Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Fragebogen zur Nutzung von cloud-basierten Diensten

I. Allgemeine Fragen zur Nutzung der Cloud

1. Nutzen Sie[1] derzeit Cloud-Dienstanbieter[2] (cloud service provider, im Folgenden: CSP) oder planen Sie dies in naher Zukunft (bis Ende 2022)?

2. Falls Sie derzeit CSP nutzen, machen Sie bitte für jeden Anbieter folgende Angaben:

   Allgemeine Informationen zum CSP und zum Vertrag
   a) Wie lautet der Name des CSP?
   b) Wie lautet der Name der juristischen Person, mit der der Vertrag unterzeichnet wurde, und welche Einrichtungen des CSP sind für die Verarbeitung relevant (z. B. weil sie an der Verarbeitung beteiligt sind oder weil der CSP eine Tochtergesellschaft eines größeren Unternehmens ist)?
   c) Welches ist das Anfangs- und Enddatum des Vertrags und gibt es ggf. Termine für die Verlängerung oder geplante Änderungen der Dienste?
   d) Welche Bereitstellungsmodelle (öffentlich/privat/hybrid/gemeinschaftlich)[3]und Dienstmodelle (SaaS, PaaS, DSaaS, IaaS...)[4] werden verwendet?
   e) Welches (nationale) Vertragsrecht gilt für den Vertrag?
   f) Gibt es eine Datenschutz-Folgenabschätzung für die Datenverarbeitung durch diesen CSP?

   Arten der verarbeiteten personenbezogenen Daten
   g) Welche Kategorien personenbezogener Daten werden vom CSP verarbeitet? Umfasst dies besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) oder höchst persönliche Daten[5], wie Finanzdaten? Bitte machen Sie nähere Angaben.
   h) Wessen personenbezogene Daten werden in der Cloud verarbeitet (personenbezogene Daten von Beschäftigten, personenbezogene Daten von Bürgerinnen und Bürgern oder anderen Personen)?
   i) Für welche Funktionen wird der Dienst genutzt (interne Bürotätigkeiten, Kommunikation, Personal, Dienstleistungen für die Bürgerinnen und Bürger, Entwicklungstools, Server), und betrifft dies die öffentliche Kernfunktion Ihrer Organisation? (Wenn dieser Fragebogen an einen zentralen Einkäufer gerichtet ist, beantworten Sie bitte diese Frage und geben Sie an, für welche öffentlichen Stellen die Dienste der CSP erworben werden und ob ihre öffentlichen Kernfunktionen betroffen sind.)

---

[1] Wenn es sich bei dem Adressaten des Fragebogens um einen zentralen Einkäufer für staatliche Stellen handelt, ist „Sie“ als Bezugnahme auf die staatlichen Stellen, für die Sie als Einkäufer Dienstleistungen erbracht haben, zu verstehen. Dies gilt für den gesamten Fragebogen.
[2] Bitte nennen Sie nur die CSP, die personenbezogene Daten verarbeiten.
[3] Siehe Anhang (die Begriffe werden aus ISO 17788 übernommen).
[4] Siehe Anhang (die Begriffe werden aus ISO 17788 übernommen).

[5] Siehe die Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) des EDSA und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung (EU) 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“.

j) Verarbeitet der CSP Telemetrie[6]-/Diagnosedaten? Bitte geben Sie die Kategorien personenbezogener Daten an, die erhoben werden. (: Bitte beachten Sie, dass ab Frage 29 weitere Fragen zu Telemetrie-/Diagnosedaten gestellt werden.)

Identifizierung der Rollen

k) Welche Rollen nehmen Ihre Organisation und der CSP bei diesem Vertrag ein (d. h. Verantwortlicher, gemeinsam Verantwortlicher oder Auftragsverarbeiter)?

l) Wenn Sie mit dem CSP in einer Beziehung als Verantwortlicher/Auftragsverarbeiter stehen: Gibt es einen Vertrag gemäß Artikel 28 Absatz 3 DSGVO[7]? (Bitte beachten Sie, dass sich Frage 13 auf die Bestimmungen dieses Vertrags bezieht, die hier nicht näher ausgeführt werden müssen.)

m) Wenn Sie mit dem CSP gemeinsam Verantwortlicher sind, verwendet der CSP Daten (einschließlich Diagnose-/Telemetriedaten) für eigene Zwecke? Falls ja, beantworten Sie bitte die nachstehenden Fragen:
   - Zu welchem Zweck verwendet der CSP die Daten?
   - Haben Sie eine Bewertung der Daten vorgenommen, die der CSP für seine eigenen Zwecke verwendet?
   - Auf welcher Rechtsgrundlage beruht die Verarbeitung durch den CSP?

n) Haben Sie Unterauftragsverarbeiter ermittelt, die vom CSP verwendet werden? Wenn ja, bitte erläutern Sie.

II. Erwerb von Diensten eines CSP

Hinweis: Wenn es sich bei dem Adressaten des Fragebogens um einen zentralen Einkäufer für staatliche Stellen handelt, beantworten Sie bitte die folgenden Fragen, die sich auf die verschiedenen staatlichen Stellen beziehen, für die Sie Dienstleistungen erbracht haben.

3. Bitte beschreiben Sie das Verfahren, das Sie befolgt haben (oder befolgen würden), einschließlich einer etwaigen Datenschutz-Risikobewertung in Bezug auf Ihre Organisation, um festzustellen, ob eine Cloud eine geeignete Lösung für Ihren Bedarf wäre, und um einen bestimmten CSP auszuwählen. Bitte geben Sie insbesondere an, welche obligatorischen Datenschutzanforderungen ein CSP, den Sie auswählen wollen, erfüllen müsste und ob diese im Rahmen des Beschaffungsverfahrens explizite Zuschlagskriterien bilden.

4. Führt Ihre Organisation vor dem Erwerb Cloud-basierter Dienste eine Datenschutz-Folgenabschätzung durch oder verlangt sie beim CSP eine Datenschutz-Folgenabschätzung? Wenn ja, wie und wo passt eine Datenschutz-Folgenabschätzung in den Erwerbsprozess? Beziehen Sie bitte bei der Beantwortung der Fragen mit ein, wie mit den ermittelten Risiken im Erwerbsprozess umgegangen wurde. Dies kann insbesondere Anwendungs- und Schnittstellensicherheit, Identitäts- und Zugangsmanagement, Verschlüsselung und Schlüsselverwaltung, physische

[6] Telemetriedaten sind Daten, die durch die Nutzung des Dienstes, auch für Sicherheitszwecke, generiert werden.

[7] Artikel 29 Absatz 3 EU-DSVO.

Sicherheit, Virtualisierung und Sicherheit der Netzarchitektur, betriebliche Trennung und Mandantenfähigkeit, Vorfallmanagement usw. umfassen.
Falls Sie keine Datenschutz-Folgenabschätzung durchgeführt haben, erläutern Sie bitte, warum Ihrer Ansicht nach die Verarbeitung wahrscheinlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen würde.

5. Stützen Sie sich bei der Bewertung des CSP auf nationale/internationale Normen oder gängige Standards (z. B. ISO 27001/ISO 27701), entweder weil Sie dieser Zertifizierung für einen Teil Ihrer eigenen Bewertung vertrauen oder weil diese eine Ihrer Anforderungen für die Auswahl ist? Wenn dies der Fall ist und wenn der Cloud-Dienst (nach einer ISO- oder nationalen Zertifizierung) zertifiziert ist[8], welche Informationen über die Zertifizierung werden Ihnen zur Verfügung gestellt (Zertifizierungsbericht, Zusammenfassung des Berichts) und wie oft?

6. Hat Ihre Organisation beim Erwerb von Cloud-basierten Diensten für ihre Verarbeitung untersucht, wo die Daten (physisch) verarbeitet (wohin übertragen, wo gespeichert und von wo abgerufen) werden?
   Falls der CSP Unterauftragsverarbeiter beauftragt hat, hat Ihre Organisation geprüft, wo (physisch) die von diesen Unterauftragsverarbeitern verarbeiteten Daten übertragen, gespeichert und abgerufen werden?

7. Ist Ihre Organisation bei der Nutzung der Cloud auf regulatorische Herausforderungen gestoßen (z. B. strenge Vorschriften für die Nutzung Cloud-basierter Dienste durch öffentliche Stellen)? Falls dies der Fall ist, geben Sie bitte an, auf welche Herausforderungen Sie gestoßen sind und wie Sie mit diesen umgegangen sind.

8. Konsultiert Ihre Organisation während des Erwerbsprozesses ihren eigenen Datenschutzbeauftragten (ungeachtet einer etwaigen Konsultation des DSB des CSPs)? Bitte erläutern Sie, warum (nicht).

9. Hat Ihre Organisation trotz einer ablehnenden Stellungnahme Ihres DSB Cloud-Dienste erworben?

10. Falls die Aufsichtsbehörde gemäß Artikel 36 Absatz 1 oder Artikel 36 Absatz 5 DSGVO[9] konsultiert wurde, wie haben Sie das Ergebnis dieser Konsultation umgesetzt?

III. Der Vertrag mit dem Cloud-Dienstanbieter

Bitte beantworten Sie die folgenden Fragen, indem Sie auf jeden der in Frage 1 aufgeführten CSP verweisen.

---

[8] Oder wenn er sich an einen Verhaltenskodex hält.
[9] Artikel 40 Absatz 1 oder Artikel 40 Absatz 4 EU-DSVO.

11. Wenn Sie in einem Verhältnis zum CSP als gemeinsam Verantwortlicher stehen: Sind die in Artikel 26 DSGVO[10] festgelegten Verpflichtungen entsprechend erfüllt? Bitte erläutern Sie überblicksweise, wie Sie sichergestellt haben, dass der CSP die Verpflichtungen erfüllt.

12. Handelt der CSP als Auftragsverarbeiter, gilt Artikel 28 DSGVO[11] für den Vertrag mit dem Auftragsverarbeiter. Bitte erläutern Sie allgemein, wie Sie sichergestellt haben, dass der CSP die folgenden Verpflichtungen erfüllt.

    Der CSP verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen.
    Der CSP gewährleistet mit allen erforderlichen Mitteln, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
    Der CSP trifft alle erforderlichen Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten.
    Der CSP beauftragt keinen Unterauftragsverarbeiter ohne Ihre vorherige Genehmigung. (Insbesondere, wenn der CSP Unterauftragsverarbeiter verwendet, haben Sie diese Genehmigung erteilt?)
    Der CSP unterstützt Sie, soweit dies möglich ist, bei der Erfüllung Ihrer Verpflichtung, Anträge auf Ausübung der Rechte der betroffenen Person zu beantworten.
    Der CSP unterstützt Sie bei der Gewährleistung der Sicherheit der Verarbeitung.
    Der CSP löscht alle personenbezogenen Daten oder gibt Ihnen bei Vertragsende alle personenbezogenen Daten zurück.
    Der CSP ermöglicht Ihnen oder einer anderen Person, die Sie beauftragt haben, Prüfungen durchzuführen oder an Prüfungen mitzuwirken. Bitte geben Sie insbesondere an, welche Prüfungsrechte Sie in Bezug auf den CSP haben und ob diese im Vertrag enthalten sind.

13. Enthält der Vertrag mit dem CSP Bestimmungen über Kontrollen/Anforderungen in Bezug auf die Meldung von Datenschutzverletzungen?

14. Hat Ihre Organisation bei der Aushandlung von Vertragsbedingungen mit CSP mit z.B. zentralen Einkäufern oder anderen Behörden in anderen Ländern, auf nationaler oder internationaler Ebene zusammengearbeitet? Bitte erläutern Sie, welche Auswirkungen diese Zusammenarbeit auf die Vertragsbedingungen hatten und ob Sie die Ergebnisse der Verhandlungen mit den Parteien, mit denen Sie zusammengearbeitet haben, geteilt haben.

15. Hat Ihre Organisation erfolgreich Verhandlungen über Vertragsbedingungen geführt, um die mit ihrer Verarbeitung verbundenen Risiken zu mindern?
    Falls ja, beschreiben Sie bitte die Ergebnisse.
    Falls nein, erläutern Sie bitte die Gründe, einschließlich etwaiger Hindernisse, die bei
    dem Verfahren aufgetreten sind.

[10] Artikel 28 EU-DSVO.
[11] Artikel 29 EU-DSVO.

16. Hat die Organisation eine Leistungsvereinbarung für die Dienste verlangt/ausgehandelt?

17. Hat Ihre Organisation vertragliche, technische und/oder organisatorische Maßnahmen ergriffen oder ausgehandelt, um die Verarbeitung personenbezogener Daten durch den CSP (insbesondere für seine eigenen Zwecke oder in Bezug auf den Ort der Verarbeitung) bei der Nutzung der beschafften Cloud-Dienste einzuschränken? Wenn ja, beschreiben Sie bitte die ergriffenen Maßnahmen und erläutern Sie die Gründe für die Einführung dieser Maßnahmen. (Bitte beachten Sie, dass ab Frage 20 weitere Fragen zu internationalen Übermittlungen gestellt werden.)

18. Haben Sie Kontrollen durchgeführt, um die Reversibilität/ Beendigung eines Vertrags sicherzustellen, z. B. wenn Sie sich für einen Wechsel zu einem anderen Anbieter entscheiden? Bitte erläutern Sie allgemein, welche Kontrollen Sie durchgeführt haben.

IV. Einzelheiten des Vertrags: internationale Übermittlungen

Bitte beantworten Sie die folgenden Fragen, indem Sie auf jeden der in Frage 1 aufgeführten CSP verweisen.

19. Übermittelt der CSP (und seine Unterauftragsverarbeiter) personenbezogene Daten (einschließlich Diagnose-/Telemetriedaten) in Drittländer? Falls ja, beantworten Sie bitte die nachstehenden Fragen.

20. Hat Ihre Organisation vertragliche, technische und/oder organisatorische Maßnahmen ergriffen oder ausgehandelt, um datenschutzkonforme internationale Datenübermittlungen zu gewährleisten? Hat Ihre Organisation insbesondere die Datenverarbeitung (Verarbeitung, Übermittlung und Speicherung) auf bestimmte Standorte oder Länder beschränkt? Falls ja, beschreiben Sie bitte die Maßnahmen.

21. Wenn Ihre Organisation personenbezogene Daten (einschließlich Diagnose -/Telemetriedaten) an Drittländer übermittelt, beschreiben Sie bitte, welches Übermittlungsinstrument gemäß Kapitel V DSGVO[12] von Ihrer Organisation genutzt wird.

22. Falls Sie sich auf Standardvertragsklauseln stützen, geben Sie bitte an, welches Muster der Kommission für den Abschluss von Standardvertragsklauseln verwendet wird (Datum und Typ, z. B. Standardvertragsklauseln für Verantwortliche an Auftragsverarbeiter oder Auftragsverarbeiter an Auftragsverarbeiter).

23. Wenn Ihre Organisation Standardvertragsklauseln für Datenübermittlungen abgeschlossen hat oder wenn sie sich auf die verbindlichen internen Datenschutzvorschriften des CSP stützt, wurde anhand des Schrems-II-Urteils geprüft, ob die Rechtsvorschriften und/oder Praktiken des Drittlandes es den Empfängern untersagen, ihren vertraglichen Verpflichtungen

[12] Kapitel V EU-DSVO oder Kapitel V DSGVO.

nachzukommen, um sicherzustellen, dass das im EWR garantierte Datenschutzniveau für natürliche Personen nicht untergraben wird?

24. Wenn Ihre Organisation zu dem Schluss gelangt ist, dass der Datenimporteur die Erfüllung der verbindlichen internen Datenschutzvorschriften oder der vertraglichen Verpflichtungen gemäß den Standardvertragsklauseln faktisch garantieren kann, erläutern Sie bitte ausführlich die Gründe für diese Schlussfolgerung.

25. Falls Ihre Organisation zu dem Schluss gelangt ist, dass die Maßnahmen für die Übermittlung gemäß Kapitel V DSGVO[13] nicht ausreichend effektiv sind (z. B. vertragliche Verpflichtungen in den Standardvertragsklauseln oder in den verbindlichen internen Datenschutzvorschriften), wurde die Umsetzung ergänzender Maßnahmen erwogen, und wenn ja, welcher? Hat Ihre Organisation geprüft, ob diese zusätzlichen Maßnahmen in der Praxis umgesetzt werden können und dass die Rechtsvorschriften und/oder Praktiken von Drittländern nicht daran hindern, diese Maßnahmen anzuwenden, um sicherzustellen, dass das im EWR garantierte Datenschutzniveau für natürliche Personen nicht untergraben wird? Bitte beschreiben Sie ausführlich das Ergebnis dieser Bewertung und die Gründe für Ihre Schlussfolgerung.

26. Hat Ihre Organisation Ihren DSB bei der Bewertung speziell zu den rechtlichen Anforderungen an internationale Übermittlungen eingebunden? Wenn ja, was hat der DSB empfohlen?

27. Wurden Sie über Anträge auf Offenlegung von Daten unterrichtet, die von Regierungsbehörden eines Drittlands an den CSP (oder einen der Unterauftragsverarbeiter) gerichtet wurden? Wenn ja, was war der Gegenstand der informativen Mitteilung?

V. Vertragliche Einzelheiten: Erhebung und Verarbeitung von Diagnose-/Telemetriedaten durch den CSP

Bitte beantworten Sie die folgenden Fragen unter Bezugnahme auf die einzelnen unter den Fragen 1 und 2 aufgeführten CSP und deren Unterauftragsverarbeiter.

28. Wenn der CSP bei der Nutzung der Cloud-Dienste Diagnose-/Telemetriedaten erhebt und verarbeitet, wie tut er dies? Bitte unterscheiden Sie nach Dienst/Art/Komponente.
    a. Werden diese Daten auf Kundenseite oder auf den Servern des CSP erhoben?
    b. Sind diese Daten anonymisiert oder pseudonymisiert?
        i. Bei Pseudonymisierung:
            (a) Wo findet die Pseudonymisierung statt? Auf Kundenseite oder auf den Servern des CSP?
            (b) Wie wird die Pseudonymisierung durchgeführt (Techniken, Kennungen usw.)?
        ii. Bei Anonymisierung:
            (a) Wo findet die Anonymisierung statt? Auf Kundenseite oder auf den Servern des CSP?

[13] Kapitel V EU-DSVO oder Kapitel V DSGVO.

(b) Wie wird die Anonymisierung durchgeführt (Techniken, Aggregationsebene, soweit zutreffend)?

c. Werden diese Daten standardmäßig erhoben oder nicht? Wenn ja, welche Kontrollen bietet der CSP an, um die Erhebung und Verarbeitung zu begrenzen?

d. Welche Sicherheitskontrollen wenden Sie an, um diese Daten in der Übermittlung, im Speicher und im Ruhezustand zu schützen?

29. Erhebt und verarbeitet der CSP Diagnose-/Telemetriedaten oder andere Informationen infolge der Nutzung der Cloud-Dienste, die Ihre Organisation und/oder der CSP nicht als personenbezogene Daten ansehen? Bitte unterscheiden Sie nach Dienst/Art/Komponente.

VI. Compliance

30. Überwachen Sie die geeigneten technischen und organisatorischen Maßnahmen, einschließlich der Sicherheitsmaßnahmen der CSP, um zu überprüfen[14], ob sie Ihren vereinbarten Anforderungen und/oder Verpflichtungen der CSP und/oder internationalen Standards entsprechen? Bitte beschreiben Sie Ihr diesbezügliches Verfahren.

31. Umfasst dies regelmäßige Datenschutz-Risikobewertungen, einschließlich Bewertungen der Risiken für die Informationssicherheit (ex-post) in Bezug auf die Umsetzung des Cloud-Computing? Wenn ja, wie überwachen Sie diese, welche Aspekte des Vertrags werden von Ihnen überwacht und wie oft?

32. Überwachen Sie unter Berücksichtigung der erforderlichen Überprüfung und Aktualisierung von Strategien und Maßnahmen (z. B. Garantien für internationale Datenübermittlungen oder allgemeiner Entwicklungen bei Leitlinien und Rechtsprechung) die Einhaltung der Anforderungen der DSGVO im Allgemeinen, über die strengen vertraglichen Vereinbarungen hinaus? Bitte beschreiben Sie kurz Ihre diesbezüglichen Handlungen.

[14] Dazu gehört auch die Überprüfung der Wirksamkeit der Maßnahmen.

Anhang – Begriffsbestimmungen

Die folgende Terminologie, die in diesem Dokument enthalten ist, wurde aus ISO 17788[15] übernommen.

Cloud-Computing	Paradigma zur Ermöglichung des Netzzugangs zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer physischer oder virtueller Ressourcen mit Selbstbedienung und Verwaltung auf Abruf.
Cloud-Dienst	Eine oder mehrere Funktionen, die über Cloud-Computing unter Verwendung einer definierten Schnittstelle angeboten
Cloud-Dienstanbieter (CSP)	Partei, die Cloud-Dienste bereitstellt
Gemeinschaftliche Cloud	Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste ausschließlich eine bestimmte Reihe von Cloud-Dienstkunden unterstützen, die diese gemeinsam nutzen und gemeinsame Anforderungen und eine Beziehung zueinander haben, und bei dem die Ressourcen von mindestens einem Mitglied dieser Reihe kontrolliert werden.
Compute as a Service (CompaaS)	Cloud-Dienstkategorie, in der die dem Cloud-Dienstkunden zur Verfügung gestellten Funktionen in der Bereitstellung und Nutzung von Verarbeitungsressourcen bestehen, die für die Bereitstellung und den Betrieb von Software erforderlich sind.
Data Storage as a Service (DSaaS)	Cloud-Dienstkategorie, in der die dem Cloud-Dienstkunden zur Verfügung gestellte Funktion die Bereitstellung und Nutzung von Datenspeicherung und damit zusammenhängenden Funktionen ist.
Hybride Cloud	Cloud-Bereitstellungsmodell unter Verwendung von mindestens zwei verschiedenen Cloud-Bereitstellungsmodellen
Infrastructure as a Service (IaaS)	Cloud-Dienstkategorie, in der die Art der Cloud-Funktionen, die dem Cloud-Dienstkunden zur Verfügung gestellt werden, eine Art von Infrastruktur ist.
Platform as a Service (PaaS)	Cloud-Dienstkategorie, in der die Art der Cloud-Funktionen, die dem Cloud-Dienstkunden zur Verfügung gestellt werden, eine Art von Plattform ist.
Private Cloud	Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste ausschließlich von einem einzigen Cloud-Dienstkunden genutzt werden und die Ressourcen von diesem Cloud-Dienstkunden kontrolliert werden.
Öffentliche Cloud	Cloud-Bereitstellungsmodell, bei dem Cloud-Dienste potenziell jedem Kunden von Cloud-Diensten zur Verfügung stehen und die Ressourcen vom Cloud-Dienstanbieter kontrolliert werden.
Umkehrbarkeit	Verfahren für Cloud-Dienstkunden, um Kundendaten und Anwendungsartefakte abzurufen und unter dem der Cloud-Dienstanbieter nach einem vereinbarten Zeitraum alle Cloud-Dienstkundendaten sowie vertraglich festgelegte Daten aus Cloud-
Software as a Service (SaaS)	Cloud-Dienstkategorie, in der die Art der Cloud-Funktionen, die dem Cloud-Dienstkunden zur Verfügung gestellt werden, eine Art von Anwendung ist.

[15] ISO/IEC 17788: Informationstechnik – Cloud Computing – Übersicht und Vokabular

Mandant	Ein oder mehrere Nutzer von Cloud-Diensten, die den Zugang zu einer Reihe physischer und virtueller Ressourcen teilen.