauf hin, dass die Datenschutz-Grundverordnung in Kapitel VII eine Verpflichtung zur **Kooperation zwischen den nationalen Aufsichtsbehörden** enthält.

In dieser Hinsicht sollte auch auf Artikel 58 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung hingewiesen werden, nach dem die Aufsichtsbehörde die Befugnis haben muss, **„gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats** Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des **Auftragsverarbeiters** zu erhalten" *(Hervorhebungen hinzugefügt).*

Wir weisen darauf hin, dass *wenn* personenbezogene Daten **außerhalb der EU** verarbeitet werden, die relevanten Vorschriften der Datenschutz-Grundverordnung gelten (nämlich Kapitel V Artikel 44 bis 50).

Für Leitlinien des EDSB, basierend auf den Vorschriften der aktuellen Verordnung (EG) Nr. 45/2001 siehe das Positionspapier des EDSB „Die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen: Artikel 9", abrufbar unter:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_DE.pdf. Dieses Papier wird im Hinblick auf die Vorschriften des Verordnungsvorschlags aktualisiert.

EU-Institution entscheidet jedoch, wie die Vertragsbedingungen organisiert werden, indem sie Geschäftsbedingungen im Vertrag und/oder in der Dienstleistungsvereinbarung festlegt).

65 Auf der Grundlage der relevantesten und am häufigsten verwendeten Vertragsklauseln[39] werden hier einige Musterklauseln aufgeführt, die in den Vertrag aufzunehmen sind. Solche **Musterklauseln** werden festgelegt, **damit die EU-Institution einfacher kontrollieren kann, ob der Vertrag angemessene Datenschutzgarantien für die Bereitstellung von Cloud-Diensten bietet**. Diese Klauseln müssen an den angebotenen spezifischen Cloud-Dienst **angepasst** werden (z. B. muss berücksichtigt werden, ob der Cloud-Anbieter Unterauftragsverarbeiter beauftragt).

66 Die Musterklauseln sind:

A - Beschreibung der unterstützten Verarbeitung

Die Beschreibung der Verarbeitung und insbesondere der Kategorien der personenbezogenen Daten, die vom Cloud-Anbieter verarbeitet werden, wird gegebenenfalls in diesem Vertrag, in der Dienstleistungsvereinbarung und ihren Anhängen, die fester Bestandteil des Vertrags sind, spezifiziert[40].

B - Geltendes Datenschutzrecht

67 Die Verarbeitung der personenbezogenen Daten erfolgt im Einklang mit den relevanten Vorschriften [des Verordnungsvorschlags], die den betroffenen Personen u. a. spezifische

---

[39] Insbesondere die Klauseln im Beschluss der Kommission C(2010)593, abrufbar unter:

http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_de.htm.

Es muss angemerkt werden, dass die Möglichkeit des Verantwortlichen, auf Standard-Datenschutzklauseln zurückzugreifen, den Auftragsverarbeiter weder daran hindern sollte, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen zu verwenden, noch ihn daran hindern sollte, weitere Klauseln hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden.

Zu berücksichtigen sind auch die kürzlichen Aktualisierungen (29. November 2017) des Arbeitsdokuments „Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules“, WP 256, (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109) und des Arbeitsdokuments „Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules“, WP 257, (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110). Diese Dokumente enthalten Tabellen mit Elementen und Grundsätzen in verbindlichen Datenschutzvorschriften, um die Anforderungen hinsichtlich der verbindlichen Datenschutzvorschriften widerzuspiegeln, die nun ausdrücklich in der Datenschutz-Grundverordnung (Artikel 47) festgelegt sind. In der Datenschutz-Grundverordnung ist keine Vorschrift festgelegt, die der Vorschrift in Artikel 47 Absatz 2 der Datenschutz-Grundverordnung über den Inhalt von verbindlichen Standardvertragsklauseln ähnelt. Es kann dennoch argumentiert werden, dass einige Sicherheitsgarantien nach Artikel 47 Absatz 2 auch für die in Artikel 46 der Datenschutz-Grundverordnung genannten Standard-Datenschutzklauseln gelten.

[40] Nach Artikel 28 Absatz 3 und Artikel 28 Absatz 9 der Datenschutz-Grundverordnung sind die folgenden Elemente, die die Verarbeitung beschreiben, in jedem Fall im Vertrag festzulegen, der schriftlich abzufassen ist, einschließlich in elektronischer Form: Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien der betroffenen Personen, Pflichten und Rechte des für die Verarbeitung Verantwortlichen.

Rechte (nach Kapitel III Artikel 14-25) gewährt und gemäß dem Vertrag, der Dienstleistungsvereinbarung und ihren Anhängen festgelegt ist.

68 Jede Änderung des für den Cloud-Anbieter geltenden Rechts, die ihn daran hindert, die von der EU-Institution erhaltenen Anweisungen auszuführen und die Verpflichtungen gemäß dem Vertrag zu erfüllen, und die sich wahrscheinlich nachteilig auf die Garantien und Verpflichtungen in den Klauseln auswirkt, ist der EU-Institution vom Cloud-Anbieter unverzüglich mitzuteilen, sobald dem Cloud-Anbieter die Gesetzesänderung bekannt ist, sogar vor dem Inkrafttreten. In diesem Fall hat die EU-Institution das Recht, den Vertrag auszusetzen und/oder zu kündigen.

69 Der Cloud-Anbieter **informiert** die EU-Institution **umfassend über den physischen Standort** der vom Cloud-Anbieter und seinen Unterauftragsverarbeitern für die bereitgestellten Cloud-Dienste genutzten Server (einschließlich für Backups, Geschäftskontinuität und Übertragung) sowie über Standorte, von denen aus Fernzugriffe durchgeführt werden. Jede geplante Änderung eines Standorts ist der EU-Institution vom Cloud-Anbieter im Voraus mitzuteilen, bevor Daten am neuen Standort verarbeitet werden, damit die EU-Institution insbesondere prüfen kann, ob diese Änderung den Vertragsbedingungen und dem geltenden Recht entspricht[41]. Die EU-Institution hat das Recht, dieser Änderung zu widersprechen.

C - Anwendbares Vertragsrecht

70 Für die Klauseln/den Vertrag gilt EU-Recht und gegebenenfalls im Einklang mit dem EU-Recht, das Recht des EU-Mitgliedstaats, in dem die EU-Institution ihren Sitz hat oder jedes andere Recht des EU-Mitgliedstaats.

D - Abweichungen des Vertrags

71 Der Cloud-Anbieter und die EU-Institution nehmen keine Änderungen an den Klauseln vor. Dies schließt nicht aus, dass der Cloud-Anbieter und die EU-Institution weitere Vertragsbedingungen zu geschäftsbezogenen Themen aufnehmen, wenn diese vereinbart wurden und sofern sie nicht dem geltenden Datenschutzrecht widersprechen.

E - Pflichten nach Beendigung der Verarbeitung personenbezogener Daten

72 Bei Beendigung der Bereitstellung der **Datenverarbeitungsdienste** führt der Cloud-Anbieter und die Unterauftragsverarbeiter nach Wahl der EU-Institution folgende Aufgaben durch:

- Er gibt entweder **alle personenbezogenen Daten und Kopien dieser Daten** unverzüglich und in einem gemeinsam vereinbarten Format an die EU-Institution **zurück** oder **übermittelt sie an einen** von der EU-Institution selbst **bestimmten Zielort** oder
- er **löscht alle personenbezogenen Daten und bestätigt der EU-Institution diese Löschung**, sobald geprüft und bestätigt wurde, dass die Daten erfolgreich und vollständig an den neuen Verarbeiter der EU-Institution übermittelt wurden.

[41] Dies kann gemäß den Anforderungen der EU-Institution auch genauer definiert werden.

F – „Übertragbarkeit" der dem Cloud-Anbieter übermittelten Daten (als Recht der EU-Institution, diese Daten zu erhalten und an einen anderen Cloud-Anbieter zu übermitteln)

73 Der Cloud-Anbieter stellt sicher und kann belegen, dass die **Daten der EU-Institution von seinen Systemen und von Systemen jedes Unterauftragsverarbeiters zu anderen** von der EU-Institution gewählten **Anbietern übertragbar sind**, und zwar innerhalb von *[..]* Stunden und in einem *[in der Dienstleistungsvereinbarung und/oder ..]* festgelegten Format und nach schriftlicher Anweisung durch die EU-Institution. Der Cloud-Anbieter muss sicherstellen, dass der Dienst der EU-Institution in dieser Zeit vollständig zur Verfügung steht und das sie Zugriff darauf hat.

74 Der Cloud-Anbieter und alle Unterauftragsverarbeiter sichern die Daten der EU-Institution, bis sie unter der Kontrolle der EU-Institution an einen anderen Standort übertragen wurden.

G - Alleinige Verantwortung

75 Der Cloud-Anbieter verarbeitet die personenbezogenen Daten **nur auf Anweisung der EU-Institution** und **gemäß den dokumentierten Anweisungen und den Klauseln**. Kann er dies nicht einhalten, so informiert er die EU-Institution unverzüglich darüber. In diesem Fall hat die EU-Institution das Recht, den Vertrag auszusetzen oder zu kündigen.

H - Unterauftragsverarbeitung

76 Der Cloud-Anbieter stellt sicher, überwacht und kontrolliert im Fall einer Unterauftragsverarbeitung, dass die Aktivität, die von einem Unterauftragsverarbeiter durchgeführt wird, mindestens dem Schutzniveau für personenbezogene Daten und Grundrechte und Grundfreiheiten der betroffenen Personen entspricht, das der Cloud-Anbieter gemäß den Klauseln erfüllen muss.

77 Der Cloud-Anbieter stellt sicher, dass er im Fall einer Unterauftragsverarbeitung **die EU-Institution im Vorfeld darüber informiert hat**, **umfassende Informationen** über den zukünftigen Unterauftragsverarbeiter (in Bezug auf dessen Fähigkeit, ausreichende Sicherheiten zu bieten - wie in Abschnitt 4.2.1 beschrieben) und dessen zukünftige Rolle im Cloud-Dienst bereitgestellt hat und er das **vorherige schriftliche Einverständnis (spezifische oder allgemeine Genehmigung)** von der EU-Institution erhalten hat. Der Cloud-Anbieter **übermittelt** der EU-Institution unverzüglich **eine Kopie jedes Vertrags über eine Unterauftragsverarbeitung**, die er abschließt.

78 Wenn der Cloud-Anbieter seine Verpflichtungen gemäß den Klauseln, mit vorherigem Einverständnis der EU-Institution **(spezifische oder allgemeine schriftliche Genehmigung)** untervergibt, so tut er dies nur mit einer **schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter, in der sämtliche Verpflichtungen für den Unterauftragsverarbeiter wie für den Cloud-Anbieter gemäß den Klauseln gelten**.

[Diese Anforderung kann erfüllt werden, indem **der Unterauftragsverarbeiter** die relevanten Teile des Rahmenvertrags zwischen der EU-Institution und dem Cloud-Anbieter an den Vertrag zwischen dem Cloud-Anbieter und dem Unterauftragsverarbeiter **anhängt**.]

Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Cloud-Anbieter gegenüber der EU-Institution für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

Die Datenschutzaspekte des Unterauftragsverarbeiters unterliegen [dem Verordnungsvorschlag].

I - Verpflichtung des Cloud-Anbieters mit der EU-Institution zusammenzuarbeiten und sie zu informieren

79 Der Cloud-Anbieter bearbeitet alle Anfragen der EU-Institution in Bezug auf die Verarbeitung personenbezogener Daten durch den Cloud-Anbieter unverzüglich und ordnungsgemäß.

80 Der Cloud-Anbieter informiert die EU-Institution unverzüglich über für ihn oder einen Unterauftragsverarbeiter geltendes Recht, das ihn daran hindert, personenbezogene Daten nur auf Anweisung der EU-Institution zu verarbeiten oder das verhindert, ein Audit des Cloud-Anbieters oder eines Unterauftragsverarbeiters durchzuführen.

81 In diesem Fall hat die EU-Institution das Recht, die Aussetzung der Datenverarbeitung durch den Cloud-Anbieter und/oder die Beendigung des Vertrags zu verlangen.

82 Der Cloud-Anbieter informiert die EU-Institution

(i) rechtzeitig über zukünftige Änderungen hinsichtlich der Cloud-Dienste, wie die Einführung weiterer Funktionen;

(ii) über zukünftige Änderungen der Infrastruktur und der Verfahren mit möglichen Folgen für den Dienst und rechtzeitig und unter Wahrung der Vertraulichkeit über die Ergebnisse relevanter Sicherheitsaudits;

(iii) über rechtlich verbindliche Anträge auf Offenlegung personenbezogener Daten von einer Strafverfolgungsbehörde, im Rahmen der in den Klauseln festgelegten Bedingungen und im Einklang mit dem geltenden Recht;

(iv) über Sicherheitsvorfälle (und bietet angemessene Unterstützung für eine geeignete Bewältigung möglicher Datenschutzrisiken durch diese Vorfälle) im Rahmen der in den Klauseln festgelegten Bedingungen und im Einklang mit dem geltenden Recht;

(v) unverzüglich über Anfragen in Bezug auf die Ausübung der Rechte betroffener Personen, die er direkt von den betroffenen Personen erhält. In diesen Fällen antwortet der Cloud-Anbieter nicht auf solche Anfragen, sofern er in dieser Hinsicht keine andere Anweisung von der EU-Institution erhalten hat, und liefert der EU-Institution die erforderlichen Informationen und Instrumente, um die personenbezogenen Daten von betroffenen Personen hinsichtlich Zugang, Löschen, Korrektur, Blockieren usw. zu verwalten.

J - Verpflichtung, den EDSB zu informieren und mit ihm zusammenzuarbeiten

83 Dem Cloud-Anbieter ist bekannt, dass der EDSB das Recht hat, einen Besuch, ein Audit oder eine Kontrolle des Cloud-Anbieters und jedes Unterauftragsverarbeiters durchzuführen[42], und zwar unter den gleichen Bedingungen, die auch für ein Audit der EU-

[42] Damit das Audit der Verarbeitung des Cloud-Anbieters (als Auftragsverarbeiter) sowohl von der EU-Institution als auch vom EDSB durchgeführt werden kann, ist die Verpflichtung nach Artikel 30 der Datenschutz-

Institution selbst gemäß [dem Verordnungsvorschlag] gelten. Bei dem Audit wird geprüft, ob bei der Verarbeitung der dem Cloud-Anbieter von der EU-Institution anvertrauten Daten die Vertragspflichten und die geltenden Datenschutzrichtlinien und -grundsätze eingehalten werden.

84 Der Cloud-Anbieter kooperiert bei diesen Kontrollen ordnungsgemäß und kostenlos.

K - Sicherheitsmaßnahmen

85 Der Cloud-Anbieter stellt sicher, dass er über einen **ordnungsgemäßen IT-Sicherheitsmanagement-Rahmen**[43] verfügt und die entsprechenden technischen Maßnahmen und Sicherheitsmaßnahmen des relevanten Rahmens sowie die im Vertrag und/oder der Dienstleistungsvereinbarung spezifizierten Maßnahmen vor der Verarbeitung der Daten im Auftrag der EU-Institution durchgeführt hat und dass er den Rahmen und das Risikomanagement für die Dauer des Vertrags ordnungsgemäß durchführt.

86 Bei der Beurteilung des angemessenen Schutzniveaus muss der Cloud-Anbieter insbesondere die Risiken berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

87 Der Cloud-Anbieter führt eine Dokumentation hinsichtlich des Rahmens und der durchgeführten Sicherheitsmaßnahmen und technischen Maßnahmen und bietet der EU-Institution angemessenen Zugang zu dieser Dokumentation, um die Anforderungen [des Verordnungsvorschlags] zu erfüllen.

L - Meldung von Datenschutzverletzungen

88 Der Cloud-Anbieter führt geeignete Mechanismen ein, um unverzüglich und effektiv auf Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten zu reagieren. Hierzu gehören Meldemechanismen, die sicherstellen, dass **die EU-Institution über alle**

Grundverordnung äußerst wichtig, die folgendes besagt: „Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

a) den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

b) die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

c) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

d) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

3. Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann."

[43] Siehe auch die Leitlinien des EDSB in Fußnote 51

möglichen Verletzungen des Schutzes personenbezogener Daten informiert wird[44] (Sicherheitsvorfälle, die die im Auftrag der EU-Institution verarbeiteten personenbezogenen Daten betreffen).

89 Der Cloud-Anbieter meldet der EU-Institution unverzüglich relevante Verletzungen des Schutzes personenbezogener Daten und, wenn möglich, rechtzeitig, damit die EU-Institution, falls dies nach den Anforderungen [des Verordnungsvorschlags] erforderlich ist, die betroffenen Personen unverzüglich und den EDSB innerhalb von 72 Stunden, nachdem der Cloud-Anbieter die Verletzung festgestellt hat, informieren kann.

90 Der Cloud-Anbieter liefert der EU-Institution mindestens folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

91 Der Cloud-Anbieter arbeitet mit den EU-Institutionen zusammen, damit alle relevanten Verpflichtungen [im Verordnungsvorschlag] über Verletzungen des Schutzes personenbezogener Daten erfüllt werden.

92 Weitere Einzelheiten über den Inhalt und die Form der Meldung werden in der Dienstleistungsvereinbarung festgelegt.

M - Audit (während und nach Beendigung der Datenverarbeitungstätigkeiten)

93 Der Cloud-Anbieter und der Unterauftragsverarbeiter führen Mechanismen ein, um die **Protokollierung der Verarbeitungsvorgänge**, die an den personenbezogenen Daten im Auftrag der EU-Institution durchgeführt werden, sicherzustellen.

94 Der Cloud-Anbieter erlaubt und beteiligt sich an möglichen von der EU-Institution durchgeführten **Audits** seiner Verarbeitungstätigkeiten gemäß den relevanten Vorschriften [des Verordnungsvorschlags][45]. Das Audit kann von einem von der EU-Institution ausgewählten **Dritten** durchgeführt werden, der über die notwendigen professionellen Qualifikationen verfügt und der Verschwiegenheit unterliegt.

95 Der Cloud-Anbieter und der Unterauftragsverarbeiter erlauben und beteiligen sich auf Anfrage der EU-Institution und/oder des EDSB an den Audits ihrer datenverarbeitenden

---

[44] Einige Leitlinien zu Verletzungen des Schutzes personenbezogener Daten finden sich im aktuellen Entwurf einer Stellungnahme der WP29, abrufbar unter: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Die Datenschutz-Grundverordnung enthält in den Artikeln 33 und 34 spezifische Vorschriften über die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und die betroffene Person.

[45] Artikel 28 Absatz 3 Buchstabe h der Datenschutz-Grundverordnung.

Betriebe, hinsichtlich der vom Cloud-Anbieter durchgeführten Maßnahmen zur Erfüllung seiner Verpflichtungen nach Beendigung der Verarbeitung personenbezogener Daten.

N - Zugriff für Strafverfolgungsbehörden

96 Nach Artikel 2 des Protokolls über die Vorrechte und Befreiungen der Europäischen Gemeinschaften sind die Archive der Union unverletzlich. Als EU-Einrichtung unterliegt die EU-Institution den Vorrechten und Befreiungen der Europäischen Gemeinschaften, insbesondere hinsichtlich der Unverletzlichkeit der Archive (einschließlich des physischen Standorts der Dienste) und der Datensicherheit.

97 Der Cloud-Anbieter informiert die EU-Institution unverzüglich über alle rechtlich verbindlichen Anträge auf Offenlegung von im Auftrag der EU-Institution verarbeiteten personenbezogenen Daten durch eine Strafverfolgungsbehörde (z. B. eines nationalen Staatsanwalts eines Mitgliedstaats), einschließlich aus Nicht-EU-Staaten.[46] Der Cloud-Anbieter gewährt keinen Zugang zu personenbezogenen Daten, sofern dies nicht von der AIPN (*Autorité investie du pouvoir de nomination*) der betreffenden EU-Institution genehmigt wurde.

O - Dienstleistung

98 Der Cloud-Anbieter betreibt den Dienst gemäß einer Dienstleistungsvereinbarung, die fester Bestandteil dieses Vertrags ist.

P - Vertraglicher Rechtsbehelf

99 Bei Abweichungen von oder Verstößen gegen die oben angeführten Punkte kann die EU-Institution den Vertrag fristlos und unbeschadet von Schadenersatzansprüchen kündigen.

4.3. Betreiben des Cloud-Dienstes

100 Während des Betriebs von Cloud-Diensten sind Sicherheitsgarantien für den Schutz personenbezogener Daten und zur Einhaltung der geltenden Datenschutzgrundsätze und -pflichten erforderlich[47].

101 Die Angelegenheiten, die dem Cloud-Anbieter als Auftragsverarbeiter übertragen werden, sollten im Vertrag beschrieben werden (siehe Abschnitt 4.2), wobei einige der operationellen Aspekte gewöhnlich in einer Dienstleistungsvereinbarung festgelegt (siehe Abschnitt 4.3.2) und geregelt werden müssen. Was direkt von der EU-Institution durchgeführt werden muss (siehe Abschnitt 4.3.1), hängt stark von dem Cloud-Dienst und dem Bereitstellungsmodell ab (siehe die Definitionen in Anhang 3)

[46] Zugang für Empfänger aus Mitgliedstaaten (wie dem oben genannten Staatsanwalt) wird von der EU-Institution nur gewährt, wenn die Bedingungen im EU-Recht für eine solche Offenlegung erfüllt sind.

[47] Die EU-Institution bleibt weiterhin als für die Verarbeitung Verantwortlicher voll verantwortlich für die Einhaltung von Vorschriften, auch wenn die Verarbeitung von einem Cloud-Anbieter durchgeführt wird. Hierzu gehören: Rechtmäßigkeit, Erforderlichkeit und Angemessenheit; Zweckbindung und -begrenzung; Qualität der Daten, einschließlich Datenaufbewahrungsfristen; Informieren der betroffenen Personen und Rechte der betroffenen Personen (Zugang, Berichtigung, Löschen, Sperrung); mögliche Übertragungen; gegebenenfalls Vorschriften zu internen Kommunikationsnetzen; Zugang durch die Aufsichtsbehörde sowie weitere geltende Vorschriften.

4.3.1. Aufgaben, die direkt der EU-Institution unterliegen

102 Die EU-Institution erstellt die organisatorische interne Infrastruktur, die notwendig ist, um sicherzustellen, dass der Cloud-Computing-Dienst im Einklang mit den Datenschutzvorschriften betrieben wird[48].

103 Zu den Aufgaben, die weiterhin direkt der EU-Institution unterliegen, gehören:

- die Einhaltung der Datenschutzbestimmungen als für die Verarbeitung Verantwortlicher, einschließlich:
  - der (erneuten) Bewertung und Bewältigung der Datenschutzrisiken;
  - Datenschutzgarantien, IT-Sicherheitskontrollen, Zielvorgaben und Verwaltung;
  - Bearbeitung von Anfragen betroffener Personen;
  - Meldung von Verletzungen des Schutzes personenbezogener Daten an den EDSB und die betroffenen Personen;
  - Datenschutzaudits beim Cloud-Anbieter;
  - die behördlichen Datenschutzbeauftragten und ihre Rolle.
- IT-Steuerung und -Verwaltung
- Vertragsverwaltung
- Dienstleistungsdefinition und Verwaltung
- Datenkontrolle und -verwaltung (politische Maßnahmen und Pläne z. B. für den Datenzugriff, die Speicherung, das Löschen, die Rückführung vom Cloud-Anbieter)
- Audits (im Allgemeinen) des Cloud-Anbieters

Für diese Aufgaben sind geeignete Experten erforderlich, vor allem in der Vertrags-, IT-, IT-Sicherheits- und Datenschutzverwaltung.

104 **Geeignete Ressourcen im IT-Bereich** können auch im SaaS-Dienstmodell in öffentlichen Cloud-Diensten noch erforderlich sein, welches das höchste Maß an Befugnisübertragung darstellt. In diesem Fall ist immer noch Personal erforderlich, das die Geeignetheit der IT-Architektur und Aspekte des Aufbaus und die IT-Sicherheitsmaßnahmen versteht und prüfen kann, auch wenn kein Personal mehr für die Einrichtung der IT-Infrastruktur und den spezifischen Dienst benötigt wird, um zu bewerten, ob die Lösung nach den Datenschutzanforderungen geeignet ist.

105 **Maßnahmen** und **Verfahren** zur Durchführung dieser Aufgaben sollten für mögliche Audits **beschrieben werden und zur Verfügung stehen**.

106 Hinsichtlich der Vertragsverwaltung sollte die EU-Institution beispielsweise **ein Verzeichnis der vom Cloud-Anbieter gemeldeten Vereinbarungen zur**

[48] Siehe in dieser Hinsicht als Quelle für bewährte Praktiken und als Prüfliste, auch einschließlich **Schulungen, Überwachung und Auditprogramme**, die Stellungnahme der Artikel-29-Datenschutzgruppe 02/2014 vom 27. Februar 2014 zu einem Regelwerk für die Anforderungen an verbindliche unternehmensinterne Regelungen, die den Datenschutzbehörden der EU vorgelegt werden, und an Regelungen für den grenzüberschreitenden Datenschutz, die den von der APEC anerkannten „CBPR Accountability Agents“ vorgelegt werden, abrufbar unter:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.

Unterauftragsverarbeitung führen, das **mindestens jährlich aktualisiert** werden sollte. Das Verzeichnis ist dem EDSB auf Verlangen vorzulegen.

107 Die **behördlichen Datenschutzbeauftragten** der EU-Institution haben die Aufgabe, die EU-Institution darüber zu beraten, wie sie das Datenschutzgesetz und die Grundsätze einhalten kann, und sollen Hilfe im Einklang mit dem Gesetz bieten[49]. Sie sollten stets **angemessen involviert** werden, vom Beginn des Prozesses und in allen Schritten, beim Aufbau und dem Betrieb des Cloud-Dienstes, einschließlich:

- bei der Bewertung von Datenschutzrisiken, Festlegung von Einhaltungsanforderungen und relevanten Sicherheitsgarantien;
- wenn eine DSFA obligatorisch durchzuführen ist;
- beim Aufsetzen der Vertragsklauseln sowie des Inhalts der Dienstleistungsvereinbarung;
- beim Umgang mit Verletzungen des Schutzes personenbezogener Daten;
- bei der Durchführung von Datenschutzaudits.

108 Die EU-Institution sollte auch geeignete **Schulungen** zu Datenschutzvorschriften für personenbezogene Daten für ihr Personal in Relation zur Nutzung des Cloud-Dienstes und zur Überwachung der Einhaltung der Datenschutzbedingungen durch den Dienst, wie sie im Vertrag festgelegt sind, anbieten. Zu den hiervon betroffenen Mitarbeitern gehören: Entscheidungsträger, Verfahrenseigner, Vertragsmanager, Mitarbeiter, die permanenten oder regelmäßigen Zugriff auf personenbezogene Daten haben, die an der Sammlung und der Verarbeitung personenbezogener Daten mitwirken, sowie IT-Personal, das an der Entwicklung und dem Einsatz von Instrumenten für die Verarbeitung personenbezogener Daten beteiligt ist.

109 Die EU-Institution sollte regelmäßig und unter erforderlichen spezifischen Umständen mögliche **Audits** planen und gegebenenfalls die Risiken der Verarbeitung berücksichtigen. Sie kann sie auch von **Dritten** durchführen lassen, die über geeignete Cloud-bezogene Zertifizierungen und Normen zugelassen sind. Folgende Aspekte sind hierbei wichtig:

- Das Auditprogramm muss alle Aspekte der Datenschutzanforderungen für personenbezogene Daten umfassen und Methoden bieten, die sicherstellen, dass korrektive Maßnahmen durchgeführt werden.
- Die Ergebnisse aller Audits sollten den behördlichen Datenschutzbeauftragten und der Verwaltung der EU-Institution mitgeteilt werden (z. B. dem Direktor der Agentur der EU). Der EDSB erhält auf Verlangen eine Kopie dieser Audits.
- Im Auditplan sollte vorgesehen werden, dass der EDSB im Vorfeld informiert wird, damit er an den Audits teilnehmen kann, wenn er möchte und die Ergebnisse der Audits erhält.

[49] Zur (erweiterten) Rolle der behördlichen Datenschutzbeauftragten gemäß der Datenschutz-Grundverordnung siehe insbesondere die Artikel 38 und 39.

4.3.2. Die Dienstleistungsvereinbarung

110 **Die Dienstleistungsvereinbarung ist ein wesentlicher Bestandteil des Vertrags und beschreibt genauer die erwarteten Dienste und deren Grad.** Es liegt im Ermessen der EU-Institution, ob diese Vorschriften im Haupttext des Vertrags oder in der Dienstleistungsvereinbarung aufgeführt werden.

111 Der Inhalt der Dienstleistungsvereinbarung hängt auch klar von dem Dienst und dem Bereitstellungsmodell ab, mit Auswirkungen **auf die jeweilige Zuweisung der direkten Kontrolle und der relevanten Verantwortlichkeiten** an die EU-Institution und den Cloud-Anbieter.

112 In der Dienstleistungsvereinbarung sollten mindestens folgende Elemente und Bereiche beschrieben und festgelegt werden[50]:

- Detaillierte **Beschreibung des bereitgestellten Dienstes**.

  Hier wird detailliert beschrieben, was im Vertrag fehlt. Unter anderem sollten die Zwecke der Verarbeitung personenbezogener Daten klar definiert werden.

- Klare **Zuweisung der Verantwortlichkeiten** (wie den Grad der Dienstleistung – wer macht was, einschließlich hinsichtlich der Sicherheitsmaßnahmen) zwischen der EU-Institution und dem Cloud-Anbieter, auf der Grundlage, wer „de facto" für einen bestimmten Punkt verantwortlich ist.

- **Kommunikationskanäle** zwischen der EU-Institution und dem Cloud-Anbieter, einschließlich des Servicedesks des Cloud-Anbieters.

- **Leistung/Qualität und Berichterstattung des Dienstes:**

  Klare Definitionen der Leistung, Überwachung und Berichterstattung des Dienstes müssen über messbare Indikatoren und Überwachungs- und Berichtsinstrumente vereinbart werden.

- Verlangte **Kapazität**.

  Dies bezieht sich beispielsweise im Fall von SaaS oder PaaS auf Instanzen und Umgebungen (Entwicklung, Tests, Produktion usw.), Speicherplatz, Anzahl der Nutzer und Verwaltungskonten usw.

- **Verfügbarkeit**

  Verfügbarkeitsziele, in unterschiedlichen Zeitbändern und Zeiträumen im Jahr oder die Nutzung von Typologie, verfügbaren Messgrößen, durchschnittliche Zeit zwischen zwei Vorfällen, Wartungsfenster usw. Die Verfügbarkeit sollte für alle geforderten Umgebungen festgelegt werden. Eine gemeinsame Definition sollte sorgfältig ausgearbeitet werden, um Missverständnisse zu vermeiden.

- **Backupmaßnahmen, Notfallmanagement, Notfallwiederherstellung und Geschäftskontinuität.**

---

[50] Weitere Leitlinien zu Dienstleistungsvereinbarungen für Cloud-Dienste finden sich in Dokumenten eines Konsortiums der Industrie unter der Koordinierung der Kommission: "Cloud Service Level Agreement Standardisation Guidelines" – Cloud Select Industry Group – Brüssel, 24. June 2014, abrufbar unter:

https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

Diese Leitlinien der Industrie sollten nicht als maßgebende Quelle betrachtet werden und spiegeln nicht unbedingt die Ansicht des EDSB wider.

Unter anderem müssen Aufbewahrungsfristen zusammen mit Maßnahmen, die durchzuführen sind, wenn die Aufbewahrungsfrist endet, festgelegt werden. Klare Verfahren zur Rückführung der Daten zu jeder Zeit, einschließlich des Datenformats, sollten vereinbart und geprüft werden.

- **Änderungsmanagement**

  Änderungsmanagementverfahren, die für den Cloud-Dienst relevant sind (von der EU-Institution verlangt, wie neue Funktionen, Änderungen der Dienstleistungsvereinbarung, und Änderungen, die der Cloud-Anbieter vorschlägt, z. B. in einem IaaS-Angebot) müssen festgelegt und vereinbart werden, so dass die EU-Institution die Kontrolle über die Mittel und Verfahren zur Datenverarbeitung behält.

- **Sicherheitsmaßnahmen und Garantien**

  Die EU-Institution muss spezifizieren, welche Sicherheitsgarantien der Cloud-Anbieter einführen muss, und die Geeignetheit der vom Cloud-Anbieter angebotenen Sicherheitsgarantien prüfen. Dies sollte Teil des Ergebnisses der durchgeführten Bewertung der Datenschutzrisiken sein und Folgendes umfassen:

  - Definition von Sicherheitszielen/Garantiekriterien/Garantiegrad, möglicherweise mit Bezug auf vorhandene bewährte Praktiken und Standards.
  - Definition spezifischer Sicherheitsmaßnahmen/-kontrollen.

  Eine effektive und erforderliche Verschlüsselung personenbezogener Daten sollte Teil dieser Maßnahmen sein.

  In Abschnitt 4.4 finden sich weitere Details zu möglichen Sicherheitskontrollen.

- **Datenschutzgarantien**

  Die EU-Institution legt in der Dienstleistungsvereinbarung neben den Sicherheitsmaßnahmen spezifische Vorschriften zum Datenschutz fest und spezifiziert oder fügt gegebenenfalls Garantien hinzu, auf die in den Klauseln nicht Bezug genommen wird.

- **Sicherheitsvorfälle und Verletzungen des Schutzes personenbezogener Daten**

  Weitere Details (einschließlich vereinbarter Meldekanäle und -formen) sollten neben den bereits in den Klauseln festgelegten Aspekten beschrieben werden. Siehe auch Fußnote 44.

- **Überwachung und Kontrolle, einschließlich Forensik**

  Der Cloud-Anbieter muss die Verarbeitungsvorgänge der personenbezogenen Daten aufzeichnen und sie gegebenenfalls der EU-Institution zur Verfügung stellen.

  Funktionen und Berichte, mit denen die EU-Institution die Kontrolle behält, sollten festgelegt werden, sowie Modalitäten und Bedingungen für Audits/Kontrollen der Geschäftsräume des Cloud-Anbieters und seiner Rechenzentren durch die EU-Institution und den EDSB.

  Sollten forensische Untersuchungen durch die EU-Institution oder den EDSB erforderlich sein, sollte der Cloud-Anbieter über Möglichkeiten zur effizienten und effektiven Kooperation verfügen.

- **Beendigung des Dienstes und Übergabe**

  Der Zeitplan und die Unterstützung bei der Beendigung des Dienstes und der Übergabe, einschließlich der Datenrückführung oder der Datenübertragung zu einem neuen Cloud-Anbieter, sollten festgelegt werden. Zur Unterstützung sollte die Datenrückführung oder

die Übergabe an einen neuen Dienstanbieter gehören. Verfahren zur dauerhaften Löschung nach der Übergabe sind einzubeziehen. Mögliche Vorschriften für relevante Überprüfungen durch Aufzeichnungen und Prüfung der Geschäftsräume sollten ebenfalls eingeschlossen werden.

- **Sicheres Löschen und Entsorgung**

  Der Cloud-Anbieter muss einen sicheren Löschmechanismus technisch gewährleisten, z. B. durch Zerstörung, Entmagnetisierung oder Überschreiben, und der EU-Institution die durchgeführte Zerstörung, einschließlich aller Backup-Kopien, belegen.

- **Strafen** für die Nichterfüllung der Dienstleistungsvereinbarung.

  Neben dem Recht auf Schadenersatz für Schäden, die infolge einer Verletzung des Vertrags oder der Dienstleistungsvereinbarung durch den Cloud-Anbieter auftreten, sollte die EU-Institution das Recht haben, den Vertrag auszusetzen und/oder zu kündigen.

- Verfahren zur **Überarbeitung der Dienstleistungsvereinbarung**

  Es sollte ein Verfahren zur Überarbeitung der Dienstleistungsvereinbarung geben. Der Cloud-Anbieter darf jedoch in keinem Fall einseitig Änderungen an der Dienstleistungsvereinbarung vornehmen.

4.4. IT-Sicherheitsmaßnahmen

113 Die Sicherheitsmaßnahmen und relevante Rechenschaftspflichten sollten sich widerspiegeln in:

- dem Vertrag (einschließlich der Dienstleistungsvereinbarung), bei den Maßnahmen, für die der Cloud-Anbieter verantwortlich ist, oder
- in internen Maßnahmen/Verfahren, sofern die EU-Institution direkt für sie verantwortlich ist.

114 Eine nicht erschöpfende **Liste möglicher IT-Sicherheitsmaßnahmen** zur Minderung spezifischer Risiken von Cloud-Computing-Diensten wird nachfolgend in Empfehlung **R2** bezogen auf diese Risiken aufgeführt. Die Risiken werden entsprechend der Liste der Risiken in Anhang 4 bezeichnet. Es werden auch andere nicht IT-bezogene Garantien beschrieben, um die risikobasierte Methodik aufzuzeigen, mit der die gleichen Risiken mit unterschiedlichen Folgen gemildert werden.

115 Der Wert ihrer Fähigkeit, ein Risiko zu mindern, ist nicht absolut, soll jedoch die Wirkung der verschiedenen Garantien in „durchschnittlichen“ Situationen bewerten.

116 Die vollständige Liste der Garantien sollte das Ergebnis der Bewertung der Datenschutzrisiken sein, einschließlich einer Bewertung der IT-Sicherheitsrisiken[51] (die natürlich auch die Risiken für extern vergebene Informationssysteme berücksichtigt).

117 Es wird in jedem Fall empfohlen, auf die vorhandenen IT-Sicherheitsmaßnahmen und Praktiken in den EU-Institutionen und verfügbare IT-Sicherheitsstandards und bewährte

[51] Weitere Details finden sich in den Leitlinien des EDSB zu "Security Measures for Personal Data Processing": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf und einem Brief des EDSB zur Klärung der Beziehung zwischen einer DSFA und dem Informationssicherheits-Risikomanagement:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Accountability/16-04-22_Mail_DPOs_WW_EN.pdf.

Praktiken, die von der Industrie und anderen Organisationen, wie der Internationalen Organisation für Normung und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), herausgegeben wurden, zurückzugreifen. Siehe auch Anhang 5 für eine Reihe von Referenzen.

R2 - Vertraulichkeits- und Integritätsrisiken bei über das Internet übertragenen Daten

Der erforderliche Dienst wird sich außerhalb des Rechenzentrums der EU-Institution befinden und nicht über Standleitungen erreichbar sein. Es muss eine andere Kommunikationsverbindung geschaffen werden, sehr wahrscheinlich das Internet, wie bei den meisten Cloud-Anbietern.

Zu den möglichen Sicherheitsgarantien gehören:

- Ausschließliche Nutzung von Cloud-Anbietern, die spezielle Leitungen für ihre Dienste + eine effektive Verschlüsselung anbieten;

  Grad der Risikominderung: hoch, sehr hoch

- Einrichtung von virtuellen privaten Netzen (Virtual Private Networks, VPN) über das Internet, gegebenenfalls Nutzung von Verschlüsselung und Authentifizierung auch auf der Ebene mehrerer Protokolle;

  Grad der Risikominderung: hoch

- Nutzung einer starken Verschlüsselung (z. B. HTTPS mit effektiver TLS-Implementierung);

  Grad der Risikominderung: mittel

R3 - Mögliche mangelnde Verfügbarkeit aufgrund von beschränktem oder keinem Zugriff auf das Internet

Zu den möglichen Sicherheitsgarantien gehören:

- Mehrere Internetprovider mit Hot-Swap;

  Grad der Risikominderung: hoch

- Redundante Leitungen desselben Providers;

  Grad der Risikominderung: mittel

- Keine Nutzung des Internets sondern von Standleitungen als Verbindung vom Nutzer zum Cloud-Anbieter;

  Grad der Risikominderung: sehr hoch

R4 - Risiken der Internetüberwachung (ISP + Internet-Backbone und Routing-Infrastruktur)

Zu den möglichen Sicherheitsgarantien gehören:

- Beschränkung zukünftiger Cloud-Anbieter auf EU-Staaten

  Grad der Risikominderung: mittel

- Keine Nutzung des Internets sondern von Standleitungen als Verbindung vom Nutzer zum Cloud-Anbieter; nur im Hoheitsgebiet der EU.

  Grad der Risikominderung: sehr hoch

- Nutzung einer wirksamen End-to-End-Verschlüsselung (z. B. HTTPS mit effektiver TLS-Implementierung);

  Grad der Risikominderung: hoch

R6 - Mögliche Verletzbarkeit bei Zugangsmaßnahmen und Sicherheitskontrollen

Dieses Risiko besteht insbesondere im Falle von Mandantenfähigkeit: öffentliche oder Community-Cloud.

Zu den möglichen Sicherheitsgarantien gehören:

- Vom Cloud-Anbieter Belege für die Einführung relevanter effektiver Sicherheitsmaßnahmen verlangen, die für die Art der verarbeiteten personenbezogenen Daten geeignet sind, durch:
  - Selbstauskunft über die Einhaltung der Cloud-Sicherheitsstandards und bewährter Praktiken

    Grad der Risikominderung: niedrig
  - Bereitstellung von Garantien durch akkreditierte Dritte (Cloud-Sicherheitszertifikate für dieses Risiko und die für die Art der verarbeiteten personenbezogenen Daten geeignet sind).

    Grad der Risikominderung: mittel/hoch, in Abhängigkeit der Vertrauenswürdigkeit der Zertifizierung.

  Diese Garantie sollte während der gesamten Dienstbereitstellung und während der Beendigung des Dienstes und der Übergabe gewährt werden.
- Den Cloud-Anbieter auffordern, die Computing-Umgebung von der anderer Nutzer zu isolieren:
  - physische Isolierung wie die Nutzung unterschiedlicher Server für unterschiedliche Nutzer

    Grad der Risikominderung: hoch
  - Nutzung unterschiedlicher virtueller Maschinen in einem Server für unterschiedliche Nutzer

    Grad der Risikominderung: mittel
- Geeignete Verschlüsselung für Daten bei der Speicherung und Übertragung innerhalb der Cloud-Infrastruktur zwischen unterschiedlichen Sicherheitsbereichen. Die Robustheit der Verschlüsselung und das Kernmanagement sollten auf der Grundlage der Risikobewertung bestimmt werden. Die Möglichkeit, die Verschlüsselung der Daten bei der Verarbeitung beizubehalten ist noch Gegenstand der Forschung, die EU-Institution wird jedoch aufgefordert, den aktuellen Stand zu prüfen. Werden die Verschlüsselungsschlüssel vom Cloud-Anbieter verwaltet, sind geeignete Sicherheitsmaßnahmen zu deren Schutz wichtig, damit die Verschlüsselung wirksam ist[52].

[52] Es können unter anderem Papiere der ENISA verwendet werden, um den Verschlüsselungsalgorithmus und die Schlüssel zu bewerten:

- Study on cryptographic protocols (Studie zu Verschlüsselungsprotokollen) und Algorithms, key size and parameters report 2014 (Bericht über Algorithmen, Schlüsselgröße und Parameter von 2014)

Grad der Risikominderung: hoch, sehr hoch in Kombination mit einer guten Isolierung gegenüber Daten anderer Nutzer

R12 - Mangelnde geeignete Prüfbarkeit (durch die EU-Institution oder beauftragte Dritte) und mangelnde Überwachung und Untersuchungen durch die zuständigen Behörden, einschließlich der Forensik

Die EU-Institution sollte sicherstellen, dass der Cloud-Anbieter einen geeigneten Grad an Prüfbarkeit garantiert, um auf Anfrage die Einhaltung der Vorschriften und die Effizienz nachweisen und effektiv auf Anfragen reagieren zu können. Einige Voraussetzungen:

- Die gesamte Verarbeitung von personenbezogenen Daten müssen in Log-Dateien sicher aufgezeichnet werden, um die Verarbeitungsvorgänge und Verantwortlichkeiten zu prüfen, und diese Log-Dateien müssen der EU-Institution für Kontrollen zur Verfügung gestellt werden. Die Log-Dateien müssen mit den gleichen Maßnahmen wie die ursprünglichen personenbezogenen Daten geschützt werden.
- Entwicklung technischer Möglichkeiten, Log-Dateien zu verwalten und zu analysieren.

Zu den möglichen Sicherheitsgarantien gehören:

- Die EU-Institution oder jeder von der EU-Institution beauftragte Dritte führt regelmäßige Audits der Infrastruktur für den beauftragten Dienst des Cloud-Anbieters durch.

  Grad der Risikominderung: im Prinzip sehr hoch, ist jedoch abhängig von der Prüfbarkeit und Komplexität der IT-Infrastruktur des Cloud-Anbieters.

- Der Cloud-Anbieter belegt, dass regelmäßige Audits von einem akkreditierten/vertrauenswürdigen Dritten durchgeführt werden. Der Dritte sollte nach einem vertrauenswürdigen Cloud-Standard/Zertifizierung akkreditiert sein und relevante Risiken und für die Art der verarbeiteten personenbezogenen Daten geeignet angehen.

  Grad der Risikominderung: hoch

- Der Cloud-Anbieter weist nach, dass regelmäßig interne Audits/Selbsteinschätzungen durchgeführt werden, die relevante Risiken angehen und für die Art der verarbeiteten personenbezogenen Daten geeignet sind.

  Grad der Risikominderung: niedrig; mittel in einem anerkannten Rahmen für Verhaltensregeln

R14 - Mögliche Anbieterbindung (Tätigkeitsverkauf oder -stopp wegen Bankrott oder aus anderen Gründen): Daten sind nicht verfügbar oder andere Datenschutzbestimmungen/anderes anwendbares Recht

Zu den möglichen Sicherheitsgarantien gehören:

- Entwickeln und regelmäßiges Testen einer Auffanglösung, um die entsprechenden Geschäftsvorgänge der EU-Institution zu unterstützen. Regelmäßige Backups außerhalb der Geschäftsräume des Cloud-Anbieters (entweder in den Geschäftsräumen der EU-Institution oder durch einen anderen Cloud-Anbieter) müssen durchgeführt werden, um mögliche Datenverluste zu minimieren.

  Grad der Risikominderung: hoch

- Entwickeln und testen eines Migrationsplans für den Wechsel des Cloud-Anbieters.

  Höhe der Risikominderung: erforderlich, aber nicht ausreichend

R18 - Andere für das Cloud-Computing spezifische IT-Sicherheitsrisiken (siehe auch Anhang 4).

Hier wird nur ein Beispiel angeführt. Wir bitten Sie, für alle anderen Cloud-spezifischen IT-Sicherheitsrisiken Ihren Sicherheitsbeauftragten und spezialisierte Quellen wie in Anhang 5 zu konsultieren.

Verletzbarkeit in Verbindung mit der Nutzung von Client-Software

Der Cloud-Dienst kann die Nutzung von (normalerweise Thin) Clients beinhalten, wie kommerzielle Browser oder andere Clients oder Apps für mobile Endgeräte, die vom Cloud-Anbieter entwickelt wurden. Hierdurch können damit zusammenhängende Risiken durch die Verletzlichkeit des Geräts, auf dem der Client genutzt wird, entstehen. Dies ist nicht nur ein Cloud-spezifisches Risiko, sondern könnte eine Änderung hinsichtlich des derzeit genutzten IT-Systems darstellen und somit neue Risiken mit sich bringen, die auch Auswirkungen auf andere Systeme und die Verwaltung personenbezogener Daten durch die EU-Institution haben können.

Zu den möglichen Sicherheitsgarantien gehören:

- Bei der Wahl und Konfiguration des Browsers sollte die EU-Institution bei den Funktionen/Schwächen besonders auf die Einhaltung der Privatsphäre achten, z. B.:
  - die Verschlüsselung des Kanals für die HTTP-Kommunikation und insbesondere die Unterstützung starker Protokolle und Verschlüsselungen;
  - andere Verarbeitungsvorgänge an den übertragenen/empfangenen Daten, die nicht für die Nutzung des Cloud-Dienstes notwendig sind (einschließlich Übertragungen von Daten an Empfänger, die nicht zum Cloud-Dienst gehören)
- Die EU-Institution könnte spezielle Browser für den Cloud-Dienst benutzen, damit die Auswirkungen von Angriffen von anderen Webseiten begrenzt werden können. Eine stärkere Maßnahme wäre die Nutzung eines virtuellen Desktops, der per Fernzugriff mit einem sicheren speziellen Server verbunden ist, auf dem ein spezieller Browser installiert ist.
- Liefert der Cloud-Anbieter seinen eigenen Client für den Cloud-Dienst, könnte die EU-Institution verlangen, dass der Cloud-Anbieter sich um die Sicherheitsrisiken in Verbindung mit dem Client kümmert.
- Besondere Vorsicht sollte bei der Sicherheitsverwaltung von Apps für mobile Endgeräte als Cloud-Clients gelten[53], da diese spezifische Risiken bergen[54].

[53] Siehe die Leitlinien des EDSB zum Schutz personenbezogener Daten durch Apps für mobile Endgeräte von Organen und Einrichtungen der EU, abrufbar unter:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-11-07_Guidelines_Mobile_apps_EN.pdf.

[54] Siehe auch die Stellungnahme der Artikel-29-Datenschutzgruppe WP202 zu Apps auf intelligenten Endgeräten, abrufbar unter:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf.

- Die EU-Institution sollte Sicherheitsupdates von kommerziellen Browser-Anbietern oder dem Cloud-Anbieter rechtzeitig installieren.

Anhang 1. Glossar

Begriff	Beschreibung
Authentifizierung	Das Verfahren, mit dem die Identität eines Benutzers oder einer Maschine, der oder die einen Vorgang (normalerweise über ein IT-System) ausführt, abgesichert und bestätigt wird.
Verschlüsselungsschlüssel	Informationsteile, die üblicherweise zur Verschlüsselung (oder Entschlüsselung) von Daten auf einzigartige Weise verwendet werden. Somit stellen sie einen „Geheimcode“ dar, mit dem letztendlich die Daten nur dem offengelegt werden, der diesen Geheimcode kennt.
Virtuelles privates Netz (Virtual Private Network, VPN)	Ein VPN ist eine sichere (verschlüsselte) Punkt-zu-Punkt-Verbindung, die üblicherweise über ein öffentliches Netz hergestellt wird.
Cloud-Anbieter	Ein Anbieter von cloudbasierten IT-Diensten.
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
Besondere Kategorien (personenbezogener Daten)	Nach der derzeitigen Verordnung sind dies personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben. Der Vorschlag für eine neue Verordnung fügt hierzu noch genetische und biometrische Daten zum Zweck der eindeutigen Identifizierung natürlicher Personen hinzu. Diese Kategorien unterliegen besonderen Vorschriften.
Für die Verarbeitung Verantwortlicher	Das Organ oder die Einrichtung der Gemeinschaft, die Generaldirektion, das Referat oder jede andere Verwaltungseinheit, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
Auftragsverarbeiter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die

	personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.
Unterauftragsverarbeiter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des Auftragsverarbeiters verarbeitet.
Datenschutzbeauftragter (DSB)	Mitarbeiter einer Organisation, die die Organisation bei der Einhaltung der Datenschutzvorschriften unterstützt. Ernennung, Aufgaben und Befugnisse sind in der Verordnung (und der neuen Verordnung) festgelegt.
Betroffene Person	Natürliche Person, deren personenbezogene Daten verarbeitet werden.
Standardvertragsklauseln	Klauseln, die in Verträgen zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter oder zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, der als Unterauftragsverarbeiter agiert, verwendet werden und die in der Verordnung (und im Vorschlag für eine neue Verordnung) festgelegt werden und von der Europäischen Kommission oder einer Aufsichtsbehörde gemäß den rechtlichen Verfahren und zur Gewährleistung der erforderlichen Vertragssicherheit angenommen wurden.
Verbindliche interne Datenschutzvorschriften	Vorschriften, die alle wesentlichen Grundprinzipien und durchsetzbaren Rechte enthalten und die von einer Gruppe von Unternehmen für internationale Übertragungen personenbezogener Daten von Organisationen in der Union innerhalb der gleichen Gruppe von Unternehmen genutzt werden, um geeignete rechtlich vorgesehene Sicherheitsgarantien sicherzustellen.
Datenschutz-Folgenabschätzung (DSFA)	Bewertung der Risiken für Rechte und Freiheiten natürlicher Personen aufgrund der Verarbeitung ihrer personenbezogenen Daten. Die neue Verordnung legt obligatorische Elemente und Umstände fest, unter denen sie vorgeschrieben ist. Die für die Verarbeitung Verantwortlichen können diese Folgenabschätzung jedoch auch ohne diese Umstände durchführen und so relevante Vorteile nutzen.
Rahmenvertrag	Der Rahmenvertrag ist ein Vertragsmuster für ein öffentliches Vergabeverfahren, das sobald der Auftrag vergeben wurde, in „spezifische Verträge“ umgesetzt werden muss, um die Vertragsbedingungen zur Bereitstellung der Dienste oder Produkte weiter und genauer zu spezifizieren.
Spezifischer Vertrag	Siehe die Definition unter „Rahmenvertrag“.
Dienstleistungsvereinbarung (Service Level Agreement)	Offizielle Verpflichtung, oft Bestandteil von Verträgen, in der die Qualität der von einem Anbieter für einen

	Kunden bereitgestellten Dienste beschrieben wird. Die monatliche durchschnittliche Mindestverfügbarkeit eines Cloud-Dienstes kann beispielsweise ein Element sein, das in einer Dienstleistungsvereinbarung festgelegt wird.
Zertifizierung	Bestätigung der Erfüllung eines Standards/bewährter Praktiken durch einen autorisierten Dritten. Zertifizierungen können Cloud-Anbietern helfen, die Einhaltung der neuen Datenschutzvorschriften sicherzustellen, wenn sie gemäß dem Gesetz vergeben werden.
Verhaltensregeln	Eine Reihe selbst festgelegter Regeln, die von Einzelpersonen oder Unternehmen genutzt werden, um sich selbst über das obligatorisch rechtliche Maß hinaus zu verpflichten oder umzusetzen, was rechtlich verpflichtend ist. Verhaltensregeln können Cloud-Anbietern helfen, die Einhaltung der neuen Datenschutzvorschriften sicherzustellen, wenn sie gemäß dem Gesetz festgelegt werden.
Virtuelle Maschine	Eine virtuelle Maschine ist ein „virtueller“ Rechner, der auf einem physischen Rechner läuft, mit eigenem Betriebssystem, eigenen Anwendungen und Geräten, isoliert von anderen virtuellen Maschinen, die auf dem gleichen physischen Rechner laufen. Dies wird durch eine „Virtualisierungssoftware“ auf diesem Rechner ermöglicht.

Anhang 2. Weiterführende rechtliche Untersuchung

Dieser Anhang bietet weitere rechtliche Einblicke und Argumente, die die Ausführungen in den Kapiteln stützen, erhebt jedoch keinen Anspruch auf Vollständigkeit.

Nachfolgend werden kurz einige Gründe (**neben der Anwendbarkeit des Protokolls über die Vorrechte und Befreiungen der Europäischen Gemeinschaften**) zur Stützung **der Empfehlung** in Randnummer 63 dieser Leitlinien angeführt, nämlich dass die Verarbeitung der dem Cloud-Anbieter von der EU-Institution anvertrauten personenbezogenen Daten und jede Unterverarbeitung **in der Regel im Hoheitsgebiet der EU** stattfindet[55].

1) Der Standort des Cloud-Anbieters und seiner Rechenzentren und/oder Server außerhalb der EU sind Faktoren, die *unter anderem* die Anwendbarkeit des Gesetzes eines Drittlandes bestimmen (Problem der Anwendbarkeit von Gesetzen und Rechtsprechung eines Drittlandes).

Einige Beispiele in Bezug auf **unterschiedliche Rechtsbereiche** (andere als dem Datenschutzrecht) werden nachfolgend kurz angeführt:

i) Hinsichtlich der Anwendung des **Strafrechts** weisen wir darauf hin, dass der Zugang durch eine Strafverfolgungsbehörde eines Drittlandes zu einem Rechenzentrum, das sich **in einem Mitgliedstaat der EU** befindet, in der Regel einen Antrag der Strafverfolgungsbehörde an den Mitgliedstaat gemäß einer spezifischen internationalen Vereinbarung, eines Rechtshilfeabkommens (MLAT) oder einer gemeinsamen Absichtserklärung, in denen geeignete Datenschutzgarantien festgelegt sind, erfordert.[56] Ein solcher MLAT-Antrag wäre im Fall des Zugangs durch eine Strafverfolgungsbehörde eines Drittlandes auf ein Rechenzentrum in seinem Hoheitsgebiet **nicht** erforderlich.

---

[55] Eine Verarbeitung außerhalb der EU sollte *die Ausnahme* sein (z. B. im Fall einer Datenverarbeitung mit geringem Risiko) und die EU-Institution beschreibt und rechtfertigt in diesem Fall die Notwendigkeit dieser Verarbeitungsvorgänge und achtet besonders auf mögliche Datenschutzrisiken und Risiken für die wirksame Überwachung durch die Aufsichtsbehörde.

In diesem Fall gelten auch die Vorschriften für die Übertragung personenbezogener Daten in Nicht-EU-Staaten. Für Leitlinien zur Übertragung personenbezogener Daten an Nicht-EU-Staaten und internationale Organisationen auf der Grundlage der derzeitigen Verordnung (EG) Nr. 45/2001 siehe das Positionspapier des EDSB „Die Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen: Artikel 9“, einschließlich der relevanten EDSB-Fälle, abrufbar unter:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_DE.pdf.

Beachten Sie bitte, dass das vorgenannte Papier des EDSB aktualisiert wird, um die überarbeiteten Vorschriften des Vorschlags für eine Verordnung über die internationale Übermittlung personenbezogener Daten zu berücksichtigen.

[56] In der Rechtssache „Microsoft Irland“ entschied das Berufungsgericht der Vereinigten Staaten für den zweiten Gerichtsbezirk am 14. Juli 2016, dass das US-Gesetz (Stored Communication Act, SCA) *ein US-Gericht nicht berechtige, eine SCA-Berechtigung gegen einen in den Vereinigten Staaten ansässigen Serviceprovider für die Inhalte der elektronischen Kommunikation eines Kunden, die auf Servern außerhalb der Vereinigten Staaten gespeichert sind, zu verhängen und durchzusetzen. Die SCA-Berechtigung könne in diesem Fall nicht rechtmäßig genutzt werden, um Microsoft zu zwingen, der Regierung die Inhalte eines E-Mail-Kontos eines Kunden, die nur in Irland gespeichert sind, offenzulegen.*“ Das US-Berufungsgericht bezog sich unter anderem auf die Regel „*locus rei sitae*“. Das Urteil ist abrufbar unter: http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412.

Gleichzeitig erinnern wir daran, dass im **Übereinkommen über Cyberkriminalität** (Budapester Übereinkommen)[57], als gemeinsame Sicherheitsgarantie, die auch für Nicht-EU-Staaten gilt, die Mitglieder dieses Übereinkommens sind, Artikel 15 Folgendes besagt: „Jede Vertragspartei stellt sicher, dass für die Schaffung, Umsetzung und Anwendung der [...] Befugnisse und Verfahren [für strafrechtliche Ermittlungen] [...] der Grundsatz der **Verhältnismäßigkeit** gehören muss."

ii) Nach dem **Zivilprozessrecht** kann ein Rechenzentrum, dass sich in einem EU-Mitgliedstaat befindet (und somit nach dem Territorialitätsgrundsatz dem Zivilprozessrecht dieses Mitgliedstaats unterliegt) nicht zivilrechtlich durchsucht werden – „**Pre-trial Discovery**" nach US-Recht (d. h. die obligatorische Offenlegung von Informationen, die nicht selbst direkt relevant sind, jedoch zur Aufdeckung relevanter Informationen für den Prozess führen können). In diesem Fall sollten Anträge auf Offenlegung, wie von der Artikel-29-Datenschutzgruppe vorgeschlagen, vorzugsweise über das Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen erfolgen, das „ein Standardverfahren für Rechtshilfeersuchen [bietet], d. h. für Anträge eines Gerichts an die benannte Zentrale Behörde eines anderen Staates auf Unterstützung bei der Erlangung relevanter Informationen, die sich in ihrem Staat befinden." Im Gegensatz dazu kann ein Rechenzentrum in den Vereinigten Staaten im Rahmen einer Pre-trial Discovery („Beweissicherung") nach der Rechtsprechung und gemäß dem geltenden Recht der Vereinigten Staaten durchsucht werden.[58]

iii) In Bezug auf die Tätigkeiten **nationaler Nachrichtendienste** stellen wir Folgendes heraus: „Alle Mitgliedstaaten [der EU] sind Vertragsparteien der Europäischen Menschenrechtskonvention [EMRK]. Daher müssen ihre **Überwachungsprogramme** den in den Artikeln 7 und 8 EMRK genannten Bedingungen genügen. [...]. Artikel 1 EMRK verpflichtet die Vertragsparteien außerdem dazu, allen ihrer Hoheitsgewalt unterstehenden Personen die in der Konvention bestimmten Rechte und Freiheiten zuzusichern. Sowohl als **EU-Mitgliedstaaten als auch als EMRK-Vertragsparteien** können sie wegen der Verletzung des Rechts auf Achtung des Privatlebens eines EU-Staatsbürgers vor den EGMR gebracht werden."[59]

Diese Sicherheitsgarantien gelten **nicht** für Staaten, die **nicht** Vertragsparteien des EMRK sind (die Liste der Staaten, die das EMRK unterzeichnet und ratifiziert haben, ist abrufbar unter:

---

[57] Das **Übereinkommen über Cyberkriminalität** des Europarats (CETS Nr. 185), das als Budapester Übereinkommen bekannt ist, abrufbar unter: http://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185.

[58] Siehe die Arbeitsunterlage 1/2009 der WP29 über **Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzüberschreitenden zivilrechtlichen Verfahren (Pre-trial Discovery)**, abrufbar unter:

http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_de.pdf.

[59] Stellungnahme 04/2014 der Artikel-29-Datenschutzgruppe zur Überwachung der elektronischen Kommunikation zu **nachrichtendienstlichen und nationalen Sicherheitszwecken**, abrufbar unter:

http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_de.pdf.

Das Europäische Parlament hat in seinen Entschließungen vom 10. Dezember 2013 zum Cloud-Computing und vom 12. März 2014 zur Überwachung Bedenken vor allem hinsichtlich des Zugriffs durch Nachrichtendienste aus Drittländern auf Cloud-Anbieter, die Server in Drittländern zur Datenspeicherung nutzen, ausgedrückt.

Siehe auch die Studie der Agentur der Europäischen Union für Grundrechte (FRA) „Überwachung durch Nachrichtendienste: Grundrechtsschutz und Rechtsbehelfe in der Europäischen Union", abrufbar unter: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf.

Dieser Bericht stellt die in den EU-Mitgliedstaaten geltenden Rechtsrahmen für die Überwachung dar. Daneben werden auch die in der EU eingeführten Aufsichtsmechanismen dargelegt, die Tätigkeiten der Organe beschrieben, die mit der Kontrolle von Überwachungsmaßnahmen betraut sind, und die verschiedenen Rechtsbehelfe dargestellt, die den Personen zur Verfügung stehen, die solche nachrichtendienstlichen Aktivitäten anfechten möchten.

https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=55fMgptN). Alle EU-Mitgliedstaaten sind Vertragsparteien des EMRK.

Im Wesentlichen ist bei der Speicherung und Verarbeitung von Daten in einem Rechenzentrum oder durch ein Unternehmen im Hoheitsgebiet eines bestimmten Landes normalerweise die Behörde dieses Landes dafür zuständig, einen Antrag auf Zugriff auf die verarbeiteten Daten in dem besagten Rechenzentrum im Zusammenhang mit einer Durchsetzungsmaßnahme **unter Anwendung des öffentlichen Rechts** dieses Landes zu stellen (z. B. Strafrecht, Verfahrensrecht, Gesetze über Vorratsdatenspeicherung usw.). Dieses **Risiko** muss von der EU-Institution sorgfältig geprüft werden.

2) Darüber hinaus weisen wir auf das kürzliche Urteil in der **Rechtssache** des Gerichtshofs der Europäischen Union (EuGH) hin:

In der Rechtssache zur „**Vorratsspeicherung von Daten**“[60] wies der EuGH (in Randnummer 68) auf den Umstand hin, dass „*die Richtlinie [über die Vorratsspeicherung von Daten] nicht [vorschreibt], dass die fraglichen Daten im **Unionsgebiet** auf Vorrat gespeichert werden, so dass **es nicht als vollumfänglich gewährleistet angesehen werden kann, dass die Einhaltung der [...] Erfordernisse des Datenschutzes und der Datensicherheit, wie in Art. 8 Abs. 3 der Charta ausdrücklich gefordert, durch eine unabhängige Stelle überwacht wird.** Eine solche **Überwachung** auf der Grundlage des **Unionsrechts** ist aber wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten*“ (*Hervorhebungen hinzugefügt*).

In der „**Rechtssache Schrems**[61]“ stellte der EuGH außerdem heraus, dass eine **effektive Überwachung durch vollkommen unabhängige Datenschutzbehörden**, die mit allen in dieser Hinsicht erforderlichen Befugnissen durchgeführt wird, ein wesentlicher Bestandteil des Schutzes personenbezogener Daten ist.

In der Rechtssache „**Tele2**“[62] erklärt der EuGH in ähnlicher Weise (in Randnummer 122) Folgendes: „Bezüglich der Vorschriften zur **Sicherheit und zum Schutz der** von den Betreibern elektronischer Kommunikationsdienste auf Vorrat gespeicherten **Daten** ist festzustellen, dass Art. 15 Abs. 1 der Richtlinie 2002/58 den **Mitgliedstaaten** nicht erlaubt, von Art. 4 Abs. 1 und Art. 4 Abs. 1a der Richtlinie abzuweichen. Nach diesen Bestimmungen haben die Betreiber geeignete technische und organisatorische Maßnahmen zu ergreifen, um zu gewährleisten, dass die auf Vorrat gespeicherten Daten wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang geschützt sind. Unter Berücksichtigung **der Menge** an gespeicherten Daten, ihres **sensiblen Charakters** und der **Gefahr eines unberechtigten Zugangs** zu ihnen müssen die Betreiber elektronischer Kommunikationsdienste, um die Unversehrtheit und Vertraulichkeit der Daten in vollem Umfang zu sichern, durch geeignete technische und organisatorische Maßnahmen ein besonders hohes Schutz- und Sicherheitsniveau gewährleisten. Die nationale Regelung muss insbesondere vorsehen, dass die Daten **im Unionsgebiet zu speichern** und nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten sind“ (*Hervorhebungen hinzugefügt*).

---

[60] Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland Ltd gegen Seitlinger und Andere* vom 8. April 2014.

[61] Urteil des Gerichtshofs (Große Kammer) vom 6. Oktober 2015 (Vorlage zur Vorabentscheidung vom Obersten Gericht (Irland)) – *Maximilian Schrems gegen Data Protection Commissioner* (Rechtssache C-362/14).

[62] Urteil des Gerichtshofs der Europäischen Union in den verbundenen Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB gegen Post- och telestyrelsen und Secretary of State for the Home Department gegen Tom Watson und Andere* vom 21. Dezember 2016.

3) Im Fall des Hostings der Cloud-Architektur in einem Nicht-EU-Staat könnte es **für den EDSB noch problematischer sein**, mit nationalen europäischen Datenschutzaufsichtsbehörden **zusammenzuarbeiten und Kontrollen zu koordinieren** und so die Durchsetzung aller Vorschriften der Verordnung sicherzustellen.

Aufgrund der oben angeführten Aspekte **empfiehlt der EDSB daher, dass *in der Regel* die Verarbeitung der dem Cloud-Anbieter von den EU-Institutionen anvertrauten personenbezogenen Daten (einschließlich für Backups, Geschäftskontinuität und zur Übertragungen sowie Standorte, von denen aus per Fernzugriff Vorgänge durchgeführt werden), *und jede Unterauftragsverarbeitung* innerhalb der EU stattfindet**.

Anhang 3. Cloud-Computing: grundlegende Konzepte und Modelle

Definition des Cloud-Computing

Cloud-Computing-Technologien und -Dienste können in einer Reihe von Architekturen in unterschiedlichen Dienst- und Bereitstellungsmodellen umgesetzt werden. Der Begriff wird in unterschiedlichen Kontexten unterschiedlich verwendet. Die am häufigsten genutzte Definition ist die des US National Institute of Standards and Technology (NIST)[63], die Cloud-Computing als Modell beschreibt, das einen ortsunabhängigen, verbraucherfreundlichen, auf Abruf verfügbaren Netzzugriff auf einen gemeinsamen Pool an konfigurierbaren Computer-Ressourcen (z. B. Netze, Server, Speicher, Anwendungen und Dienste) erlaubt, der schnell bereitgestellt und mit geringfügigem Verwaltungsaufwand bzw. minimalen Eingriffen durch den Dienstanbieter freigegeben werden kann. In dem NIST-Dokument werden drei Dienstmodelle (Software as a Service - SaaS; Platform as a Service - PaaS und Infrastructure as a Service - IaaS) und vier Bereitstellungsmodelle beschrieben: öffentliche, private, Community- und hybride (eine Zusammensetzung aus den anderen drei Modellen) Cloud-Umgebungen. In diesen Leitlinien sind die Begriffe und Akronyme in der Bedeutung dieser Definition zu verstehen.

Wie bereits erwähnt, konzentrieren sich diese Leitlinien auf öffentliche Cloud-Umgebungen, da sich hier besondere Herausforderungen für den Schutz personenbezogener Daten ergeben. Hybride Cloud-Dienste mit privaten und öffentlichen Cloud-Infrastrukturen gehören ebenfalls aufgrund der öffentlichen Komponente und dem Zusammenspiel mit privaten Infrastrukturen bei der Bereitstellung der Dienste dazu.

Traditionelle externe Auftragsvergabe und Cloud-Computing

Die Nutzung von Cloud-Diensten ist tatsächlich eine neue Art der externen Auftragsvergabe. Dies ist der Fall, wenn sich eine Organisation, die ihre Daten bisher in ihrem eigenen Rechenzentrum verarbeitet hat, entscheidet, einen cloudbasierten Dienst zu nutzen. Dies bringt sowohl Risiken der traditionellen externen Auftragsvergabe als auch die besonderen Risiken des Cloud-Computing mit sich, die in Anhang 4 näher beschrieben werden. Somit ist Cloud-Computing nicht „lediglich eine andere Art der externen Auftragsvergabe“ und erfordert daher besondere Untersuchungen und Sicherheitsgarantien.

Es sollte darauf hingewiesen werden, dass einige IT-Unternehmen jeden Dienst, der über das öffentliche Internet angeboten wird, als cloudbasiert anpreisen, auch wenn er nicht die Kriterien für Cloud-Dienste erfüllt, wie beispielsweise:

- Selbstbereitstellung von Computing-Fähigkeiten auf Abruf, z. B. Serverzeit und Netzwerkspeicher.
- Einfache und schnelle Ressourcenbereitstellung und Skalierbarkeit, mit dem Pay-per-Use-Modell.
- Breiter Zugang über das Internet mit Standard-Clients (z. B. Browser).
- Bündelung der dynamisch zugewiesenen Ressourcen des Anbieters zur Bedienung mehrerer Cloud-Nutzer, ohne Kenntnisse und/oder Kontrolle des Nutzers über den Ressourcenstandort.

[63] US NIST SP 800-145, The NIST Definition of Cloud Computing, September 2011. Abrufbar unter: https://csrc.nist.gov/publications/detail/sp/800-145/final.

- Nahtlose Optimierung der bemessenen Ressourcen, die vom Dienstanbieter zugewiesen werden.

Nicht alle über das Internet angebotenen Dienste erfüllen diese Eigenschaften, die je nach Dienstmodell auch in unterschiedlichem Maß vorhanden sein können. Darüber hinaus sind private, Community- und andere vermischte Bereitstellungsmodelle aufgetaucht, bei denen auch auf der Grundlage ihrer Besonderheiten einige Eigenschaften beibehalten oder fallen gelassen werden. Die besonderen Risiken des Cloud-Computing sind mit diesen Eigenschaften, der Art, wie sie bereitgestellt werden, und der Art, wie Cloud-Computing-Unternehmen und Dienste entwickelt wurden, verbunden.

Beispiele für öffentlich verfügbare Cloud-Dienste

Auch wenn jeder IT-Dienst heutzutage in einer Cloud-Umgebung bereitgestellt und betrieben werden kann, gibt es einige Beispiele für cloudbasierte Dienste, die in Bezug auf das besprochene Thema und die damit verbundenen Risiken für die EU-Institutionen von Interesse sind. Es folgt eine nicht erschöpfende Liste:

- SaaS: grundlegende Datenspeicherdienste, Suites zur Büroautomatisierung, Dokumenten- und Workflow-Management-Dienste, Personalverwaltungsanwendungen, Managementplattformen für mobile Endgeräte.
- PaaS: Software-Infrastruktur, wie virtualisierte Server mit speziellen Betriebssystemen und grundlegender Software, z. B. Internet- und Anwendungsserver, Datenbanken, gemeinsam genutzte Umgebungen für Programmiersprachen und andere Tools. Linux-basierte virtuelle Maschinen mit relevanter Software und Open-Source-Datenbanken und Software-Dienstprogrammen könnten von den EU-Institutionen beispielsweise für die Bereitstellung und den Betrieb von Webseiten genutzt werden.
- IaaS: Computing-Infrastruktur, bestehend aus virtuellen Maschinen, Speicher- und Netzinfrastruktur, einschließlich Sicherheitseinrichtungen, bei denen im Prinzip jede Art von Software-Dienst auf jeder Plattform bereitgestellt und betrieben werden kann. Die EU-Institutionen könnten IaaS-Dienste nutzen, um ihre eigenen Rechenzentren zu ersetzen.
- Hybrid: eine EU-Institution könnte eine Technologie suchen, die einen idealen nahtlosen Lastausgleich oder eine dynamische Zuweisung von öffentlichen Cloud-Ressourcen bietet, um ihre eigene Speicher- oder Computing-Infrastruktur zu integrieren oder zu ergänzen.

Dies könnte entweder über einen kommerziellen Cloud-Anbieter oder durch „externe Vergabe von „privaten (oder Community)-Cloud"-Infrastrukturen (bei denen Maschinen von der EU-Institution an ein Hosting-Unternehmen in einer Cloud-Konfiguration extern vergeben werden) oder durch rein private oder Community-Cloud-Infrastrukturen geschehen, die einer oder mehreren EU-Institutionen gehören[64].

[64] Siehe die Quellenangabe in der vorherigen Fußnote für eine tiefergehende Beschreibung möglicher Bereitstellungsmodelle.

Anhang 4. Besondere Datenschutzrisiken des Cloud-Computing

In diesem Abschnitt werden die Hauptrisiken in Verbindung mit Cloud-Computing-Diensten beschrieben. Zunächst werden Risiken in Verbindung mit allgemeinen Cloud-Computing-Merkmalen einer öffentlichen Cloud-Infrastruktur aufgeführt. Danach werden diese Risiken in Bezug auf spezifische Arten von Cloud-Diensten, die auf anderen bestehenden Dienst- und Bereitstellungsmodellen basieren, weiter untersucht (siehe Anhang 3 und es wird eine relative Bewertung hinsichtlich der anderen Modelle vorgenommen).

Diese Risiken müssen integriert und möglichst weiter in einer umfassenden Bewertung der Datenschutzrisiken (oder DFSA - siehe Abschnitt 4.1) aufgeschlüsselt werden, wobei alle möglichen Gefahren und Verletzlichkeiten, die Auswirkungen auf den Schutz personenbezogener Daten haben, und alle Einhaltungsanforderungen berücksichtigt werden.

Jedes besondere Merkmal des Cloud-Computing bringt relevante Datenschutzrisiken mit sich. Einige Cloud-Merkmale können zusammen bestimmte Risiken hervorrufen oder verstärken.

- *Fx – Beschreibung des Cloud-Computing-Merkmals*
  - *Rx –Beschreibung des Risikos*

- ***F1 - Die EU-Institution hat bisher keine cloudbasierten Dienste genutzt und daher nur begrenzt Erfahrungen damit.***
  - **R1 - Keine bisherige ausreichende Erfahrung mit der Bereitstellung von Cloud-Computing-Diensten** kann zur Unterschätzung der Risiken oder zur Wahl ungeeigneter Sicherheitsgarantien führen. Der Einsatz von Cloud-Diensten für wichtige institutionelle Geschäftsprozesse oder für die Verarbeitung sensibler Daten ohne Erfahrungen könnte institutionelle Aufgaben und Verantwortlichkeiten im Bereich des Datenschutzes gefährden und Auswirkungen auf betroffene Personen haben.
- ***F2 - Dienste werden über das öffentliche Internet bereitgestellt****, was der gewöhnliche Kommunikationsweg zwischen dem Cloud-Anbieter und den Cloud-Nutzern ist. Dies wäre für die EU-Institution eine Änderung, da ihre Daten im Allgemeinen in ihrem eigenen Rechenzentrum oder im Rechenzentrum einer anderen EU-Institution verarbeitet werden (z. B. Kommission - DIGIT), die üblicherweise über spezielle Kommunikationsverbindungen miteinander verbunden sind.*
  - **R2 - Vertraulichkeits- und Integritätsrisiken bei Daten, die über das Internet übertragen werden**. Über die Internetverbindung zwischen dem Cloud-Anbieter und dem Cloud-Nutzer, einschließlich der festen und mobilen Infrastruktur für den Zugang zum Internetanbieter, können unbefugte Zugriffe auf und Änderungen an den übertragenen Daten geschehen. Der unbefugte Zugang zu personenbezogenen Daten kann zur Folge haben, dass die Daten für andere als die zulässigen und vereinbarten Zwecke genutzt werden und der Datenschutz und die Privatsphäre der betroffenen Personen verletzt werden.
  - **R3 - Mangelnde Verfügbarkeit** infolge eines beschränkten oder nicht vorhandenem Internetzugangs aufgrund einer fehlerhaften Kapazitätsplanung, Nichtverfügbarkeit des Dienstanbieters, Netzwerküberlastung, Cyberangriffen usw. In diesem Fall wären die EU-Institution und die betroffenen Personen nicht in der Lage, auf die Daten zuzugreifen.

- **R4 - Internetüberwachung durch Regierungen und Sicherheitsdienste** bei den Internetdienstanbietern, dem Internet-Backbone und der Routing-Infrastruktur. Regierungen und Sicherheitsdienste der Länder, durch die die Internetverbindung zum zukünftigen Cloud-Anbieter möglicherweise verläuft, könnten Interesse an bestimmten von der EU-Institution verarbeiteten personenbezogenen Daten haben.
- **R5 - Einschneidende rechtliche Vorschriften zur Vorratsdatenspeicherung für die Zwecke der Strafverfolgung**, die für den Cloud-Anbieter und die Internetanbieter gelten, können die übliche Aufbewahrungsfrist verlängern, so dass die Wahrscheinlichkeit eines möglichen Missbrauchs und von Datenverlusten ansteigt. Dies kann von Land zu Land variieren, auch innerhalb der EU. Wie in Anhang 2 betont wurde, sind nichtsdestotrotz eine stärkere Zusammenarbeit mit dem EDSB und höhere Datenschutzgarantien in EU-Staaten im Gegensatz zu Nicht-EU-Staaten zu erwarten.

- ***F3 - Mandantenfähigkeit von öffentlichen Cloud-Diensten**, die üblicherweise Daten von verschiedenen Kunden im gleichen Rechenzentrum oder sogar im gleichen Sicherheitsbereich oder auf dem gleichen Server hosten.*
  - **R6 - Mögliche Verletzbarkeit beim Zugang und bei Sicherheitskontrollen**, wie Zwischenfälle und Cyberangriffe ausgehend von der Client-Infrastruktur eines oder mehrerer Nutzer des Cloud-Anbieters könnten die Daten der EU-Institution gefährden. Darüber hinaus könnten sich die verschiedenen Nutzer des Cloud-Anbieters in Ländern mit einem anderen (niedrigeren) Niveau des Schutzes personenbezogener Daten als in einem der EU-Staaten befinden (siehe auch R7).

- ***F4 - Der physische Standort der Daten der Cloud-Nutzer kann dem Nutzer unbekannt sein oder, wenn er bekannt ist, schwer überprüfbar sein.** Mittlere bis große Cloud-Anbieter verfügen üblicherweise über Rechenzentren in vielen Ländern. Die Daten können dynamisch in Abhängigkeit der verfügbaren Ressourcen, Redundanzerfordernisse und wirtschaftlicher Faktoren in den verschiedenen Rechenzentren gespeichert werden. Der Speicherort der Daten wird dem Cloud-Nutzer nicht oder nur sehr ungenau mitgeteilt (z. B. nur der Ländername).*
  - Probleme bezüglich ausländischer Rechtsprechung:
    - **R7 - Unterschiedliches geltendes Recht** und somit mögliche unterschiedliche Niveaus des Datenschutzes, das vor allem davon abhängt, ob die Daten innerhalb oder außerhalb der EU gespeichert werden. Es kann auch passieren, dass der Hauptsitz des Cloud-Anbieters in der EU ist, das Unternehmen aber Tochtergesellschaften hat oder Unterauftragsverarbeiter nutzt, die außerhalb der EU ansässig sind. In diesem Fall gelten für die EU-Institution unterschiedliche Anforderungen, wie in der Verordnung (EG) Nr. 45/2001 und zukünftig im Verordnungsvorschlag beschrieben[65], die sich auf die Anwendbarkeit der Vorschriften für die Übertragung von personenbezogenen Daten in Nicht-EU-Staaten auswirken.
    - **R8** - Erhöhtes Risiko, dass **Cloud-Anbieter aufgrund von anderen Rechtsvorschriften als in der EU mit Strafverfolgungsbehörden**

[65] Siehe Artikel 9 der Verordnung; Artikel 44-50 der Datenschutz-Grundverordnung.

zusammenarbeiten oder Daten offenlegen müssen oder anderweitig nicht die für EU-Institutionen geltenden Rechtsvorschriften einhalten.

- **R9** - Erhöhtes Risiko, dass **Cloud-Nutzer und betroffene Personen keine Kontrolle mehr über ihre Daten haben** (Standort).

- ***F5 - Trend zur „Kommerzialisierung" von IT-Diensten.***

  Cloud-Dienste bieten den EU-Institutionen die Möglichkeit, das IT-Management (mehr oder weniger, je nach Dienst- und Bereitstellungsmodell) an den Cloud-Anbieter zu delegieren, häufig mit minimalen Eingriffen bei der Bereitstellung und Konfiguration des Dienstes.

  Aufgrund der Notwendigkeit, eine kritische Masse an Computing-Ressourcen zu verwalten, um einen Cloud-Dienst anzubieten, und der Marktkonzentration der Cloud-Anbieter, besteht häufig ein vertragliches Ungleichgewicht zwischen dem Cloud-Anbieter und dem Cloud-Nutzer, insbesondere wenn letzterer eine Einzelperson oder ein KMU ist. Im Kontext der EU-Institutionen kann dies insbesondere bei kleineren Organisationseinheiten oder kleineren Institutionen und Einrichtungen geschehen.

  Größenvorteile, die geringere Dienstleistungskosten ermöglichen, unterliegen ebenfalls strengen vertraglichen Bedingungen und wenig Anpassung der Merkmale und Bedingungen.

  - **R10 - Unfaire und strenge Nutzungsbedingungen und Dienstleistungsverträge**. Mögliche aufgezwungene Nutzungs- und Vertragsbedingungen werden mit wenigen oder keinen Verhandlungsoptionen und einseitiger möglicher Änderung der Bedingungen durch den Cloud-Anbieter, mit kurzer oder gar keiner Vorankündigung, angeboten. Solche Verträge bieten der EU-Institution möglicherweise nicht die geeigneten Instrumente, um personenbezogene Daten ausreichend zu schützen und die Anforderungen der Verordnung (EG) Nr. 45/2001 und noch weniger des Verordnungsvorschlags zu erfüllen.
  - **R9 - Erhöhtes Risiko, dass Cloud-Nutzer und betroffene Personen keine Kontrolle mehr über ihre Daten haben** (allgemein). Dieses Risiko ist nicht neu und ist typisch für jede externe Auftragsvergabe, doch es gilt insbesondere für Cloud-Dienste. Trotz des Grads der Befugnisübertragung an den Cloud-Anbieter bleibt die EU-Institution weiterhin als „für die Verarbeitung Verantwortlicher" für die Einhaltung der Datenschutzvorschriften verantwortlich.
  - **R11 - Mangelnde Kontrolle über die Sicherheitsmaßnahmen** Die EU-Institutionen können die Sicherheitsmaßnahmen zum Schutz personenbezogener Daten für den Teil des Cloud-Dienstes erstellen und umsetzen, über den sie die Kontrolle haben. Dies ist stark abhängig von dem Dienst- und Bereitstellungsmodell (siehe die folgenden Abschnitte). Bei den Bereichen, die dem Cloud-Anbieter übertragen wurden, haben die Nutzer normalerweise keine Möglichkeit, die Sicherheitsrisiken zu steuern und geeignete technische und organisatorische Sicherheitskontrollen, wie sie in der Verordnung (EG) Nr. 45/2001[66] und im Verordnungsvorschlag verlangt werden, zu wählen[67].
  - **R12 - Mangelnde Prüfbarkeit** durch den Cloud-Nutzer oder einen Dritten, um Gewissheit zu erlangen, dass der Cloud-Anbieter als Auftragsverarbeiter auf

[66] Artikel 22, 35 und 36 der Verordnung.

[67] Artikel 32 bis 34 der Datenschutz-Grundverordnung.

Weisung der EU-Institution handelt und ausreichende Garantien zur Durchführung der Sicherheitskontrollen gewährt[68]; hierzu gehören auch **mögliche Hemmnisse bei der Überwachung und Untersuchung** durch die zuständigen Behörden, einschließlich der Forensik.

- **R13 - Schwierigkeiten, betroffenen Personen , die ihre Rechte als betroffene Personen ausüben, zu antworten**, wie z. B. bei Anträgen auf umfassende Auskunft über die verarbeiteten personenbezogenen Daten, Anträge auf Sperrung und Löschen von Daten usw. gemäß der Verordnung (EG) Nr. 45/2001[69] und dem Verordnungsvorschlag[70].
- **R14 - „Anbieterbindung" nach dem Verkauf oder der Beendigung der Aktivitäten des Cloud-Anbieters** aufgrund von Bankrott oder anderer unerwarteter Ereignisse: Die Daten könnten nicht mehr verfügbar sein oder es könnten andere Gesetze oder vertragliche Vorschriften für den Datenschutz für den neuen Cloud-Anbieter gelten, ohne dass die EU-Institution eingreifen könnte.
- **R15 - Mangelnde Datenübertragbarkeit** Proprietäre Formate, spezifische Datenmodelle und die Nutzung anderer Hilfsanwendungen könnten eine effiziente und effektive Rückübertragung der Daten und der virtuellen Maschinenkonfiguration der EU-Institution oder deren Übergabe an einen neuen Cloud-Anbieter gefährden. Darüber hinaus besteht das Risiko, dass die personenbezogenen Daten von (früheren) Cloud-Anbietern nach der Übergabe nicht dauerhaft gelöscht werden.

- ***F6 - Mehrere Anbieter und Unterauftragsverarbeiter können zusammenarbeiten, z. B. in einem komplexen und mehrschichtigen Ansatz, um den beauftragten Dienst bereitzustellen, und es ist häufig eine dynamische Integration neuer Beteiligter möglich.***
  - **R16 - Keine klare Zuweisung der Verantwortlichkeiten innerhalb der Dienstanbieterkette (Cloud-Anbieter und Unterauftragsverarbeiter)** bei der Umsetzung von Sicherheitsmaßnahmen und Anforderungen an die Verarbeitung personenbezogener Daten wie Datenqualität, Datensicherheit, Wahrung der Rechte betroffener Personen und Prüfbarkeit. Die Verantwortlichkeiten der Auftragsverarbeiter und Unterauftragsverarbeiter könnten innerhalb der Gruppe verloren gehen, so dass niemand die Verantwortung übernimmt.
- ***F7 - Höhere Anzahl an nahtlosen und schnellen Übertragungen personenbezogener Daten, an der viele Parteien beteiligt sind und Grenzen überschritten werden, und Datenreplikation für eine bessere Verfügbarkeit und einen schnelleren Zugriff.***
  - **R9 - Erhöhtes Risiko, dass Cloud-Nutzer und betroffene Personen keine Kontrolle mehr über ihre Daten haben** (Standort, Rechtsprechung, Schutzniveau).
  - **R13 - Mögliche Schwierigkeiten für eine effektive Ausübung der Rechte betroffener Personen** (siehe oben).
  - **R17 - Schwierigkeiten für die Vorratsdatenspeicherung und ein effektives Löschen der Daten**. Die verfügbaren cloudbasierten Anwendungen könnten über keine geeigneten Funktionen zur korrekten Verwaltung der

[68] Gemäß Artikel 23 der Verordnung.

[69] Gemäß Artikel 28 der Datenschutz-Grundverordnung.

[70] Artikel 13 bis 20 der Verordnung; Artikel 17 bis 23 der Datenschutz-Grundverordnung.

Aufbewahrungsfristen verfügen, so dass Daten dauerhaft gelöscht werden, wenn sie für die rechtlich verfolgten Zwecke nicht länger erforderlich sind. Darüber hinaus könnte der Cloud-Anbieter eine Cloud-Infrastruktur nutzen, in der die Daten für Hot-Swap-Funktionen und für eine Notfallwiderherstellung repliziert werden, wobei das Risiko besteht, dass auch nach dem Löschen der Daten über die Funktionen des Cloud-Dienstes noch Kopien der Daten vorhanden sind. Datenbestände könnten auch zur Cloud-Optimierung von einem Server auf einen anderen übertragen werden, so dass durch einen möglichen Fehler im Mechanismus unnötige Kopien der Daten auf einem Server verbleiben könnten.

- ***F8 - Für die Datensicherheit (personenbezogener Daten) in einer Cloud-Infrastruktur gibt es besondere Risiken im Vergleich zu „traditionellen" Rechenzentren in den eigenen Gebäuden.***

  Auch wenn die Cloud-Anbieter in einigen Fällen bessere Sicherheitsmaßnahmen als in einem „traditionellen" von der EU geführten Rechenzentren bieten, so bringt der cloudbasierte Aufbau doch besondere Risiken mit sich oder verstärkt die vorhandenen Risiken.

  Einige Sicherheitsaspekte im Zusammenhang mit der Cloud, die Auswirkungen auf den Datenschutz haben, wurden bereits an anderer Stelle in diesem Abschnitt beschrieben. Es müssen jedoch auch andere spezifische IT-Sicherheitsrisiken bewältigt werden.

  - **R18 - Andere für das Cloud-Computing spezifische IT-Sicherheitsrisiken (nicht erschöpfend):**
    - Sicherheit des Benutzer-Clients (z. B. Browser, Apps für mobile Endgeräte)
    - Authentizität des beauftragten Dienstes
    - Schwierigkeiten bei der Verwaltung der Verschlüsselungsschlüssel
    - Schwierigkeiten bei der Verwaltung der Identitäten und Authentifizierungen
    - Verletzbarkeit der Virtualisierungsschicht und der virtuellen Maschinen.

Besondere Aspekte des IaaS-Dienstmodells

In diesem Modell werden dem Nutzer die virtuellen Maschinen durch den Cloud-Anbieter aus einem Pool gemeinsamer Ressourcen zugewiesen. Der Cloud-Nutzer kann viele Konfigurationsaspekte der IT-Infrastruktur, die Software-Plattform und die darauf entwickelten Anwendungen kontrollieren. Er hat keinerlei Kontrolle über die physische Sicherheit des Rechenzentrums.

- ***F5***
  - Mangelnde Transparenz bei einigen Aspekten der zugrunde liegenden technischen Infrastruktur (grundlegende Virtualisierungssoftware, Hardware und Netze) und der relevanten technischen und organisatorischen Sicherheitsgarantien.
  - Kontrolle über die Sicherheitsmaßnahmen auf Ebene der Anwendungen und der Plattform. Eingeschränkte Kontrolle über die Sicherheit eines Teils der tiefer liegenden Rechnersoftware, der Netzsicherheit und keine Kontrolle über die physische Sicherheit des Rechenzentrums.
  - Mögliche Umsetzung der Prüfbarkeit auf Ebene der Anwendung, der Plattform und der Rechnerkonfiguration. Begrenzte (sofern das Netz konfigurierbar ist)

oder keine Umsetzung der Prüfbarkeit auf Netzebene und keine Kontrolle über mögliche Prüfbarkeit der physischen Sicherheit.

- Es können Instrumente zur Wahrung der Rechte betroffener Personen entwickelt werden.
- Weniger mit der Datenübertragbarkeit zusammenhängende Risiken.

- ***F3***
  - Hier gibt es vor allem Risiken in Bezug auf gemeinsam genutzte Ressourcen (grundlegende Netz-Infrastruktur, Hardware und physische Sicherheit); das Risiko ist geringer als bei den SaaS- und PaaS-Modellen.

Besondere Aspekte des PaaS-Dienstmodells

Bei diesem Dienstmodell werden dem Nutzer Betriebssysteme mit Programmiersprachen und anderer Software, einschließlich kompatibler Datenbestände vom Cloud-Anbieter angeboten und über virtuelle Maschinen bereitgestellt. Der Cloud-Nutzer hat nur Kontrolle über einige Konfigurationsaspekte der Plattform, die auf dieser Plattform entwickelten Anwendungen und die verarbeiteten Daten. Er hat keine Kontrolle über die zugrunde liegende Infrastruktur und die physische Sicherheit des Rechenzentrums.

- ***F5***
  - Mangelnde Transparenz bei einigen Aspekten der zugrunde liegenden technischen Infrastruktur (jedoch der Konfiguration der Softwareplattform und der Anwendungen, der Hardware und des Netzes) und bei relevanten technischen und organisatorischen Sicherheitsgarantien.
  - Kontrolle über die Sicherheitsmaßnahmen auf Ebene der Anwendungen und einiger auf Plattformebene. Eingeschränkte Kontrolle über die Sicherheit des Netzwerks und keine Kontrolle über die physische Sicherheit des Rechenzentrums.
  - Mögliche Umsetzung der Prüfbarkeit auf Ebene der Anwendung und der Plattform. Begrenzte oder keine Prüfbarkeit auf Netzwerkebene und keine Kontrolle über mögliche Audits der physischen Sicherheit.
  - Es können Instrumente zur Wahrung der Rechte betroffener Personen entwickelt werden.
  - Einige Herausforderungen bei der Datenübertragbarkeit aufgrund möglicher unterschiedlicher Umsetzungen der Software-Plattformen und mögliche Probleme bei unterschiedlichen Leistungen.

- ***F3***
  - Neben den bereits erwähnten Aspekten gehören hierzu auch die Verarbeitungsvorgänge durch unterschiedliche Nutzer auf dem gleichen Server.

Besondere Aspekte des SaaS-Dienstmodells

Dem Benutzer wird eine Software-Anwendung bereitgestellt, die spezifische Geschäftsvorgänge unterstützt. Der Cloud-Nutzer hat nur Kontrolle über die Konfiguration der cloudbasierten Anwendung und die verarbeiteten Daten. Er hat keinerlei Kontrolle über den OSS-Anwendungscode, die Datenbanken, die Webserver, die Anwendungsserver, die virtuellen Maschinen und die grundlegende Virtualisierungssoftware, die physischen Server, die Netz- und Sicherheitseinrichtungen sowie die physische Sicherheit des Rechenzentrums.

- ***F1***

- Das Risiko einer Unterminierung der Risiken oder der Auswahl ungeeigneter Sicherheitsgarantien ist höher, da die Unternehmensbereiche SaaS-Cloud-Dienste ohne ausreichende Beratung durch IT- und Datenschutzexperten vergeben könnten.

- ***F5***
  - Mangelnde Transparenz und Kontrolle über den Anwendungscode und die zugrunde liegende technische Infrastruktur und die technischen und organisatorischen Sicherheitsgarantien.
  - Keine Kontrolle über die Sicherheitsmaßnahmen, jedoch bei einigen auf Anwendungsebene (z. B. Nutzerauthentifizierung und Autorisierung für Anwendungsfunktionen).
  - Die mangelnde Umsetzung der Prüfbarkeit ist besonders hoch.
  - Möglicherweise fehlende Instrumente zur Wahrung der Rechte betroffener Personen.
  - Mangelnde Datenübertragbarkeit könnte durch spezifische Formate und andere mögliche Hindernisse wie Geschäftsregeln, spezifische Workflows, Einstellungen und Abhängigkeiten von anderen Anwendungen erhöht werden.

- ***F3***
  - Neben den bereits genannten Aspekten, können hier insbesondere z. B. Verarbeitungsvorgänge anderer Nutzer auf der gleichen virtuellen Maschine oder auch in der gleichen Anwendungsinstanz durchgeführt werden, was die Risiken weiter verstärkt.

Spezifische Probleme bei den Bereitstellungsmodellen ausgelagerter privater/Community-Clouds

Hier werden einige Rechner innerhalb des spezifischen Sicherheitsbereichs des oder der Nutzer in den Rechenzentren des Cloud-Anbieters für die ausschließliche Nutzung durch den oder die Cloud-Nutzer bereitgestellt.

- ***F2***

  Die Dienste werden nicht notwendigerweise über das öffentliche Internet angeboten: in diesem Fall bestehen keine relevanten Risiken.

  Eine spezielle Kommunikationsverbindung könnte verfügbar sein oder bereitgestellt werden. In diesem Fall:

  - Mögliche Vertraulichkeits- und Integritätsrisiken beschränken sich auf den Kommunikationsdienstanbieter.
  - Mangelnde Verfügbarkeit in Verbindung mit einer Nichtverfügbarkeit des Kommunikationsdienstanbieters (aufgrund einer technischen Störung o. ä.).
  - Mögliche Risiken in Verbindung mit der Vorratsdatenspeicherung für die Zwecke der Strafverfolgung.

- ***F3***
  - Das Risiko ist niedriger (auch des öffentlichen IaaS) und beschränkt sich häufig auf einige grundlegende Netz-Ressourcen und die physische Sicherheit. Nichtsdestotrotz befinden sich Systeme, die zuvor in unterschiedlichen Sicherheitsbereichen und mit unterschiedlichen Verantwortlichkeiten

bereitgestellt wurden, nun zusammen in einer Cloud und sind verschiedenen Sicherheitsrisiken ausgesetzt. Dies gilt umso mehr für Community-Clouds.

- ***F4***
  - Das Risiko ist wesentlich geringer oder besteht häufig gar nicht in einer ausgelagerten privaten Cloud.
- ***F5***
  - Die Risiken in Bezug auf die Transparenz, die Wahl der Sicherheitsmaßnahmen, die Prüfbarkeit sind wesentlich geringer, da der Nutzer im Allgemeinen hierüber mehr Kontrolle hat.
  - Wesentlich geringeres Risiko für die Wahrung der Rechte betroffener Personen, da eine im Allgemeinen stärkere Kontrolle als bei öffentlichen IaaS-Modell besteht.
  - Weniger mit der Datenübertragbarkeit zusammenhängende Risiken.
- ***F6***
  - Im Fall von externen Vertragspartnern bleibt das Risiko hoch, auch wenn es gewöhnlich niedriger ist als in öffentlichen Clouds, da der Nutzer mehr Macht bei Vertragsverhandlungen hat.
- ***F7***

Die Standorte sind dem Nutzer üblicherweise bekannt und er hat die Verarbeitung stärker unter Kontrolle:

- Wesentlich geringeres Risiko in Bezug auf Datenübertragungen und die Rechte betroffener Personen.
- Niedrigeres Risiko in Bezug auf die Vorratsdatenspeicherung und eine effektive Löschung, aufgrund der intrinsischen nahtlosen Mechanismen für die Zuweisung von Ressourcen in einer cloudbasierten Infrastruktur (Redundanz, dynamische Zuweisung, verteiltes Paradigma).

- ***F8***
  - Die folgenden Risiken sind sehr begrenzt, wenn das öffentliche Internet nicht als Kommunikationsverbindung zu den ausgelagerten Diensten verwendet wird:
    - Authentizität des beauftragten Dienstes
  - Die folgenden Risiken sind im Allgemeinen sehr begrenzt:
    - Schwierigkeiten bei der Verwaltung der Verschlüsselungsschlüssel
    - Schwierigkeiten bei der Verwaltung der Identitäten und Authentifizierungen

Spezifische Probleme beim Bereitstellungsmodell privat vor Ort/Community-Cloud

Hier wird die Infrastruktur innerhalb des Sicherheitsbereichs des oder der Cloud-Nutzer in deren Gebäuden bereitgestellt. Im Falle von Community-Clouds wird die Infrastruktur für alle bei einem oder mehreren Beteiligten gehostet.

- ***F2***
  - Die Dienste werden nicht über das öffentliche Internet angeboten: keine relevanten Risiken für private Clouds. Im Falle von Community-Clouds werden einige Cloud-Nutzer Kommunikationseinrichtungen für die Verbindung nutzen

müssen. In diesem Fall gelten die gleichen Aspekte wir bei ausgelagerten Community-Clouds.

- ***F3***
  - Grundsätzlich wesentlich geringere Risiken. Nichtsdestotrotz befinden sich Systeme, die zuvor in unterschiedlichen Sicherheitsbereichen und mit unterschiedlichen Verantwortlichkeiten bereitgestellt wurden, nun zusammen in einer Cloud und sind somit verschiedenen Sicherheitsrisiken ausgesetzt. Dies gilt umso mehr für Community-Clouds.
- ***F4***

Der physische Standort der Daten der Cloud-Nutzer ist den Nutzern bekannt: keine relevanten Risiken.

- ***F5***

  Im Allgemeinen sehr geringe oder keine Risiken, aber:
  - Einige sehr geringe Risiken in Bezug auf die Transparenz aufgrund der intrinsischen dynamischen und nahtlosen Mechanismen zur Zuweisung der Ressourcen in einer cloudbasierten Infrastruktur bleiben bestehen. Der Nutzer hat jedoch die vollständige Kontrolle darüber.
  - Es bleiben einige sehr geringe Risiken in Bezug auf die effektive Anwendung der Rechte betroffener Personen aufgrund der intrinsischen nahtlosen Mechanismen für die Zuweisung von Ressourcen in einer cloudbasierten Infrastruktur bestehen (Redundanz, dynamische Zuweisung, verteiltes Paradigma). Der Nutzer hat jedoch die vollständige Kontrolle darüber.
- ***F6***
  - Keine Risiken aufgrund unklarer Zuweisungen von Verantwortlichkeiten, wenn die Cloud-Infrastruktur vom eigenen Personal verwaltet wird.
- ***F7***

  Die Standorte sind dem Nutzer bekannt und er hat die Verarbeitung stärker unter Kontrolle:
  - Wesentlich geringeres oder kein Risiko in Bezug auf Datenübertragungen und die Rechte betroffener Personen.
  - Einige sehr geringe Risiken in Bezug auf die Vorratsdatenspeicherung bleiben lediglich aufgrund der intrinsischen nahtlosen Mechanismen für die Zuweisung von Ressourcen in einer cloudbasierten Infrastruktur bestehen (Redundanz, dynamische Zuweisung, verteiltes Paradigma).
- ***F8***
  - Die folgenden Risiken sind wesentlich geringer oder nicht länger spezifisch für die Cloud, da die Cloud-Infrastruktur privat und nicht ausgelagert ist:
    - Schwierigkeiten bei der Verwaltung der Verschlüsselungsschlüssel
    - Schwierigkeiten bei der Verwaltung der Identitäten und Authentifizierungen
    - Authentizität der beauftragten Dienste.

Anhang 5. Literaturangaben und weitere nützliche Quellen

Politische Schriften des EDSB, der Artikel-29-Datenschutzgruppe

- Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa“, November 2012:

  https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_de.pdf

- Stellungnahme 05/2012 der Artikel-29-Datenschutzgruppe zum Cloud-Computing:

  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf

Politische Schriften von anderen Datenschutzbehörden der EU

- „Guidance on the use of cloud computing“ - UK Information Commissioner’s Office (ICO), Oktober 2012:

  https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

- „Personal data protection and cloud computing“ - Informationsbeauftragter von Slowenien, Juni 2012:

  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf

- „Data protection ‘in the cloud“ - Datenschutzbeauftragter von Irland, Juli 2012:

  https://www.dataprotection.ie/docs/03/07/12_Cloud_Computing/1221.htm

- „Recommendations for companies planning to use Cloud computing services“ - Commission Nationale de l’Informatique et des Libertés (Frankreich), Juni 2012:

  https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

- „Cloud computing: how to protect your data without falling from a cloud“ - Vademecum - Garante per la Protezione dei Dati Personali:

  http://194.242.234.211/documents/10160/2052659/CLOUD+COMPUTING+%E2%80%93+PROTECT+YOUR+DATA+WITHOUT+FALLING+FROM+A+CLOUD.pdf

- Guía para clientes que contraten servicios de Cloud Computing - 2013, Agencia Española de Protección de Datos:

  http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

- Resolution on cloud computing, Punta del Este, Uruguay, 26. Oktober 2012, 34° Conferencia Internacional de Autoridades de protección dos datos y privacidad:

  http://194.242.234.211/documents/10160/2150357/Resolution+on+Cloud+Computing.pdf

Schriften und Referenzen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA)

- ENISA zum Cloud-Computing https://www.enisa.europa.eu/topics/cloud-and-big-data

Siehe insbesondere:

- Einschlägige Veröffentlichungen: https://www.enisa.europa.eu/topics/cloud-and-big-data?tab=publications
- Einschlägige Artikel: https://www.enisa.europa.eu/topics/cloud-and-big-data?tab=articles
- Zur Cloud-Sicherheit: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

Schriften von Normungseinrichtungen

- „Privacy in Cloud Computing" - International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) Watch Report, März 2012:

  http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

- ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services:

  https://www.iso.org/standard/43757.html

- ISO/IEC 27018:2014 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors:

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

Schriften der Industrie: die Cloud Select Industry Group (CSIG)

- „Cloud Service Level Agreement Standardisation Guidelines" - Cloud Select Industry Group - Brüssel, 24. Juni 2014:

  https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

Schriften der Industrie: die Cloud Security Alliance (CSA)

https://cloudsecurityalliance.org/download/

Schriften der Internationalen Arbeitsgruppe für den Datenschutz in der Telekommunikation (Berliner Gruppe)

- Arbeitspapier Cloud-Computing - Fragen des Schutzes der Privatsphäre und des Datenschutzes - „Sopot Memorandum", Berliner Gruppe, April 2012:

  https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2012/2012-WP-Sopot_Memorandum-de.pdf

Technisches Dokument des NIST

- NIST Cloud Computing Program

  https://www.nist.gov/programs-projects/cloud-computing

- „The NIST Definition of Cloud Computing“ - NIST Special Publication 800-145, September 2011:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- „Cloud Computing Synopsis and Recommendations“ - NIST Special Publication 800-146, Mai 2012:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

- „Guidelines on Security and Privacy in Public Cloud Computing“ - NIST Special Publication 800-144, Dezember 2011:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Sonstige technische und politische Schriften

- „Cloud Computing Security Considerations“ - Australisches Verteidigungsministerium - Abteilung Intelligence and Security - Cyber Security Operations Centre, September 2012:

  http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf