c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob die Prävention vor bzw. die Reaktion auf Notfälle oder Krisen durch die Cloud-Nutzung geändert werden muss. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.

2.2 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters.

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) vom Cloud-Diensteanbieter erfüllt werden können.[25]

b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der „*Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5*“[26] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN

- die angemessene und wirksame Umsetzung der Basiskriterien nach C5[27],
- die aktuelle Dokumentation der Systembeschreibung[28],
- die Aktualität von vertraglich zugesicherten Zertifizierungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

umfassen und durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise DARF die Einrichtung NUR in begründeten Einzelfallentscheidungen zulassen.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

g) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

h) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen abdecken oder diese Risiken transferieren oder diese Risiken tragen.

---

[25] Hinweis: Liegt ein Prüfbericht nach C5 vor, können diese Informationen daraus entnommen werden.

[26] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, welche die Einrichtung darin unterstützt, einen C5-Bericht systematisch auszuwerten. Dies beinhaltet, die Sicherheitsmaßnahmen des Cloud-Diensteanbieters (und die zugehörigen Prüfergebnisse) aufzunehmen, die eigenen Nutzerkontrollen für die Nutzung einzurichten und hierdurch das mit der Cloud-Nutzung verbundene Risiko einzuschätzen und steuern zu können. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), https://www.bsi.bund.de

[27] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[28] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (BSI 2020a), Kap. 4.4.5, S.16f.) enthält der Bericht keine Systembeschreibung vom Anbieter, sondern eine vom Prüfer im Rahmen der Prüfung erhobene Beschreibung mit vergleichbarem Inhalt, die im Rahmen der Tätigkeiten dieses Mindeststandards herangezogen werden kann.

Feldfunktion geändert

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.

i) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

i) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit Rechtsvorschriften nicht entgegenstehen.

ii) Die Einrichtung MUSS darauf achten, dass die Prüfrechte so ausgestaltet sind, dass die Einrichtung ihre gesetzlichen Anforderungen erfüllt.

iii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Einrichtung selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.

iv) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS die Einrichtung dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern

a) Die Einrichtung MUSS sich die Beteiligung von relevanten Unterauftragnehmern und anderen externen Dritten vom Cloud-Diensteanbieter vollständig in Art und Umfang benennen lassen. Die Entscheidung, welcher Unterauftragnehmer hier zu nennen ist, MUSS gemäß den Vorgaben des C5[29] erfolgen.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass beabsichtigte Änderungen hierüber unverzüglich schriftlich oder per E-Mail mitgeteilt werden.

c) Diese Mitteilungen KÖNNEN über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).

d) Falls Unterauftragnehmer wesentliche Teile[30] zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

- Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und
- zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.

NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

[29] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), Kap. 4.4.5, S.18f.
[30] Hinweis: Hinsichtlich Bestimmung „wesentlicher Teile“ siehe C5, (BSI 2020a), S.91

NCD.2.2.04 Lokation vertraglich zusichern

a) Die Einrichtung MUSS sämtliche Lokationen, an denen dienstliche Daten verarbeitet werden, vertraglich festlegen.

b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten.

NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.[31]

b) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS bei Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf achten.

ii) Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln

a) Die Einrichtung MUSS Kündigungsfristen dem Einsatzszenario angemessen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern

a) Die Einrichtung MUSS die Rückgabe der Daten regeln (Format, Datenträger, Protokolle, usw.).

b) Die Einrichtung MUSS berücksichtigen, dass die Maßnahmen zur Datenlöschung dem ermittelten Schutzbedarf entsprechen.

2.3 Einsatzphase

Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

NCD.2.3.01 ISMS einbinden

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen des Cloud-Dienstes bei sich einrichten. Die Einrichtung SOLLTE bei der Einbindung in das eigene ISMS zusätzlich die korrespondierenden Kriterien des C5[32] berücksichtigen.

NCD.2.3.02 Sicherheitsnachweise prüfen

[31] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (BMI 2014), S.1

[32] Hinweis: Der C5 führt mit Version 2020 Mitwirkungspflichten des Kunden als korrespondierende Kriterien ein. Die Umsetzung liegt im Verantwortungsbereich des Kunden und ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[33]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellte Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

NCD.2.3.03 Leistungsfähigkeit prüfen

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, beurteilen.

b) Die Einrichtung MUSS auf Abweichungen reagieren und die eigene IT-Infrastruktur und Netzanbindung den Ergebnissen der Überprüfung anpassen.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieter, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen.[34]

NCD.2.3.04 Informationspflichten nachhalten

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

i) einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,

ii) einem Austausch von Unterauftragnehmern oder Dritten.

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren

a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung als Identitätsnachweis seiner Benutzer (Log-in) an, SOLLTE die Einrichtung diese nutzen.

2.4 Beendigungsphase

Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[35]

NCD.2.4.01 Datenrückgabe durchführen

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

NCD.2.4.02 Datenlöschung bestätigen

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die Datenlöschung dokumentieren.

[33] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI CS“, (BSI 2020c), https://www.bsi.bund.de

[34] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann. Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden.

[35] Siehe OPS.2.2.A14 *Geordnete Beendigung eines Cloud-Nutzungsverhältnisses*, (BSI 2020b), S.1ff

Feldfunktion geändert

2.5 Sicherheitsanforderungen bei einer Mitnutzung

Nehmen Benutzer einer Einrichtung einen externen Cloud-Dienst in Anspruch, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[36] Für diesen Anwendungsfall regeln die nachfolgenden Sicherheitsanforderungen das Mindestsicherheitsniveau.

NCD.2.5.01 Mitnutzung von externen Cloud-Diensten

a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d) bis i) umsetzen und einhalten.

b) Die Einrichtung MUSS ermitteln, an welchen Lokationen dienstliche Daten verarbeitet werden.

i) Die Einrichtung MUSS dann bewerten, ob aus ihrer Sicht die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung heranziehen.

c) Die Einrichtung MUSS ermitteln, welche Rechte dem Cloud-Diensteanbieter oder Dritten an den dienstlichen Daten eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit der eigenen Sicherheitsrichtlinie vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar sind.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

e) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS dann bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen IT-Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[37]

[36] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen sind nicht als ein Vertragsverhältnis im Sinne dieses Mindeststands anzusehen.
[37] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017), S.1ff.

Literaturverzeichnis

AKTM (2011) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014

BMI (2014) Bundesministerium des Innern, Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung

BMI (2018) Bundesministerium des Innern, für Bau und Heimat: Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 – Notfallmanagement, Version 1.0

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management, Version 1.0

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/11916758, abgerufen am 17.11.2020

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: Kriterienkatalog Cloud Computing, Version 1.0 – Stand Februar 2020

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 3. Edition 2020

BSI (2020c) Bundesamt für Sicherheit in der Informationstechnik: Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5, https://www.bsi.bund.de/dok/14020574, abgerufen am 17.11.2020

DIN (2018) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119, abgerufen am 17.11.2020

Feldfunktion geändert

Feldfunktion geändert

Feldfunktion geändert

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BDSG	Bundesdatenschutzgesetz
C5	Kriterienkatalog Cloud Computing
DIN	Deutsches Institut für Normierung e.V.
FAQ	Frequently Asked Questions
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
IT-SiBe	IT-Sicherheitsbeauftragte
StGB	Strafgesetzbuch
RFC	Request for Comments
VSA	Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)

Von: [redacted]@polizei.bund.de im Auftrag von [redacted]@polizei.bund.de
An: GP Mindeststandards Bund
Cc: [redacted]@polizei.bund.de; [redacted]@polizei.bund.de
Betreff: WG: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Datum: Mittwoch, 6. Januar 2021 12:53:07
Anlagen: CDR_MST-NCD-RfC-Beta-1.0.5.docx

BPOLP - Referat 55
19 11 00 - 0001 - 0023

Sehr geehrte Damen und Herren,

Die im Anschreiben aufgeführten wesentlichen Änderungen begrüße ich ausdrücklich.

die Hinweise aus der Bundespolizei sind in den Entwurf zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste im Überarbeitungsmodus eingearbeitet.

Ich bedanke mich für die Beteiligung.

Mit freundlichen Grüßen
[redacted]

Bundespolizeipräsidium | Referat 55 | Heinrich-Mann-Allee 103 | 14473 Potsdam

Telefon: [redacted] | Mobil: [redacted] | Fax: -[redacted]
E-Mail: [redacted]@polizei.bund.de
E-Mail: [redacted]@polizei.bund.de
Internet: www.bundespolizei.de

-----Ursprüngliche Nachricht-----
Von: CI4@bmi.bund.de <CI4@bmi.bund.de>
Gesendet: Dienstag, 24. November 2020 15:55
An: [redacted]@bdbos.bmi.bund.de; P Post [redacted]@polizei.bund.de>; [redacted]@bva.bund.de; [redacted]@bsi.bund.de; [redacted]@bbk.bund.de; [redacted]@badv.bund.de; [redacted]@bakoev.bund.de; [redacted]@bamf.bund.de; [redacted]@bbk.bund.de; [redacted]@bbr.bund.de; [redacted]@bescha.bund.de; [redacted]@bfv.bund.de; [redacted]@bib.bund.de; [redacted]@bisp.de; [redacted]@bka.bund.de; [redacted]@bkg.bund.de; [redacted]@bpb.bund.de; [redacted]@polizei.bund.de>; [redacted]@bsi.bund.de; [redacted]@hsbund.de; [redacted]@destatis.de; [redacted]@thw.bund.de; [redacted]@zitis.bund.de; [redacted]@ZITiS.bund.de; [redacted]@bmi.bund.de; [redacted]@bakoev.bund.de

Cc: CI4@bmi.bund.de; RegCI4@bmi.bund.de
Betreff: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0

CI 4 - 17002/20#11

Liebe Kolleginnen und Kollegen,
im Zuge der Überarbeitung und Anpassung des Mindeststandards zur

Nutzung externer Cloud-Dienste finden Sie im Anhang das Anschreiben des AL BL im BSI, Herrn Samsel, sowie den Entwurf zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1.0.5 vom 17.11.2020. Die Änderungstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Bitte senden Sie Kommentierungen und Rückmeldungen bis zum 8. Januar 2021 per E-Mail an das Postfach mindeststandards@bsi.bund.de.

Mit freundlichen Grüßen
im Auftrag

[redacted]

Bundeministerium des Innern, für Bau und Heimat
Referat CI 4
Cybersicherheit in der Bundesverwaltung
D-10557 Berlin, Alt-Moabit 140
Telefon: [redacted]
eMail: CI4@bmi.bund.de; Cc [redacted]@bmi.bund.de
Internet: www.bmi.bund.de; www.cio.bund.de

-----Ursprüngliche Nachricht-----
Von: [redacted]@bsi.bund.de> Im Auftrag von GP Geschaeftszimmer_BL
Gesendet: Freitag, 20. November 2020 11:06
An: poststelle@bk.bund.de; poststelle@auswaertiges-amt.de; poststelle@bmi.bund.de; poststelle@bmf.bund.de; poststelle@bmjv.bund.de; poststelle@bmvg.bund.de; info@bmwi.bund.de; poststelle@bmas.bund.de; poststelle@bmel.bund.de; poststelle@bmfsfj.bund.de; poststelle@bmg.bund.de; poststelle@bmvi.bund.de; Poststelle@bmu.bund.de; information@bmbf.bund.de; poststelle@bmz.bund.de; bverfg@bundesverfassungsgericht.de; poststelle@bpra.bund.de; bundesrat@bundesrat.de; Poststelle@brh.bund.de; [redacted]@bundestag.de; Poststelle@bkm.bund.de; Poststelle@bfdi.bund.de; [redacted]@itzbund.de; [redacted]@jm nrw.de; GP AG-InfoSic <[redacted]@bsi.bund.de>

Cc: GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Fachbereich BL 3 <fachbereich-bl3@bsi.bund.de>; GP Referat BL 35 <referat-bl35@bsi.bund.de>; GP Poststelle <poststelle@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>

Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1.0.5 vom 17.11.2020. Die Abgleichstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon:+49 228 99 9582-[redacted]
Fax:+49 228 99 10 9582-[redacted]
E-Mail:geschaeftszimmer-bl@bsi.bund.de
Internet:www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – RfC-Beta-Version 1.0.5 vom 17.11.2020

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	24.04.2017	Erstveröffentlichung
1.0.1	13.07.2020	RfC-Alpha-Version, Rohentwurf auf Basis der Delta-Dokumentation
1.0.2	25.09.2020	Prüfung, Überarbeitung und Freigabe durch Fachreferat
1.0.3	29.09.2020	RfC-Alpha-Version zur hausinternen Abstimmung
1.0.4	09.11.2020	Kommentare und Rückmeldungen aus der hausinternen Abstimmung eingearbeitet
1.0.5	17.11.2020	Ressorts erhalten Entwurf zur Kommentierung

Tabelle 1: Versionsgeschichte des Mindeststandards. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de/mindeststandards~~ (**Hinweis:** wird vor Release konkretisiert)

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. Umsetzungsplan Bund 2017 (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (BSI 2020)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

Inhalt

Feldfunktion geändert

1 Beschreibung

Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. ~~Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend.~~ Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsanforderungen erfolgen. ~~Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche.~~[5]

Kommentiert [JMR1]: Empfehlung Löschung: M.E. eine zu einseitige Feststellung, ohne an dieser Stelle auf den Prozess einzugehen. Der Folgesatz zeigt dies ausreichend auf.

Kommentiert [JMR2]: Empfehlung Löschung: Wiederholung zum Vorwort

1.1 Begriffsbestimmung und Abgrenzung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[6]

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.[7]

Als Nutzung ist eine Verarbeitung von dienstlichen Daten[8] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird. Werden externe Cloud-Dienste durch Benutzer[9] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2.5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend. Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat.

Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e)).

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[10] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2018[12].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

~~[5] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31~~
[6] Definition nach Fehler! Linkreferenz ungültig. ~~https://www.bsi.bund.de/cloud~~
[7] Hinweis: IT-Dienstleistungen der „Bundescloud" fallen somit nicht unter diese Bestimmung.
[8] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden. Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden.
[9] Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[10] Vgl. BSI-Standard 200-2 (BSI 2017), S. 18
[11] Vgl. Key words for use in RFCs (IETF 1997)
[12] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[13] auf.

2.1 Planungsphase

Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS.2.2: *Cloud-Nutzung*

- die Cloud-Nutzungs-Strategie
- die darauf basierende Sicherheitsrichtlinie sowie
- das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.

Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend.

NCD.2.1.01 Cloud-Nutzungs-Strategie

a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist.[14]

b) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn Ziele, Chancen und Risiken der Cloud-Nutzungs-Strategie angemessen berücksichtigt werden können.

NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[15] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[16]

c) Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutzbeauftragten, in jedem Fall aber ~~und~~den IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.

Kommentiert [JMR3]: Wenn keine Daten gem. VS-NfD oder keine Daten i.S.d. BDSG verarbeitet werden, bedarf es auch nicht der Beteiligung der Datenschutz-/Geheimschutzbeauftragten.

NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[17]

c) Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutz-beauftragten, in jedem Fall aber den ~~und~~ IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen.

Kommentiert [JMR4]: Wenn keine Daten gem. VS-NfD oder keine Daten i.S.d. BDSG verarbeitet werden, bedarf es auch nicht der Beteiligung der Datenschutz-/Geheimschutzbeauftragten.

d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

[13] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[14] Hinweis: OPS.2.2.A1 *Erstellung einer Cloud-Nutzungs-Strategie* sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.
[15] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[16] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S.1ff.
[17] Siehe Veröffentlichungen unter Fehler! Linkreferenz ungültig.~~https://www.bsi.bund.de/cloud~~

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten – sofern betroffen – Geheim- und Datenschutzaspekte[18] sowie Personen- und Dienstgeheimnisse ermitteln.

Kommentiert [JMR5]: Wenn keine Daten gem. VS-NfD oder keine Daten i.S.d. BDSG verarbeitet werden, bedarf es auch nicht der Beteiligung der Datenschutz-/Geheimschutzbeauftragten.

g) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB
- Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG
- Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[19]
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 oder 3 gleichzeitig zuordnen.

i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln.[20]

i) Die Einrichtung MUSS die ermittelten Risiken mit denen in der eigenen Cloud-Nutzungs-Strategie (siehe NCD.2.1.01) festgelegten Richtlinien der Risikobewertung abgleichen und bewerten.

ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn die ermittelten Risiken gemäß der in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobewertung wirksam vermieden oder hinreichend reduziert oder getragen werden können.

NCD.2.1.04 Notfall- und Kontinuitätsmanagement

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[21] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im weiteren die Begrifflichkeit des BSI-Standards 100-4[22].

a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss. [23]

b) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen einnehmen würde.[24]

---

[18] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff.
[19] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), (BMI 2018)
[20] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Cloud-Szenario mit der Cloud-Nutzung-Strategie vereinbar ist (z.B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?)
[21] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[22] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[23] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?
[24] Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt?

c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob die Prävention vor bzw. die Reaktion auf Notfälle oder Krisen durch die Cloud-Nutzung geändert werden muss. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.

2.2 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters.

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) vom Cloud-Diensteanbieter erfüllt werden können.[25]

b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der „*Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5*“[26] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN

- die angemessene und wirksame Umsetzung der Basiskriterien nach C5[27],
- die aktuelle Dokumentation der Systembeschreibung[28],
- die Aktualität von vertraglich zugesicherten Zertifizierungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

umfassen und durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise DARF die Einrichtung NUR in begründeten Einzelfallentscheidungen zulassen.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

g) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

h) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen abdecken oder diese Risiken transferieren oder diese Risiken tragen.

[25] Hinweis: Liegt ein Prüfbericht nach C5 vor, können diese Informationen daraus entnommen werden.

[26] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, welche die Einrichtung darin unterstützt, einen C5-Bericht systematisch auszuwerten. Dies beinhaltet, die Sicherheitsmaßnahmen des Cloud-Diensteanbieters (und die zugehörigen Prüfergebnisse) aufzunehmen, die eigenen Nutzerkontrollen für die Nutzung einzurichten und hierdurch das mit der Cloud-Nutzung verbundene Risiko einzuschätzen und steuern zu können. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de~~

[27] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[28] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (BSI 2020a), Kap. 4.4.5, S.16f.) enthält der Bericht keine Systembeschreibung vom Anbieter, sondern eine vom Prüfer im Rahmen der Prüfung erhobene Beschreibung mit vergleichbarem Inhalt, die im Rahmen der Tätigkeiten dieses Mindeststandards herangezogen werden kann.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.

i) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

i) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit Rechtsvorschriften nicht entgegenstehen.

ii) Die Einrichtung MUSS darauf achten, dass die Prüfrechte so ausgestaltet sind, dass die Einrichtung ihre gesetzlichen Anforderungen erfüllt.

iii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Einrichtung selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.

iv) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS die Einrichtung dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern

a) Die Einrichtung MUSS sich die Beteiligung von relevanten Unterauftragnehmern und anderen externen Dritten vom Cloud-Diensteanbieter vollständig in Art und Umfang benennen lassen. Die Entscheidung, welcher Unterauftragnehmer hier zu nennen ist, MUSS gemäß den Vorgaben des C5[29] erfolgen.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass beabsichtigte Änderungen hierüber unverzüglich schriftlich oder per E-Mail mitgeteilt werden.

c) Diese Mitteilungen KÖNNEN über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).

d) Falls Unterauftragnehmer wesentliche Teile[30] zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

- Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und
- zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.

NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

[29] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), Kap. 4.4.5, S.18f.
[30] Hinweis: Hinsichtlich Bestimmung „wesentlicher Teile“ siehe C5, (BSI 2020a), S.91

NCD.2.2.04 Lokation vertraglich zusichern

a) Die Einrichtung MUSS sämtliche Lokationen, an denen dienstliche Daten verarbeitet werden, vertraglich festlegen.

b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten.

NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.[31]

Kommentiert [JMR6]: Diese Anforderung ist grds. zu begrüßen. Gleichwohl muss diese aus rechtsstaatlichen Gründen i.R.d. geltenden Rechtes bewertet werden. Insofern wird auf die zu bevorzugenden Formulierungen im C5:2020 verwiesen.

b) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS bei Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf achten.

ii) Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln

a) Die Einrichtung MUSS Kündigungsfristen dem Einsatzszenario angemessen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern

a) Die Einrichtung MUSS die Rückgabe der Daten regeln (Format, Datenträger, Protokolle, usw.).

b) Die Einrichtung MUSS berücksichtigen, dass die Maßnahmen zur Datenlöschung dem ermittelten Schutzbedarf entsprechen.

2.3 Einsatzphase

Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

NCD.2.3.01 ISMS einbinden

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen des Cloud-Dienstes bei sich einrichten. Die Einrichtung SOLLTE bei der Einbindung in das eigene ISMS zusätzlich die korrespondierenden Kriterien des C5[32] berücksichtigen.

NCD.2.3.02 Sicherheitsnachweise prüfen

[31] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (BMI 2014), S.1

[32] Hinweis: Der C5 führt mit Version 2020 Mitwirkungspflichten des Kunden als korrespondierende Kriterien ein. Die Umsetzung liegt im Verantwortungsbereich des Kunden und ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[33]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellte Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

NCD.2.3.03 Leistungsfähigkeit prüfen

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, beurteilen.

b) Die Einrichtung MUSS auf Abweichungen reagieren und die eigene IT-Infrastruktur und Netzanbindung den Ergebnissen der Überprüfung anpassen.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieter, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen.[34]

NCD.2.3.04 Informationspflichten nachhalten

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

i) einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,

ii) einem Austausch von Unterauftragnehmern oder Dritten.

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren

a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung als Identitätsnachweis seiner Benutzer (Log-in) an, SOLLTE die Einrichtung diese nutzen.

2.4 Beendigungsphase

Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[35]

NCD.2.4.01 Datenrückgabe durchführen

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

NCD.2.4.02 Datenlöschung bestätigen

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die Datenlöschung dokumentieren.

[33] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de~~

[34] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann. Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden.

[35] Siehe OPS.2.2.A14 *Geordnete Beendigung eines Cloud-Nutzungsverhältnisses*, (BSI 2020b), S.1ff

2.5 Sicherheitsanforderungen bei einer Mitnutzung

Nehmen Benutzer einer Einrichtung einen externen Cloud-Dienst in Anspruch, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[36] Für diesen Anwendungsfall regeln die nachfolgenden Sicherheitsanforderungen das Mindestsicherheitsniveau.

NCD.2.5.01 Mitnutzung von externen Cloud-Diensten

a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d) bis i) umsetzen und einhalten.

b) Die Einrichtung MUSS ermitteln, an welchen Lokationen dienstliche Daten verarbeitet werden.

i) Die Einrichtung MUSS dann bewerten, ob aus ihrer Sicht die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung heranziehen.

c) Die Einrichtung MUSS ermitteln, welche Rechte dem Cloud-Diensteanbieter oder Dritten an den dienstlichen Daten eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit der eigenen Sicherheitsrichtlinie vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar sind.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

e) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS dann bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen IT-Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[37]

[36] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen sind nicht als ein Vertragsverhältnis im Sinne dieses Mindeststands anzusehen.
[37] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017), S.1ff.

Literaturverzeichnis

AKTM (2011) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014

BMI (2014) Bundesministerium des Innern, Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung

BMI (2018) Bundesministerium des Innern, für Bau und Heimat: Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 – Notfallmanagement, Version 1.0

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management, Version 1.0

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de/dok/11916758~~, abgerufen am 17.11.2020

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: Kriterienkatalog Cloud Computing, Version 1.0 – Stand Februar 2020

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 3. Edition 2020

BSI (2020c) Bundesamt für Sicherheit in der Informationstechnik: Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5, **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de/dok/14020574~~, abgerufen am 17.11.2020

DIN (2018) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, **Fehler! Linkreferenz ungültig.**~~https://tools.ietf.org/html/rfc2119~~, abgerufen am 17.11.2020

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BDSG	Bundesdatenschutzgesetz
C5	Kriterienkatalog Cloud Computing
DIN	Deutsches Institut für Normierung e.V.
FAQ	Frequently Asked Questions
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
IT-SiBe	IT-Sicherheitsbeauftragte
StGB	Strafgesetzbuch
RFC	Request for Comments
VSA	Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)

Von:	Itsicherheit (C202)
An:	GP Mindeststandards Bund
Betreff:	Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Datum:	Dienstag, 5. Januar 2021 10:51:59
Anlagen:	Julia Parser Messages.txt

Sehr geehrte Damen und Herren,

das BMI hat mir zur Kommentierung den Entwurf des Mindeststandards zur Nutzung externer Cloud-Dienste zur Verfügung gestellt.

Fachlich gibt es dazu keinen Korrekturbedarf, wenngleich die Umsetzung hinsichtlich der Findung geeigneter Anbieter und das Erfüllungsprozedere sehr schwierig bzw. aufwändig werden wird.
Die Abgrenzung zum Outsourcing, das kein Cloud-Computing darstellt, ist m.E. hinreichend klar geworden, wenn man die Erläuterungen auf der BSI-Seite /cloud mit berücksichtigt.

Die Frage, ob der Baustein OPS.2.1 anzuwenden ist, hat sich mit der Erwähnung eines neuen Bausteins OPS.2.2 auch geklärt. Ich vermute, dass sowohl der Baustein OPS.2.2 wie auch die Anforderungen des Mindeststandards von den dem UP Bund unterliegenden Behörden parallel bearbeitet werden sollen und die Abarbeitung des Mindeststandards die Abarbeitung des Bausteins OPS.2.2 nicht ersetzt. Ggf. könnte hier aber auch ein ergänzender Hinweis für einen ggf. verpflichtend doppelten Aufwand in einer Fußnote hilfreich sein.

Aus Diskussionen mit unserer behördlichen Gleichstellungsbeauftragten bei der Gestaltung hausinterner Richtlinien und dem Rückgriff auf BSI-Unterlagen ist jedoch anzumerken, dass die Wortwahl im Mindeststandard der geschlechtergerechten Darstellung nach hiesiger Interpretation des BGleiG nicht entspricht. Es würde manche Diskussion und Zusatzarbeit ersparen, wenn das BSI jeweils die männliche und weibliche Form (oder eine neutrale) in seinen Vorgabetexten und Grafiken pflegen würde. Beispiel: Auditoren und Auditorinnen bzw. Auditierende, Anbietende, Prüfende ... Dies betrifft insbesondere auch die BSI-Standards und das Kompendium.

Freundliche Grüße
Im Auftrag
[redacted]
Informationssicherheitsbeauftragter

Telefon +[redacted] oder [redacted]

[redacted]@destatis.de
www.destatis.de

www.dashboard-deutschland.de

Von: GP Mindeststandards Bund
An: 1-IT-SI-0[redacted]
Cc: 1-IT-SI-L[redacted] 1-IT-SI-R[redacted] ; GP Mindeststandards Bund
Betreff: BSI-Mindeststandard NCD 2.0 - war: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Datum: Freitag, 3. September 2021 12:52:00

Sehr geehrter Herr[redacted]

der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste wurde am 07 07 2021 in der neuen Version 2 0 veröffentlicht Diesen finden Sie inkl der zugehörigen Referenztabelle auf den Webseiten des BSI:

https://www bsi bund de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node html

Vielen Dank für hre Beteiligung am Konsultationsverfahren

Die folgende Tabelle enthält die Ergebnisse der Überarbeitung des Mindeststandards bezüglich hrer Kommentare und Anmerkungen:
(Hervorhebungen/Streichungen sind leider nicht in der Formatierung erhalten geblieben – melden Sie sich bitte bei Problemen mit dieser „Inline"-Tabelle)

Kap. / Anf.	Version RFC-Beta-1.0.5	Kommentar / Hinweis	Rückmeldung	Neu
1	Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche [1] [1] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S 31	Aus welchem Grund ist die Rolle Beschaffer entfallen?	Änderung nicht übernommen Begründung: Satz gestrichen, Doppelung mit Vorwort Hinweis zu Rolle "Beschaffer": Orientierung an Rollen des IT-Grundschutz-Kompendiums, hier Baustein OPS 2 2 Cloud-Nutzung	
1 14	Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden [1] [1] Hinweis: IT-Dienstleistungen der „Bundescloud" fallen somit nicht unter diese Bestimmung	Die Begrifflichkeit „Bundescloud" muss allgemeiner gefasst werden, so dass auch weitere Clouds-Dienste des Bundes unter diese Vorgabe fallen Vorschlag: Die Formulierung sollte sich an der AG Cloud orientieren „Clouds des Bundes, der Länder und Kommunen"	Änderungen teilweise übernommen Bitte prüfen, ob die neue Formulierung jetzt konkret genug ist	Externe Cloud-Dienste im Sinne dieses Mindeststandards sind Cloud-Dienste, die von Anbietern der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes erbracht werden [1] [1] Hinweis: Private Cloud-Dienste der IT-Dienstleister des Bundes (z B Bundescloud) fallen somit nicht unter diese Bestimmung
1 15	Als Nutzung ist eine Verarbeitung von dienstlichen Daten[1] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird Werden externe Cloud-Dienste durch Benutzer[2] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2 5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend [1] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden [2] Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2020b), S 31	Der Begriff „dienstliche Daten" ist nicht hinreichend konkret definiert Jedwede Daten, die bei der dienstlichen Nutzung externer Cloud-Dienste in einer Einrichtung verarbeitet werden, sind aus hiesiger Sicht als dienstliche Daten anzusehen Welche Daten außer personenbezogene Daten (wie Stammdaten, Nutzungsdaten) werden vom BSI bei der dienstlichen Nutzung von externen Cloud-Diensten als „nicht dienstlich" angesehen?	Änderungen teilweise übernommen Bitte prüfen, ob die neue Formulierung jetzt konkret genug ist	Als Nutzung eines Cloud-Dienstes sind das Speichern und Verarbeiten dienstlicher Daten[1] durch einen externen Cloud-Dienst zu verstehen Dieser kann durch eine oder mehrere Einrichtungen beauftragt werden Regelungen für das Mitnutzen externer Cloud-Dienste durch Benutzer[2] einer Einrichtung sind in Kapitel 2 5 beschrieben " [1] Dienstliche Daten können gleichzeitig auch personenbezogene Daten sein Für den Zweck dieses Mindeststandards sind jedoch nicht solche personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden gemeint [2] Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2021): Ein Benutzer ist ein Mitarbeiter einer Institution, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben verwendet
1 16	Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat	Vorschlag: „Von einer Mitnutzung wird insbesondere ausgegangen, wenn eine Einrichtung die	Änderung übernommen	Von einer Mitnutzung wird insbesondere ausgegangen, wenn eine Einrichtung den externen Cloud-Dienst nicht selbst beauftragt hat

		externen Cloud-Dienste nicht beauftragt hat “		
1 17	Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD 2 1 03, Buchstabe e))	Wenn keine dienstlichen Daten in einem externen Cloud-Dienst verarbeitet werden, welche anderen Arten von Daten (außer personenbezogener Daten) sieht das BSI bei einer dienstlichen Nutzung externer Cloud-Dienste? Bei der Nutzung externer Cloud-Dienste ohne einen dienstlichen Kontext entfällt der Regelungsbedarf	Auf Hinweis eingegangen Bitte prüfen, ob die neue Formulierung jetzt konkret genug ist	Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards dennoch hilfreiche Empfehlungen enthalten und trotzdem angewendet werden (siehe NCD 2 1 03, Buchstabe e))xx xx Hinweis: Für eine Beschreibung, wie sich die Anforderungsnummerierung zusammensetzt, siehe FAQ zu den Mindeststandards siehe unter https://www bsi bund de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/FAQ_MST/faq_mst_node html
1 2	SOLLTE bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können	Begründung der „Nicht-Umsetzung“ muss dokumentiert werden	Änderung nicht übernommen Standardtext der für alle Mindeststandards gilt	SOLLTE bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können
1 2	SOLLTE NICHT / SOLLTE KEIN bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können	Begründung der „Umsetzung“ muss dokumentiert werden	Änderung nicht übernommen Standardtext der für alle Mindeststandards gilt	SOLLTE NICHT / SOLLTE KEIN bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können
2 1 01	a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist [1] [1] Hinweis: OPS 2 2 A1 Erstellung einer Cloud-Nutzungs-Strategie sieht die Erstellung einer Cloud-Nutzungs-Strategie vor In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können	Vorschlag: "Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in ihrer Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist [1]" [1] Hinweis: OPS 2 2 A1 Erstellung einer Cloud-Nutzungs-Strategie sieht die Erstellung einer Cloud-Nutzungs-Strategie vor In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können	Änderung übernommen	a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in ihrer Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist [1]" [1] Hinweis: OPS 2 2 A1 Erstellung einer Cloud-Nutzungs-Strategie sieht die Erstellung einer Cloud-Nutzungs-Strategie vor In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können
2 1 02	b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen [1]	I Ein risikoorientiertes Vorgehen wird mit dieser Anforderung ausgeschlossen Nicht für jedes Anwendungsszenario ist die Einhaltung der Basiskriterien des C5 Kriterienkatalogs notwendig	Änderungen nicht übernommen Hinsichtlich risikoorientiertes Vorgehen regen wir einen bilateralen Beratungstermin an Ein Widerspruch zum IT-	

	[1] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S 1ff	oder auch möglich (z B ein durch eine Auslandsvertretung nach lokalem Recht des Gastlandes verpflichtend zu nutzender externer Cloud-Dienste Anbieter) Da die C5 Kriterien aus etablierten Standards zur Informationssicherheit abgeleitet wurden, sollte es bei der Nutzung von Cloud-Diensten in einem Gastland möglich sein, die Umsetzung und Einhaltung von international anerkannten Standards/Kriterienkataloge (z B ISO 27001, SOC-2) als spezielle Sicherheitsanforderungen an einen Cloud-Diensteanbieter in der Sicherheitsrichtlinie festzulegen II Es besteht weiterhin ein Widerspruch zur BSI IT-GS Anforderung „OPS 2 2 A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung“ hinsichtlich der verwendeten Modalverben: MST: „Die Einrichtung MUSS in dieser Sicherheitsrichtlinie […]“ OPS 2 2 A13: „Der Cloud-Kunde SOLLTE sich vom“ Auch handelt es sich im BSI IT-GS um eine Standardanforderung Sind lediglich die Basis-Anforderungen umzusetzen, findet diese Anforderung im BSI IT-GS keine Anwendung, was im Widerspruch zum MST steht	Grundschutz besteht nicht, da hier der MST diesen konkretisiert (MUSS anstatt SOLLTE)	
2 1 03	d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen	I Es wird auch an dieser Stelle die Abgrenzung zu „nicht-dienstlichen Daten“ gefordert (s o) II Die Durchführung der Datenkategorisierung wird auch unter g) beschrieben und gefordert, weshalb sie nicht bereits unter d) bei der Identifizierung der verarbeiteten Daten zu berücksichtigen wäre (Zirkelschluss) Vorschlag zur Änderung der Formulierung zu d): „Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen III Um die Vorgabe praxistauglich und effizient zu gestalten, wird angeregt, eine Formulierung zu finden, welche die Identifikation der zukünftig zu verarbeitenden Informationen auf der Grundlage von Clustern (z B Nutzerdaten, Mitarbeiterdaten, Rechts-	Änderung übernommen	d) Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen

		und Konsulardaten, Daten zur Abwicklung von Finanztransaktionen, etc) vorsieht und nicht auf Einzeldatenebene, wie es aktuell der Fall ist		
2 1 03	f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[1] sowie Personen- und Dienstgeheimnisse ermitteln [1] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S 1ff	Ist an dieser Stelle mit Personengeheimnis das unter g) beschriebene Privatgeheimnis gemeint? Wenn nicht, wieso werden unterschiedliche Begriffe verwendet?	Änderung übernommen	f) Falls Daten den Kategorien 1, 2 oder 3 zugeordnet wurden: Die Einrichtung MUSS für die identifizierten Daten dieser Kategorien die Geheim- und Datenschutzaspekte[1] sowie Anforderungen hinsichtlich Privat- und Dienstgeheimnisse ermitteln und aus diesen ggf entstehende, weitere Anforderungen ableiten [1] Hinsichtlich Datenschutzaspekten siehe insbesondere (AKTM 2011), S 1ff
2 1 04	a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss [1] [1] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?	Schreibfehler zeitkritisch Kommafehler in Fußnote: Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?	Änderung übernommen	a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss xx xx Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant? (a und b tauschen!)
2 2 05	a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen [1] [1] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen (BMI 2014), S 1	Die Formulierung unterbindet ein risikoorientiertes, abgestuftes Vorgehen in Abhängigkeit zum tatsächlichen Schutzbedarf der bei einem Cloud-Dienst verarbeiteten „dienstlichen“ Daten Bsp : Die Nutzung eines Cloud-Dienstes zur Sammlung/zum Zusammentragen öffentlich verfügbarer Informationen hat einen geringeren Schutzbedarf als die Verarbeitung vertraulicher dienstlicher Informationen	Änderung teilweise übernommen Anforderung entfallen, Fußnote nach NCD 2 1 03 Sicherheitskonzept für den externen Cloud-Dienst Buchstabe j) verschoben	
2 3 01	a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden	Die Formulierung unterbindet ein risikoorientiertes, abgestuftes Vorgehen in Abhängigkeit zum tatsächlichen Schutzbedarf der bei einem Cloud-Dienst verarbeiteten „dienstlichen“ Daten Bsp : Die Nutzung eines	Änderung nicht übernommen Einbindung in das ISMS heißt ja gerade, ein risikoorientiertes, abgestuftes Vorgehen zu verfolgen	a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden

		Cloud-Dienstes zur Sammlung/zum Zusammentragen öffentlich verfügbarer Informationen hat einen geringeren Schutzbedarf als die Verarbeitung vertraulicher dienstlicher Informationen		
2 5 01	d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden	Die Anforderung, dienstliche Daten im externen Cloud-Dienst verschlüsselt zu speichern ergibt sich aus dem Abgleich identifizierter Risiken mit der Cloud-Strategie einer Einrichtung (siehe NCD 2 2 03 i) Daher wäre es zielführender, basierend auf den bereits ermittelten Risiken zu entscheiden, ob in Erfahrung gebracht werden muss, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden Existieren keine Risiken für die dienstlichen Daten, besteht keine Notwendigkeit die dienstlichen Daten verschlüsselt zu speichern und die hier beschriebene Aktivität ist obsolet	Änderung übernommen	d) Die Einrichtung MUSS bewerten, ob und wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt zu speichern sind Für die anschließende Bewertung SOLLTE die Einrichtung die identifizierten Risiken mit der eigenen Cloud-Strategie (siehe NCD 2 1 01) abgleichen Verweis auf Cloud-Strategie prüfen
3		(Es) bleibt grundsätzlich festzuhalten, dass der Mindeststandard zur (Mit-)Nutzung von Cloud-Diensten so zu formulieren ist, dass die praxisrelevanten Besonderheiten des Auswärtigen Amts, wie z B die Einhaltung des lokalen Rechts eines Gastlandes, Berücksichtigung finden	Bitte kontaktieren Sie uns bei konkreten Anwendungsproblemen	

Mit freundlichen Grüßen
Im Auftrag
[redacted]

Referat BL 35 - Mindeststandards Bund
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: [redacted]
Hotline: +49 (0)228 99 9582[redacted]
E-Mail: mindeststandards@bsi bund de
Internet: www bsi bund de

#DeutschlandDigitalSicherBSI

++
Haben Sie schon unseren Mindeststandard-Newsletter abonniert?
https://www bsi bund de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen_node html
++

-----Ursprüngliche Nachricht-----
Von [redacted] @auswaertiges-amt de>
Gesendet: Freitag, 8 Januar 2021 15:23
An: GP Mindeststandards Bund <mindeststandards@bsi bund de>
Cc: [redacted] @auswaertiges-amt de>; [redacted] @auswaertiges-amt de>
Betreff: AW: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2 0

1-IT-SI-204 04/110

Sehr geehrte Damen und Herren,

anliegend erhalten Sie die mit hrem Schreiben BL35 - 750 00 07 vom 20 11 2020 erbetene Rückmeldung

Neben den beigefügten, konkreten inhaltlichen Anmerkungen in der Spalte "Bemerkungen" bleibt grundsätzlich festzuhalten, dass der Mindeststandard zur (Mit-)Nutzung von Cloud-Diensten so zu formulieren ist, dass die praxisrelevanten Besonderheiten des Auswartigen Amts, wie z B die Einhaltung des lokalen Rechts eines Gastlandes, Berücksichtigung finden

Mit freundlichen Grüßen
[redacted]

IT-Sicherheitsmanagement

[redacted]
[redacted]@diplo de

Auswärtiges Amt
Werderscher Markt 1
10117 Berlin

-----Ursprüngliche Nachricht-----
Von [redacted]@bsi bund de] Im Auftrag von GP Geschaeftszimmer_BL
Gesendet: Freitag, 20 November 2020 11:06
An: poststelle@bk bund de - (Extern); Poststelle des AA; poststelle@bmi bund de; poststelle@bmf bund de - (Extern); poststelle@bmjv bund de; poststelle@bmvg bund de; info@bmwi bund de; poststelle@bmas bund de; poststelle@bmel bund de; poststelle@bmfsfj bund de - (Extern); poststelle@bmg bund de; poststelle@bmvi bund de; poststelle@bmu bund de; information@bmbf bund de; poststelle@bmz bund de; bverfg@bundesverfassungsgericht de; poststelle@bpra bund de; bundesrat@bundesrat de; Poststelle@brh bund de; [redacted]@bundestag de; Poststelle@bkm bund de; poststelle@bfdi bund de - (Extern) [redacted]@itzbund de; [redacted]@jm nrw de; GP AG-InfoSic
Cc: GP Abteilung BL; GP Fachbereich BL 3; GP Referat BL 35; GP Poststelle; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_BL
Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2 0

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1 0 5 vom 17 11 2020 Die Abgleichstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 228 99 9582[redacted]
Fax: +49 228 99 10 9582[redacted]
E-Mail: geschaeftszimmer-bl@bsi bund de
Internet: www bsi bund de
www bsi-fuer-buerger de

Von: GP Mindeststandards Bund
An: [redacted] 21C
Cc: [redacted] *BAMF [redacted] GL21; [redacted] GL22; *22B-RL; *22E-RL; CI4@bmi.bund.de; GP Mindeststandards Bund
Betreff: AW: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Datum: Freitag, 3. September 2021 12:55:00

Sehr geehrte Frau [redacted]

der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste wurde am 07 07 2021 in der neuen Version 2 0 veröffentlicht Diesen finden Sie inkl der zugehörigen Referenztabelle auf den Webseiten des BSI:

https://www bsi bund de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node html

Vielen Dank für Ihre Beteiligung am Konsultationsverfahren

Die folgende Tabelle enthält die Ergebnisse der Überarbeitung des Mindeststandards bezüglich hrer Kommentare und Anmerkungen:
(Hervorhebungen/Streichungen sind leider nicht in der Formatierung erhalten geblieben – melden Sie sich bitte bei Problemen mit dieser „Inline"-Tabelle)

Kap. / Anf.	Version RFC-Beta-1.0.5	Kommentar / Hinweis	Rückmeldung	Neu
1 14	Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden [1] [1] Hinweis: IT-Dienstleistungen der „Bundescloud" fallen somit nicht unter diese Bestimmung	Sofern der Cloud-Dienst des privatwirtschaftlichen Anbieters als „Blackbox" innerhalb der Netze der öffentlichen Verwaltung (im Sinne einer Appliance / Disconnected-Modes) angeboten/betrieben wird, könnte dieser ebenfalls als „externer Cloud-Dienst" gelten (insbesondere, wenn eine Anbindung dieses Dienstes ans Internet erfolgt) M E ist die Verortung des Cloud-Dienstes nicht (alleine) ausschlaggebend	Änderungen teilweise übernommen Bitte prüfen, ob die neue Formulierung jetzt konkret genug ist	Externe Cloud-Dienste im Sinne dieses Mindeststandards sind Cloud-Dienste, die von Anbietern der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes erbracht werden [1] [1] Hinweis: Private Cloud-Dienste der IT-Dienstleister des Bundes (z B Bundescloud) fallen somit nicht unter diese Bestimmung
1 15	Als Nutzung ist eine Verarbeitung von dienstlichen Daten[1] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird Werden externe Cloud-Dienste durch Benutzer[2] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2 5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend [1] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden [2] Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2020b), S 31	Vorschlag: " Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden Zu dienstlichen Daten gehören grundsätzlich auch personenbezogene Daten Darunter fallen jedoch nicht solche personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden "	Änderungen teilweise übernommen Bitte prüfen, ob die neue Formulierung jetzt konkret genug ist	Als Nutzung eines Cloud-Dienstes sind das Speichern und Verarbeiten dienstlicher Daten[1] durch einen externen Cloud-Dienst zu verstehen Dieser kann durch eine oder mehrere Einrichtungen beauftragt werden Regelungen für das Mitnutzen externer Cloud-Dienste durch Benutzer[2] einer Einrichtung sind in Kapitel 2 5 beschrieben " [1] Dienstliche Daten können gleichzeitig auch personenbezogene Daten sein Für den Zweck dieses Mindeststandards sind jedoch nicht solche personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden gemeint [2] Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2021): Ein Benutzer ist ein Mitarbeiter einer Institution, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt IT-Benutzer und Benutzer

				sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben verwendet
1 15	Als Nutzung ist eine Verarbeitung von dienstlichen Daten[1] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird Werden externe Cloud-Dienste durch Benutzer[2] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2 5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend [1] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden [2] Analog Rolle „Benutzer“ nach IT-Grundschutz-Kompendium, (BSI 2020b), S 31	Sofern unter den zu verarbeitenden dienstlichen Daten auch personenbezogene Daten sind, ist ggf ein Fall der Auftragsverarbeitung gemäß Artikel 28 DSGVO anzunehmen Der Zusammenhang zur DSGVO sollte m E hier deutlicher herausgestellt oder, falls keiner besteht, bewusst davon abgegrenzt werden	Änderung nicht übernommen Begründung: Datenschutzaspekte werden nicht im MST geregelt Anknüpfungspunkte sind in der Datenkategorisierung gelegt Textstelle wurde angepasst Bitte prüfen, ob diese jetzt ausreichend konkret ist	Als Nutzung eines Cloud-Dienstes sind das Speichern und Verarbeiten dienstlicher Daten[1] durch einen externen Cloud-Dienst zu verstehen Dieser kann durch eine oder mehrere Einrichtungen beauftragt werden Regelungen für das Mitnutzen externer Cloud-Dienste durch Benutzer[2] einer Einrichtung sind in Kapitel 2 5 beschrieben " [1] Dienstliche Daten können gleichzeitig auch personenbezogene Daten sein Für den Zweck dieses Mindeststandards sind jedoch nicht solche personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden gemeint [2] Analog Rolle „Benutzer“ nach IT-Grundschutz-Kompendium, (BSI 2021): Ein Benutzer ist ein Mitarbeiter einer Institution, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben verwendet
1 16	Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat	Tippfehler: "Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat "	Änderung übernommen	Von einer Mitnutzung wird insbesondere ausgegangen, wenn eine Einrichtung den externen Cloud-Dienst nicht selbst beauftragt hat
2	2 Sicherheitsanforderungen	Der gesamte Abschnitt 2 sollte m E noch klarer zwischen Nutzung und Mitnutzung unterscheiden [...]	Die Rückmeldungen konnten nicht gänzlich berücksichtigt werden Wir haben diese aber zum Anlass genommen, auf diese Aspekte im Hilfsdokument einzugehen Unabhängig davon, kontaktieren Sie uns bitte bei konkreten Anwendungsproblemen	2 Sicherheitsanforderungen

2 1	Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS 2 2: Cloud-Nutzung die Cloud-Nutzungs-Strategie die darauf basierende Sicherheitsrichtlinie sowie das jeweilige Sicherheitskonzept für den externen Cloud-Dienst Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend	Es ist zu hinterfragen, ob diese Strategie zwingend erforderlich ist Das Erfordernis gemäß OPS 2 2 basiert auf der darin geäußerten Annahme, dass Cloud-Nutzung eine strategische Entscheidung ist Gilt das so pauschal? Es könnte zunehmend Services geben, die nur noch (effizient) in Cloud-Technologien zur Verfügung gestellt werden bzw für die eine andere Bereitstellung einen unverhältnismäßigen und auch sonst nicht gerechtfertigten Aufwand erfordern würde Wenn heutzutage Cloud-Dienste immer üblicher werden, warum sollte man speziell für jeden Einzelnen eine dedizierte Cloud-Strategie haben müssen? Schließlich ist es ja auch nicht üblich eine „Strategie“ für die Nutzung von Wasser und Strom zu haben, sondern man behandelt solche Themen in Betriebs- und Sicherheitskonzepten, i d R ohne strategische Ziele damit zu verfolgen Wenn allerdings generell eine IT-Strategie in der Behörde erstellt wird, könnte darin natürlich ein Abschnitt bzgl Cloud-Nutzung enthalten sein	Änderung nicht übernommen Eine Cloud-Strategie wird pro Einrichtung einmal erstellt und gilt dann für alle Cloud-Dienste	Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS 2 2 Cloud-Nutzung die Cloud-Nutzungs-Strategie die darauf basierende Sicherheitsrichtlinie sowie das jeweilige Sicherheitskonzept für den externen Cloud-Dienst Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend
2 1 03	e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen	Da dieser Punkt zu dem letzten Satz in Kapitel 1 1 redundant ist, kann er entfallen	Änderung nicht übernommen Hier als Anforderung formuliert	e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards In diesen Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen
2 1 03	h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 oder 3 gleichzeitig zuordnen	"Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und 3 gleichzeitig zuordnen "	Änderung übernommen	h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und 3 gleichzeitig zuordnen
2 3 02	b) Die Einrichtung MUSS prüfen, ob festgestellte Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist	Tippfehler "Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist	Änderung übernommen	b) Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist
2 3 02	c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieter, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen [1] [1] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so	Tippfehler "Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen "	Änderung übernommen	

	dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden			
2 4 02	a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen	"Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gemäß NCD2 2 07 erfolgte Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen " Ggf hier noch klarstellen, dass neben den Nutzdaten auch Protokoll-/Transaktionsdaten zu löschen sind, sofern so vorgesehen	Änderung übernommen Fußnote eingearbeitet	a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gemäß NCD2 2 07 erfolgte Löschung aller dienstlichen Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen xx Dies umfasst die Bestätigung, dass die dienstlichen Daten gemäß der vertraglich vereinbarten Verfahren gelöscht wurden xxHinweis: Neben Nutzdaten können auch Protokoll-/Transaktionsdaten zu löschen sein
2 5 01	a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD 2 1 03, Buchstaben d) bis i) umsetzen und einhalten	Auf welcher Annahme basiert diese Einschränkung? M E ist nicht ersichtlich, warum für die Mitnutzung eines Cloud-Dienstes nicht ebenfalls die Erstellung eines Sicherheitskonzeptes notwendig sein sollte, insbesondere wenn die Bandbreite der extern verarbeitenden Daten nicht eingeschränkt ist Sollte der Anwendungsfall „Mitnutzung“ auf Grund des fehlenden Vertragsverhältnisses nicht genauso kritisch oder gar noch kritischer betrachtet werden als die „Nutzung“? Jede Art von Datenübertragung und Datenverarbeitung im Rahmen einer Nutzung oder Mitnutzung von Cloud-Diensten (selbst wenn es sich nur Metadaten handelt) sorgt für eine Vergrößerung des Angriffsvektors Das spricht dafür, beim Szenario „Mitnutzung“ mindestens dieselben Maßstäbe anzulegen (z B Kriterienkatalog C5) wie beim Szenario „Nutzung“	Änderung übernommen Anforderung konkretisiert	a) Die Einrichtung MUSS sicherstellen, dass die Mitnutzung mit der eigenen Cloud-Strategie (siehe NCD 2 1 01) vereinbar ist b) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD 2 1 03, Buchstabe d) bis i) umsetzen und einhalten
2 5 01	d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden	Betrifft das Thema „Daten-Verschlüsselung“ nur die Mitnutzung? Warum gilt es in diesem Mindeststandard nicht übergreifend für Nutzung und Mitnutzung?	Hinweis: Bei Nutzung wird das durch die C5-Kriterien bereits vorgegeben Da bei Mitnutzung ggf kein C5 vorliegt, wird zumindest auf diesen Punkt hier gesondert hingewiesen	
3		Zudem kam unabhängig von dem Konsultationsverfahren bei uns die Frage auf, ob/welche spezifischen Rahmenbedingungen für Sourcecode-Veröffentlichungen auf Github gelten Nach kurzer Recherche auf der BSI-Website bin ich auf Beispielprojekte wie z B Persosim von HJP und Botan 2 X des BSI gestoßen, wobei zu Letzterem ein umfangreiches Handbuch vorliegt (https://botan randombit net/handbook/contents html), aber beispielhafte IT-Sicherheitskonzepte oder Sicherheitsprofile (wie es z B für SaaS gibt, https://www bsi bund de/DE/Themen/DigitaleGesellschaft/CloudComputing/Sicherheitsprofile/sicherheitsprofil_saas_node html) habe ich zu "Sourcecode-Veröffentlichungen auf Github" bislang nicht entdeckt Falls Sie mir den hier geltenden (ggf spezifischen) Rahmenbedingungen einen weiterführenden Hinweis geben können, wäre ich hnen sehr dankbar	Rechtliche Fragestellung, kann durch Konsultationsverfahren nicht gelöst werden Bitte an die Sicherheitsberatung des BSI wenden	

Mit freundlichen Grüßen
Im Auftrag
[redacted]

Referat BL 35 - Mindeststandards Bund
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: [redacted]
Hotline: +49 (0)228 99 9582[redacted]
E-Mail: mindeststandards@bsi bund de
Internet: www bsi bund de

#DeutschlandDigitalSicherBSI

++
Haben Sie schon unseren Mindeststandard-Newsletter abonniert?
https://www bsi bund de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen_node html
++

-----Ursprüngliche Nachricht-----
Von [redacted], 21C[redacted] @bamf bund de>
Gesendet: Montag, 11 Januar 2021 06:52
An: GP Mindeststandards Bund <mindeststandards@bsi bund de>
Cc: *IT-Sibe BAMF <[redacted]@bamf bund de>; [redacted], GL21 <[redacted] @bamf bund de>; [redacted], GL22 <[redacted] @bamf bund de>; *22B-RL <[redacted]@bamf bund de>; *22E-RL[redacted]@bamf bund de>; CI4@bmi bund de
Betreff: AW: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2 0

Sehr geehrte Damen und Herren,

vielen Dank für die Beteiligung am Konsultationsverfahren zu Version
2 0 des Mindeststandards zur Nutzung externer Cloud-Dienste

Im Anhang finden Sie die Anmerkungen aus der IT-Abteilung des BAMF
Diese zielen u a darauf ab, einerseits Definitionen und
Anwendungsgebiete zu schärfen und andererseits den mit der Einhaltung
des Mindeststandards vergleichsweise (zu) hohen Sonderaufwand in Grenzen
zu halten, zumal es sich bei externen Cloud-Diensten um keine Seltenheit
in der Softwareentwicklung und -nutzung handelt und diese in
IT-Sicherheitskonzepten wie andere Dienste auch bereits regulär
berücksichtigt werden

Zudem kam unabhängig von dem Konsultationsverfahren bei uns die Frage
auf, ob/welche spezifischen Rahmenbedingungen für
Sourcecode-Veröffentlichungen auf Github gelten

Nach kurzer Recherche auf der BSI-Website bin ich auf Beispielprojekte
wie z B Persosim von HJP und Botan 2 X des BSI gestoßen, wobei zu
Letzterem ein umfangreiches Handbuch vorliegt (
https://botan randombit net/handbook/contents html), aber beispielhafte
IT-Sicherheitskonzepte oder Sicherheitsprofile (wie es z B für SaaS
gibt,
https://www bsi bund de/DE/Themen/DigitaleGesellschaft/CloudComputing/Si
cherheitsprofile/sicherheitsprofil_saas_node html) habe ich zu
"Sourcecode-Veröffentlichungen auf Github" bislang nicht entdeckt Falls
Sie mir den hier geltenden (ggf spezifischen) Rahmenbedingungen einen
weiterführenden Hinweis geben können, wäre ich hnen sehr dankbar

Für Rückfragen stehe ich gern zur Verfügung

Freundliche Grüße
[redacted]
Referatsleiterin
Referat 21C Prozessentwicklung, IT-Architektur und Testmanagement
Bundesamt für Migration und Flüchtlinge, Frankenstr 210, 90461
Nürnberg
Tel 1:[redacted], Tel 2:[redacted]
E-Mail[redacted]@bamf bund de

-----Ursprüngliche Nachricht-----
Von: CI4@bmi bund de <CI4@bmi bund de>
Gesendet: Dienstag, 24 November 2020 15:55

An [redacted] @bdbos bmi bund de [redacted] @polizei bund de;
[redacted] @bva bund de [redacted] @bsi bund de;
[redacted] @bbk bund de; [redacted] @badv bund de;
[redacted] @bakoev bund de; [redacted] BAMF
[redacted] @bamf bund de> [redacted] @bbk bund de; [redacted] @bbr bund de;
[redacted] @bescha bund de [redacted] @bfv bund de [redacted] @bib bund de;
[redacted] @bisp de; [redacted] @bka bund de;
[redacted] @bkg bund de; [redacted] @bpb bund de;
[redacted] @polizei bund de; [redacted] @bsi bund de [redacted] @hsbund de;
[redacted] @destatis de; [redacted] @thw bund de;
[redacted] t@zitis bund de; [redacted] @ZITiS bund de;
[redacted] @bmi bund de; [redacted] @bakoev bund de

Cc: CI4@bmi bund de; RegCI4@bmi bund de
Betreff: Mindeststandard zur Nutzung externer Cloud-Dienste, hier:
Konsultationsverfahren zum Major-Release Version 2 0

CI 4 - 17002/20#11

Liebe Kolleginnen und Kollegen,
im Zuge der Überarbeitung und Anpassung des Mindeststandards zur
Nutzung externer Cloud-Dienste finden Sie im Anhang das Anschreiben des
AL BL im BSI, Herrn Samsel, sowie den Entwurf zum Mindeststandard des
BSI zur Nutzung externer Cloud-Dienste nach § 8Absatz 1 Satz 1 BSIG -
RfC-Beta-Version 1 0 5 vom 17 11 2020 Die Änderungstabelle zum
Mindeststandard ist der E-Mail ebenfalls beigefügt

Bitte senden Sie Kommentierungen und Rückmeldungen bis zum 8 Januar
2021 per E-Mail an das Postfach mindeststandards@bsi bund de

Mit freundlichen Grüßen
im Auftrag

[redacted]
_____
Bundeministerium des Innern, für Bau und Heimat Referat CI 4
Cybersicherheit in der Bundesverwaltung
D-10557 Berlin, Alt-Moabit 140
Telefon [redacted]
eMail: CI4@bmi bund de; Cc [redacted] @bmi bund de
Internet: www bmi bund de; www cio bund de

-----Ursprüngliche Nachricht-----
Von [redacted] @bsi bund de> Im Auftrag von GP
Geschaeftszimmer_BL
Gesendet: Freitag, 20 November 2020 11:06
An: poststelle@bk bund de; poststelle@auswaertiges-amt de;
poststelle@bmi bund de; poststelle@bmf bund de; poststelle@bmjv bund de;
poststelle@bmvg bund de; info@bmwi bund de; poststelle@bmas bund de;
poststelle@bmel bund de; poststelle@bmfsfj bund de;
poststelle@bmg bund de; poststelle@bmvi bund de; Poststelle@bmu bund de;
information@bmbf bund de; poststelle@bmz bund de;
bverfg@bundesverfassungsgericht de; poststelle@bpra bund de;
bundesrat@bundesrat de; Poststelle@brh bund de;
[redacted] @bundestag de; Poststelle@bkm bund de;
Poststelle@bfdi bund de [redacted] @itzbund de;
[redacted] @jm nrw de; GP AG-InfoSic <[redacted] @bsi bund de>

Cc: GP Abteilung BL <abteilung-bl@bsi bund de>; GP Fachbereich BL 3
<fachbereich-bl3@bsi bund de>; GP Referat BL 35
<referat-bl35@bsi bund de>; GP Poststelle <poststelle@bsi bund de>; GP
Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi bund de>; GP
Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi bund de>

Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste,
hier: Konsultationsverfahren zum Major-Release Version 2 0

Sehr geehrte Damen und Herren,

anbei übersende ich hnen das Anschreiben sowie den Mindeststandard des
BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG -
RfC-Beta-Version 1 0 5 vom 17 11 2020 Die Abgleichstabelle zum
Mindeststandard ist der E-Mail ebenfalls beigefügt

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn

Telefon: +49 228 99 9582[redacted]
Fax: +49 228 99 10 9582[redacted]
E-Mail: geschaeftszimmer-bl@bsi bund de
Internet: www bsi bund de
www bsi-fuer-buerger de

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – RfC-Beta-Version 1.0.5 vom 17.11.2020

Änderungshistorie

Version	Datum	Beschreibung
1.0	24.04.2017	Erstveröffentlichung
1.0.1	13.07.2020	RfC-Alpha-Version, Rohentwurf auf Basis der Delta-Dokumentation
1.0.2	25.09.2020	Prüfung, Überarbeitung und Freigabe durch Fachreferat
1.0.3	29.09.2020	RfC-Alpha-Version zur hausinternen Abstimmung
1.0.4	09.11.2020	Kommentare und Rückmeldungen aus der hausinternen Abstimmung eingearbeitet
1.0.5	17.11.2020	Ressorts erhalten Entwurf zur Kommentierung

Tabelle 1: Versionsgeschichte des Mindeststandards. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/mindeststandards (Hinweis: wird vor Release konkretisiert)

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. Umsetzungsplan Bund 2017 (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (BSI 2020)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

Inhalt

1 Beschreibung

Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend. Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsanforderungen erfolgen. Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche.[5]

1.1 Begriffsbestimmung und Abgrenzung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[6]

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.[7]

Als Nutzung ist eine Verarbeitung von dienstlichen Daten[8] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird. Werden externe Cloud-Dienste durch Benutzer[9] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2.5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend. Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat.

Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e)).

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[10] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2018[12].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

DARF NICHT / DARF KEIN

Kommentiert [FH21]: Sofern der Cloud-Dienst des privatwirtschaftlichen Anbieters als „Blackbox" innerhalb der Netze der öffentlichen Verwaltung (im Sinne einer Appliance / Disconnected-Modes) angeboten/betrieben wird, könnte dieser ebenfalls als „externer Cloud-Dienst" gelten (insbesondere, wenn eine Anbindung dieses Dienstes ans Internet erfolgt). M.E. ist die Verortung des Cloud-Dienstes nicht (alleine) ausschlaggebend.

Kommentiert [h2]: Sofern unter den zu verarbeitenden dienstlichen Daten auch personenbezogene Daten sind, ist ggf. ein Fall der Auftragsverarbeitung gemäß Artikel 28 DSGVO anzunehmen.
Der Zusammenhang zur DSGVO sollte m.E. hier deutlicher herausgestellt oder, falls keiner besteht, bewusst davon abgegrenzt werden.

[5] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[6] Definition nach https://www.bsi.bund.de/cloud
[7] Hinweis: IT-Dienstleistungen der „Bundescloud" fallen somit nicht unter diese Bestimmung.
[8] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden. Zu dienstlichen Daten gehören grundsätzlich auch personenbezogene Daten. Darunter fallen jedoch nicht solche personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden.
[9] Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[10] Vgl. BSI-Standard 200-2 (BSI 2017), S. 18
[11] Vgl. Key words for use in RFCs (IETF 1997)
[12] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 Cloud-Nutzung[13] auf.

2.1 Planungsphase

Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS.2.2: Cloud-Nutzung

- die Cloud-Nutzungs-Strategie
- die darauf basierende Sicherheitsrichtlinie sowie
- das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.

Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend.

NCD.2.1.01 Cloud-Nutzungs-Strategie

a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist.[14]

b) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn Ziele, Chancen und Risiken der Cloud-Nutzungs-Strategie angemessen berücksichtigt werden können.

NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung[15] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[16]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.

NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[17]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen.

d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

[13] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: Cloud-Nutzung
[14] Hinweis: OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.
[15] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: Cloud-Nutzung
[16] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S.1ff.
[17] Siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud

Kommentiert [h3]: Der gesamte Abschnitt 2 sollte m.E. noch klarer zwischen Nutzung und Mitnutzung unterscheiden.
Bspw.:
Gilt wirklich nur Kapitel 2.5 für Mitnutzung-Dienste und gelten die Kapitel 2.1-2.4 nur für Nutzung-Dienste? Wenn ja, dann sollte das am Anfang von Abschnitt 2 klargestellt werden. Wenn Teile der Kapitel 2.1-2.4 auch für Mitnutzung-Dienste gelten, wäre das kenntlich zu machen.

Dass Kapitel 2.2 nur für Nutzung-Dienste gilt (weil diese mit Beschaffung und Beauftragung verbunden sind), leuchtet ein. Aber eine Planungsphase sollte es ggf. auch bei Mitnutzung-Diensten geben, wobei dabei vermutlich nicht das ganze Kapitel 2.1 zu beachten ist.

Grundsätzlich sei hier angemerkt, dass es sehr schlanke Mitnutzung-Möglichkeiten gibt, z.B. Cloud-Dienste, die im Internet leicht verfügbar und oftmals auch als freeware (ggf. mit Apache Lizenz, mit AGG, aber nicht unbedingt mit Vertrag – was ja dann keine Nutzung, sondern nur Mitnutzung ist) angeboten werden. Hierfür die gesamten Aufgaben aus Kap. 2.1 ff. abzuarbeiten, wäre ein unverhältnismäßiger und auch nicht erforderlicher Aufwand. Es sollte also insbesondere bei OSS darauf geachtet werden, dass Sicherheitsmaßnahmen ausreichend umgesetzt, aber keine übermäßigen konzeptionellen Aufwände für jeden kleinen Individualfall der Cloud-(Mit)Nutzung betrieben werden müssen.

Außerdem gibt es sicherlich auch schlanke Nutzung-Dienste. Hier ein Beispiel (mit der hypothetischen Annahme, dass es solch einen Service noch nicht als geeignete OSS gibt und folgende neue Beauftragung erfolgt): Eine Behörde beauftragt eine Firma mit der Entwicklung eines Wechselkursrechners, der an dem offiziellen Wechselkurs der betroffenen Nationalbanken orientiert ist. Die Firma entwickelt den Wechselkursrechner und bietet den Service in Form eines Cloud-Dienst eines externen Anbieters an. Die Behörde nimmt die Leistung auf Basis des mit der Firma geschlossenen Vertrages an. Die Behörde nutzt den Wechselkursrechner, indem sie Zahlenbeträge und d ... [1]

Kommentiert [h4]: Es ist zu hinterfragen, ob diese Strategie zwingend erforderlich ist.
Das Erfordernis gemäß OPS.2.2 basiert auf der darin geäußerten Annahme, dass Cloud-Nutzung eine strategische Entscheidung ist.
Gilt das so pauschal?
Es könnte zunehmend Services geben, die nur noch (effizient) in Cloud-Technologien zur Verfügung gestellt werden bzw. für die eine andere Bereitstellung einen unverhältnismäßigen und auch sonst nicht gerechtfertigten Aufwand erfordern würde.
Wenn heutzutage Cloud-Dienste immer üblicher werden, warum sollte man speziell für jeden Einzelnen eine dedizierte Cloud-Strategie haben müssen? Schließlich ist es ja auch nicht üblich eine „Strategie" für die Nutzung von Wasser und Strom zu haben, sondern man behandelt solche Themen in Betriebs- und Sicherheitskonzepten, i.d.R. ohne strategische Ziele damit zu verfolgen.
Wenn allerdings generell eine IT-Strategie in der Behörde erstellt wird, könnte darin natürlich ein Abschnitt bzgl. Cloud-Nutzung enthalten sein.

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

Kommentiert [h5]: Da dieser Punkt zu dem letzten Satz in Kapitel 1.1 redundant ist, kann er entfallen.

f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[18] sowie Personen- und Dienstgeheimnisse ermitteln.

g) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB
- Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG
- Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[19]
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und~~oder~~ 3 gleichzeitig zuordnen.

i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln.[20]

i) Die Einrichtung MUSS die ermittelten Risiken mit denen in der eigenen Cloud-Nutzungs-Strategie (siehe NCD.2.1.01) festgelegten Richtlinien der Risikobewertung abgleichen und bewerten.

ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn die ermittelten Risiken gemäß der in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobewertung wirksam vermieden oder hinreichend reduziert oder getragen werden können.

NCD.2.1.04 Notfall- und Kontinuitätsmanagement

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[21] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im weiteren die Begrifflichkeit des BSI-Standards 100-4[22].

a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss. [23]

b) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen einnehmen würde.[24]

[18] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff.
[19] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), (BMI 2018)
[20] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Cloud-Szenario mit der Cloud-Nutzung-Strategie vereinbar ist (z.B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?)
[21] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[22] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[23] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?
[24] Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt?

c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob die Prävention vor bzw. die Reaktion auf Notfälle oder Krisen durch die Cloud-Nutzung geändert werden muss. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.

2.2 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters.

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) vom Cloud-Diensteanbieter erfüllt werden können.[25]

b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“[26] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN

- die angemessene und wirksame Umsetzung der Basiskriterien nach C5[27],
- die aktuelle Dokumentation der Systembeschreibung[28],
- die Aktualität von vertraglich zugesicherten Zertifizierungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

umfassen und durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise DARF die Einrichtung NUR in begründeten Einzelfallentscheidungen zulassen.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

g) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

h) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen abdecken oder diese Risiken transferieren oder diese Risiken tragen.

[25] Hinweis: Liegt ein Prüfbericht nach C5 vor, können diese Informationen daraus entnommen werden.

[26] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, welche die Einrichtung darin unterstützt, einen C5-Bericht systematisch auszuwerten. Dies beinhaltet, die Sicherheitsmaßnahmen des Cloud-Diensteanbieters (und die zugehörigen Prüfergebnisse) aufzunehmen, die eigenen Nutzerkontrollen für die Nutzung einzurichten und hierdurch das mit der Cloud-Nutzung verbundene Risiko einzuschätzen und steuern zu können. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), https://www.bsi.bund.de

[27] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[28] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (BSI 2020a), Kap. 4.4.5, S.16f.) enthält der Bericht keine Systembeschreibung vom Anbieter, sondern eine vom Prüfer im Rahmen der Prüfung erhobene Beschreibung mit vergleichbarem Inhalt, die im Rahmen der Tätigkeiten dieses Mindeststandards herangezogen werden kann.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.

i) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

i) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit Rechtsvorschriften nicht entgegenstehen.

ii) Die Einrichtung MUSS darauf achten, dass die Prüfrechte so ausgestaltet sind, dass die Einrichtung ihre gesetzlichen Anforderungen erfüllt.

iii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Einrichtung selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.

iv) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS die Einrichtung dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern

a) Die Einrichtung MUSS sich die Beteiligung von relevanten Unterauftragnehmern und anderen externen Dritten vom Cloud-Diensteanbieter vollständig in Art und Umfang benennen lassen. Die Entscheidung, welcher Unterauftragnehmer hier zu nennen ist, MUSS gemäß den Vorgaben des C5[29] erfolgen.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass beabsichtigte Änderungen hierüber unverzüglich schriftlich oder per E-Mail mitgeteilt werden.

c) Diese Mitteilungen KÖNNEN über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).

d) Falls Unterauftragnehmer wesentliche Teile[30] zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

- Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und
- zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.

NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

[29] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), Kap. 4.4.5, S.18f.
[30] Hinweis: Hinsichtlich Bestimmung „wesentlicher Teile“ siehe C5, (BSI 2020a), S.91

NCD.2.2.04 Lokation vertraglich zusichern

a) Die Einrichtung MUSS sämtliche Lokationen, an denen dienstliche Daten verarbeitet werden, vertraglich festlegen.

b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten.

NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.[31]

b) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS bei Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf achten.

ii) Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln

a) Die Einrichtung MUSS Kündigungsfristen dem Einsatzszenario angemessen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern

a) Die Einrichtung MUSS die Rückgabe der Daten regeln (Format, Datenträger, Protokolle, usw.).

b) Die Einrichtung MUSS berücksichtigen, dass die Maßnahmen zur Datenlöschung dem ermittelten Schutzbedarf entsprechen.

2.3 Einsatzphase

Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

NCD.2.3.01 ISMS einbinden

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen des Cloud-Dienstes bei sich einrichten. Die Einrichtung SOLLTE bei der Einbindung in das eigene ISMS zusätzlich die korrespondierenden Kriterien des C5[32] berücksichtigen.

NCD.2.3.02 Sicherheitsnachweise prüfen

[31] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (BMI 2014), S.1

[32] Hinweis: Der C5 führt mit Version 2020 Mitwirkungspflichten des Kunden als korrespondierende Kriterien ein. Die Umsetzung liegt im Verantwortungsbereich des Kunden und ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[33]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

NCD.2.3.03 Leistungsfähigkeit prüfen

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, beurteilen.

b) Die Einrichtung MUSS auf Abweichungen reagieren und die eigene IT-Infrastruktur und Netzanbindung den Ergebnissen der Überprüfung anpassen.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen.[34]

NCD.2.3.04 Informationspflichten nachhalten

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

i) einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,

ii) einem Austausch von Unterauftragnehmern oder Dritten.

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren

a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung als Identitätsnachweis seiner Benutzer (Log-in) an, SOLLTE die Einrichtung diese nutzen.

2.4 Beendigungsphase

Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[35]

NCD.2.4.01 Datenrückgabe durchführen

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

NCD.2.4.02 Datenlöschung bestätigen

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gemäß NCD2.2.07 erfolgte Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.

Kommentiert [h6]: Ggf. hier noch klarstellen, dass neben den Nutzdaten auch Protokoll-/Transaktionsdaten zu löschen sind, sofern so vorgesehen.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die Datenlöschung dokumentieren.

[33] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5", (BSI 2020c), https://www.bsi.bund.de

[34] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann. Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden.

[35] Siehe OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungsverhältnisses, (BSI 2020b), S.1ff

2.5 Sicherheitsanforderungen bei einer Mitnutzung

Nehmen Benutzer einer Einrichtung einen externen Cloud-Dienst in Anspruch, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[36] Für diesen Anwendungsfall regeln die nachfolgenden Sicherheitsanforderungen das Mindestsicherheitsniveau.

NCD.2.5.01 Mitnutzung von externen Cloud-Diensten

a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d) bis i) umsetzen und einhalten.

b) Die Einrichtung MUSS ermitteln, an welchen Lokationen dienstliche Daten verarbeitet werden.

i) Die Einrichtung MUSS dann bewerten, ob aus ihrer Sicht die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung heranziehen.

c) Die Einrichtung MUSS ermitteln, welche Rechte dem Cloud-Diensteanbieter oder Dritten an den dienstlichen Daten eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit der eigenen Sicherheitsrichtlinie vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar sind.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

e) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS dann bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen IT-Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[37]

Kommentiert [FH27]: Auf welcher Annahme basiert diese Einschränkung? M.E. ist nicht ersichtlich, warum für die Mitnutzung eines Cloud-Dienstes nicht ebenfalls die Erstellung eines Sicherheitskonzeptes notwendig sein sollte, insbesondere wenn die Bandbreite der extern verarbeitenden Daten nicht eingeschränkt ist. Sollte der Anwendungsfall „Mitnutzung" auf Grund des fehlenden Vertragsverhältnisses nicht genauso kritisch oder gar noch kritischer betrachtet werden als die „Nutzung"? Jede Art von Datenübertragung und Datenverarbeitung im Rahmen einer Nutzung oder Mitnutzung von Cloud-Diensten (selbst wenn es sich nur Metadaten handelt) sorgt für eine Vergrößerung des Angriffsvektors. Das spricht dafür, beim Szenario „Mitnutzung" mindestens dieselben Maßstäbe anzulegen (z.B. Kriterienkatalog C5) wie beim Szenario „Nutzung".

Kommentiert [h8]: Betrifft das Thema „Daten-Verschlüsselung" nur die Mitnutzung? Warum gilt es in diesem Mindeststandard nicht übergreifend für Nutzung und Mitnutzung?

[36] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen sind nicht als ein Vertragsverhältnis im Sinne dieses Mindeststands anzusehen.
[37] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017), S.1ff.

Literaturverzeichnis

AKTM (2011) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014

BMI (2014) Bundesministerium des Innern, Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung

BMI (2018) Bundesministerium des Innern, für Bau und Heimat: Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 – Notfallmanagement, Version 1.0

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management, Version 1.0

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/11916758, abgerufen am 17.11.2020

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: Kriterienkatalog Cloud Computing, Version 1.0 – Stand Februar 2020

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 3. Edition 2020

BSI (2020c) Bundesamt für Sicherheit in der Informationstechnik: Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5, https://www.bsi.bund.de/dok/14020574, abgerufen am 17.11.2020

DIN (2018) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119, abgerufen am 17.11.2020

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BDSG	Bundesdatenschutzgesetz
C5	Kriterienkatalog Cloud Computing
DIN	Deutsches Institut für Normierung e.V.
FAQ	Frequently Asked Questions
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
IT-SiBe	IT-Sicherheitsbeauftragte
StGB	Strafgesetzbuch
RFC	Request for Comments
VSA	Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)

Seite 7: [1] Kommentiert [h3]	h726	10.12.2020 18:54:00

Der gesamte Abschnitt 2 sollte m.E. noch klarer zwischen Nutzung und Mitnutzung unterscheiden.

Bspw.:

Gilt wirklich nur Kapitel 2.5 für Mitnutzung-Dienste und gelten die Kapitel 2.1-2.4 nur für Nutzung-Dienste? Wenn ja, dann sollte das am Anfang von Abschnitt 2 klargestellt werden. Wenn Teile der Kapitel 2.1-2.4 auch für Mitnutzung-Dienste gelten, wäre das kenntlich zu machen.

Dass Kapitel 2.2 nur für Nutzung-Dienste gilt (weil diese mit Beschaffung und Beauftragung verbunden sind), leuchtet ein. Aber eine Planungsphase sollte es ggf. auch bei Mitnutzung-Diensten geben, wobei dabei vermutlich nicht das ganze Kapitel 2.1 zu beachten ist.

Grundsätzlich sei hier angemerkt, dass es sehr schlanke Mitnutzung-Möglichkeiten gibt, z.B. Cloud-Dienste, die im Internet leicht verfügbar und oftmals auch als freeware (ggf. mit Apache Lizenz, mit AGG, aber nicht unbedingt mit Vertrag – was ja dann keine Nutzung, sondern nur Mitnutzung ist) angeboten werden. Hierfür die gesamten Aufgaben aus Kap. 2.1 ff. abzuarbeiten, wäre ein unverhältnismäßiger und auch nicht erforderlicher Aufwand. Es sollte also insbesondere bei OSS darauf geachtet werden, dass Sicherheitsmaßnahmen ausreichend umgesetzt, aber keine übermäßigen konzeptionellen Aufwände für jeden kleinen Individualfall der Cloud-(Mit)Nutzung betrieben werden müssen.

Außerdem gibt es sicherlich auch schlanke Nutzung-Dienste. Hier ein Beispiel (mit der hypothetischen Annahme, dass es solch einen Service noch nicht als geeignete OSS gibt und folgende neue Beauftragung erfolgt): Eine Behörde beauftragt eine Firma mit der Entwicklung eines Wechselkursrechners, der an dem offiziellen Wechselkurs der betroffenen Nationalbanken orientiert ist. Die Firma entwickelt den Wechselkursrechner und bietet den Service in Form eines Cloud-Dienst eines externen Anbieters an. Die Behörde nimmt die Leistung auf Basis des mit der Firma geschlossenen Vertrages an. Die Behörde nutzt den Wechselkursrechner, indem sie Zahlenbeträge und die zugehörige Währung (dies sind die dienstlichen Daten) an den Wechselkursrechner sendet und den Zahlenbetrag in einer anderen Währung vom Cloud-Dienst zurückerhält. All das ist eng eingebunden in eine Fachanwendung der Behörde. Es werden keine personenbezogenen Daten gesendet.

- ➔ Für solch einen Anwendungsfall ist m.E. zu hinterfragen, ob es dafür wirklich eine Cloud-Strategie und ein für den Cloud-Dienst spezifisches eigenes Sicherheitskonzept geben muss. Den Service im Sicherheitskonzept der Fachanwendung zu erwähnen und dort die Abhängigkeiten zu dem externen Anbieter darzustellen, würde m.E. den Zweck ausreichend erfüllen.

Von:	GP Mindeststandards Bund
An:	KdoCIR FaeEntw-InfoSichh
Cc:	FKT-BMVg CIT II 2; GP Mindeststandards Bund
Betreff:	BSI-Mindeststandard NCD 2.0 - war: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Datum:	Freitag, 3. September 2021 12:25:00
Anlagen:	image003.png image006.png image007.jpg

Sehr geehrter Herr [redacted],

der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste wurde am 07.07.2021 in der neuen Version 2.0 veröffentlicht. Diesen finden Sie inkl. der zugehörigen Referenztabelle auf den Webseiten des BSI:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

Vielen Dank für Ihre Beteiligung am Konsultationsverfahren.

Auf Ihre Rückmeldung hin haben wir die Fußnote zum Anwendungsbereich (Seite 5, Fußnote 7) angepasst:

„Hinweis: Private Cloud-Dienste der IT-Dienstleister des Bundes (z. B. Bundescloud) fallen somit nicht unter diese Bestimmung."

Mit freundlichen Grüßen
Im Auftrag
[redacted]

Referat BL 35 - Mindeststandards Bund
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: [redacted]
Hotline: +49 (0)228 99 9582-[redacted]
E-Mail: mindeststandards@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

++
Haben Sie schon unseren Mindeststandard-Newsletter abonniert?
https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen_node.html
++

Von: [redacted]@bundeswehr.org> **Im Auftrag von** KdoCIR FaeEntw-InfoSichh
Gesendet: Freitag, 8. Januar 2021 12:58
An: GP Mindeststandards Bund <mindeststandards@bsi.bund.de>
Cc: FKT-BMVg CIT II 2 <[redacted]@bmvg.bund.de>
Betreff: AW: : [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0

Sehr geehrte Damen und Herren,

herzlichen Dank für die Beteiligung an der Erarbeitung des Mindeststandards.
Im Auftrag des BMVg habe ich die Mitprüfung in Federführung übernommen.
Für das Verteidigungsressort bitte ich, die Anmerkungen siehe Anlage zu berücksichtigen. Eine entsprechende Erläuterung ist ebenfalls enthalten.

Bei Fragen stehe ich Ihnen gern zur Verfügung.

Mit freundlichem Gruß,
im Auftrag

[redacted]
Oberstleutnant
Referent IT-Grundschutz

Kommando Cyber- und Informationsraum
Ref Informationssicherheit I 5

Johanna-Kinkel-Straße 2-
4 | D 53175 Bonn
Büro: Etage 2 Raum C.3.10

Telefon: [redacted]
E-Mail: [redacted]@bundeswehr.org
[redacted]
[redacted]@bundeswehr.org
Internet:
Twitter: https://cir.bundeswehr.de
https://twitter.com/cirbw

----- Weitergeleitet von [redacted]/BMVg/BUND/DE am 20.11.2020 11:07 -----

Von: "GP Geschaeftszimmer_BL" <geschaeftszimmer-bl@bsi.bund.de>
An: "poststelle@bk.bund.de" <poststelle@bk.bund.de>, "poststelle@auswaertiges-amt.de" <poststelle@auswaertiges-amt.de>, "poststelle@bmi.bund.de" <poststelle@bmi.bund.de>, "poststelle@bmf.bund.de" <poststelle@bmf.bund.de>, "poststelle@bmjv.bund.de" <poststelle@bmjv.bund.de>, "poststelle@bmvg.bund.de" <poststelle@bmvg.bund.de>, "info@bmwi.bund.de" <info@bmwi.bund.de>, "poststelle@bmas.bund.de" <poststelle@bmas.bund.de>, "poststelle@bmel.bund.de" <poststelle@bmel.bund.de>, "poststelle@bmfsfj.bund.de" <poststelle@bmfsfj.bund.de>,

"poststelle@bmg.bund.de" <poststelle@bmg.bund.de>,
"poststelle@bmvi.bund.de" <poststelle@bmvi.bund.de>,
"Poststelle@bmu.bund.de" <Poststelle@bmu.bund.de>,
"information@bmbf.bund.de" <information@bmbf.bund.de>,
"poststelle@bmz.bund.de" <poststelle@bmz.bund.de>,
"bverfg@bundesverfassungsgericht.de"
<bverfg@bundesverfassungsgericht.de>, "poststelle@bpra.bund.de"
<poststelle@bpra.bund.de>, "bundesrat@bundesrat.de"
<bundesrat@bundesrat.de>, "Poststelle@brh.bund.de"
<Poststelle@brh.bund.de>, "[redacted]@bundestag.de"
<[redacted]@bundestag.de>, "Poststelle@bkm.bund.de"
<Poststelle@bkm.bund.de>, "Poststelle@bfdi.bund.de"
<Poststelle@bfdi.bund.de>, "[redacted]@itzbund.de" [redacted]@itzbund.de>,
[redacted]@jm.nrw.de"
[redacted]@jm.nrw.de>, "GP AG-InfoSic" <[redacted]
@bsi.bund.de>
Kopie: "GP Abteilung BL" <abteilung-bl@bsi.bund.de>, "GP Fachbereich BL 3" <fachbereich-bl3@bsi.bund.de>, "GP Referat BL 35" <referat-bl35@bsi.bund.de>, "GP Poststelle" <poststelle@bsi.bund.de>, "GP Stab 3 - Strategie und Leitungsunterstuetzung" <stab3@bsi.bund.de>, "GP Geschaeftszimmer_BL" <geschaeftszimmer-bl@bsi.bund.de>
Datum: 20.11.2020 11:06
Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Gesendet von: "[redacted]"
[redacted]@bsi.bund.de>

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1.0.5 vom 17.11.2020. Die Abgleichstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Fax: +49[redacted] 99 10

9582[redacted]
E-Ma
geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de

Von: GP Mindeststandards Bund
An: [redacted]@po.izei.bund.de
Cc: [redacted]@po.izei.bund.de; [redacted]@polizei.bund.de; GP Mindeststandards Bund
Betreff: BSI-Mindeststandard NCD 2.0 - war: AW: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Datum: Freitag, 3. September 2021 12:35:00

Sehr geehrter Frau [redacted],

der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste wurde am 07 07 2021 in der neuen Version 2 0 veröffentlicht Diesen finden Sie inkl der zugehörigen Referenztabelle auf den Webseiten des BSI:

https://www bsi bund de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node html

Vielen Dank für hre Beteiligung am Konsultationsverfahren

Die folgende Tabelle enthält die Ergebnisse der Überarbeitung des Mindeststandards bezüglich Ihrer Kommentare und Anmerkungen:
(Hervorhebungen/Streichungen sind leider nicht in der Formatierung erhalten geblieben – melden Sie sich bitte bei Problemen mit dieser „Inline"-Tabelle)

Kap. / Anf.	ALT	Kommentar BPOL	Rückmeldung	NEU
1	Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend	Empfehlung Löschung: M E eine zu einseitige Feststellung, ohne an dieser Stelle auf den Prozess einzugehen Der Folgesatz zeigt dies ausreichend auf	Satz gelöscht Begründung: Standardformulierung	
1	Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche [1] [1] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S 31	Empfehlung Löschung: Wiederholung zum Vorwort	Änderung übernommen Satz gestrichen	
2 1 02	c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen	Wenn keine Daten gem VS-NfD oder keine Daten i S d BDSG verarbeitet werden, bedarf es auch nicht der Beteiligung der Datenschutz-/Geheimschutzbeauftragten Vorschlag: "Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen "	Änderung übernommen	c) Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen
2 1 03	c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen	Wenn keine Daten gem VS-NfD oder keine Daten i S d BDSG verarbeitet werden, bedarf es auch nicht der Beteiligung der Datenschutz-/Geheimschutzbeauftragten Vorschlag: "Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen "	Änderung übernommen	c) Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen
2 1 03	f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[1] sowie Personen- und Dienstgeheimnisse ermitteln [1] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S 1ff	Wenn keine Daten gem VS-NfD oder keine Daten i S d BDSG verarbeitet werden, bedarf es auch nicht der Beteiligung der Datenschutz-/Geheimschutzbeauftragten Vorschlag: "Die Einrichtung MUSS für die identifizierten dienstlichen Daten – sofern betroffen – Geheim- und Datenschutzaspekte[1] sowie Personen- und Dienstgeheimnisse ermitteln " [1] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S 1ff	Änderung teilweise übernommen Anforderung wurde entsprechend konkretisiert	f) Falls Daten den Kategorien 1, 2 oder 3 zugeordnet wurden: Die Einrichtung MUSS für die identifizierten Daten dieser Kategorien die Geheim- und Datenschutzaspekte[1] sowie Anforderungen hinsichtlich Privat- und Dienstgeheimnisse ermitteln und aus diesen ggf entstehende, weitere Anforderungen ableiten [1] Hinsichtlich Datenschutzaspekten siehe insbesondere (AKTM 2011), S 1ff
2 2 05	a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher	Diese Anforderung ist grds zu begrüßen Gleichwohl muss diese aus rechtsstaatlichen Gründen i R d geltenden Rechtes bewertet werden Insofern wird auf die zu bevorzugenden Formulierungen im C5:2020 verwiesen	Änderung teilweise übernommen Anforderung entfallen, Fußnote nach NCD 2 1 03 Sicherheitskonzept für den externen Cloud-Dienst Buchstabe j) verschoben	

	Offenbarungspflichten und Ermittlungsbefugnisse gelangen [1] [1] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen (BMI 2014), S 1			

Mit freundlichen Grüßen
Im Auftrag
[redacted]

_____
Referat BL 35 - Mindeststandards Bund
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +[redacted]
Hotline: +49 (0)228 99 9582[redacted]
E-Mail: mindeststandards@bsi bund de
Internet: www bsi bund de

#DeutschlandDigitalSicherBSI

++
Haben Sie schon unseren Mindeststandard-Newsletter abonniert?
https://www bsi bund de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen_node html
++

-----Ursprüngliche Nachricht-----
Von: [redacted] @polizei bund de [redacted] @polizei bund de> Im Auftrag von [redacted] @polizei bund de
Gesendet: Mittwoch, 6 Januar 2021 12:53
An: GP Mindeststandards Bund <mindeststandards@bsi bund de>
Cc: [redacted] @polizei bund de; [redacted] @polizei bund de
Betreff: WG: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2 0

BPOLP - Referat 55
19 11 00 - 0001 - 0023

Sehr geehrte Damen und Herren,

Die im Anschreiben aufgeführten wesentlichen Änderungen begrüße ich ausdrücklich

die Hinweise aus der Bundespolizei sind in den Entwurf zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste im Überarbeitungsmodus eingearbeitet

Ich bedanke mich für die Beteiligung

Mit freundlichen Grüßen
[redacted]

_____
Bundespolizeipräsidium | Referat 55 | Heinrich-Mann-Allee 103 | 14473 Potsdam

Telefon: [redacted] | Mobil [redacted] | Fax: [redacted]
E-Mail: [redacted] @polizei bund de
E-Mail: [redacted] @polizei bund de
Internet: www bundespolizei de

-----Ursprüngliche Nachricht-----
Von: CI4@bmi bund de <CI4@bmi bund de>
Gesendet: Dienstag, 24 November 2020 15 55

An [redacted] @bdbos bmi bund de; P Post <[redacted] @polizei bund de>;
[redacted] @bva bund de; [redacted] @bsi bund de;
[redacted] @bbk bund de; [redacted] @badv bund de;
[redacted] @bakoev bund de; [redacted] @bamf bund de;
[redacted] @bbk bund de [redacted] @bbr bund de;
[redacted] @bescha bund de; [redacted] @bfv bund de[redacted] @bib bund de;
[redacted] @bisp de; [redacted] @bka bund de;
[redacted] @bkg bund de [redacted] @bpb bund de; P Post Ref 55
[redacted] polizei bund de>; [redacted] @bsi bund de; [redacted] @hsbund de;
[redacted] @destatis de; [redacted] @thw bund de;
[redacted] @zitis bund de; [redacted] @ZITiS bund de;
[redacted] r@bmi bund de; [redacted] @bakoev bund de

Cc: CI4@bmi bund de; RegCI4@bmi bund de
Betreff: Mindeststandard zur Nutzung externer Cloud-Dienste, hier:
Konsultationsverfahren zum Major-Release Version 2 0

CI 4 - 17002/20#11

Liebe Kolleginnen und Kollegen,
im Zuge der Überarbeitung und Anpassung des Mindeststandards zur Nutzung externer Cloud-Dienste finden Sie im Anhang das Anschreiben des AL BL im BSI, Herrn Samsel, sowie den Entwurf zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1 0 5 vom 17 11 2020 Die Änderungstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt

Bitte senden Sie Kommentierungen und Rückmeldungen bis zum 8 Januar 2021 per E-Mail an das Postfach mindeststandards@bsi bund de

Mit freundlichen Grüßen
im Auftrag

[redacted]
_____
Bundeministerium des Innern, für Bau und Heimat
Referat CI 4
Cybersicherheit in der Bundesverwaltung
D-10557 Berlin, Alt-Moabit 140
Telefon: [redacted]
eMail: CI4@bmi bund de; [redacted] @bmi bund de
Internet: www bmi bund de; www cio bund de

-----Ursprüngliche Nachricht-----
Von: [redacted] @bsi bund de> Im Auftrag von GP Geschaeftszimmer_BL
Gesendet: Freitag, 20 November 2020 11:06
An: poststelle@bk bund de; poststelle@auswaertiges-amt de; poststelle@bmi bund de; poststelle@bmf bund de; poststelle@bmjv bund de; poststelle@bmvg bund de; info@bmwi bund de; poststelle@bmas bund de; poststelle@bmel bund de; poststelle@bmfsfj bund de; poststelle@bmg bund de; poststelle@bmvi bund de; Poststelle@bmu bund de; information@bmbf bund de; poststelle@bmz bund de; bverfg@bundesverfassungsgericht de; poststelle@bpra bund de; bundesrat@bundesrat de; Poststelle@brh bund de; [redacted] @bundestag de; Poststelle@bkm bund de; Poststelle@bfdi bund de [redacted] @itzbund de; [redacted] @jm nrw de; GP AG-InfoSic [redacted] @bsi bund de>

Cc: GP Abteilung BL <abteilung-bl@bsi bund de>; GP Fachbereich BL 3 <fachbereich-bl3@bsi bund de>; GP Referat BL 35 <referat-bl35@bsi bund de>; GP Poststelle <poststelle@bsi bund de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi bund de>; GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi bund de>

Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2 0

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1 0 5 vom 17 11 2020 Die Abgleichstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon:+49 228 99 9582[redacted]
Fax:+49 228 99 10 9582[redacted]
E-Mail:geschaeftszimmer-bl@bsi bund de
Internet:www bsi bund de
www bsi-fuer-buerger de

Von:	GP Mindeststandards Bund
An:	Itsicherheit (C202)
Cc:	GP Mindeststandards Bund
Betreff:	BSI-Mindeststandard NCD 2.0 - war: AW: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
Datum:	Freitag, 3. September 2021 12:27:00

Sehr geehrter Herr [redacted]

der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste wurde am 07.07.2021 in der neuen Version 2.0 veröffentlicht. Diesen finden Sie inkl. der zugehörigen Referenztabelle auf den Webseiten des BSI:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

Vielen Dank für Ihre Beteiligung am Konsultationsverfahren.

Zu Ihren Rückmeldungen im Einzelnen:
1. Der geschlechtergerechte Sprachgebrauch in den Dokumenten der Mindeststandards des BSI ist derzeit noch in der Abstimmung. Es ist jedoch davon auszugehen, dass es hier noch zu Anpassungen kommt, etwa im Rahmen von Minor-Releases (meist einmal jährlich).
2. Das Verhältnis zum IT-Grundschutz-Baustein wird im kommenden Hilfsdokument dargestellt. Zur Arbeitsunterstützung steht eine entsprechende Referenztabelle zur Verfügung, welche die Anforderungen des Mindeststandards mit denen aus dem IT-Grundschutz verknüpft.
3. Bitte kontaktieren Sie uns, wenn Sie bei konkreten Anwendungen noch Probleme erkennen.

Mit freundlichen Grüßen
Im Auftrag
[redacted]

Referat BL 35 - Mindeststandards Bund
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582 [redacted]
Mobil: [redacted]
Hotline: +49 (0)228 99 9582-[redacted]
E-Mail: mindeststandards@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

++
Haben Sie schon unseren Mindeststandard-Newsletter abonniert?
https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Newsletter/Newsletter-bestellen/newsletter-bestellen_node.html
++

-----Ursprüngliche Nachricht-----
Von: Itsicherheit (C202) [redacted]@destatis.de>
Gesendet: Dienstag, 5. Januar 2021 10:52
An: GP Mindeststandards Bund <mindeststandards@bsi.bund.de>
Betreff: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0

Sehr geehrte Damen und Herren,

das BMI hat mir zur Kommentierung den Entwurf des Mindeststandards zur Nutzung externer Cloud-Dienste zur Verfügung gestellt.

Fachlich gibt es dazu keinen Korrekturbedarf, wenngleich die Umsetzung hinsichtlich der Findung geeigneter Anbieter und das Erfüllungsprozedere sehr schwierig bzw. aufwändig werden wird.
Die Abgrenzung zum Outsourcing, das kein Cloud-Computing darstellt, ist m.E. hinreichend klar geworden, wenn man die Erläuterungen auf der BSI-Seite /cloud mit berücksichtigt.

Die Frage, ob der Baustein OPS.2.1 anzuwenden ist, hat sich mit der Erwähnung eines neuen Bausteins OPS.2.2 auch geklärt. Ich vermute, dass sowohl der Baustein OPS.2.2 wie auch die Anforderungen des Mindeststandards von den dem UP Bund unterliegenden Behörden parallel bearbeitet werden sollen und die Abarbeitung des Mindeststandards die Abarbeitung des Bausteins OPS.2.2 nicht ersetzt. Ggf. könnte hier aber auch ein ergänzender Hinweis für einen ggf. verpflichtend doppelten Aufwand in einer Fußnote hilfreich sein.

Aus Diskussionen mit unserer behördlichen Gleichstellungsbeauftragten bei der Gestaltung hausinterner Richtlinien und dem Rückgriff auf BSI-Unterlagen ist jedoch anzumerken, dass die Wortwahl im Mindeststandard der geschlechtergerechten Darstellung nach hiesiger Interpretation des BGleiG nicht entspricht. Es würde manche Diskussion und Zusatzarbeit ersparen, wenn das BSI jeweils die männliche und weibliche Form (oder eine neutrale) in seinen Vorgabetexten und Grafiken pflegen würde. Beispiel: Auditoren und Auditorinnen bzw. Auditierende, Anbietende, Prüfende ... Dies betrifft insbesondere auch die BSI-Standards und das Kompendium.

Freundliche Grüße
Im Auftrag
[redacted]
Informationssicherheitsbeauftragter

Telefon [redacted] oder [redacted]

[redacted]@destatis.de
www.destatis.de

www.dashboard-deutschland.de

Von:	[redacted] im Auftrag von GP Geschaeftszimmer_BL
An:	GP Abteilung BL; GP Abteilung TK; GP Abteilung KM; GP Abteilung OC; GP Abteilung SZ; GP Abteilung DI; GP Abteilung WG; GP Abteilung Z; GP Referat BL 11; GP Referat BL 12; GP Referat BL 13; GP Referat BL 14; GP Referat BL 16; GP Referat BL 17; GP Referat BL 21; GP Referat BL 22; GP Referat BL 23; GP Referat BL 25; GP Referat BL 31; GP Referat BL 32; GP Referat BL 33; GP Referat BL 34; GP Referat BL 35
Cc:	GP Mindeststandards Bund; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_BL
Betreff:	[n.A.z.K.] Mindeststandard des BSI gem. § 8 Abs. 1 BSIG hier: Nutzung externer Cloud-Dienste
Datum:	Donnerstag, 8. Juli 2021 11:21:29
Anlagen:	20210708-Mindeststandard des BSI gem. § 8 Abs. 1 BSIG hier_Nutzung externer Cloud-Dienste.pdf Mindeststandard_Nutzung_externer_Cloud-Dienste_v2.0.pdf Referenztabelle_NCD20_ITG2021.xlsx

---

Liebe Kolleginnen und Kollegen,

nachfolgende E-Mail n.A.z.K.

Viele Grüße
[redacted]

-----Ursprüngliche Nachricht-----
Von: [redacted]@bsi.bund.de> Im Auftrag von GP Geschaeftszimmer_BL
Gesendet: Donnerstag, 8. Juli 2021 11:20
An: poststelle@bk.bund.de; poststelle@auswaertiges-amt.de; poststelle@bmi.bund.de; poststelle@bmf.bund.de; poststelle@bmjv.bund.de; poststelle@bmvg.bund.de; info@bmwi.bund.de; poststelle@bmas.bund.de; poststelle@bmel.bund.de; poststelle@bmfsfj.bund.de; poststelle@bmg.bund.de; poststelle@bmvi.bund.de; Poststelle@bmu.bund.de; information@bmbf.bund.de; poststelle@bmz.bund.de; bverfg@bundesverfassungsgericht.de; poststelle@bpra.bund.de; bundesrat@bundesrat.de; Poststelle@brh.bund.de; [redacted]@bundestag.de; Poststelle@bkm.bund.de; Poststelle@bfdi.bund.de; [redacted]@itzbund.de; [redacted]@jm.nrw.de; GP AG-InfoSic <[redacted]@bsi.bund.de>
Cc: GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>
Betreff: Mindeststandard des BSI gem. § 8 Abs. 1 BSIG hier: Nutzung externer Cloud-Dienste

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021. Die Referenztabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +[redacted]
E-Mail: geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital·Sicher·BSI·

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Per Mail

Dienststellen der obersten Bundesbehörden

ITZ Bund (ISB)

Landes-CISOs über Geschäftsstelle der AG InfoSic

Geschäftsstelle BLK

[redacted]
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185 189
53175 Bonn
Postanschrift:
Postfach 20 03 63
53133 Bonn
Tel. +49 228 99 9582 [redacted]
Fax +49 228 99 10 9582 [redacted]
mindeststandards@bsi.bund.de
www.bsi.bund.de

Betreff: Mindeststandard des BSI gem. § 8 Abs. 1 BSIG
hier: Nutzung externer Cloud-Dienste

Bezug: Mein Schreiben BL35 – 750 00 07 vom 20.11.2020
RESSORTKONSULTATION
Geschäftszeichen: BL35 – 750 07
Datum: 08.07.2021

Sehr geehrte Damen und Herren,

Cloud-Dienste können eine wertvolle Ergänzung zur eigenen IT-Infrastruktur darstellen. Um auch in der Bundesverwaltung einen sicheren Einsatz von Cloud-Diensten externer Anbieter zu ermöglichen, hat das BSI bereits 2017 den Mindeststandard zur Nutzung externer Cloud-Dienste veröffentlicht. Nach Überarbeitung des Kriterienkatalogs Cloud Computing (C5:2020) habe ich nun auch den Mindeststandard aktualisiert und übersende Ihnen als Anlage die neue Version 2.0 inklusive Referenztabelle zum IT-Grundschutz. Eine Änderungsübersicht finden Sie auf der BSI-Webseite unter https://www.bsi.bund.de/mindeststandards. Dort werde ich zeitnah auch ein aktualisiertes Hilfsdokument zum Mindeststandard zur Verfügung stellen.

Für die zahlreichen und konstruktiven Rückmeldungen aus dem vorgelagerten Konsultationsverfahren (siehe Bezugsschreiben) möchte ich mich auf diesem Wege ganz herzlich bei Ihnen bedanken.

Im Bezugsschreiben hatte ich Sie bereits darauf hingewiesen, dass der frühere Informationsaustausch zur Cloud-Nutzung entfallen ist. Mit Veröffentlichung des aktualisierten Mindeststandards möchte ich Sie nun bitten, stattdessen an einer einmaligen Bedarfsabfrage zur Nutzung von

externer Cloud-Diensten ("Public Cloud") teilzunehmen. Hier geht es nicht, wie beim früheren Informationsaustausch, ausschließlich um bereits genutzte Cloud-Dienste, sondern um eine unverbindliche Einschätzung, welchen Bedarf an Cloud Services Sie in Ihrem Haus für die nächsten Jahre sehen. Die Ergebnisse der Umfrage sollen uns dabei helfen, unsere Vorhaben zur Cloud-Nutzung besser auf die tatsächlichen Bedürfnisse der Bundesverwaltung anpassen zu können. Die Abfrage erreichen Sie unter dem folgenden Link: https://www.bsi.bund.de/dok/946674

Für Ihre Teilnahme bedanke ich mich im Voraus.

Der Mindeststandard sowie die Bedarfsabfrage richten sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte, IT-Betriebspersonal sowie mit der Beschaffung beauftragte Stellen. Ich möchte Sie daher bitten, diesen Mindeststandard sowie den Link zur Umfrage in Ihrem Bereich entsprechend bekannt zu geben.

Rückfragen und Anregungen nehmen die Kolleginnen und Kollegen des Fachreferates über das zentrale Postfach mindeststandards@bsi.bund.de gerne entgegen.

Mit freundlichen Grüßen
Im Auftrag

Samsel

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	24.04.2017	Erstveröffentlichung
2.0	07.07.2021	Major Release - Zusammenführung der Mindeststandards zur Nutzung und Mitnutzung externer Cloud-Dienste

Tabelle 1: Versionsgeschichte des Mindeststandards. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/dok/930566

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. Umsetzungsplan Bund 2017 (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (BSI 2019)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

Inhalt

1 Beschreibung

Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste.

1.1 Begriffsbestimmung und Abgrenzung

Zur Begriffsbestimmung nutzt dieser Mindeststandard die Definition für Cloud-Dienste des C5:2020[5], die sich an die internationale Begriffsdefinition des ISO 17788 anlehnt.[6] Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen („Cloud-Dienste“) erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der in diesem Rahmen angebotenen Cloud-Dienste umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Anwendungen.

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind Cloud-Dienste, die von Anbietern der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes erbracht werden .[7]

Als Nutzung eines Cloud-Dienstes sind das Speichern und Verarbeiten von dienstlichen Daten[8] durch einen externen Cloud-Dienst zu verstehen. Dieser kann durch eine oder mehrere Einrichtungen beauftragt werden. Regelungen für das Mitnutzen externer Cloud-Dienste durch Benutzer[9] einer Einrichtung sind in Kapitel 2.5 beschrieben. Von einer Mitnutzung wird insbesondere ausgegangen, wenn eine Einrichtung den externen Cloud-Dienst nicht selbst beauftragt hat.

Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards dennoch hilfreiche Empfehlungen enthalten und trotzdem angewendet werden (siehe NCD.2.1.02c), Buchstabe e)).[10]

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[11] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN

[5] Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing), (BSI 2020a)

[6] Der Standard „ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary“ (ISO 2014) definiert Cloud Computing als Paradigma für die Ermöglichung über ein Netz auf ein skalierbaren und elastischen Pool von geteilten virtuellen oder physischen Ressourcen (Server, Plattform, Anwendung, Software, etc.) zuzugreifen und über ein Selbst-Service Portal zu bestellen und selbst zu administrieren. Ein Cloud-Service ist als über eine definierte Schnittstelle buchbare und über Cloud Computing angebotene Fähigkeiten („capabilities“) definiert. Cloud-Fähigkeiten werden nach Infrastruktur, Plattform und Anwendung unterschieden.

[7] Hinweis: Private Cloud-Dienste der IT-Dienstleister des Bundes (z. B. Bundescloud) fallen somit nicht unter diese Bestimmung.

[8] Dienstliche Daten können gleichzeitig auch personenbezogene Daten sein. Für den Zweck dieses Mindeststandards sind jedoch nicht solche personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden, gemeint.

[9] Analog Rolle „Benutzer“ nach IT-Grundschutz-Kompendium, (BSI 2021): „Ein Benutzer ist ein Mitarbeiter einer Institution, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt. IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben verwendet.“, Kap. Rollen, S. 27

[10] Hinweis: Für eine Beschreibung, wie sich die Anforderungsnummerierung zusammensetzt, siehe FAQ zu den Mindeststandards (BSI 2019)

[11] Vgl. BSI-Standard 200-2 (BSI 2017a), S. 18

für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[12] und DIN 820-2: 2018.[13]

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

[12] Vgl. Key words for use in RFCs (IETF 1997)
[13] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[14] auf.

2.1 Planungsphase

Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*

- die Cloud-Nutzungs-Strategie,
- die darauf basierende Sicherheitsrichtlinie sowie
- das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.

Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend.

NCD.2.1.01 Cloud-Nutzungs-Strategie

a) Die Einrichtung MUSS eine Cloud-Nutzungs-Strategie nach OPS.2.2.A1 *Erstellung einer Strategie für die Cloud-Nutzung*[15] erstellen.

b) Die Einrichtung MUSS in dieser Cloud-Nutzungs-Strategie festlegen, wie sie mit Risiken bei der Nutzung externer Cloud-Dienste umgeht. Hierzu **MUSS** eine Richtlinie zur Risikobewertung und -behandlung erstellt werden.

c) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in ihrer Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist. [16] Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn dieser die in der Cloud-Nutzungs-Strategie definierten Ziele, Chancen und Risiken angemessen unterstützt.

d) Die Einrichtung MUSS vor der Nutzung des externen Cloud-Dienstes eine Risikoanalyse gemäß der in NCD.2.1.01 b) festgelegten Richtlinie durchführen.

NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[17] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Cloud Computing Compliance Criteria Catalogue – C5 (Kriterienkatalog Cloud Computing) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[18]

c) Die Einrichtung MUSS - sofern betroffen - die zuständigen Datenschutz- und Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.

[14] IT-Grundschutz-Kompendium, (BSI 2021), OPS.2.2 *Cloud-Nutzung*
[15] IT-Grundschutz-Kompendium, (BSI 2021), OPS.2.2 *Cloud-Nutzung*
[16] Hinweis: OPS.2.2.A1 *Erstellung einer Cloud-Nutzungs-Strategie* sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.
[17] IT-Grundschutz-Kompendium, (BSI 2021), OPS.2.2 *Cloud-Nutzung*
[18] Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing), (BSI 2020a), S.1ff.

NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[19]

c) Die Einrichtung MUSS - sofern betroffen - die zuständigen Datenschutz- und Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen.

d) Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesen Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

f) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß Strafgesetzbuch (StGB) §§ 203 und 353b
- Kategorie 2 = personenbezogene Daten gemäß Datenschutzgrundverordnung (DSGVO) Art. 4 Nr. 1
- Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[20]
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

g) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und 3 gleichzeitig zuordnen.

h) Falls Daten den Kategorien 1, 2 oder 3 zugeordnet wurden: Die Einrichtung MUSS für die identifizierten dienstlichen Daten dieser Kategorien die Geheim- und Datenschutzaspekte[21] sowie Anforderungen hinsichtlich Privat- und Dienstgeheimnisse ermitteln und aus diesen ggf. entstehende, weitere Anforderungen ableiten.

> i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln und bewerten.[22] Die Einrichtung MUSS die ermittelten Risiken gemäß den in der Cloud-Nutzungs-Strategie festgelegten Richtlinien zur Risikobewertung bewerten.
>
> ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn alle ermittelten Risiken gemäß den in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobehandlung wirksam vermieden oder hinreichend reduziert oder in Übereinstimmung mit den Risikoakzeptanzkriterien bei der Cloud-Nutzung getragen werden können.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen)[23] unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese

[19] Siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud

[20] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), (BMI 2018)

[21] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff.

[22] Hinweis: Es gilt, zu bewerten, inwiefern die mit dem betrachteten Cloud-Dienst im beabsichtigten Anwendungsfall verbundenen rechtlichen, technischen und organisatorischen Risiken mit der Cloud-Nutzungs-Strategie vereinbar sind.

[23] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (BMI 2014), S.1

Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

NCD.2.1.04 Notfall- und Kontinuitätsmanagement

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[24] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint. Es umfasst sowohl präventive als auch reaktive Maßnahmen, mit denen eine Einrichtung auf Notfälle und Krisensituationen reagiert. Es gilt im Weiteren die Begrifflichkeit des BSI-Standards 100-4.[25]

a) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen und Krisensituationen einnehmen würde.[26]

b) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss.[27]

c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob sich die Cloud-Nutzung auf Maßnahmen, die Notfällen und Krisensituationen präventiv und/oder reaktiv entgegenwirken, auswirkt und inwiefern diese Maßnahmen ggf. anzupassen sind. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.

2.2 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters.

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss bewerten, inwiefern der externe Cloud-Dienst die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) erfüllt.[28]

b) Die Einrichtung MUSS die Erfüllung dieser Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der *Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5*[29] verwendet werden.

---

[24] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[25] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[26] Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt?
[27] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?
[28] Hinweis: Liegt ein C5-Prüfbericht vor, können diesem Informationen entnommen und der Bewertung zugrunde gelegt werden.
[29] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, die dabei unterstützt, einen C5-Prüfbericht systematisch auszuwerten. Diese Auswertung beinhaltet, die Sicherheitsmaßnahmen (Kontrollen) des Cloud-Diensteanbieters inklusive der zugehörigen Prüfergebnisse sowie der auf Cloud-Nutzerseite einzurichtenden Kontrollen aufzunehmen. In Verbindung mit den aufseiten der Einrichtung eingerichteten Kontrollen sowie weiterer, vom individuellen Anwendungsfall abhängenden Informationen lassen sich die mit der Nutzung des betrachteten Cloud-Dienstes verbundenen Risiken identifizieren und bewerten. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020b), https://www.bsi.bund.de

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN mindestens

- die angemessene und wirksame Erfüllung der Basiskriterien nach C5[30],
- die aktuelle Dokumentation der Systembeschreibung[31],
- die Aktualität von vertraglich zugesicherten Zertifizierungen und Berichterstattungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

umfassen und KÖNNEN vom Cloud-Diensteanbieter durch die regelmäßige Bereitstellung einer aktuellen C5-Berichterstattung vom Typ2 erbracht werden.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten und eventuellen Unklarheiten und insbesondere darin ausgewiesene Abweichungen in geeigneter Form nachgehen. Hierbei MUSS die Einrichtung auch abwägen, ob und inwiefern ein Risiko entsteht und wie mit diesem umzugehen ist.

g) Insbesondere MÜSSEN Zertifikate, Prüfberichte und Nachweise den Zeitraum, in dem die Einrichtung den Cloud-Dienst nutzt, jeweils vollständig abdecken und DÜRFEN KEINE zeitlichen Lücken enthalten oder entstehen lassen. Dies MUSS die Einrichtung in ihre Sicherheitsanforderungen sowie demzufolge in die Leistungsbeschreibung aufnehmen.

h) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

i) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen, die vom Cloud-Diensteanbieter zu erfüllen sind, abdecken oder diese Risiken transferieren oder diese Risiken tragen.

> i) Die Einrichtung MUSS die weiteren Anforderungen nach NCD.2.1.03, Buchstabe i) in ihre Sicherheitsanforderungen aufnehmen. Soweit die Einrichtung diese weiteren Anforderungen nur gemeinsam mit dem Cloud-Diensteanbieter erfüllen kann, MUSS die Einrichtung diese in die Leistungsbeschreibung bzw. in das Vertragsverhältnis mit dem Cloud-Diensteanbieter aufnehmen.
>
> ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.

j) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

> i) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass die Einrichtung ihre weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) erfüllt.
>
> ii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang eine Bewertung des vom Cloud-Diensteanbieter für den betrachteten Cloud-Dienst gebotenen Informationssicherheitsniveaus ermöglichen und die Einrichtung selbst oder Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) die Prüfrechte wahrnehmen können.

[30] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[31] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (BSI 2020a), Kap. 4.4.5, S.16f.) enthält der Bericht keine vom Cloud-Diensteanbieter angefertigte Systembeschreibung, sondern eine vom Prüfer im Rahmen der Prüfung angefertigte Systembeschreibung.

iii) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS sich die Einrichtung vom Cloud-Diensteanbieter dazu berechtigen lassen, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

iv) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) nicht entgegenstehen.

NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter vollständig benennen lassen, welche seiner Unterauftragnehmer gemäß C5 als Subdienstleistungsunternehmen[32] anzusehen sind und auf welche Art und welchem Umfang er diese in die Bereitstellung des Cloud-Dienstes einbezieht.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass er der Einrichtung beabsichtigte Änderungen an vertraglichen Vereinbarungen mit Subdienstleistungsunternehmen, die in die Bereitstellung des Cloud-Dienstes involviert sind, unverzüglich schriftlich oder per E-Mail mitteilt.

i) Diese Mitteilung SOLLTE zeitlich vor Umsetzung der Änderung erfolgen.

ii) Der Cloud-Diensteanbieter MUSS der Einrichtung insbesondere mitteilen, wenn er bestehende Vertragsverhältnisse beendet oder neue Vertragsverhältnisse mit Cloud-Diensteanbietern eingeht. Vertragsverhältnisse in diesem Sinne schließen alle mitgeltenden Dokumente und Regelungen, wie z. B. Leistungsscheine, Dienstgütevereinbarungen oder Allgemeine Geschäfts- und Einkaufsbedingungen ein.

c) Diese Mitteilungen KANN der Cloud-Diensteanbieter z. B. über Internetportale oder Push-Benachrichtigungen bereitstellen, wenn die Einrichtung diese Anforderungen als erfüllt ansieht.

d) Falls der Cloud-Diensteanbieter Subdienstleistungsunternehmen einbezieht oder anderweitig wesentliche Teile der Entwicklung oder Bereitstellung des Cloud-Dienstes an Unterauftragnehmer auslagert, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

- die Subdienstleistungsunternehmen und Unterauftragnehmer die zwischen der Einrichtung und dem Cloud-Diensteerbringer vertraglich festgelegten Vorgaben ebenfalls erfüllen und
- sich die Prüfrechte, die der Cloud-Diensteerbringer der Einrichtung zugesichert hat, auch auf die Subdienstleistungsunternehmen und Unterauftragnehmer des Cloud-Diensteerbringers beziehen.

NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

NCD.2.2.04 Lokation vertraglich zusichern

a) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Hierzu MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und der Risikoanalyse, das mögliche Risiko eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder

[32] Kriterienkatalog Cloud Computing (C5:2020), (BSI 2020a), Kap. 4.4.5, S.18f.

Ermittlungsbehörden) sowie weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) bewerten.

b) Die Einrichtung MUSS sämtliche Lokationen, an denen der Cloud-Diensteerbringer mit dem Cloud-Dienst dienstliche Daten speichert und verarbeitet, vertraglich festlegen. Dabei MUSS die Einrichtung auch Datensicherungen berücksichtigen, da diese ggf. an Drittlokationen durchgeführt werden.

NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

a) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS beim Festlegen von Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf der mit dem Cloud-Dienst verarbeiteten dienstlichen Daten achten.

ii) Beim Festlegen von Vertragsstrafen und Haftungsregelungen sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln

a) Die Einrichtung MUSS dem Anwendungsfall angemessene Kündigungsfristen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern

a) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, wie dieser die mit dem Cloud-Dienst verarbeiteten dienstlichen Daten nach Beendigung der Nutzung an die Einrichtung übergibt (z. B. Fristen, Datenformat, Datenträger, Protokolle usw.).

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, welche Maßnahmen dieser zur Löschung der dienstlichen Daten durchführt. Dabei MUSS die Einrichtung sicherstellen, dass die Maßnahmen dem zuvor ermittelten Schutzbedarf entsprechen.

2.3 Einsatzphase

Die Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

NCD.2.3.01 ISMS einbinden

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die in der C5-Berichterstattung genannten korrespondierenden Kontrollen für Cloud-Kunden[33] in ihrem ISMS einrichten. Die Einrichtung SOLLTE darüber hinaus die im C5 beschriebenen korrespondierenden Kriterien für Kunden berücksichtigen.

[33] Hinweis: Der C5 führt in Version 2020 mit den korrespondierenden Kriterien für Kunden bestimmte Mitwirkungspflichten des Cloud-Kunden ein. Der C5 hält Cloud-Diensteanbieter dazu an, diese Mitwirkungspflichten, abhängig von der Art des Cloud-Dienstes, zu definieren und in den C5-Prüfbericht aufzunehmen. Es liegt im Verantwortungsbereich des Cloud-Kunden und damit der Einrichtung, den Mitwirkungspflichten entsprechende Kontrollen zu gestalten, einzurichten und durchzuführen. Dies ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9

NCD.2.3.02 Sicherheitsnachweise prüfen

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[34]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

NCD.2.3.03 Leistungsfähigkeit prüfen

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, vor dem Hintergrund der Nutzung des Cloud-Dienstes beurteilen.

b) Die Einrichtung MUSS ggf. auftretende Abweichungen bewerten und auf diese durch geeignete Anpassungen an der eigenen IT-Infrastruktur und Netzanbindung reagieren.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters und des Cloud-Dienstes sowie der Netzverbindung zum Cloud-Diensteanbieter beurteilen.[35]

NCD.2.3.04 Informationspflichten nachhalten

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

i) einer Eingliederung des Cloud-Diensteanbieters in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihm,

ii) einem Austausch von Unterauftragnehmern oder Dritten (siehe hierzu auch NCD.2.2.02).

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und auf diese gemäß der vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren

a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung für Anmeldungen von Benutzern (Log-in) an, SOLLTE die Einrichtung diese nutzen.

b) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung für Anmeldungen von Benutzern mit privilegierten Rechten (Log-in) wie bspw. Administratoren an, MUSS die Einrichtung diese nutzen.

2.4 Beendigungsphase

Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[36]

NCD.2.4.01 Datenrückgabe durchführen

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle dienstlichen Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

[34] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020b)

[35] Hinweis: Viele Cloud-Diensteanbieter stellen für die Beurteilung ihrer Leistungsfähigkeit geeignete Information kontinuierlich (bspw. in Portalen oder auf Webseiten) bereit. Einrichtungen können basierend auf diesen sowie ggf. weiteren, selbst erhobenen Informationen die Leistungsfähigkeit von Cloud-Diensteanbietern kontinuierlich überwachen. Eine in geeigneter Weise durchgeführte kontinuierliche Überwachung kann die Basis für die geforderte, mindestens jährlich durchzuführende Bewertung der Leistungsfähigkeit eines Cloud-Diensteanbieters sein, aber sie nicht vollständig ersetzen.

[36] Siehe OPS.2.2.A14 *Geordnete Beendigung eines Cloud-Nutzungsverhältnisses*, (BSI 2021)

NCD.2.4.02 Datenlöschung bestätigen

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gem. NCD.2.2.07 erfolgte Löschung aller dienstlichen Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.[37] Dies umfasst die Bestätigung, dass die dienstlichen Daten gemäß der vertraglich vereinbarten Verfahren gelöscht wurden.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern (z. B. Subdienstleistungsunternehmen) und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die durch den Cloud-Diensteanbieter bestätigte Datenlöschung dokumentieren.

2.5 Sicherheitsanforderungen bei einer Mitnutzung

Nutzen die Benutzer einer Einrichtung einen externen Cloud-Dienst, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[38] Die nachfolgenden Sicherheitsanforderungen regeln die Mitnutzung externer Cloud-Dienste.

NCD.2.5.01 Mitnutzung externer Cloud-Dienste

a) Die Einrichtung MUSS sicherstellen, dass die Mitnutzung mit der eigenen Cloud-Strategie (siehe NCD.2.1.01) vereinbar ist.

b) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstabe d) bis i) umsetzen und einhalten.

c) Die Einrichtung MUSS ermitteln, an welchen Lokationen mit dem externen Cloud-Dienst dienstliche Daten verarbeitet werden. Dies schließt auch Datensicherungen sowie, sofern gegeben, Unterauftragnehmer und Subdienstleister des Cloud-Diensteanbieters ein.

> i) Die Einrichtung MUSS bewerten, ob die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.
>
> ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung sowie, sofern gegeben, weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) heranziehen.

d) Die Einrichtung MUSS ermitteln, welche Rechte an den dienstlichen Daten dem Cloud-Diensteanbieter oder Dritten durch das Akzeptieren der vom Cloud-Diensteanbieter vorgegebenen Allgemeinen Geschäftsbedingungen (AGB), Datenschutzerklärung oder sonstigen Nutzungsbedingungen eingeräumt werden.

> i) Die Einrichtung MUSS bewerten, ob diese Rechte mit den eigenen Sicherheitsanforderungen, die sie in der Sicherheitsrichtlinie und dem eigenen Sicherheitskonzept definiert hat, vereinbar sind.
>
> ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

e) Die Einrichtung MUSS bewerten, ob und wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt zu speichern sind. Für die anschließende Bewertung SOLLTE die Einrichtung die identifizierten Risiken mit der eigenen Cloud-Strategie (siehe NCD.2.1.01) abgleichen.

> i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.
>
> ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

[37] Hinweis: Neben Nutzdaten können auch Protokoll-/Transaktionsdaten zu löschen sein.

[38] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen ist nicht als ein Vertragsverhältnis im Sinne dieses Mindeststandards anzusehen.

f) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[39]

[39] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017b), S.1ff.

Literaturverzeichnis

AKTM (2011) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014, https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHCloudComputing.html

BMI (2014) Bundesministerium des Innern, Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/08/no-spy-erlass.html

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html

BMI (2018) Bundesministerium des Innern, für Bau und Heimat: Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018, https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 – Notfallmanagement, Version 1.0, https://www.bsi.bund.de/dok/128600

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, https://www.bsi.bund.de/dok/128640

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management, Version 1.0, https://www.bsi.bund.de/dok/453264

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/11916758, abgerufen am 17.11.2020

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing) – Stand Februar 2020, https://www.bsi.bund.de/dok/452204

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5, https://www.bsi.bund.de/dok/14020574, abgerufen am 17.11.2020

BSI (2021) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Edition 2021, https://www.bsi.bund.de/dok/128568

DIN (2018) Deutsches Institut für Normung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119, abgerufen am 17.11.2020

ISO (2014) ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Criteria Catalogue (Kriterienkatalog Cloud Computing)
DIN	Deutsches Institut für Normung e.V.
DSGVO	Datenschutzgrundverordnung
FAQ	Frequently Asked Questions
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
ISO/IEC	International Organisation for Standardization / International Electrotechnical Commission
IT-SiBe	IT-Sicherheitsbeauftragte
StGB	Strafgesetzbuch
RFC	Request for Comments
VSA	Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)

Nr.	Bezeichnung	Absatz
NCD.2.1.01	Cloud-Nutzungs-Strategie	a
NCD.2.1.01	Cloud-Nutzungs-Strategie	b
NCD.2.1.01	Cloud-Nutzungs-Strategie	c
NCD.2.1.01	Cloud-Nutzungs-Strategie	d
NCD.2.1.02	Sicherheitsrichtlinie externe Cloud-Dienste	a
NCD.2.1.02	Sicherheitsrichtlinie externe Cloud-Dienste	b
NCD.2.1.02	Sicherheitsrichtlinie externe Cloud-Dienste	c
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	a
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	b
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	c
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	d
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	e
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	f
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	g
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	h

NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	h i
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	h ii
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	h ii
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	i
NCD.2.1.03	Sicherheitskonzept für den externen Cloud-Dienst	i
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	a
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	a
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	a
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	b
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	b
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	c
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	c
NCD.2.1.04	Notfall- und Kontinuitätsmanagement	c
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	a

NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	b
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	c
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	d
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	d
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	e
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	f
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	g
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	h
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	h
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	i
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	i
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	i i
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	i i

NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	i ii
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	i ii
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	i ii
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	j
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	j i
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	j ii
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	j iii
NCD.2.2.01	Umsetzung der Sicherheitsanforderungen	j iv
NCD.2.2.02	Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	a
NCD.2.2.02	Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	b
NCD.2.2.02	Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	b i
NCD.2.2.02	Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	b ii

NCD.2.2.02	Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	c
NCD.2.2.02	Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern	d
NCD.2.2.03	Gerichtsbarkeit vertraglich zusichern	a
NCD.2.2.03	Gerichtsbarkeit vertraglich zusichern	b
NCD.2.2.03	Gerichtsbarkeit vertraglich zusichern	c
NCD.2.2.04	Lokation vertraglich zusichern	a
NCD.2.2.04	Lokation vertraglich zusichern	b
NCD.2.2.05	Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern	a
NCD.2.2.05	Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern	a i
NCD.2.2.05	Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern	a ii
NCD.2.2.06	Beendigung des Vertragsverhältnisses regeln	a
NCD.2.2.06	Beendigung des Vertragsverhältnisses regeln	a
NCD.2.2.06	Beendigung des Vertragsverhältnisses regeln	b
NCD.2.2.06	Beendigung des Vertragsverhältnisses regeln	b

NCD.2.2.07	Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern	a
NCD.2.2.07	Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern	a
NCD.2.2.07	Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern	b
NCD.2.2.07	Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern	b
NCD.2.3.01	ISMS einbinden	a
NCD.2.3.01	ISMS einbinden	a
NCD.2.3.01	ISMS einbinden	a
NCD.2.3.01	ISMS einbinden	b
NCD.2.3.01	ISMS einbinden	b
NCD.2.3.02	Sicherheitsnachweise prüfen	a
NCD.2.3.02	Sicherheitsnachweise prüfen	a i
NCD.2.3.02	Sicherheitsnachweise prüfen	a ii
NCD.2.3.02	Sicherheitsnachweise prüfen	b
NCD.2.3.03	Leistungsfähigkeit prüfen	a
NCD.2.3.03	Leistungsfähigkeit prüfen	b
NCD.2.3.03	Leistungsfähigkeit prüfen	c
NCD.2.3.04	Informationspflichten nachhalten	a

NCD.2.3.04	Informationspflichten nachhalten	b
NCD.2.3.04	Informationspflichten nachhalten	b
NCD.2.3.04	Informationspflichten nachhalten	b
NCD.2.3.05	Zwei-Faktor-Authentifizierungen aktivieren	a
NCD.2.3.05	Zwei-Faktor-Authentifizierungen aktivieren	b
NCD.2.4.01	Datenrückgabe durchführen	a
NCD.2.4.01	Datenrückgabe durchführen	a
NCD.2.4.01	Datenrückgabe durchführen	b
NCD.2.4.02	Datenlöschung bestätigen	a
NCD.2.4.02	Datenlöschung bestätigen	a
NCD.2.4.02	Datenlöschung bestätigen	b
NCD.2.4.02	Datenlöschung bestätigen	c
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	a
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	b
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	c
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	c i
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	c ii
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	d

NCD.2.5.01	Mitnutzung externer Cloud-Dienste	d i
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	d ii
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	e
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	e
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	e i
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	e ii
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	f
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	f i
NCD.2.5.01	Mitnutzung externer Cloud-Dienste	f ii

Sicherheitsanforderung (MST-NCD V20)
Die Einrichtung MUSS eine Cloud-Nutzungs-Strategie nach OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung erstellen.
Die Einrichtung MUSS in dieser Cloud-Nutzungs-Strategie festlegen, wie sie mit Risiken bei der Nutzung externer Cloud-Dienste umgeht. Hierzu muss eine Richtlinie zur Risikobewertung und -behandlung erstellt werden.
Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in ihrer Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist. Sie DARF den externen Cloud-Dienst NUR nutzen, wenn dieser die in der Cloud-Nutzungs-Strategie definierten Ziele, Chancen und Risiken angemessen unterstützt.
Die Einrichtung MUSS vor der Nutzung des externen Cloud-Dienstes eine Risikoanalyse gemäß der in NCD.2.1.01 b) festgelegten Richtlinie durchführen.
Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung erstellen.
Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.
Die Einrichtung MUSS - sofern betroffen - die zuständigen Datenschutz- und Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.
Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung erstellen.
Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.
Die Einrichtung MUSS - sofern betroffen - die zuständigen Datenschutz- und Geheimschutzbeauftragten, in jedem Fall aber den IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen.
Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.
Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesen Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.
Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen: − Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB − Kategorie 2 = personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO − Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA − Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)
Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und 3 gleichzeitig zuordnen.
Falls Daten den Kategorien 1, 2 oder 3 zugeordnet wurden: Die Einrichtung MUSS für die identifizierten dienstlichen Daten dieser Kategorien die Geheim- und Datenschutzaspekte sowie Anforderungen hinsichtlich Privat- und Dienstgeheimnisse ermitteln und aus diesen ggf. entstehende, weitere Anforderungen ableiten.

Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln und bewerten. Die Einrichtung MUSS die ermittelten Risiken gemäß den in der Cloud-Nutzungs-Strategie festgelegten Richtlinien zur Risikobewertung bewerten.
Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn alle ermittelten Risiken gemäß den in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobehandlung wirksam vermieden oder hinreichend reduziert oder in Übereinstimmung mit den Risikoakzeptanzkriterien bei der Cloud-Nutzung getragen werden können.
Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn alle ermittelten Risiken gemäß den in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobehandlung wirksam vermieden oder hinreichend reduziert oder in Übereinstimmung mit den Risikoakzeptanzkriterien bei der Cloud-Nutzung getragen werden können.
Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.
Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.
Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen und Krisensituationen einnehmen würde.
Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen und Krisensituationen einnehmen würde.
Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen und Krisensituationen einnehmen würde.
Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss.
Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss.
Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob sich die Cloud-Nutzung auf Maßnahmen, die Notfällen und Krisensituationen präventiv und/oder reaktiv entgegenwirken, auswirkt und inwiefern diese Maßnahmen ggf. anzupassen sind. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.
Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob sich die Cloud-Nutzung auf Maßnahmen, die Notfällen und Krisensituationen präventiv und/oder reaktiv entgegenwirken, auswirkt und inwiefern diese Maßnahmen ggf. anzupassen sind. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.
Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob sich die Cloud-Nutzung auf Maßnahmen, die Notfällen und Krisensituationen präventiv und/oder reaktiv entgegenwirken, auswirkt und inwiefern diese Maßnahmen ggf. anzupassen sind. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.
Die Einrichtung MUSS vor Vertragsabschluss bewerten, inwiefern der externe Cloud-Dienst die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) erfüllt.

Die Einrichtung MUSS die Erfüllung dieser Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.
Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5 verwendet werden.
Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.
Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.
Diese Sicherheitsnachweise SOLLTEN mindestens − die angemessene und wirksame Erfüllung der Basiskriterien nach C5 , − die aktuelle Dokumentation der Systembeschreibung , − die Aktualität von vertraglich zugesicherten Zertifizierungen und Berichterstattungen sowie − die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen umfassen und KÖNNEN vom Cloud-Diensteanbieter durch die regelmäßige Bereitstellung einer aktuellen C5-Berichterstattung vom Typ2 erbracht werden.
Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten und eventuellen Unklarheiten und insbesondere darin ausgewiesene Abweichungen in geeigneter Form nachgehen. Hierbei MUSS die Einrichtung auch abwägen, ob und inwiefern ein Risiko entsteht und wie mit diesem umzugehen ist.
Insbesondere MÜSSEN Zertifikate, Prüfberichte und Nachweise den Zeitraum, in dem die Einrichtung den Cloud-Dienst nutzt, jeweils vollständig abdecken und DÜRFEN KEINE zeitlichen Lücken enthalten oder entstehen lassen. Dies MUSS die Einrichtung in ihre Sicherheitsanforderungen sowie demzufolge in die Leistungsbeschreibung aufnehmen.
Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.
Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.
Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen, die vom Cloud-Diensteanbieter zu erfüllen sind, abdecken oder diese Risiken transferieren oder diese Risiken tragen.
Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen, die vom Cloud-Diensteanbieter zu erfüllen sind, abdecken oder diese Risiken transferieren oder diese Risiken tragen.
Die Einrichtung MUSS die weiteren Anforderungen nach NCD.2.1.03, Buchstabe i) in ihre Sicherheitsanforderungen aufnehmen. Soweit die Einrichtung diese weiteren Anforderungen nur gemeinsam mit dem Cloud-Diensteanbieter erfüllen kann, MUSS die Einrichtung diese in die Leistungsbeschreibung bzw. in das Vertragsverhältnis mit dem Cloud-Diensteanbieter aufnehmen.
Die Einrichtung MUSS die weiteren Anforderungen nach NCD.2.1.03, Buchstabe i) in ihre Sicherheitsanforderungen aufnehmen. Soweit die Einrichtung diese weiteren Anforderungen nur gemeinsam mit dem Cloud-Diensteanbieter erfüllen kann, MUSS die Einrichtung diese in die Leistungsbeschreibung bzw. in das Vertragsverhältnis mit dem Cloud-Diensteanbieter aufnehmen.

Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.
Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.
Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.
Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.
Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass die Einrichtung ihre weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) erfüllt.
Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang eine Bewertung des vom Cloud-Diensteanbieter für den betrachteten Cloud-Dienst gebotenen Informationssicherheitsniveaus ermöglichen und die Einrichtung selbst oder Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) die Prüfrechte wahrnehmen können.
Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS sich die Einrichtung vom Cloud-Diensteanbieter dazu berechtigen lassen, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.
Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) nicht entgegenstehen.
Die Einrichtung MUSS sich vom Cloud-Diensteanbieter vollständig benennen lassen, welche seiner Unterauftragnehmer gemäß C5 als Subdienstleistungsunternehmen anzusehen sind und auf welche Art und welchem Umfang er diese in die Bereitstellung des Cloud-Dienstes einbezieht.
Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass er der Einrichtung beabsichtigte Änderungen an vertraglichen Vereinbarungen mit Subdienstleistungsunternehmen, die in die Bereitstellung des Cloud-Dienstes involviert sind, unverzüglich schriftlich oder per E-Mail mitteilt.
Diese Mitteilung SOLLTE zeitlich vor Umsetzung der Änderung erfolgen.
Der Cloud-Diensteanbieter MUSS der Einrichtung insbesondere mitteilen, wenn er bestehende Vertragsverhältnisse beendet oder neue Vertragsverhältnisse mit Cloud-Diensteanbietern eingeht. Vertragsverhältnisse in diesem Sinne schließen alle mitgeltenden Dokumente und Regelungen, wie z. B. Leistungsscheine, Dienstgütevereinbarungen oder Allgemeine Geschäfts- und Einkaufsbedingungen ein.

Diese Mitteilungen KANN der Cloud-Diensteanbieter z. B. über Internetportale oder Push-Benachrichtigungen bereitstellen, wenn die Einrichtung diese Anforderungen als erfüllt ansieht.
Falls der Cloud-Diensteanbieter Subdienstleistungsunternehmen einbezieht oder anderweitig wesentliche Teile der Entwicklung oder Bereitstellung des Cloud-Dienstes an Unterauftragnehmer auslagert, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass − die Subdienstleistungsunternehmen und Unterauftragnehmer die zwischen der Einrichtung und dem Cloud-Diensteerbringer vertraglich festgelegten Vorgaben ebenfalls erfüllen und − sich die Prüfrechte, die der Cloud-Diensteerbringer der Einrichtung zugesichert hat, auch auf die Subdienstleistungsunternehmen und Unterauftragnehmer des Cloud-Diensteerbringers beziehen.
Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.
Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.
Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.
Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Hierzu MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und der Risikoanalyse, das mögliche Risiko eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) sowie weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) bewerten.
Die Einrichtung MUSS sämtliche Lokationen, an denen der Cloud-Diensteerbringer mit dem Cloud-Dienst dienstliche Daten speichert und verarbeitet, vertraglich festlegen. Dabei MUSS die Einrichtung auch Datensicherungen berücksichtigen, da diese ggf. an Drittlokationen durchgeführt werden.
Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.
Die Einrichtung MUSS beim Festlegen von Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf der mit dem Cloud-Dienst verarbeiteten dienstlichen Daten achten.
Beim Festlegen von Vertragsstrafen und Haftungsregelungen sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.
Die Einrichtung MUSS dem Anwendungsfall angemessene Kündigungsfristen festlegen.
Die Einrichtung MUSS dem Anwendungsfall angemessene Kündigungsfristen festlegen.
Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.
Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, wie dieser die mit dem Cloud-Dienst verarbeiteten dienstlichen Daten nach Beendigung der Nutzung an die Einrichtung übergibt (z. B. Fristen, Datenformat, Datenträger, Protokolle usw.).
Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, wie dieser die mit dem Cloud-Dienst verarbeiteten dienstlichen Daten nach Beendigung der Nutzung an die Einrichtung übergibt (z. B. Fristen, Datenformat, Datenträger, Protokolle usw.).
Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, welche Maßnahmen dieser zur Löschung der dienstlichen Daten durchführt. Dabei MUSS die Einrichtung sicherstellen, dass die Maßnahmen dem zuvor ermittelten Schutzbedarf entsprechen.
Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, welche Maßnahmen dieser zur Löschung der dienstlichen Daten durchführt. Dabei MUSS die Einrichtung sicherstellen, dass die Maßnahmen dem zuvor ermittelten Schutzbedarf entsprechen.
Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.
Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.
Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.
Die Einrichtung MUSS die in der C5-Berichterstattung genannten korrespondierenden Kontrollen für Cloud-Kunden in ihrem ISMS einrichten. Die Einrichtung SOLLTE darüber hinaus die im C5 beschriebenen korrespondierenden Kriterien für Kunden berücksichtigen.
Die Einrichtung MUSS die in der C5-Berichterstattung genannten korrespondierenden Kontrollen für Cloud-Kunden in ihrem ISMS einrichten. Die Einrichtung SOLLTE darüber hinaus die im C5 beschriebenen korrespondierenden Kriterien für Kunden berücksichtigen.
Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.
Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.
Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.
Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.
Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, vor dem Hintergrund der Nutzung des Cloud-Dienstes beurteilen.
Die Einrichtung MUSS ggf. auftretende Abweichungen bewerten und auf diese durch geeignete Anpassungen an der eigenen IT-Infrastruktur und Netzanbindung reagieren.
Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters und des Cloud-Dienstes sowie der Netzverbindung zum Cloud-Diensteanbieter beurteilen.
Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei i) einer Eingliederung des Cloud-Diensteanbieters in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihm, ii) einem Austausch von Unterauftragnehmern oder Dritten (siehe hierzu auch NCD.2.2.02).

Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und auf diese gemäß der vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.
Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und auf diese gemäß der vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.
Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und auf diese gemäß der vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.
Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung für Anmeldungen von Benutzern (Log-in) an, SOLLTE die Einrichtung diese nutzen.
Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung für Anmeldungen von Benutzern mit privilegierten Rechten (Log-in) wie bspw. Administratoren an, MUSS die Einrichtung diese nutzen.
Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle dienstlichen Daten in der vereinbarten Form zurück übergeben hat.
Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle dienstlichen Daten in der vereinbarten Form zurück übergeben hat.
Die Einrichtung MUSS die Übergabe dokumentieren.
Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gem. NCD.2.2.07 erfolgte Löschung aller dienstlichen Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen. Dies umfasst die Bestätigung, dass die dienstlichen Daten gemäß der vertraglich vereinbarten Verfahren gelöscht wurden.
Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gem. NCD.2.2.07 erfolgte Löschung aller dienstlichen Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen. Dies umfasst die Bestätigung, dass die dienstlichen Daten gemäß der vertraglich vereinbarten Verfahren gelöscht wurden.
Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern (z. B. Subdienstleistungsunternehmen) und anderen externen Dritten umfassen.
Die Einrichtung MUSS die durch den Cloud-Diensteanbieter bestätigte Datenlöschung dokumentieren.
Die Einrichtung MUSS sicherstellen, dass die Mitnutzung mit der eigenen Cloud-Strategie (siehe NCD.2.1.01) vereinbar ist.
Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstabe d) bis i) umsetzen und einhalten.
Die Einrichtung MUSS ermitteln, an welchen Lokationen mit dem externen Cloud-Dienst dienstliche Daten verarbeitet werden. Dies schließt auch Datensicherungen sowie, sofern gegeben, Unterauftragnehmer und Subdienstleister des Cloud-Diensteanbieters ein.
Die Einrichtung MUSS bewerten, ob die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.
Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung sowie, sofern gegeben, weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) heranziehen.
Die Einrichtung MUSS ermitteln, welche Rechte an den dienstlichen Daten dem Cloud-Diensteanbieter oder Dritten durch das Akzeptieren der vom Cloud-Diensteanbieter vorgegebenen Allgemeinen Geschäftsbedingungen (AGB), Datenschutzerklärung oder sonstigen Nutzungsbedingungen eingeräumt werden.

Die Einrichtung MUSS bewerten, ob diese Rechte mit den eigenen Sicherheitsanforderungen, die sie in der Sicherheitsrichtlinie und dem eigenen Sicherheitskonzept definiert hat, vereinbar sind.
Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.
Die Einrichtung MUSS bewerten, ob und wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt zu speichern sind. Für die anschließende Bewertung SOLLTE die Einrichtung die identifizierten Risiken mit der eigenen Cloud-Strategie (siehe NCD.2.1.01) abgleichen.
Die Einrichtung MUSS bewerten, ob und wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt zu speichern sind. Für die anschließende Bewertung SOLLTE die Einrichtung die identifizierten Risiken mit der eigenen Cloud-Strategie (siehe NCD.2.1.01) abgleichen.
Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.
Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.
Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.
Die Einrichtung MUSS bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.
Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.

IT-Grundschutz-Kompendium 2021
OPS.2.2.A1
OPS.2.2.A1
OPS.2.2.A1
OPS.2.2.A1
OPS.2.2.A2
OPS.2.2.A2
OPS.2.2.A2
OPS.2.2.A7
OPS.2.2.A7
OPS.2.2.A7
OPS.2.2.A7
OPS.2.2.A7
OPS.2.2.A7
OPS.2.2.A7
OPS.2.2.A7

OPS.2.2.A7
OPS.2.2.A1
OPS.2.2.A7
OPS.2.2.A7
ORP.5
OPS.2.2.A11
OPS.2.2.A15
OPS.2.2.A16
OPS.2.2.A11
OPS.2.2.A16
OPS.2.2.A11
OPS.2.2.A15
OPS.2.2.A16
OPS.2.2.A8

OPS.2.2.A8
OPS.2.2.A8
OPS.2.2.A9
OPS.2.2.A13
OPS.2.2.A13
OPS.2.2.A13
OPS.2.2.A13
OPS.2.2.A9
OPS.2.2.A13
OPS.2.2.A8
OPS.2.2.A9
OPS.2.2.A8
OPS.2.2.A9

OPS.2.2.A8
OPS.2.2.A9
OPS.2.2.A13
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9

OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A14
OPS.2.2.A9
OPS.2.2.A14

OPS.2.2.A9
OPS.2.2.A14
OPS.2.2.A9
OPS.2.2.A14
OPS.2.2.A7
OPS.2.2.A12
ISMS.1
OPS.2.2.A12
ISMS.1
OPS.2.2.A13
OPS.2.2.A13
OPS.2.2.A13
OPS.2.2.A13
OPS.2.2.A12
OPS.2.2.A12
OPS.2.2.A12
OPS.2.2.A12

DER.2.1
OPS.2.2.A4
OPS.2.2.A12
ORP.4.A21
ORP.4.A10
OPS.2.2.A14
OPS.2.2.A15
OPS.2.2.A14
OPS.2.2.A9
OPS.2.2.A14
OPS.2.2.A14
OPS.2.2.A14
OPS.2.2.A1
OPS.2.2
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A9
OPS.2.2.A8

OPS.2.2.A8
OPS.2.2.A8
OPS.2.2.A1
OPS.2.2.A17
OPS.2.2.A17
OPS.2.2.A17
OPS.2.2.A6
OPS.2.2.A6
SYS.3.2.2

Von:	GP Geschaeftszimmer_BL
An:	BSI VL Abteilungsleiter; GP Fachbereich BL 1; GP Fachbereich BL 2; GP Fachbereich BL 3; BSI VL ReferatsleiterBL
Cc:	GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_BL
Betreff:	[n.A.z.K.] [MST-NCD] Mindeststandard zur Nutzung externer Cloud-Dienste
Datum:	Montag, 19. Dezember 2022 15:47:44
Anlagen:	MST_NCD_Umsetzungshinweise_v2.1.pdf MST_NCD_v2.1.pdf Referenztabelle_NCD21_ITG2022.xlsx 20221219-Anschreiben Mindeststandard zur Nutzung externer Cloud-Dienste.pdf

---

Liebe Kolleginnen und Kollegen,

nachfolgende E-Mail n.A.z.K.

Vielen Dank und viele Grüße
Im Auftrag

[redacted]

Von: GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>
Gesendet: Montag, 19. Dezember 2022 15:45
An: BK <poststelle@bk.bund.de>; AA <poststelle@auswaertiges-amt.de>; BMI <poststelle@bmi.bund.de>; BMF <poststelle@bmf.bund.de>; poststelle@bmjv.bund.de; BMVg <poststelle@bmvg.bund.de>; BMWi <info@bmwi.bund.de>; BMAS <poststelle@bmas.bund.de>; poststelle@bmel.bund.de; BMFSFJ <poststelle@bmfsfj.bund.de>; poststelle@bmg.bund.de; poststelle@bmvi.bund.de; Maileingang BMU <Poststelle@bmu.bund.de>; [redacted]@bmbf.bund.de; poststelle@bmz.bund.de; [redacted]@bmwsb.bund.de; bverfg@bundesverfassungsgericht.de; poststelle@bpra.bund.de; bundesrat@bundesrat.de; Poststelle@brh.bund.de; [redacted]@bundestag.de; Poststelle@bkm.bund.de; Poststelle@bfdi.bund.de; [redacted]@itzbund.de; GP AG-InfoSic[redacted]@bsi.bund.de>
Cc: GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>
Betreff: [MST-NCD] Mindeststandard zur Nutzung externer Cloud-Dienste

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard zur Nutzung externer Cloud-Dienste Version 2.1 nach § 8 Absatz 1 Satz 1 BSIG. Die Referenztabelle zum Mindeststandard ebenso wie die Umsetzungshinweise sind der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189

53175 Bonn
Telefon: +49 (0)228 99 9582-[redacted]
Mobil: +49[redacted]
E-Mail: geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Umsetzungshinweise zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste 2.1

Version 2.1 vom 15.12.2022

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	20.06.2018	Erstveröffentlichung
2.0	03.02.2022	Anpassung an MST-Version 2.0
2.1	15.12.2022	Anpassung an MST-Version v2.1

Tabelle 1: Versionsgeschichte der Umsetzungshinweise zum Mindeststandard zur Nutzung externer Cloud-Dienste

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Allgemeine Umsetzungshinweise

Das vorliegende Dokument unterstützt IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[1] und IT-Betriebspersonal bei der Interpretation und Umsetzung des Mindeststandards (MST) des Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Nutzung externer Cloud-Dienste – Version 2.1 vom 15.12.2022[2].

Im ersten Kapitel dieses Dokumentes werden allgemeine Hinweise zur Umsetzung der Anforderungen des Mindeststandards gegeben. Dazu gehört die Erläuterung zentraler Begriffe sowie der Anwendungsbereiche dieses Mindeststandards. Nach Hinweisen zur Kategorisierung der mittels eines Cloud-Dienstes verarbeiteten Daten werden wesentliche Rahmendokumente für die Umsetzung dieses Mindeststandards beschrieben. Mit einem kurzen Überblick über den C5-Kriterienkatalog[3] endet das erste Kapitel.

Das zweite Kapitel dieses Dokumentes gibt Hinweise zur konkreten Umsetzung der Anforderungen des Mindeststandards und ist untergliedert nach den vier Phasen des Lebenszyklus einer Cloud-Nutzung. Dabei wird auch die Mitnutzung eines Cloud-Dienstes betrachtet, die zuvor in einem eigenen Mindeststandard behandelt wurde.[4]

1.1 Begriffsbestimmung und Abgrenzung

Für die korrekte Anwendung dieses Mindeststandards müssen Cloud-Dienste auch als solche klar identifiziert werden können. Oftmals sind die Grenzen zwischen einem Outsourcing von IT-Leistungen und dem Bezug von Cloud-Diensten fließend. Der Mindeststandard nutzt die Definition für Cloud-Dienste des C5[5], die sich an die internationale Begriffsdefinition des ISO 17788 anlehnt.[6] Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen („Cloud-Dienste“) erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der in diesem Rahmen angebotenen Cloud-Dienste umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Anwendungen.

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind Cloud-Dienste, die von Anbietern außerhalb der Verwaltung des Bundes erbracht werden.[7] Cloud-Dienste, die von IT-Dienstleistern des Bundes angeboten werden, gehören daher nicht dazu. Unabhängig von der Anwendung der Mindeststandards richten IT-Dienstleister des Bundes ihre IT-Angebote auf die Sicherheitsbedürfnisse der Bundesverwaltung aus.

---

[1] Analog „Informationssicherheitsbeauftragte (ISB)“

[2] MST NCD 2.1 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022a)

[3] Der Cloud Computing Compliance Criteria Catalogue – C5 (Kriterienkatalog Cloud Computing) liegt in zwei Ausgaben vor: der Ausgabe C5:2020 (Erscheinungsjahr 2020) und der Ausgabe C5:2016 (Erscheinungsjahr 2016). Sofern nicht anders angegeben, wird hier die Ausgabe C5:2020 referenziert.

[4] MST MCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)

[5] Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing) (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)

[6] Der Standard „ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary“ (International Organization for Standardization (ISO), 2014) definiert Cloud Computing als Paradigma für die Ermöglichung über ein Netz auf ein skalierbaren und elastischen Pool von geteilten virtuellen oder physischen Ressourcen (Server, Plattform, Anwendung, Software, etc.) zuzugreifen und über ein Selbst-Service Portal zu bestellen und selbst zu administrieren. Ein Cloud-Service ist als über eine definierte Schnittstelle buchbare und über Cloud Computing angebotene Fähigkeiten („capabilities“) definiert. Cloud-Fähigkeiten werden nach Infrastruktur, Plattform und Anwendung unterschieden.

[7] Hinweis: Private Cloud-Dienste der IT-Dienstleister des Bundes (z. B. Bundescloud) fallen somit nicht unter diese Bestimmung.

1.2 Anwendungsbereiche

Der Bedarf an sicheren Cloud-Diensten nimmt auch in der Bundesverwaltung stetig zu. Dabei können sich in der Praxis die Anwendungsbereiche stark unterscheiden. In Abhängigkeit vom Schutzbedarf der zu verarbeitenden Daten nimmt die Informationssicherheit eine zunehmend zentrale Rolle ein. Die Einforderung und Umsetzung von Sicherheitsanforderungen ist daher ein wichtiger Bestandteil bei der Inanspruchnahme von Cloud-Diensten.

Das BSI trägt diesem Bedarf Rechnung durch seinen aktuellen Mindeststandard zur Nutzung externer Cloud-Dienste 2.1 (s.o.), welcher aus den ursprünglichen Mindeststandards zur Nutzung[8] bzw. Mitnutzung[9] externer Cloud-Dienste hervorging. Der aktualisierte Mindeststandard umfasst somit zwei grundsätzliche Anwendungsbereiche: die Nutzung externer Cloud-Dienste sowie die Mitnutzung externer Cloud-Dienste.

1.2.1 Nutzung externer Cloud-Dienste

In dem ersten Anwendungsbereich hat die Einrichtung (Stelle des Bundes gemäß § 8 Absatz 1 BSIG) einen Bedarf an einer IT-Leistung, die nicht durch eigene IT-Ressourcen, sondern über einen externen Cloud-Dienst gedeckt werden soll. Hierbei handelt es sich letztendlich um eine sogenannte Make-or-Buy-Entscheidung der Einrichtung. Sofern sich die Einrichtung für die „Buy“-Option entscheidet, schließt diese mit einem Dienstleister (Cloud-Anbieter) einen Vertrag über die Erbringung der IT-Leistung ab. Die Einrichtung nimmt somit die Rolle des Auftraggebers ein. In diesem Anwendungsbereich finden die Regelungen des BSI zur Nutzung externer Cloud-Dienste Anwendung. Nach Einschätzung des BSI handelt es sich hierbei um den Regelfall bei der Inanspruchnahme externer Cloud-Dienste durch Einrichtungen.

1.2.2 Mitnutzung externer Cloud-Dienste

Der zweite Anwendungsbereich stellt einen Sonderfall dar, in dem IT-Anwender einer Einrichtung externe Cloud-Dienste zwar in Anspruch nehmen, jedoch ohne dass zwischen der Einrichtung und dem Cloud-Anbieter ein Vertragsverhältnis darüber besteht. Damit ist die Einrichtung nicht Auftraggeber des externen Cloud-Dienstes. Dieser Anwendungsbereich nimmt insbesondere in (internationalen) Projekten oder Arbeitsgruppen eine bedeutende Rolle ein. Die Sicherheitsanforderungen zur Nutzung externer Cloud-Dienste würden hier in einigen Bereichen zu weit greifen.

Trotz der unterschiedlichen Rahmenbedingungen haben beide Anwendungsbereiche auch Gemeinsamkeiten. Insofern gelten die in Kapitel 1 gemachten Aussagen für beide Anwendungsbereiche. Darauf aufbauend sind im weiteren Verlauf die Umsetzungshinweise zu den Sicherheitsanforderungen zur Nutzung (Kapitel 2.1 bis 0) und Mitnutzung (Kapitel 2.5) externer Cloud-Dienste aufgeführt.

1.2.3 Praxisbeispiele

Um die Differenzierung zwischen den beiden Anwendungsbereichen zu veranschaulichen, sind nachfolgend sechs unterschiedliche Praxisbeispiele aufgeführt. Dabei wird angegeben, in welchen Anwendungsbereich die Praxisbeispiele jeweils fallen bzw. ob der Mindeststandard überhaupt anzuwenden ist. Die jeweilige Begründung soll den Transfer in die Praxis erleichtern.

[8] MST CD 1.0 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017a)
[9] MST MCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)

Beispiel	Begründung
Eine Einrichtung hat sich gegen den Eigenbetrieb einer CRM-Software entschieden. Sie bezieht diese IT-Leistung als Cloud-Dienst über ein externes Wirtschaftsunternehmen. Mithilfe dieser Software verwaltet die Einrichtung u. a. Adressdaten von Außenkontakten.	Die Einrichtung hat mit dem Cloud-Anbieter einen Vertrag geschlossen und ist damit Auftraggeber des externen Cloud-Dienstes. Eine Verarbeitung von dienstlichen Daten erfolgt zumindest im Rahmen der Adressdatenverwaltung. Diese sind der Datenkategorie 2 – personenbezogene Daten gemäß Artikel 4 Nr. 1 DSGVO – zuzuordnen (siehe Kapitel 1.3).
Das IT-Referat einer Einrichtung bezieht skalierbaren Datenspeicher über einen externen Cloud-Anbieter. Der Datenspeicher wird genutzt, um kurzfristig auch große Datenmengen nicht eingestufter Informationen mit externen Partnern teilen zu können.	Auftraggeber ist das IT-Referat und somit die Einrichtung. Diese hat mit dem Cloud-Anbieter einen Vertrag geschlossen. Es ist zu klären, welche Daten künftig über den externen Cloud-Dienst verarbeitet werden dürfen (siehe Kapitel 1.3).

Tabelle 2: Anwendungsbereich: Nutzung externer Cloud-Dienste

Beispiel	Begründung
IT-Anwender eines Fachreferates sind eingeladen im Rahmen einer internationalen Arbeitsgruppe für den Austausch von Dokumenten eine Webplattform zu nutzen. Dieser Cloud-Dienst wird im Auftrag einer europäischen Institution von einem externen Cloud-Anbieter betrieben. Die IT-Anwender laden in diesem Zusammenhang Dokumente auf ihre dienstlichen Arbeitsplatzrechner herunter, bearbeiten diese dort mit einem Textverarbeitungsprogramm und stellen die neuen Versionen in den externen Cloud-Dienst ein. Weiterhin nutzen sie die Möglichkeit, an virtuellen Diskussionen teilzunehmen.	Auftraggeber des externen Cloud-Dienstes ist die europäische Institution. Die Einrichtung hat keinen Einfluss auf die Verträge und damit auch nicht auf Sicherheitsanforderungen die vom Cloud-Anbieter umzusetzen sind. Die Einrichtung muss daher bewerten, ob die eigenen Daten künftig in diesem externen Cloud-Dienst verarbeitet werden dürfen. Hierzu sind die Daten zunächst auf Basis der Datenkategorisierung zu bewerten. Zusammen mit den Ergebnissen aus der Risikoanalyse erfolgt nun ein Abgleich mit den vom Cloud-Anbieter umgesetzten Sicherheitsanforderungen nach Kapitel 2.5 des Mindeststandards. Danach erfolgt eine bewusste Entscheidung für oder gegen die Mitnutzung des externen Cloud-Dienstes.
Im Rahmen eines Forschungsprojektes arbeiten IT-Anwender aus einem Fachreferat einer Einrichtung mit einer internationalen Universität zusammen. Der dortige Lehrstuhl hat zur Berechnung komplexer geometrischer Forschungsdaten einen leistungsstarken virtuellen Server gemietet. Dieser wird von einem Wirtschaftsunternehmen in einer externen Cloud betrieben. Die IT-Anwender des Fachreferates können über einen Remote-Fernzugriff auf den virtuellen Server zugreifen und so die hohe Rechenleistung des virtuellen Servers nutzen. In diesem Zusammenhang werden auch wissenschaftliche Daten der Einrichtung verarbeitet.	Auftraggeber ist der Lehrstuhl der internationalen Universität. Die Einrichtung hat keinen Einfluss auf die Verträge und damit auch nicht auf die Sicherheitsanforderungen die vom Cloud-Anbieter umzusetzen sind. Auch hier muss die Einrichtung zunächst bewerten, ob die wissenschaftlichen Daten künftig in diesem externen Cloud-Dienst verarbeitet werden dürfen. Hierzu sind die eigenen wissenschaftlichen Daten zunächst auf Basis der Datenkategorisierung zu bewerten. Zusammen mit den Ergebnissen aus der Risikoanalyse erfolgt nun ein Abgleich mit den vom Cloud-Anbieter umgesetzten Sicherheitsanforderungen nach Kapitel 2.5 des Mindeststandards. Danach erfolgt eine bewusste Entscheidung für oder gegen die Mitnutzung des externen Cloud-Dienstes.

Tabelle 3: Anwendungsbereich: Mitnutzung externer Cloud-Dienste

Beispiel	Begründung
IT-Anwender der behördeneigenen Bibliothek greifen für Literaturrecherchen auch auf externe Datenbanken zu. Die Datenbanken werden als Webdienst angeboten und ausschließlich mit Inhalten und Daten des externen Anbieters befüllt. Der Dienst steht als lizenzpflichtiger Service zur Verfügung	Auf dem ersten Blick scheinen alle Voraussetzungen für die Anwendung des Mindeststandards zur Nutzung externer Cloud-Dienste erfüllt zu sein. So handelt es sich vermutlich um einen externen Cloud-Dienst, den die Einrichtung als Auftragnehmer nutzt. Jedoch zielen beide Anwendungsbereiche insbesondere darauf ab, für die Verarbeitung von (dienstlichen) Daten entsprechende Sicherheitsanforderungen zu setzen. Eine Verarbeitung dieser besonders schützenswerten Daten (siehe Kapitel 1.3) erfolgt aber bei sogenannten Such- und Recherchediensten oder auch Webdiensten mit Registrierungszwang grundsätzlich nicht. Die Prüfung und Umsetzung der Sicherheitsanforderungen aus den beiden Anwendungsbereichen würde in diesen Fällen zu weit greifen. Unabhängig davon sind solche Dienste trotzdem hinsichtlich ihrer Anforderungen zur Informationssicherheit zu überprüfen und zu bewerten. Sie sind jedoch nicht Regelungsgegenstand dieses Mindeststandards.
Das IT-Referat einer Einrichtung bezieht für ein Webprojekt einen Cloud-Dienst über das Informationstechnikzentrum Bund (ITZBund). Über die Nutzung des Cloud-Dienstes wurde ein entsprechendes Service Level Agreement (SLA) abgeschlossen.	Zwar ist die Einrichtung hier in der Rolle des Auftraggebers, jedoch handelt es sich beim ITZBund nicht um ein Unternehmen aus der Wirtschaft. Cloud-Angebote der IT-Dienstleister des Bundes sind daher nicht externe Cloud-Dienste im Sinne des Mindeststandards zur Nutzung externer Cloud-Dienste (siehe Kapitel 1.1). Der Mindeststandard finden in diesen Fällen daher keine Anwendung.

Tabelle 4: Anwendungsbereich: Keine Nutzung/Mitnutzung eines externen Cloud-Dienstes im Sinne dieses Mindeststandards

1.3 Datenkategorisierung

Ein wesentlicher Punkt auch hinsichtlich einer Risikoanalyse – wie sie in den Anforderungen NCD.2.1.01 und NCD.2.1.03 gefordert wird – ist die Bestimmung bzw. Bewertung der zu verarbeitenden Daten. So ist die Einforderung von Sicherheitsanforderungen insbesondere abhängig von den Daten, die in der externen Cloud verarbeitet werden sollen. Aus diesem Grund schreibt der Mindeststandard eine Datenkategorisierung vor. In diesem Zusammenhang wird ein Schema eingeführt, anhand dessen die Behörden die Ableitung notwendiger Sicherheitsanforderungen ermitteln können. In der nachfolgenden Tabelle sind die Datenkategorien mit Beschreibungen und Erläuterungen aufgeführt:

Datenkategorie	Erläuterung
Datenkategorie 1: Privat- und Dienst-, Betriebs- und Geschäftsgeheimnisse gemäß §§ 203 und 353b StGB	Hierunter fallen alle Daten, die durch das Strafgesetzbuch besonders geschützt sind. Daraus ergeben sich auch erhöhte Sicherheitsanforderungen an die Verarbeitung in einer externen Cloud. Hier reicht die Umsetzung der Basisanforderungen des C5[10] durch den Cloud-Anbieter allein in der Regel nicht aus. In diesem Zusammenhang ist daher zunächst zu prüfen, ob mit der Umsetzung der optionalen weitergehenden Anforderungen des C5 die Risiken ausreichend abgedeckt sind.
Datenkategorie 2: Personenbezogene Daten gemäß Artikel 4 Nummer 1 DSGVO (vormals § 3 Absatz 1 BDSG)	Nach der Datenschutz-Grundverordnung (DSGVO) sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (zur weiteren Konkretisierung siehe Artikel 4 DSGVO). Für den Schutz personenbezogener Daten ergeben sich daher ebenfalls erhöhte Sicherheitsanforderungen. Es ist deshalb zu prüfen, welche optionalen weitergehenden Anforderungen des C5 der Cloud-Anbieter zusätzlich umzusetzen hat. Es wird empfohlen in diesem Zusammenhang die behördlichen Datenschutzbeauftragten einzubinden.
Datenkategorie 3: Verschlusssachen gemäß allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA)[11]	Hierunter fallen Daten die nach der VSA eingestuft sind (VS - Nur für den Dienstgebrauch, VS - Vertraulich, Geheim, Streng Geheim). Es wird empfohlen in diesem Zusammenhang die zuständigen Geheimschutzbeauftragten einzubinden.
Datenkategorie 4: Sonstige Daten	Kategorie 4 ist eine sogenannte „Auffangkategorie". Hierunter sind alle Daten zu fassen, die nicht den Kategorien 1, 2 oder 3 zu zuordnen sind. Dabei handelt es sich im Regelfall um Daten, für die eine Umsetzung der Basisanforderungen nach C5 ausreichend ist.

Tabelle 5: Anwendungsbereich: Keine Nutzung/Mitnutzung eines externen Cloud-Dienstes im Sinne dieses Mindeststandards

1.4 Rahmendokumente

Der Mindeststandard setzt die Erstellung verschiedener Rahmendokumente voraus. Diese sind auch Bestandteil der Vorgehensweise nach IT-Grundschutz. Konkret wird das Thema Cloud Computing im Baustein OPS.2.2 des IT-Grundschutz-Kompendiums[12] behandelt. Weitere hilfreiche Quellen für die Umsetzung des Mindeststandards sind die Umsetzungshinweise zu OPS.2.2 zum IT-Grundschutz-

[10] Cloud Computing Compliance Criteria Catalogue – C5:2020. Kriterienkatalog Cloud Computing (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)
[11] VSA (Bundesministerium des Innern und für Heimat (BMI), 2018)
[12] IT-Grundschutz-Kompendium 2022 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022c)

Kompendium 2019[13], sowie die BSI-Veröffentlichung „Sichere Nutzung von Cloud-Diensten – Schritt für Schritt von der Strategie bis zum Vertragsende“[14]. Im Folgenden werden diese Quellen auszugsweise wiedergegeben. Über den IT-Grundschutz hinaus, stellt der Mindeststandard zusätzliche Anforderungen, welche in die genannten Rahmendokumente einfließen müssen (siehe Kapitel 2.1).

1.4.1 Strategie für die Cloud-Nutzung

Entscheidet sich eine Einrichtung für die Nutzung externer Cloud-Dienste, hat dies immer eine strategische Komponente, auch wenn der Umfang des Cloud-Dienstes gering ist. Letzteres kann dazu verleiten, die Konsequenzen dieses Outsourcings zu unterschätzen oder zu ignorieren, zumal es häufig der erste Fall von Outsourcing von IT-Dienstleistungen in einer Einrichtung ist. Im Rahmen der Erstellung einer Strategie für die Cloud-Nutzung sind wirtschaftliche, technische, organisatorische sowie sicherheitsrelevante Aspekte ausführlich zu betrachten.

Einbindung in die Institutionsstrategie

Der strategische Umgang der Einrichtung mit einer Cloud-Nutzung muss geregelt werden. Unter Berücksichtigung einer grundsätzlichen Entscheidung für die Nutzung von Cloud-Diensten ist zu ermitteln, in welchem Umfang klassische IT durch Cloud-Dienste abgelöst werden soll und welche Dienste dafür prinzipiell in Frage kommen.

Darüber hinaus ist festzulegen, welche Ziele die Einrichtung mit der Cloud-Nutzung erreichen möchte. Dies könnten beispielsweise sein: Kosteneinsparungen, flexiblerer Service, Ersatz bisheriger oder Einführung neuer Dienste.

Machbarkeitsstudie mit Zusammenstellung aller Rahmenbedingungen

Die Entscheidung zur Nutzung von Cloud-Diensten kann durch unterschiedliche externe Faktoren bedingt oder beeinflusst werden, wie

- rechtlichen Rahmenbedingungen (beispielsweise Vorgaben des Datenschutzes, von Aufsichtsbehörden oder von anderen Vertragspartnern),
- organisatorischen Rahmenbedingungen (beispielsweise Reife der Einrichtung hinsichtlich Organisation und IT) als auch
- technischen Anforderungen (beispielsweise Vorgaben bezüglich des benötigten Datennetzes, Leistungsfähigkeit der Internetanbindung, Verfügbarkeit der Datennetze und der IT-Systeme).

Die Ergebnisse dieser Untersuchung sind in einer Machbarkeitsstudie zu dokumentieren, welche die Eignung des untersuchten Cloud-Dienstes prüft.

Betriebswirtschaftliche Aspekte mit erster Kosten-Nutzen-Abschätzung

Da die Einführung von Cloud-Diensten oft der Kostenreduktion dient, steht die Relation von Kosten und Nutzen besonders im Fokus. Eine Kosten-Nutzen-Abschätzung gibt erste Hinweise auf die Wirtschaftlichkeit der Nutzung eines solchen Dienstes.

Neben den reinen Betriebskosten der Nutzung eines Cloud-Dienstes sind dabei auch die Kosten für die Migration, Schulung der Mitarbeitenden und des Administrationspersonals sowie gegebenenfalls für neue Hardware und den Ausbau der Netzkapazitäten zu berücksichtigen.

In die Kosten-Nutzen-Abschätzung sollte auch der strategische Wert der Ressourcen Know-how, Mitarbeitende, IT-Systeme und Anwendung eingehen. Durch die Nutzung eines Cloud-Dienstes könnten diese Ressourcen teilweise verloren gehen. Auf der Nutzenseite stehen beispielsweise Kostenersparnisse bei der Erneuerung obsoleter Hard- und Software, erhöhte Flexibilität der Leistungsfähigkeit der IT sowie

[13] Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)

[14] Sichere Nutzung von Cloud-Diensten (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016a)

möglicherweise Sicherheitsgewinne. Eine detailliertere Kosten-Nutzen-Analyse (siehe OPS.2.2.M8 *Sorgfältige Auswahl eines Cloud-Diensteanbieters*) kann erfolgen, sobald der Cloud-Dienst genauer definiert ist und erste konkrete Angebote einzelner Cloud-Diensteanbieter vorliegen.

Auswahl der Dienste und des Bereitstellungsmodells

Anhand der zuvor genannten strategischen Überlegungen sollte festgehalten werden, welche konkreten Dienste zukünftig von einem Cloud-Diensteanbieter bezogen werden könnten. Die Entscheidung für ein geeignetes Bereitstellungsmodell (beispielsweis Private, Public oder Hybrid Cloud) erfolgt basierend auf den erhobenen Anforderungen. Dies wird auch als „Sourcing" bezeichnet.

Berücksichtigung von Sicherheitsaspekten von Anfang an

Bereits zu Beginn der Planungsmaßnahmen zur Cloud-Nutzung müssen grundlegende technische und organisatorische Sicherheitsaspekte ausreichend berücksichtigt werden. Insbesondere ist zu klären, ob und inwieweit das Cloud Computing in der Sicherheitsleitlinie behandelt wird. Folgender Cloud-Spezifika sollten sich die Verantwortlichen einer Einrichtung dabei bewusstmachen:

- Abhängig vom Cloud-Nutzungsmodell kann der Cloud-Dienstleister auf die Daten der beauftragenden Einrichtung zugreifen. Dies kann auch Daten mit erhöhtem Schutzbedarf betreffen.
- Zwischen der beauftragenden Einrichtung und dem Cloud-Dienstleister werden kontinuierlich Daten übertragen. Daraus erhöht sich das Gefahrenpotential, welches durch die Einrichtung zu ermitteln und zu bewerten ist.
- Mit der Einführung der Nutzung von Cloud-Diensten werden neue Prozesse und Arbeitsabläufe erforderlich. Diese müssen entworfen, eingeführt und umgesetzt werden. Die Folgen der dafür notwendigen Umstellungen müssen ermittelt und abgeschätzt werden.

Im Rahmen eines Einführungsvorhabens von Cloud-Diensten sollten alle Vor- und Nachteile mit Bezug zur Informationssicherheit durch die Einrichtung betrachtet, bewertet und dokumentiert werden.

Durchführung einer Risikoanalyse

Es muss seine Risikoanalyse nach BSI-Standard 200-3[15] durchgeführt werden. Weitere Informationen sind unter NCD.2.1.01, Buchstabe d) zu finden.

Erstellung einer Roadmap

Nach der Untersuchung strategischer und sicherheitsrelevanter Aspekte steht die Planung der Realisierung der gewünschten Cloud-Dienste im Fokus. Im Falle mehrerer Dienste hat sich die Erstellung einer Cloud-Roadmap bewährt. Dieser Fahrplan zur Einführung der Cloud-Dienste beschreibt anhand eines Phasenmodells den konkreten Roll-Out der Dienste. Ziel ist dabei die Erhöhung der Nutzendenakzeptanz bei gleichzeitiger Risikominimierung technischer Probleme bei der Umsetzung.

1.4.2 Sicherheitsrichtlinie für die Nutzung externer Cloud-Dienste

In einer Sicherheitsrichtlinie werden die Schutzziele und die allgemeinen Sicherheitsanforderungen einer Einrichtung formuliert. Sofern die Strategie für die Cloud-Nutzung bereits Sicherheitsvorgaben für die Nutzung externer Cloud-Dienste enthält, müssen diese in der Sicherheitsrichtlinie weiter ausgearbeitet werden. Dies dient auch als Entscheidungsgrundlage für die Auswahl geeigneter Cloud-Dienste und Diensteanbieter.

In diesem Zusammenhang müssen grundsätzlich alle Sicherheitsanforderungen betrachtet werden, die sich aus den organisatorischen, technischen und rechtlichen Rahmenbedingungen sowie den ermittelten Schnittstellen ergeben. Dies betrifft neben Sicherheitsanforderungen an die verwendete Technik inklusive der benötigten Kommunikationswege und -dienste beispielsweise auch Datenschutzaspekte. In der

[15] BSI-Standard 200-3 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017b)

Sicherheitsrichtlinie sollten außerdem auch organisatorische Aspekte, wie erforderliche Schulungsmaßnahmen für das Administrationspersonal und die Nutzenden, beachtet werden.

Weitere wesentliche Aspekte sind:

- Sicherheitsanforderungen an den Cloud-Dienstanbieter (beispielsweise die Einhaltung des Vier-Augen-Prinzips bei der Administration),
- Sicherheitsanforderungen in Abhängigkeit vom Bereitstellungsmodell (beispielsweise Zutritts- und Zugangsrechte für den Dienstleister beim Betrieb einer Private Cloud On-Premise),
- Sicherheitsanforderungen aus relevanten Gesetzen und Vorschriften (beispielsweise gesetzliche Bestimmungen bei international agierenden Dienstleistern).

1.4.3 Sicherheitskonzept für den externen Cloud-Dienst

Bei Verwendung von Cloud-Diensten muss für jeden verwendeten Cloud-Dienst ein Sicherheitskonzept basierend auf der IT-Grundschutz-Vorgehensweise erstellt werden. Grundlage des Dokumentes sind die Anforderungen, welche sich aus der Sicherheitsrichtlinie zur Cloud-Nutzung für einen konkreten Anwendungsfall ableiten lassen. Weiter werden die im Zusammenhang mit der Nutzung von Cloud-Diensten notwendigen Sicherheitsmaßnahmen im Sicherheitskonzept dokumentiert. Als Orientierung für die Erstellung des Sicherheitskonzeptes dienen dabei die Sicherheitsanforderungen an einen klassischen IT-Dienst.

In einem Sicherheitskonzept für die Cloud-Nutzung sollte darüber hinaus die durch die Nutzung von Cloud-Diensten entstehende besondere Gefährdungslage beschrieben werden. Insbesondere folgende Aspekte sollten dabei betrachtet werden:

- Ungeplante vorzeitige Vertragsbeendigung,
- mangelnde Portabilität von Daten (Software as a Service), Anwendungen (Platform as a Service) oder IT-Systemen (Infrastructure as a Service),
- generelle Abhängigkeit vom Cloud-Diensteanbieter mangels Wechselmöglichkeit (Vendor Lock-in),
- Gefährdung der Integrität von Informationen durch proprietäre Datenformate,
- gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Kunden (multi tenancy),
- Unkenntnis über den Speicherort der Informationen,
- hohe Mobilität der Informationen sowie
- unbefugter Zugriff auf Informationen beispielsweise durch Administrationspersonal des Cloud-Dienstanbieters oder andere Parteien.

Aus den erkannten spezifischen Gefährdungen für den jeweiligen Cloud-Dienst müssen konkrete Sicherheitsanforderungen abgeleitet werden. Deren Einhaltung sollte im Rahmen der Vertragsgestaltung mit dem Cloud-Dienstanbieter verbindlich vereinbart werden. Insbesondere die folgenden Punkte sollten dabei betrachtet werden:

- Vorgaben zur sicheren Administration des Cloud-Dienstes,
- Vorgaben zu Betriebsprozessen und Prozessen im Sicherheitsmanagement,
- Regelungen zur Überwachung der Service-Erbringung und zum Berichtswesen,
- Verschlüsselung der Informationen,
- Vergabe und Entzug von Berechtigungen sowie
- Durchführung von Datensicherungen, sowohl durch den Cloud-Diensteanbieter als auch durch die Einrichtung.

Das Sicherheitskonzept des Cloud-Diensteanbieter sollte regelmäßig durch unabhängige Dritte auf Aktualität sowie vollständige und korrekte Umsetzung überprüft werden.

1.5 Der C5-Kriterienkatalog des BSI

Ein wesentliches Dokument für diesen Mindeststandard ist der „Cloud Computing Compliance Criteria Catalogue – C5:2020“[16] des BSI (C5). Der C5 ist ein Kriterienkatalog und beschreibt Mindestanforderungen an die Informationssicherheit für Cloud-Dienste, die nicht unterschritten werden sollten. Ziel ist die transparente Darstellung der Informationssicherheit eines Cloud-Dienstes auf Basis einer standardisierten Prüfung. Diese kann von Kunden im Rahmen einer eigenen Risikoanalyse verwendet werden. Es obliegt also dem Kunden, das vorliegende Sicherheitsniveau in Relation zum eigenen Schutzbedarf zu bewerten. Der Kriterienkatalog wird von Cloud-Anbietern, Auditoren und Cloud-Kunden verwendet. Jede dieser Parteien hat eine Mitwirkungspflicht hinsichtlich der Informationssicherheit.

Cloud-Anbieter können die C5-Kriterien umsetzen, um die IT-Sicherheit ihrer Cloud-Dienste zu erhöhen und sich damit einen attraktiven Wettbewerbsvorteil zu verschaffen. Die Erfüllung der Kriterien kann beispielsweise durch Wirtschafts- oder andere geeignete Prüfer testiert und somit gegenüber Kunden nachgewiesen werden. Diese Prüfer werden in diesem Fall direkt vom Cloud-Anbieter beauftragt.

Die Verwendung von Cloud-Diensten bietet Chancen, birgt aber auch Risiken, sodass ein eigenes Risikomanagement durch jeden Kunden unerlässlich ist. Der Kunde ist auch in der Verantwortung zu prüfen, ob die Mindestkriterien für seinen konkreten Anwendungsfall durch weitergehende Kriterien ergänzt werden müssen. Verbleibende Restrisiken müssen durch den Kunden getragen und im Eintrittsfall verantwortet werden. Der C5 unterstützt den Kunden dabei, Transparenz hinsichtlich der Aufteilung sicherheitskritischer Aufgaben zwischen Cloud-Anbieter und -Kunden zu erhalten.

Die Kriterien des C5 sind untergliedert in 17 Bereiche, denen jeweils eine Zielsetzung zugewiesen ist, welche durch die Kriterien erreicht werden soll. Für einige C5-Kriterien bestehen korrespondierende Kriterien für Kunden, die aufzeigen sollen, wo potentiell Mitwirkungspflichten bestehen. Die Kunden müssen den Mitwirkungspflichten in ihrem Verantwortungsbereich nachkommen.

[16] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)

2 Umsetzungshinweise zu den Sicherheitsanforderungen

Der Mindeststandard führt einen Prozess ein, mit dem sich Risiken der externen Cloud-Nutzung zuverlässig identifizieren, bewerten und behandeln lassen. Damit bleiben diese für die Behörde als Cloud-Kunde beherrschbar. Hierfür werden die Phasen Planung, Beschaffung, Einsatz und Beendigung externer Cloud-Dienste betrachtet. Für jede Phase werden entsprechende Sicherheitsanforderungen zur Gewährleistung der Informationssicherheit aufgestellt.

Die Sicherheitsanforderungen sind bereits in existierenden Standards, Normen und Regelungen als relevant identifiziert worden und sind daher den Cloud-Anbietern schon bekannt. Eine ganz zentrale Bedeutung bei der Bewertung externer Cloud-Dienste nimmt der C5-Kriterienkatalog zum Cloud Computing ein (siehe Kapitel 1.5). Er adressiert vorrangig Cloud-Anbieter und definiert Basisanforderungen für die Informationssicherheit, die aus Sicht des BSI nicht unterschritten werden sollten. Die Kompatibilität der Basisanforderungen zu international anerkannten Standards stellt dabei die Akzeptanz und Praktikabilität der Umsetzung und Einhaltung auf Seiten der Cloud-Anbieter sicher.

Zentrale Forderung des Mindeststandards ist daher, dass Einrichtungen bei einer Nutzung externer Cloud-Dienste von ihren externen Cloud-Anbietern mindestens die Umsetzung der Basisanforderungen des C5 fordern.

Neben Basisanforderungen an die Informationssicherheit von Cloud-Diensten sind jedoch auch Rahmenbedingungen, unter denen der Cloud-Dienst erbracht wird, für die sichere Nutzung relevant. Bei der Entscheidung, einen Cloud-Dienst zu nutzen, benötigt die Einrichtung Transparenz über die Rahmenbedingungen. Durch diese Transparenz wird die Einrichtung erst in die Lage versetzt, ein Cloud-Angebot hinsichtlich ihrer eigenen Anforderungen an die Informationssicherheit beurteilen zu können. Der C5 folgt diesem Ansatz mit den sogenannten Rahmenbedingungen. Die Transparenzanforderungen erfragen relevante Angaben über die Diensterbringung, wie z. B. die Lokation der Daten oder welche Funktionen an Unterauftragnehmer ausgelagert sind.

Ob die vom Cloud-Anbieter getroffenen Maßnahmen zur Umsetzung der Basisanforderungen angemessen und wirksam sind, wird im Rahmen von transparenten Prüfungen durch ein Prüfteam mindestens jährlich validiert.[17] Der C5 stellt für seine Prüfung Anforderungen an Prüfteam, Audit und Prüfbericht. So wie die Anforderungen an die Informationssicherheit basieren auch die Anforderungen an Prüfteam, Audit und Prüfbericht auf etablierten internationalen Prüfungsstandards.[18]

Der Mindeststandard greift die Themenkomplexe Informationssicherheit, Transparenz der Cloud-Diensterbringung und Nachweis über diese Aspekte durch geeignete Prüfungen auf. Rahmenbedingungen für die Cloud-Diensterbringung werden konkretisiert. Zudem wird vorgegeben, wie die Prüfnachweise des Cloud-Anbieters für das Informationssicherheitsmanagement der jeweiligen Einrichtung genutzt werden sollen. Daneben bleibt die Verantwortung für die IT-Objekte, welche die Einrichtung im Rahmen ihrer IT-Grundschutz-Konzeption innehat, unberührt und wird durch die Nutzung externer Cloud-Dienste lediglich angepasst.

Nachfolgend sind die Sicherheitsanforderungen mit entsprechenden Umsetzungshinweisen gegliedert nach den Phasen Planung (Kapitel 2.1), Beschaffung (Kapitel 2.2), Einsatz (Kapitel 2.3) und Beendigung (Kapitel 2.4) dargestellt.

[17] Die Prüfung beauftragt der jeweilige Cloud-Anbieter. Dieser kann dann den Prüfbericht seinen Kunden zur Verfügung stellen.

[18] Siehe hierzu auch https://www.bsi.bund.de/c5

2.1 Planungsphase

Der Lebenszyklus der Nutzung eines Cloud-Dienstes beginnt mit der Planung der Nutzung und den dafür erforderlichen Vorarbeiten bzw. Überlegungen.

NCD.2.1.01 Strategie für die Cloud-Nutzung

a) Die Einrichtung MUSS eine Strategie für die Cloud-Nutzung nach OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung[19] erstellen.

b) Die Einrichtung MUSS in dieser Strategie für die Cloud-Nutzung festlegen, wie sie mit Risiken bei der Nutzung externer Cloud-Dienste umgeht. Hierzu MUSS eine Richtlinie zur Risikoanalyse erstellt werden.[20]

c) Die Einrichtung MUSS prüfen, ob ein externer Cloud-Dienst grundsätzlich mit den in ihrer Strategie für die Cloud-Nutzung definierten Zielen, Chancen und Risiken vereinbar ist.[21] Die Einrichtung DARF einen externen Cloud-Dienst NUR nutzen, wenn dieser die in der Strategie für die Cloud-Nutzung definierten Ziele, Chancen und Risiken angemessen unterstützt.

d) Die Einrichtung MUSS vor der Nutzung eines externen Cloud-Dienstes eine Risikoanalyse gemäß der in NCD.2.1.01 b) festgelegten Richtlinie durchführen.

Zu a): Die Umsetzungshinweise zum IT-Grundschutz-Kompendium der Edition 2019 nennen in der Maßnahme OPS.2.2.M1 *Erstellung einer Cloud-Nutzungs-Strategie* wichtige Gesichtspunkte, welche in einer Strategie für die Cloud-Nutzung betrachtet und dokumentiert werden sollten.[22]

Zu b): Das Verfahren zur Erstellung einer Richtlinie wird im BSI-Standard 200-3 behandelt.

Zu d): Der Schutz der zu verarbeitenden Daten nimmt sowohl bei Nutzung, als auch bei Mitnutzung externer Cloud-Dienste eine entscheidende Rolle ein. Aus diesem Grund wird eine Risikoanalyse gefordert. Die Ergebnisse sind für das weitere Beschaffungs- und Einsatzverfahren maßgeblich. Für den Mindeststandard gilt daher, dass die Risikoanalyse nach BSI-Standard 200-3 zu erfolgen hat. Die ermittelten Risiken für die Daten müssen betrachtet und bewertet werden. Für die Risikoanalyse sind insbesondere die aktuellen Veröffentlichungen des BSI zur Cloud-Sicherheit heranzuziehen. Um identifizierten Risiken entgegenwirken, können auch zusätzliche Maßnahmen auf Seite der Behörde erforderlich sein.

NCD.2.1.02 Sicherheitsrichtlinie für externe Cloud-Dienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung[23] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Cloud Computing Compliance Criteria

[19] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022c), OPS.2.2 *Cloud-Nutzung*

[20] Siehe BSI-Standard 200-3, (BSI 2017b), S. 9f.

[21] Hinweis: OPS.2.2.A1 *Erstellung einer Strategie für die Cloud-Nutzung* sieht die Erstellung einer Strategie für die Cloud-Nutzung vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Strategie für die Cloud-Nutzung nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.

[22] Umsetzungshinweise IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)

[23] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022c), OPS.2.2 *Cloud-Nutzung*

Catalogue – C5 (Kriterienkatalog Cloud Computing) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[24]

c) Die Einrichtung MUSS die IT-Sicherheitsbeauftragten bei der Erstellung der Sicherheitsrichtlinie beteiligen und ebenfalls – sofern betroffen – die zuständigen Datenschutz- und Geheimschutzbeauftragten.

Zu a): Die Umsetzungshinweise zum IT-Grundschutz-Kompendium der Edition 2019 nennen in der Maßnahme OPS.2.2.M2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung* wichtige Aspekte, welche in die Sicherheitsrichtlinie für die Cloud-Nutzung eingehen sollten.[25]

Zu b): Die Basiskriterien nach dem C5 spiegeln aus Sicht des BSI das Niveau an Informationssicherheit wider, das ein Cloud-Dienst mindestens bieten muss, wenn Cloud-Kunden mit diesem Informationen verarbeiten, die einen normalen Schutzbedarf haben. Die Basiskriterien bilden den Mindestumfang einer Prüfung nach dem C5 ab. Nichtsdestotrotz obliegt es den Cloud-Kunden, für ihren individuellen Anwendungsfall zu bewerten, inwiefern die Basiskriterien den Schutzbedarf ihrer Informationen angemessen reflektieren. Für Cloud-Kunden, deren Informationen einen höheren Schutzbedarf haben, können die Zusatzkriterien einen Ausgangs- bzw. Ansatzpunkt darstellen, um diese Bewertung vorzunehmen.[26]

NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[27]

c) Die Einrichtung MUSS die IT-Sicherheitsbeauftragten bei der Erstellung des Sicherheitskonzeptes beteiligen und ebenfalls – sofern betroffen – die zuständigen Datenschutz- und Geheimschutzbeauftragten.

d) Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesen Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

f) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

– Kategorie 1 = Privat- und Dienst-, Betriebs- und Geschäftsgeheimnisse gemäß Strafgesetzbuch (StGB) §§ 203 und 353b

– Kategorie 2 = personenbezogene Daten gemäß Datenschutzgrundverordnung (DSGVO) Art. 4 Nr. 1

[24] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a)
[25] Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)
[26] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), S. 15
[27] Siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud

– Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[28]

– Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

g) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und 3 gleichzeitig zuordnen.

h) Falls Daten den Kategorien 1, 2 oder 3 zugeordnet wurden: Die Einrichtung MUSS für die identifizierten dienstlichen Daten dieser Kategorien die Geheim- und Datenschutzaspekte[29] sowie Anforderungen hinsichtlich Privat-, Dienst-, Betriebs- und Geschäftsgeheimnisse ermitteln und aus diesen ggf. entstehende, weitere Anforderungen ableiten.

i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln und bewerten.[30] Die Einrichtung MUSS die ermittelten Risiken gemäß den in der Strategie für die Cloud-Nutzung festgelegten Richtlinien zur Risikoanalyse bewerten.

ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn alle ermittelten Risiken gemäß den in der Strategie für die Cloud-Nutzung genannten Richtlinien zur Risikoanalyse wirksam vermieden oder hinreichend reduziert oder in Übereinstimmung mit den Risikoakzeptanzkriterien bei der Cloud-Nutzung getragen werden können.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen)[31] unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

Zu a): Ein Sicherheitskonzept für Cloud-Dienste unterscheidet sich oft nur wenig von Sicherheitskonzepten für Informationsverbünde, die durch die Einrichtung selbst betrieben werden. Die Umsetzungshinweise zum IT-Grundschutz-Kompendium der Edition 2019 nennen in der Maßnahme OPS.2.2.M7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* Besonderheiten, welche dabei berücksichtigt werden sollten.[32]

Zu d): Das Vorgehen zur Datenkategorisierung wurde bereits in Kapitel 1.3 ausführlich erläutert.

[28] VSA (Bundesministerium des Innern und für Heimat (BMI), 2018)

[29] Hinsichtlich der Datenschutzaspekte siehe insbesondere Orientierungshilfe – Cloud Computing (Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, 2014)

[30] Hinweis: Es gilt, zu bewerten, inwiefern die mit dem betrachteten Cloud-Dienst im beabsichtigten Anwendungsfall verbundenen rechtlichen, technischen und organisatorischen Risiken mit der Strategie für die Cloud-Nutzung vereinbar sind.

[31] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (Bundesministerium des Innern (BMI), 2014)

[32] Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)

2.2 Beschaffungsphase

Die Beschaffungsphase eines Cloud-Dienstes baut auf der Planungsphase und den darin erarbeiteten Strategien und Konzepten auf. Hinsichtlich der Beschaffung externer Cloud-Dienste sollte die Einrichtung insbesondere die einschlägigen „Ergänzenden Vertragsbedingungen für Cloudleistungen (EVB-IT Cloud)“[33] beachten und nutzen.

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss bewerten, inwiefern der externe Cloud-Dienst die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) erfüllt.[34]

b) Die Einrichtung MUSS die Erfüllung dieser Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5[35] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN mindestens

– die angemessene und wirksame Erfüllung der Basiskriterien nach C5[36],

– die aktuelle Dokumentation der Systembeschreibung[37],

– die Aktualität von vertraglich zugesicherten Zertifizierungen und Berichterstattungen sowie

– die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

[33] Vgl. EVB-IT Cloud, https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html

[34] Hinweis: Liegt ein C5-Prüfbericht vor, können diesem Informationen entnommen und der Bewertung zugrunde gelegt werden.

[35] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, die dabei unterstützt, einen C5-Prüfbericht systematisch auszuwerten. Diese Auswertung beinhaltet, die Sicherheitsmaßnahmen (Kontrollen) des Cloud-Diensteanbieters inklusive der zugehörigen Prüfergebnisse sowie der auf Cloud-Nutzerseite einzurichtenden Kontrollen aufzunehmen. In Verbindung mit den aufseiten der Einrichtung eingerichteten Kontrollen sowie weiterer, vom individuellen Anwendungsfall abhängenden Informationen lassen sich die mit der Nutzung des betrachteten Cloud-Dienstes verbundenen Risiken identifizieren und bewerten. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“ (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020b).

[36] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[37] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), Kapitel 3.4.3.2, S. 23f.) enthält der Bericht keine vom Cloud-Diensteanbieter angefertigte Systembeschreibung, sondern eine vom Prüfer im Rahmen der Prüfung angefertigte Systembeschreibung.

umfassen und KÖNNEN vom Cloud-Diensteanbieter durch die regelmäßige Bereitstellung einer aktuellen C5-Berichterstattung vom Typ2 erbracht werden.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten und eventuellen Unklarheiten und insbesondere darin ausgewiesene Abweichungen in geeigneter Form nachgehen. Hierbei MUSS die Einrichtung auch abwägen, ob und inwiefern ein Risiko entsteht und wie mit diesem umzugehen ist.

g) Insbesondere MÜSSEN Zertifikate, Prüfberichte und Nachweise den Zeitraum, in dem die Einrichtung den Cloud-Dienst nutzt, jeweils vollständig abdecken und DÜRFEN KEINE zeitlichen Lücken enthalten oder entstehen lassen. Dies MUSS die Einrichtung in ihre Sicherheitsanforderungen sowie demzufolge in die Leistungsbeschreibung aufnehmen.

h) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

i) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen, die vom Cloud-Diensteanbieter zu erfüllen sind, abdecken oder diese Risiken transferieren oder akzeptieren, und MUSS dies entsprechend dokumentieren.

> *i) Die Einrichtung MUSS die weiteren Anforderungen nach NCD.2.1.03, Buchstabe i) in ihre Sicherheitsanforderungen aufnehmen. Soweit die Einrichtung diese weiteren Anforderungen nur gemeinsam mit dem Cloud-Diensteanbieter erfüllen kann, MUSS die Einrichtung diese in die Leistungsbeschreibung bzw. in das Vertragsverhältnis mit dem Cloud-Diensteanbieter aufnehmen.*
>
> *ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.*

j) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

> *i) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass die Einrichtung ihre weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) erfüllt.*
>
> *ii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang eine Bewertung des vom Cloud-Diensteanbieter für den betrachteten Cloud-Dienst gebotenen Informationssicherheitsniveaus ermöglichen und die Einrichtung selbst oder Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revision oder Wirtschaftsprüfende) die Prüfrechte wahrnehmen können.*
>
> *iii) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS sich die Einrichtung vom Cloud-Diensteanbieter dazu berechtigen lassen, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.*
>
> *iv) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) nicht entgegenstehen.*

Zu e): Die Basisanforderungen nach C5 bestehen aus 114 Anforderungen, die sich in 17 Themengebiete gliedern. Damit setzen sie die untere Schwelle der Informationssicherheit, die aus Sicht des BSI nicht unterschritten werden sollte. Weiter soll sichergestellt werden, dass vertraglich zugesicherte Zertifizierungen und Berichterstattungen aktuell sind sowie Datensicherungskonzepte in der Praxis regelmäßig getestet und erprobt werden. Der C5 gibt hinsichtlich Prüfung und Berichterstattung entsprechende Regelungen vor (siehe C5, Kapitel 3.2 - 3.4). Der Prüfbericht muss der Einrichtung zugänglich gemacht werden, damit diese die Umsetzung prüfen kann. Verfügt ein Cloud-Anbieter über kein Testat oder kann dieser keinen Prüfbericht nach C5 vorlegen, können auch andere Nachweise genutzt werden, um die Umsetzung der geforderten Sicherheitsanforderungen nachzuweisen. Diese Ausnahmen sind aber besonders zu begründen. Die Gleichwertigkeit ist durch den Cloud-Anbieter nachzuweisen. Das BSI berät auch hier auf Anfrage.

Zu f): Ist der Cloud-Anbieter vertraglich verpflichtet Nachweise zu erbringen (siehe Buchstabe d)), muss die Einrichtung festlegen, wie diese intern geprüft und ausgewertet werden können.

Zu g): Bei der Prüfung ist insbesondere darauf zu achten, dass die vorgelegten Nachweise den gesamten Cloud-Dienst und Nutzungszeitraum abdecken.

Zu h): In diesem Zusammenhang soll geregelt werden, was nicht durch den Prüfbericht abgedeckt werden kann. Dies können z. B. zusätzlich geforderte regelmäßige Penetrationstests durch externe Sicherheitsanbieter sein. Diese Regelungen sind optional und auf den Anwendungsfall abzustimmen.

Die hier thematisierten Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen werden von dem Cloud-Diensteanbieter selbst beauftragt. Im Gegensatz hierzu werden die Prüfungen unter j) von der Einrichtung selbst beauftragt oder durchgeführt.

Zu j): Prüfrechte nehmen bei der Inanspruchnahme von Cloud-Diensten eine wichtige Funktion ein. Sie sind insbesondere dann relevant, wenn Daten der Kategorien 1 oder 3 in der Cloud verarbeitet werden sollen. Die vertraglich zugesicherten Prüfrechte nimmt die Einrichtung insbesondere dann wahr, wenn Zweifel an der korrekten Umsetzung der vereinbarten Sicherheitsanforderungen bestehen. Mit der Prüfung kann die Einrichtung auch einen Dritten – z. B. ein Wirtschaftsprüfungsunternehmen, das Testierungen nach C5 vornimmt – beauftragen. Das Ergebnis der Überprüfung ist zu dokumentieren.

Auf den Anwendungsfall bezogen ist zu bewerten, ob eigene Prüfrechte erforderlich sind und wie diese auszugestalten sind. In begründeten Ausnahmefällen kann auf eigene Prüfrechte verzichtet werden.

Kann der Cloud-Anbieter den geforderten Prüfbericht nach C5 oder gleichwertige Nachweise nicht vorlegen (siehe NCD.2.2.01, Buchstabe i), ii)), soll dies nicht zwingend zu einem Ausschluss des Anbieters führen. Daher wird hier die Möglichkeit geschaffen, die Prüfung durch die Einrichtung beauftragen zu lassen. Die dabei entstehenden Kosten sind in der Regel zumindest teilweise durch die Einrichtung selbst zu tragen.

NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter vollständig benennen lassen, welche seiner Unterauftragnehmer gemäß C5 als Subdienstleistungsunternehmen[38] anzusehen sind und auf welche Art und welchem Umfang er diese in die Bereitstellung des Cloud-Dienstes einbezieht.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass er der Einrichtung beabsichtigte Änderungen an vertraglichen Vereinbarungen mit Subdienstleistungsunternehmen, die in die Bereitstellung des Cloud-Dienstes involviert sind, unverzüglich schriftlich oder per E-Mail mitteilt.

[38] C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), Kapitel 3.4.5, S. 25f.

i) Diese Mitteilung SOLLTE zeitlich vor Umsetzung der Änderung erfolgen.

ii) Der Cloud-Diensteanbieter MUSS der Einrichtung insbesondere mitteilen, wenn er bestehende Vertragsverhältnisse beendet oder neue Vertragsverhältnisse mit Subdienstleistungsunternehmen eingeht. Vertragsverhältnisse in diesem Sinne schließen alle mitgeltenden Dokumente und Regelungen, wie z. B. Leistungsscheine, Dienstgütevereinbarungen oder Allgemeine Geschäfts- und Einkaufsbedingungen ein.

c) Diese Mitteilungen KANN der Cloud-Diensteanbieter z. B. über Internetportale oder Push-Benachrichtigungen bereitstellen, wenn die Einrichtung diese Anforderungen als erfüllt ansieht.

d) Falls der Cloud-Diensteanbieter Subdienstleistungsunternehmen einbezieht oder anderweitig wesentliche Teile der Entwicklung oder Bereitstellung des Cloud-Dienstes an Unterauftragnehmer auslagert, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

– die Subdienstleistungsunternehmen und Unterauftragnehmer die zwischen der Einrichtung und dem Cloud-Diensteanbieter vertraglich festgelegten Vorgaben ebenfalls erfüllen und

– sich die Prüfrechte, die der Cloud-Diensteanbieter der Einrichtung zugesichert hat, auch auf die Subdienstleistungsunternehmen und Unterauftragnehmer des Cloud-Diensteanbieters beziehen.

Zu a): Liegt ein Prüfbericht nach C5 vor sind diese Informationen in der Systembeschreibung aufgeführt (siehe NCD.2.2.01, Buchstabe e)).

Zu b): Da Cloud-Angebote in der Regel flexibel gestaltet sind, können sich während der Vertragslaufzeit Änderungen bei der Einbindung von Unterauftragnehmern ergeben. Darüber ist die Einrichtung als Vertragspartner unverzüglich zu informieren.

Zu c): In der Regel bieten Cloud-Anbieter hierfür Informationsportale an. Es ist zu klären, wie die Einrichtung informiert wird. Insbesondere ob diese auch aktiv vom Cloud-Anbieter auf Änderungen hingewiesen wird (z. B. durch E-Mails).

Zu d): Wesentliche Teile des Cloud-Dienstes müssen bestimmt werden. Wesentlich sind Teilleistungen insbesondere dann, wenn ohne diese ein Anbieten des Cloud-Dienstes nicht möglich wäre (z. B. Rechenzentrumsbetrieb). Werden diese von Unterauftragnehmern wahrgenommen, müssen diese vom Cloud-Anbieter nicht nur benannt werden, sondern die vertraglich festgelegten Sicherheitsanforderungen erfüllen. Weiterhin ist zu prüfen, ob zugesicherte Prüfrechte (siehe NCD.2.2.01, Buchstabe j)) auch auf diese Unterauftragnehmer auszuweiten sind.

NCD.2.2.03 Gerichtsbarkeit

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

Vor dem Hintergrund des jeweiligen Anwendungsfalles ist zu prüfen, welche Bedeutung ein Gerichtsstand außerhalb von Deutschland hätte. Hierbei ist insbesondere zu bewerten, inwiefern Durchsetzungsrechte oder Eilrechtsschutz von Bedeutung sind. Gleiches gilt für das anzuwendende Recht.

Liegt ein Prüfbericht nach C5:2020 vor, können diese Angaben der Rahmenbedingung „BC-01 Angaben zu Gerichtsbarkeit und Lokationen“ entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

Eine Bewertung des anwendbaren Rechts könnte aufgeteilt nach Regionen erfolgen:

- Deutsches Recht,
- Recht eines EU-Mitgliedstaates,
- Recht eines Nicht-EU-Mitgliedstaates.

Kommt es zu einer gerichtlichen Auseinandersetzung nimmt der Gerichtsstand eine wichtige Rolle ein. Vor diesem Hintergrund könnte die Zuordnung des Gerichtsstandes nach Regionen erfolgen:

- Deutschland,
- EU-Mitgliedsstaat,
- Nicht EU-Mitgliedsstaat.

NCD.2.2.04 Lokation der Datenverarbeitung

a) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Hierzu MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und der Risikoanalyse, das mögliche Risiko eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) sowie weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) bewerten.

b) Die Einrichtung MUSS sämtliche Lokationen, an denen der Cloud-Diensteanbieter mit dem Cloud-Dienst dienstliche Daten speichert und verarbeitet, vertraglich festlegen. Dabei MUSS die Einrichtung auch Datensicherungen berücksichtigen, da diese ggf. an Drittlokationen durchgeführt werden.

Die Einrichtung muss vor dem Hintergrund des Anwendungsfalles entscheiden, welche Lokationen für die Verarbeitung der Daten akzeptiert werden können. Dies bezieht Backup-Daten, Rechnungs- und Metadaten ein. Auch eine mögliche Verarbeitung von Daten durch Unterauftragnehmer ist zu berücksichtigen. Für die Bewertung können die Zonen

- Deutschland,
- EU-Mitgliedsstaat,
- Nicht EU-Mitgliedsstaat

genutzt werden.

Liegt ein Prüfbericht nach C5:2020 vor, können Angaben zu Datenlokationen des Cloud-Anbieters den Angaben zur Rahmenbedingung „BC-01 Angaben zu Gerichtsbarkeit und Lokationen“ entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden. Alternativ können dazu auch Informationen in den Verträgen oder Dienstegütevereinbarungen (Service Level Agreements) stehen.

NCD.2.2.05 Meldepflicht sicherheitsrelevanter Vorfälle

a) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS beim Festlegen von Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf der mit dem Cloud-Dienst verarbeiteten dienstlichen Daten achten.

ii) Beim Festlegen von Vertragsstrafen und Haftungsregelungen sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

Anmerkung: Der Titel der Anforderung enthält noch den Aspekt der Ermittlungsbefugnisse, da dieser in der Version 1.0 des Mindeststandards hier thematisiert wurde. Bei der Überarbeitung wurde der entsprechende Unterpunkt entfernt (einen Hinweis dazu befindet sich noch in Fußnote 23 des Mindeststandards), die Überschrift aber nicht angepasst. Dies wir bei der nächsten Aktualisierung des Mindeststandards korrigiert werden.

Zu a): Sicherheitsrelevante Vorfälle gefährden im Regelfall die Informationssicherheit des Cloud-Dienstes und damit auch die Daten der Einrichtung. Um das Risiko für die eigenen Daten einschätzen zu können sind sicherheitsrelevante Vorfälle der Einrichtung gegenüber zu melden. Hierbei sollten Fristen und Meldewege vertraglich zugesichert werden.

Vertragsstrafen und Haftungsfragen sind durch entsprechende Regelungen festzulegen. Hierbei ist die Kritikalität des Cloud-Dienstes für die Einrichtung zu berücksichtigen (Risikoanalyse, Datenkategorisierung). Die Sicherheitsanforderung gibt weiterhin mit 5% des Auftragsvolumens eine Empfehlung ab.

NCD.2.2.06 Beendigung des Vertragsverhältnisses

a) Die Einrichtung MUSS dem Anwendungsfall angemessene Kündigungsfristen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

Kündigungsfristen sind unter Beachtung des Anwendungsfalles und insbesondere unter Berücksichtigung der Ergebnisse aus Risikoanalyse und Datenkategorisierung zu vereinbaren. Daher sind diese durch die Einrichtung für den jeweiligen Anwendungsfall zu ermitteln und festzulegen. Dabei gilt: je „kritischer“ ein Cloud-Dienst für die Einrichtung ist, desto länger sollten Kündigungsfristen seitens des Cloud-Anbieters ausgestaltet sein.

NCD.2.2.07 Regelung der Datenrückgabe und Datenlöschung

a) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, wie dieser die mit dem Cloud-Dienst verarbeiteten dienstlichen Daten nach Beendigung der Nutzung an die Einrichtung übergibt (z. B. Fristen, Datenformat, Datenträger, Protokolle).

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, welche Maßnahmen dieser zur Löschung der dienstlichen Daten durchführt. Dabei MUSS die Einrichtung sicherstellen, dass die Maßnahmen dem zuvor ermittelten Schutzbedarf entsprechen.

Zu a): Die Einrichtung muss Regelungen zur Datenrückgabe festlegen. Dies beinhaltet u.a. Format, Datenträger, Protokolle und die Dokumentation der Übergabe muss definiert werden. Hierbei sind

insbesondere die Ergebnisse der Datenkategorisierung zu berücksichtigen, so dass eine Datenrückgabe nicht unbedingt zwingend sein muss.

Zu b): Für die Festlegung der Maßnahmen zur Datenlöschung und ggf. Datenmigration ist analog zu verfahren. Die hier festgelegten Regelungen sind für die Sicherheitsanforderungen NCD.2.4.01 und NCD.2.4.02 relevant (siehe Kapitel 2.4).

2.3 Einsatzphase

Die Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

NCD.2.3.01 Einbindung in das ISMS

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen für Cloud-Kunden[39] in ihrem ISMS einrichten. Die Einrichtung SOLLTE darüber hinaus die im C5 beschriebenen korrespondierenden Kriterien für Kunden berücksichtigen.

Zu a): Die Einrichtung hat zu prüfen und festzulegen, wie der externe Cloud-Dienst in das eigene ISMS eingebunden werden kann. Schnittstellen sind zu identifizieren und zu dokumentieren. Insbesondere ist zu prüfen, wie Mitteilungen des Cloud-Anbieters über Änderungen bei Unterauftragnehmern (siehe NCD.2.2.02) oder Meldungen von sicherheitsrelevanten Vorfällen (siehe NCD.2.2.05) in das ISMS der Einrichtung eingebunden werden können. Ziel sollte dabei sein, dass eine Verarbeitung der Informationen ohne Zeitverlust durch die zuständigen Verantwortlichen erfolgt.

NCD.2.3.02 Auswertung von Sicherheitsnachweisen

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[40]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

Zu a): Ist der Cloud-Anbieter vertraglich verpflichtet Nachweise zu erbringen (siehe NCD.2.2.01) muss die Einrichtung festlegen, wie diese intern geprüft und ausgewertet werden können. Bei der Prüfung ist insbesondere darauf zu achten, dass die vorgelegten Nachweise den gesamten Cloud-Dienst und Nutzungszeitraum abdecken.

[39] Hinweis: Der C5 führt in Version 2020 mit den korrespondierenden Kriterien für Kunden bestimmte Mitwirkungspflichten des Cloud-Kunden ein. Der C5 hält Cloud-Diensteanbieter dazu an, diese Mitwirkungspflichten, abhängig von der Art des Cloud-Dienstes, zu definieren und in den C5-Prüfbericht als korrespondierende Kontrollen für Cloud-Kunden aufzunehmen. Es liegt im Verantwortungsbereich des Cloud-Kunden und damit der Einrichtung, den Mitwirkungspflichten entsprechende Kontrollen zu gestalten, einzurichten und durchzuführen. Dies ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Vgl. C5 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020a), S. 15.

[40] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“ (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020b).

Zu b): Sollten Unklarheiten nach Buchstabe a), ii) nicht auf andere Weise aufgeklärt werden können und die zugesicherten Prüf- und Kontrollrechte wahrgenommen werden, ist festzulegen, wie diese im konkreten Fall auszuüben sind.

NCD.2.3.03 Prüfung der Leistungsfähigkeit

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, vor dem Hintergrund der Nutzung des Cloud-Dienstes beurteilen.

b) Die Einrichtung MUSS ggf. auftretende Abweichungen bewerten und auf diese durch geeignete Anpassungen an der eigenen IT-Infrastruktur und Netzanbindung reagieren.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters und des Cloud-Dienstes sowie der Netzverbindung zum Cloud-Diensteanbieter beurteilen.[41]

Zu a): Die Netzwerkanbindung an den Cloud-Dienst nimmt vor allem für die Verfügbarkeit eine zentrale Rolle ein. Die Einrichtung muss daher ihre eigene Infrastruktur hinsichtlich der benötigten Leistungsfähigkeit überprüfen (z. B. SLA für externe Netzanbindung, eingesetzte Firewalls, Anbindung der Arbeitsplatzrechner usw.).

NCD.2.3.04 Informationspflichten

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

- einer Eingliederung des Cloud-Diensteanbieters in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihm,

- einem Austausch von Unterauftragnehmern oder Dritten (siehe hierzu auch NCD.2.2.02).

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und auf diese gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

Zu b): Die Einrichtung muss festlegen, wie die Informationen des Cloud-Anbieters (z. B. zu den Anforderungen NCD.2.2.02 und NCD.2.2.05) innerhalb des eigenen ISMS weiterverarbeitet werden sollen.

NCD.2.3.05 Multi-Faktor-Authentisierung

a) Bietet der externe Cloud-Dienst eine Multi-Faktor-Authentisierung für Anmeldungen von Benutzern (Log-in) an, SOLLTE die Einrichtung diese nutzen.

b) Bietet der externe Cloud-Dienst eine Multi-Faktor-Authentisierung für Anmeldungen von Benutzern mit privilegierten Rechten (Log-in) wie bspw. zur Administration an, MUSS die Einrichtung diese nutzen.

[41] Hinweis: Viele Cloud-Diensteanbieter stellen für die Beurteilung ihrer Leistungsfähigkeit geeignete Information kontinuierlich (bspw. in Portalen oder auf Webseiten) bereit. Einrichtungen können basierend auf diesen sowie ggf. weiteren, selbst erhobenen Informationen die Leistungsfähigkeit von Cloud-Diensteanbietern kontinuierlich überwachen. Eine in geeigneter Weise durchgeführte kontinuierliche Überwachung kann die Basis für die geforderte, mindestens jährlich durchzuführende Bewertung der Leistungsfähigkeit eines Cloud-Diensteanbieters sein, aber sie nicht vollständig ersetzen.

2.4 Beendigungsphase

Im Falle der Beendigung der Nutzung eines Cloud-Dienstes, kommen die in der Betriebsphase geregelten Mechanismen zum Abschluss der Nutzungsphase zur Anwendung.

NCD.2.4.01 Datenrückgabe bei Beendigung

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle dienstlichen Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

Einforderung und Umsetzung der festgelegten Regelungen zur Datenrückgabe. Die Regelungen ergeben sich aus dem jeweiligen Vertrag (siehe hierzu NCD.2.2.07).

NCD.2.4.02 Datenlöschung bei Beendigung

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gem. NCD.2.2.07 erfolgte Löschung aller dienstlichen Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.[42] Dies umfasst die Bestätigung, dass die dienstlichen Daten gemäß der vertraglich vereinbarten Verfahren gelöscht wurden.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern (z. B. Subdienstleistungsunternehmen) und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die durch den Cloud-Diensteanbieter bestätigte Datenlöschung dokumentieren.

Wurde die Löschung aller Daten nach Vertragsende vereinbart, hat sich die Einrichtung die tatsächliche Löschung dann vom Cloud-Anbieter schriftlich bestätigen zu lassen.

2.5 Mitnutzung

Der Mindeststandard zur Nutzung externer Cloud-Dienste integriert in seiner nun vorliegenden Form auch den Mindeststandard des BSI zur Mitnutzung von externen Cloud-Diensten[43]. Die sogenannte Mitnutzung weicht von der Nutzung im Sinne dieses Mindeststandards ab, da zwischen der nutzenden Einrichtung und dem Cloud-Diensteanbieter für diese Dienstleistung kein eigenes Vertragsverhältnis besteht. Die dabei geltenden Sicherheitsanforderungen referenzieren die Anforderungen zur Nutzung externer Cloud-Dienste (Kapitel 2.1 bis 2.4), sofern dies geboten ist.

NCD.2.5.01 Mitnutzung externer Cloud-Dienste

a) Die Einrichtung MUSS sicherstellen, dass die Mitnutzung mit der eigenen Strategie für die Cloud-Nutzung (siehe NCD.2.1.01) vereinbar ist.

b) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d bis i, umsetzen und einhalten.

c) Die Einrichtung MUSS ermitteln, an welchen Lokationen mit dem externen Cloud-Dienst dienstliche Daten verarbeitet werden. Dies schließt auch Datensicherungen sowie, sofern gegeben, Unterauftragnehmer und Subdienstleister des Cloud-Diensteanbieters ein.

[42] Hinweis: Neben Nutzdaten können auch Protokoll-/Transaktionsdaten zu löschen sein.
[43] MST MCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)

i) Die Einrichtung MUSS bewerten, ob die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung sowie, sofern gegeben, weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) heranziehen.

d) Die Einrichtung MUSS ermitteln, welche Rechte an den dienstlichen Daten dem Cloud-Diensteanbieter oder Dritten durch das Akzeptieren der vom Cloud-Diensteanbieter vorgegebenen Allgemeinen Geschäftsbedingungen (AGB), Datenschutzerklärung oder sonstigen Nutzungsbedingungen eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit den eigenen Sicherheitsanforderungen, die sie in der Sicherheitsrichtlinie und dem eigenen Sicherheitskonzept definiert hat, vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

e) Die Einrichtung MUSS bewerten, ob und wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt zu speichern sind. Für die anschließende Bewertung SOLLTE die Einrichtung die identifizierten Risiken mit der eigenen Strategie für die Cloud-Nutzung (siehe NCD.2.1.01) abgleichen.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

f) Die Einrichtung MUSS erheben, wie und wann Daten durch den Cloud-Anbieter gelöscht werden (z.B. Löschfristen). Die Einrichtung MUSS dann bewerten, ob dies mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.

g) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[44]

Zu c): Liegt ein Prüfbericht nach C5:2020 vor, können diese Angaben der Rahmenbedingung „BC-01 Angaben zu Gerichtsbarkeit und Lokationen“ entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

[44] Siehe MST MDM (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2022b), S. 1ff.

Alternativ können dazu auch Informationen in den Verträgen oder Dienstgütevereinbarungen (Service Level Agreement) stehen. Hierzu sollte der Auftraggeber des externen Cloud-Dienstes kontaktiert werden. Können diese Informationen nicht ermittelt werden, ist dies zu vermerken und entsprechend zu bewerten.

Eine Zuordnung der Datenlokationen nach Regionen könnte wie folgt vorgenommen werden:

- Deutschland,
- EU-Mitgliedsstaat,
- Nicht EU-Mitgliedsstaat,
- unbekannt.

Wie einleitend beschrieben sind die Risikobehandlungsoptionen immer auf den Anwendungsfall bezogen auszuwählen. So kann eine Datenverarbeitung ausschließlich von Daten der Kategorie 4 durchaus vertretbar sein.

Zu d): Die hier eingeräumten Rechte sind insbesondere von Bedeutung, wenn Daten der Kategorie 1 bis 3 verarbeitet werden sollen. Aber auch bei einer ausschließlichen Verarbeitung von Daten der Kategorie 4 ist hier eine kritische Bewertung notwendig.

Für die Bewertung der Nutzung und Weitergabe von Daten an Dritte könnte folgende Unterteilung genutzt werden:

- keine Rechte für die Nutzung und Weitergabe von Daten an Dritte,
- Rechte, die eine Weitergabe und Verarbeitung durch Unterauftragnehmer ermöglichen,
- Rechte, die einen Verkauf der Daten an Dritte zu kommerziellen Zwecken ermöglichen,
- Rechte, die eine Nutzung der Daten außerhalb der konkreten vorgesehenen Leistungserbringung ermöglichen,
- unbekannt.

Zu e): Es sollte eine Verschlüsselung der Daten im Cloud-Dienst erfolgen. Hierfür muss der Cloud-Anbieter Verfahren und technische Maßnahmen zur Verschlüsselung bei der Speicherung etablieren. Ausnahmen können für Daten akzeptiert werden, wenn diese für die Erbringung des Cloud-Dienstes funktionsbedingt nicht verschlüsselt sein können.

Daher ist hierzu ermitteln ob und mit welcher Technologie eine Verschlüsselung erfolgt. Das Ergebnis kann entsprechend eingeordnet werden.

- Verschlüsselung der Daten erfolgt auf Basis von: ...,
- keine Verschlüsselung der Daten,
- unbekannt ob und welche Technik zur Verschlüsselung eingesetzt wird.

Zu f): Ist für die Mitnutzung die Installation von Software auf den Arbeitsplatzrechner erforderlich, können dadurch weitere Risiken entstehen. Daher sind hierzu entsprechende Informationen zu ermitteln. Das Ergebnis kann dann entsprechend eingeordnet werden:

- Softwareinstallation ist erforderlich: Name der Anwendung,
- Softwareinstallation ist optional: Name der Anwendung,
- Softwareinstallation nicht erforderlich,
- unbekannt.

Zu f) i): In diesem Zusammenhang ist zu überprüfen, welche Berechtigungen die Software benötigt. (z. B. lokale Administrationsrechte) Hier sollte insbesondere hinterfragt werden, ob diese mit den sonstigen behördeninternen Regelungen vereinbar sind.

Zu f) ii): Weiterhin ist zu ermitteln, ob ein Zugriff über mobile Endgeräte möglich ist. Auch hier kann das Ergebnis entsprechend zugeordnet werden:

- Nutzung mobiler Endgeräte erforderlich,
- Nutzung mobile Endgeräte nicht erforderlich,
- unbekannt.

Ist eine Mitnutzung auch über mobile Endgeräte möglich, muss dieses Szenario entsprechend bewertet werden. Hier sind verschiedene technische (Zugriff nur über verwaltete Geräte) oder organisatorische Maßnahmen (z. B. Verbot des Zugriffs über private Geräte) möglich, um Risiken zu reduzieren oder zu vermeiden.

Literaturverzeichnis

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises. 2014. Orientierungshilfe – Cloud Computing, Version 2.0. [Online] Oktober 2014. [Zitat vom: 12. 01 2022.] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Orientierungshilfen/OHCloudComputing.html.

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2016b. Anforderungskatalog Cloud Computing (C5). Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten. [Online] 2016b. [Zitat vom: 03. 02 2022.] https://www.bsi.bund.de/dok/452180.

—. 2017b. BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz. [Online] 2017b. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/407502.

—. 2020a. Cloud Computing Compliance Criteria Catalogue – C5:2020. Kriterienkatalog Cloud Computing. [Online] 2020a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/452204.

—. 2022c. IT-Grundschutz-Kompendium, Edition 2022. [Online] 2022c. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/128568.

—. 2020b. Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5. [Online] 2020b. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/14020574.

—. 2022b. Mindeststandard des BSI für Mobile Device Management (Version 2.0 vom 05.09.2022). [Online] 2022b. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/453264.

—. 2018. Mindeststandard des BSI zur Mitnutzung von externen Cloud-Diensten (Version 1.0 vom 20.06.2018). [Online] 2018. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/397100.

—. 2017a. Mindeststandard des BSI zur Nutzung externer Cloud-Dienste (Version 1.0 vom 24.04.2017). [Online] 2017a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/397130.

—. 2022a. Mindeststandard des BSI zur Nutzung externer Cloud-Dienste (Version 2.1 vom xx.xx.2022). [Online] 2022a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/452272.

—. 2016a. Sichere Nutzung von Cloud-Diensten – Schritt für Schritt von der Strategie bis zum Vertragsende. [Online] 2016a. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/128914.

—. 2019. Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019. [Online] 2019. [Zitat vom: 12. 01 2022.] https://www.bsi.bund.de/dok/407450.

Bundesministerium des Innern (BMI). 2014. Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14. [Online] 2014. [Zitat vom: 12. 01 2022.] https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/08/no-spy-erlass.html.

Bundesministerium des Innern und für Heimat (BMI). 2018. Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018. [Online] 2018. [Zitat vom: 12. 01 2022.] https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm.

International Organization for Standardization (ISO). 2014. International Standard ISO/IEC 17788:2014. *Information technology — Cloud computing — Overview and vocabulary.* [Online] 2014. [Zitat vom: 12. 01 2022.] https://www.iso.org/standard/60544.html.

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Criteria Catalogue
CRM	Customer Relationship Management
DSGVO	Datenschutz-Grundverordnung
EU	Europäische Union
FAQ	Frequently Asked Questions
IEC	International Electrotechnical Commission
ISB	Informationssicherheitsbeauftragte
ISO	International Standards Organization
IT	Informationstechnik
ITZBund	Informationstechnikzentrum Bund
IT-GS	IT-Grundschutz
IT-SiBe	IT-Sicherheitsbeauftragte
MCD	Mitnutzung externer Cloud-Dienste
MDM	Mobile Device Management
MST	Mindeststandard
NCD	Nutzung externer Cloud-Dienste
RFC	Request for Comments
SLA	Service Level Agreement
StGB	Strafgesetzbuch
UMH	Umsetzungshinweise
VS	Verschlusssache
VSA	Verschlusssachenanweisung
z. B.	zum Beispiel

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.1 vom 15.12.2022

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	24.04.2017	Erstveröffentlichung
2.0	07.07.2021	Major Release - Zusammenführung der Mindeststandards zur Nutzung und Mitnutzung externer Cloud-Dienste
2.1	15.12.2022	Korrekturen, Ergänzungen und Begriffsanpassungen

Tabelle 1: Versionsgeschichte des Mindeststandards. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/dok/930566

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Risiken für die Cyber- und Informationssicherheit sind nicht zuletzt aufgrund der zunehmenden Komplexität und Vernetzung von IT-Systemen allgegenwärtig. Dadurch betreffen potenzielle Schwachstellen und Cyber-Angriffe in der Regel nicht nur einzelne Stellen.

Umso wichtiger ist die Vorgabe verbindlicher Sicherheitsanforderungen an die Informationstechnik des Bundes. So kann ein einheitliches Mindestsicherheitsniveau mit effektiven Maßnahmen zur Abwehr von Cyber-Angriffen innerhalb der heterogenen Behördenlandschaft etabliert werden.

Dazu legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes[1] fest. Dies erfolgt auf der Grundlage des § 8 Absatz 1 BSIG im Benehmen mit den Ressorts. Als gesetzliche Vorgabe definieren Mindeststandards somit ein verbindliches Mindestniveau für die Informationssicherheit.

Bereits 2017 hat das Bundeskabinett mit dem Umsetzungsplan Bund 2017 (UP Bund 2017) eine Leitlinie für Informationssicherheit in der Bundesverwaltung in Kraft gesetzt. Damit wurde die Beachtung der Mindeststandards für den Bereich der Stellen des Bundes verbindlich. Durch das IT-Sicherheitsgesetz 2.0 wurde die Einhaltung der Mindeststandards des BSI auch gesetzlich geregelt. Die Umsetzungspflicht der Mindeststandards ergibt sich aus dem dadurch neu gefassten § 8 BSIG.

Die Mindeststandards richten sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe), Informationssicherheitsbeauftragte (ISB), IT-Betriebspersonal und Beschaffungsstellen. Die Gesamtverantwortung für die Informationssicherheit und damit auch für die Einhaltung der Mindeststandards trägt gemäß UP Bund 2017 die Leitung der jeweiligen Einrichtung[1].

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf dem Mindestsicherheitsniveau sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[2] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Einrichtung auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Einrichtungen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Die von den Mindeststandards adressierten Stellen werden in § 8 Absatz 1 BSI-Gesetz (BSIG) definiert (siehe https://www.gesetze-im-internet.de/bsig_2009/__8.html). Zur besseren Lesbarkeit wird im weiteren Verlauf für alle dort genannten Stellen der Begriff „Einrichtung“ verwendet.

[2] Siehe FAQ zu den MST: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/FAQ_MST/faq_mst_node.html

Inhalt

1 Beschreibung

Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste.

1.1 Begriffsbestimmung und Abgrenzung

Zur Begriffsbestimmung nutzt dieser Mindeststandard die Definition für Cloud-Dienste des Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing)[3], die sich an die internationale Begriffsdefinition des ISO 17788 anlehnt.[4] Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen („Cloud-Dienste“) erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der in diesem Rahmen angebotenen Cloud-Dienste umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Anwendungen.

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind Cloud-Dienste, die von Anbietern der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes erbracht werden.[5]

Als Nutzung eines Cloud-Dienstes sind das Speichern und Verarbeiten von dienstlichen Daten durch einen externen Cloud-Dienst zu verstehen. Dieser kann durch eine oder mehrere Einrichtungen beauftragt werden. Regelungen für das Mitnutzen externer Cloud-Dienste durch Benutzende[6] einer Einrichtung sind in Kapitel 2.5 beschrieben. Von einer Mitnutzung wird ausgegangen, wenn eine Einrichtung den externen Cloud-Dienst nicht selbst beauftragt hat bzw. zwischen dieser Einrichtung und dem Cloud-Diensteanbieter kein unmittelbares Vertragsverhältnis besteht.

Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards dennoch hilfreiche Empfehlungen enthalten und trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e).[7]

[3] Im Weiteren mit “C5” abgekürzt, vgl. (BSI 2020a).

[4] Der Standard „ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary“ (ISO 2014) definiert Cloud Computing als Paradigma für die Ermöglichung über ein Netz auf einen skalierbaren und elastischen Pool von geteilten virtuellen oder physischen Ressourcen (Server, Plattform, Anwendung, Software, etc.) zuzugreifen und über ein Selbst-Service Portal zu bestellen und selbst zu administrieren. Ein Cloud-Service ist als über eine definierte Schnittstelle buchbare und über Cloud Computing angebotene Fähigkeiten („capabilities“) definiert. Cloud-Fähigkeiten werden nach Infrastruktur, Plattform und Anwendung unterschieden.

[5] Hinweis: Private Cloud-Dienste der IT-Dienstleister des Bundes (z. B. Bundescloud) fallen somit nicht unter diese Bestimmung.

[6] Analog Rolle „Benutzer“ nach IT-Grundschutz-Kompendium, (BSI 2022a): „Ein Benutzer ist ein Mitarbeiter einer Institution, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt. IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben verwendet.“, Kap. Rollen, S. 27

[7] Hinweis: Für eine Beschreibung, wie sich die Anforderungsnummerierung zusammensetzt, siehe FAQ zu den Mindeststandards (BSI 2019).

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[8] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[9] und DIN 820-2: 2018[10].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung oder Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

[8] Vgl. BSI-Standard 200-2 (BSI 2017a), S. 18
[9] Vgl. Key words for use in RFCs (IETF 1997)
[10] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[11] auf.

2.1 Planungsphase

Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*

- die Strategie für die Cloud-Nutzung,
- die darauf basierende Sicherheitsrichtlinie sowie
- das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.

Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend.

NCD.2.1.01 Strategie für die Cloud-Nutzung

a) Die Einrichtung MUSS eine Strategie für die Cloud-Nutzung nach OPS.2.2.A1 *Erstellung einer Strategie für die Cloud-Nutzung*[12] erstellen.

b) Die Einrichtung MUSS in dieser Strategie für die Cloud-Nutzung festlegen, wie sie mit Risiken bei der Nutzung externer Cloud-Dienste umgeht. Hierzu MUSS eine Richtlinie zur Risikoanalyse erstellt werden.[13]

c) Die Einrichtung MUSS prüfen, ob ein externer Cloud-Dienst grundsätzlich mit den in ihrer Strategie für die Cloud-Nutzung definierten Zielen, Chancen und Risiken vereinbar ist. [14] Die Einrichtung DARF einen externen Cloud-Dienst NUR nutzen, wenn dieser die in der Strategie für die Cloud-Nutzung definierten Ziele, Chancen und Risiken angemessen unterstützt.

d) Die Einrichtung MUSS vor der Nutzung eines externen Cloud-Dienstes eine Risikoanalyse gemäß der in NCD.2.1.01 b) festgelegten Richtlinie durchführen.

NCD.2.1.02 Sicherheitsrichtlinie für externe Cloud-Dienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[15] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Cloud Computing Compliance Criteria Catalogue – C5 (Kriterienkatalog Cloud Computing) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[16]

c) Die Einrichtung MUSS die IT-Sicherheitsbeauftragten bei der Erstellung der Sicherheitsrichtlinie beteiligen und ebenfalls - sofern betroffen - die zuständigen Datenschutz- und Geheimschutzbeauftragten.

[11] IT-Grundschutz-Kompendium, (BSI 2022a), OPS.2.2 *Cloud-Nutzung*
[12] IT-Grundschutz-Kompendium, (BSI 2022a), OPS.2.2 *Cloud-Nutzung*
[13] Siehe BSI-Standard 200-3, (BSI 2017b), S. 9f.
[14] Hinweis: OPS.2.2.A1 *Erstellung einer Strategie für die Cloud-Nutzung* sieht die Erstellung einer Strategie für die Cloud-Nutzung vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Strategie für die Cloud-Nutzung nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.
[15] IT-Grundschutz-Kompendium, (BSI 2022a), OPS.2.2 *Cloud-Nutzung*
[16] Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing), (BSI 2020a), S.1ff.

NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung*[17] erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[18]

c) Die Einrichtung MUSS die IT-Sicherheitsbeauftragten bei der Erstellung des Sicherheitskonzeptes beteiligen und ebenfalls – sofern betroffen – die zuständigen Datenschutz- und Geheimschutzbeauftragten.

d) Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten[19] verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesen Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

f) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

- Kategorie 1 = Privat-, Dienst-, Betriebs- und Geschäftsgeheimnisse gemäß Strafgesetzbuch (StGB) §§ 203 und 353b
- Kategorie 2 = personenbezogene Daten gemäß Datenschutz-Grundverordnung (DSGVO) Art. 4 Nr. 1
- Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[20]
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

g) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und 3 gleichzeitig zuordnen.

h) Falls Daten den Kategorien 1, 2 oder 3 zugeordnet wurden: Die Einrichtung MUSS für die identifizierten dienstlichen Daten dieser Kategorien die Geheim- und Datenschutzaspekte[21] sowie Anforderungen hinsichtlich Privat-, Dienst, Betriebs- und Geschäftsgeheimnisse ermitteln und aus diesen ggf. entstehende weitere Anforderungen ableiten.

> i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln und bewerten.[22] Die Einrichtung MUSS die ermittelten Risiken gemäß der in der Strategie für die Cloud-Nutzung festgelegten Richtlinie zur Risikoanalyse bewerten.
>
> ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn alle ermittelten Risiken gemäß der in der Strategie für die Cloud-Nutzung genannten Richtlinie zur Risikoanalyse wirksam vermieden oder hinreichend reduziert oder in Übereinstimmung mit den Risikoakzeptanzkriterien bei der Cloud-Nutzung getragen werden können.

[17] IT-Grundschutz-Kompendium, (BSI 2022a), OPS.2.2 *Cloud-Nutzung*
[18] Siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud
[19] Dienstliche Daten können gleichzeitig auch personenbezogene Daten sein. Für den Zweck dieses Mindeststandards sind jedoch nicht solche personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden, gemeint.
[20] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), (BMI 2018)
[21] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2014), S.1ff.
[22] Hinweis: Es gilt, zu bewerten, inwiefern die mit dem betrachteten Cloud-Dienst im beabsichtigten Anwendungsfall verbundenen rechtlichen, technischen und organisatorischen Risiken mit der Strategie für die Cloud-Nutzung vereinbar sind.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen)[23] unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

NCD.2.1.04 Notfall- und Kontinuitätsmanagement

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[24] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint. Es umfasst sowohl präventive als auch reaktive Maßnahmen, mit denen eine Einrichtung auf Notfälle und Krisensituationen reagiert. Es gilt im Weiteren die Begrifflichkeit des BSI-Standards 100-4.[25]

a) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen und Krisensituationen einnehmen würde.[26]

b) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss.[27]

c) Die Einrichtung MUSS die zuständigen Notfallbeauftragten entsprechend einbinden. Diese MÜSSEN prüfen, ob sich die Cloud-Nutzung auf Maßnahmen, die Notfällen und Krisensituationen präventiv und/oder reaktiv entgegenwirken, auswirkt und inwiefern diese Maßnahmen ggf. anzupassen sind. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.[28]

2.2 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters. Hinsichtlich der Beschaffung externer Cloud-Dienste sollte die Einrichtung insbesondere die einschlägigen „Ergänzenden Vertragsbedingungen für Cloudleistungen (EVB-IT Cloud)“[29] beachten und nutzen.

NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss bewerten, inwiefern der externe Cloud-Dienst die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a) erfüllt.[30]

b) Die Einrichtung MUSS die Erfüllung dieser Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.[31]

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe 0 hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie

[23] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (BMI 2014), S.1

[24] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.

[25] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.

[26] Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt?

[27] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?

[28] Siehe OPS.2.2.A11 Erstellung eines Notfallkonzeptes für einen Cloud-Dienst, (BSI 2022a)

[29] Vgl. EVB-IT Cloud, (BMI 2022)

[30] Hinweis: Liegt ein C5-Prüfbericht vor, können diesem Informationen entnommen und der Bewertung zugrunde gelegt werden.

[31] Siehe OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters, (BSI 2022a)

Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der *Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5*[32] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN mindestens

- die angemessene und wirksame Erfüllung der Basiskriterien nach C5[33],
- die aktuelle Dokumentation der Systembeschreibung[34],
- die Aktualität von vertraglich zugesicherten Zertifizierungen und Berichterstattungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

umfassen und KÖNNEN vom Cloud-Diensteanbieter durch die regelmäßige Bereitstellung einer aktuellen C5-Berichterstattung vom Typ2 erbracht werden.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten und eventuellen Unklarheiten und insbesondere darin ausgewiesene Abweichungen in geeigneter Form nachgehen. Hierbei MUSS die Einrichtung auch abwägen, ob und inwiefern ein Risiko entsteht und wie mit diesem umzugehen ist.

g) Insbesondere MÜSSEN Zertifikate, Prüfberichte und Nachweise den Zeitraum, in dem die Einrichtung den Cloud-Dienst nutzt, jeweils vollständig abdecken und DÜRFEN KEINE zeitlichen Lücken enthalten oder entstehen lassen. Dies MUSS die Einrichtung in ihre Sicherheitsanforderungen sowie demzufolge in die Leistungsbeschreibung aufnehmen.

h) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

i) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen, die vom Cloud-Diensteanbieter zu erfüllen sind, abdecken oder diese Risiken transferieren oder akzeptieren, und MUSS dies entsprechend dokumentieren.

> i) Die Einrichtung MUSS die weiteren Anforderungen nach NCD.2.1.03, Buchstabe i, in ihre Sicherheitsanforderungen aufnehmen. Soweit die Einrichtung diese weiteren Anforderungen nur gemeinsam mit dem Cloud-Diensteanbieter erfüllen kann, MUSS die Einrichtung diese in die Leistungsbeschreibung bzw. in das Vertragsverhältnis mit dem Cloud-Diensteanbieter aufnehmen.
>
> ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung mit dem Cloud-Diensteanbieter vereinbaren, dass dieser regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorlegt. Falls die Anforderungen nur gemeinsam erfüllt werden können, erstrecken sich die Nachweise nur auf den Anteil, der vom Cloud-Diensteanbieter umgesetzt wird.

[32] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, die dabei unterstützt, einen C5-Prüfbericht systematisch auszuwerten. Diese Auswertung beinhaltet, die Sicherheitsmaßnahmen (Kontrollen) des Cloud-Diensteanbieters inklusive der zugehörigen Prüfergebnisse sowie der auf Cloud-Nutzendenseite einzurichtenden Kontrollen aufzunehmen. In Verbindung mit den aufseiten der Einrichtung eingerichteten Kontrollen sowie weiterer, vom individuellen Anwendungsfall abhängenden Informationen lassen sich die mit der Nutzung des betrachteten Cloud-Dienstes verbundenen Risiken identifizieren und bewerten. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020b).

[33] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[34] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (BSI 2020a), Kap. 3.4.3.2, S.23f.) enthält der Bericht keine vom Cloud-Diensteanbieter angefertigte Systembeschreibung, sondern eine vom Prüfenden im Rahmen der Prüfung angefertigte Systembeschreibung.

j) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

i) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass die Einrichtung ihre weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) erfüllt.

ii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang eine Bewertung des vom Cloud-Diensteanbieter für den betrachteten Cloud-Dienst gebotenen Informationssicherheitsniveaus ermöglichen und die Einrichtung selbst oder Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revision, Wirtschaftsprüfende) die Prüfrechte wahrnehmen können.

iii) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS sich die Einrichtung vom Cloud-Diensteanbieter dazu berechtigen lassen, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

iv) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) nicht entgegenstehen.

NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter vollständig benennen lassen, welche seiner Unterauftragnehmer gemäß C5 als Subdienstleistungsunternehmen[35] anzusehen sind und auf welche Art und in welchem Umfang er diese in die Bereitstellung des Cloud-Dienstes einbezieht.[36]

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass er der Einrichtung beabsichtigte Änderungen an vertraglichen Vereinbarungen mit Subdienstleistungsunternehmen, die in die Bereitstellung des Cloud-Dienstes involviert sind, unverzüglich schriftlich oder per E-Mail mitteilt.

i) Diese Mitteilung SOLLTE zeitlich vor Umsetzung der Änderung erfolgen.

ii) Der Cloud-Diensteanbieter MUSS der Einrichtung insbesondere mitteilen, wenn er bestehende Vertragsverhältnisse beendet oder neue Vertragsverhältnisse mit Subdienstleistungsunternehmen eingeht. Vertragsverhältnisse in diesem Sinne schließen alle mitgeltenden Dokumente und Regelungen, wie z. B. Leistungsscheine, Dienstgütevereinbarungen oder Allgemeine Geschäfts- und Einkaufsbedingungen ein.

c) Diese Mitteilungen KANN der Cloud-Diensteanbieter z. B. über Internetportale oder Push-Benachrichtigungen bereitstellen, wenn die Einrichtung diese Anforderungen als erfüllt ansieht.

d) Falls der Cloud-Diensteanbieter Subdienstleistungsunternehmen einbezieht oder anderweitig wesentliche Teile der Entwicklung oder Bereitstellung des Cloud-Dienstes an Unterauftragnehmer auslagert, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

- die Subdienstleistungsunternehmen und Unterauftragnehmer die zwischen der Einrichtung und dem Cloud-Diensteanbieter vertraglich festgelegten Vorgaben ebenfalls erfüllen und
- sich die Prüfrechte, die der Cloud-Diensteanbieter der Einrichtung zugesichert hat, auch auf die Subdienstleistungsunternehmen und Unterauftragnehmer des Cloud-Diensteanbieters beziehen.

NCD.2.2.03 Gerichtsbarkeit

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

[35] Kriterienkatalog Cloud Computing (C5:2020), (BSI 2020a), Kap. 3.4.5, S.25f.
[36] Siehe OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter, (BSI 2022a)

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

NCD.2.2.04 Lokation der Datenverarbeitung

a) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Hierzu MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und der Risikoanalyse, das mögliche Risiko eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) sowie weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) bewerten.

b) Die Einrichtung MUSS sämtliche Lokationen, an denen der Cloud-Diensteanbieter mit dem Cloud-Dienst dienstliche Daten speichert und verarbeitet, vertraglich festlegen. Dabei MUSS die Einrichtung auch Datensicherungen berücksichtigen, da diese ggf. an Drittlokationen durchgeführt werden.[37]

NCD.2.2.05 Meldepflicht sicherheitsrelevanter Vorfälle

a) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

> i) Die Einrichtung MUSS beim Festlegen von Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf der mit dem Cloud-Dienst verarbeiteten dienstlichen Daten achten.
>
> ii) Beim Festlegen von Vertragsstrafen und Haftungsregelungen sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

NCD.2.2.06 Beendigung des Vertragsverhältnisses

a) Die Einrichtung MUSS dem Anwendungsfall angemessene Kündigungsfristen festlegen.[38]

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

NCD.2.2.07 Regelung der Datenrückgabe und Datenlöschung

a) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, wie dieser die mit dem Cloud-Dienst verarbeiteten dienstlichen Daten nach Beendigung der Nutzung an die Einrichtung übergibt (z. B. Fristen, Datenformat, Datenträger, Protokolle).

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vertraglich regeln, welche Maßnahmen dieser zur Löschung der dienstlichen Daten durchführt. Dabei MUSS die Einrichtung sicherstellen, dass die Maßnahmen dem zuvor ermittelten Schutzbedarf entsprechen.[39]

2.3 Einsatzphase

Die Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

[37] Siehe OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter, (BSI 2022a)
[38] Siehe OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter und OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses, (BSI 2022a)
[39] Siehe OPS.2.2.A9 Vertragsgestaltung mit dem Cloud-Diensteanbieter, (BSI 2022a)

NCD.2.3.01 Einbindung in das ISMS

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheits-managementsystem (ISMS) einbinden.[40]

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen für Cloud-Kunden[41] in ihrem ISMS einrichten. Die Einrichtung SOLLTE darüber hinaus die im C5 beschriebenen korrespondierenden Kriterien für Kunden berücksichtigen.

NCD.2.3.02 Auswertung von Sicherheitsnachweisen

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[42][43]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

NCD.2.3.03 Prüfung der Leistungsfähigkeit

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, vor dem Hintergrund der Nutzung des Cloud-Dienstes beurteilen.

b) Die Einrichtung MUSS ggf. auftretende Abweichungen bewerten und auf diese durch geeignete Anpassungen an der eigenen IT-Infrastruktur und Netzanbindung reagieren.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters und des Cloud-Dienstes sowie der Netzverbindung zum Cloud-Diensteanbieter beurteilen.[44][45]

NCD.2.3.04 Informationspflichten

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informations-pflichten stets nachkommt. Dies gilt insbesondere bei

- einer Eingliederung des Cloud-Diensteanbieters in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihm,
- einem Austausch von Unterauftragnehmern oder Dritten (siehe hierzu auch NCD.2.2.02).

[40] Siehe OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb, (BSI 2022a)

[41] Hinweis: Der C5 führt in Version 2020 mit den korrespondierenden Kriterien für Kunden bestimmte Mitwirkungspflichten des Cloud-Kunden ein. Der C5 hält Cloud-Diensteanbieter dazu an, diese Mitwirkungspflichten, abhängig von der Art des Cloud-Dienstes, zu definieren und in den C5-Prüfbericht als korrespondierende Kontrollen für Cloud-Kunden aufzunehmen. Es liegt im Verantwortungsbereich des Cloud-Kunden und damit der Einrichtung, den Mitwirkungspflichten entsprechende Kontrollen zu gestalten, einzurichten und durchzuführen. Dies ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.15

[42] Siehe OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung, (BSI 2022a)

[43] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020b)

[44] Siehe OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb, (BSI 2022a)

[45] Hinweis: Viele Cloud-Diensteanbieter stellen für die Beurteilung ihrer Leistungsfähigkeit geeignete Information kontinuierlich (bspw. in Portalen oder auf Webseiten) bereit. Einrichtungen können basierend auf diesen sowie ggf. weiteren, selbst erhobenen Informationen die Leistungsfähigkeit von Cloud-Diensteanbietern kontinuierlich überwachen. Eine in geeigneter Weise durchgeführte kontinuierliche Überwachung kann die Basis für die geforderte, mindestens jährlich durchzuführende Bewertung der Leistungsfähigkeit eines Cloud-Diensteanbieters sein, aber sie nicht vollständig ersetzen.

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und auf diese gemäß der vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c, reagieren.

NCD.2.3.05 Multi-Faktor-Authentisierung

a) Bietet der externe Cloud-Dienst eine Multi-Faktor-Authentisierung für Anmeldungen von Benutzenden (Log-in) an, SOLLTE die Einrichtung diese nutzen.

b) Bietet der externe Cloud-Dienst eine Multi-Faktor-Authentisierung für Anmeldungen von Benutzenden mit privilegierten Rechten (Log-in), wie bspw. zur Administration, an, MUSS die Einrichtung diese nutzen.[46]

2.4 Beendigungsphase

Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[47]

NCD.2.4.01 Datenrückgabe bei Beendigung

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle dienstlichen Daten in der vereinbarten Form zurück übergeben hat.[48]

b) Die Einrichtung MUSS die Übergabe dokumentieren.

NCD.2.4.02 Datenlöschung bei Beendigung

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gem. NCD.2.2.07 erfolgte Löschung aller dienstlichen Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.[49] Dies umfasst die Bestätigung, dass die dienstlichen Daten gemäß der vertraglich vereinbarten Verfahren gelöscht wurden.

b) Die Bestätigung nach Buchstabe a MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern (z. B. Subdienstleistungsunternehmen) und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die durch den Cloud-Diensteanbieter bestätigte Datenlöschung dokumentieren.

2.5 Sicherheitsanforderungen bei einer Mitnutzung

Nutzen die Benutzenden einer Einrichtung einen externen Cloud-Dienst, ohne dass zwischen dieser Einrichtung und dem Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[50] Die nachfolgenden Sicherheitsanforderungen regeln die Mitnutzung externer Cloud-Dienste.

NCD.2.5.01 Mitnutzung externer Cloud-Dienste

a) Die Einrichtung MUSS sicherstellen, dass die Mitnutzung mit der eigenen Strategie für die Cloud-Nutzung (siehe NCD.2.1.01) vereinbar ist.

b) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d bis i, umsetzen und einhalten.

c) Die Einrichtung MUSS ermitteln, an welchen Lokationen mit dem externen Cloud-Dienst dienstliche Daten verarbeitet werden. Dies schließt auch Datensicherungen sowie, sofern gegeben, Unterauftragnehmer und Subdienstleister des Cloud-Diensteanbieters ein.

> i) Die Einrichtung MUSS bewerten, ob die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

[46] Siehe ORP.4.A10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen, (BSI 2022a)
[47] Siehe OPS.2.2.A14 *Geordnete Beendigung eines Cloud-Nutzungsverhältnisses*, (BSI 2022a)
[48] Siehe OPS.2.2.A15 Sicherstellung der Portabilität von Cloud-Diensten, (BSI 2022a)
[49] Hinweis: Neben Nutzdaten können auch Protokoll-/Transaktionsdaten zu löschen sein.
[50] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen im Zuge einer Mitnutzung ist nicht als ein Vertragsverhältnis im Sinne dieses Mindeststandards anzusehen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung sowie, sofern gegeben, weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) heranziehen.

d) Die Einrichtung MUSS ermitteln, welche Rechte an den dienstlichen Daten dem Cloud-Diensteanbieter oder Dritten durch das Akzeptieren der vom Cloud-Diensteanbieter vorgegebenen Allgemeinen Geschäftsbedingungen (AGB), Datenschutzerklärung oder sonstigen Nutzungsbedingungen eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit den eigenen Sicherheitsanforderungen, die sie in der Sicherheitsrichtlinie und dem eigenen Sicherheitskonzept definiert hat, vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

e) Die Einrichtung MUSS bewerten, ob und wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt zu speichern sind.[51] Für die anschließende Bewertung SOLLTE die Einrichtung die identifizierten Risiken mit der eigenen Strategie für die Cloud-Nutzung (siehe NCD.2.1.01) abgleichen.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

f) Die Einrichtung MUSS erheben, wie und wann Daten durch den Cloud-Anbieter gelöscht werden (z.B. Löschfristen). Die Einrichtung MUSS dann bewerten, ob dies mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar ist.

g) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[52]

[51] Siehe OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung, (BSI 2022a)
[52] Vgl. Mindeststandard des BSI für Mobile Device Management, (BSI 2022b)

Literaturverzeichnis

AKTM (2014) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014, https://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHCloudComputing.html

BMI (2014) Bundesministerium des Innern, Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/08/no-spy-erlass.html

BMI (2017) Bundesministerium des Innern und für Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html

BMI (2018) Bundesministerium des Innern und für Heimat: Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018, https://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm

BMI (2022) Bundesministerium des Innern und für Heimat: Ergänzende Vertragsbedingungen für Cloudleistungen; Verweis unter:
Aktuelle EVB-IT – EVB-IT Cloud, https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 – Notfallmanagement, Version 1.0, https://www.bsi.bund.de/dok/128600

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0, https://www.bsi.bund.de/dok/128640

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, https://www.bsi.bund.de/dok/407502

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/11916758

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: Cloud Computing Compliance Criteria Catalogue – C5:2020 (Kriterienkatalog Cloud Computing) – Stand Februar 2020, https://www.bsi.bund.de/dok/452204

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5, https://www.bsi.bund.de/dok/14020574

BSI (2022a) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Edition 2022, https://www.bsi.bund.de/dok/128568

BSI (2022b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management, Version 2.0, https://www.bsi.bund.de/dok/453264

DIN (2018) Deutsches Institut für Normung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119

ISO (2014) ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Criteria Catalogue (Kriterienkatalog Cloud Computing)
DIN	Deutsches Institut für Normung e.V.
DSGVO	Datenschutz-Grundverordnung
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik
FAQ	Frequently Asked Questions
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
ISO/IEC	International Organisation for Standardization / International Electrotechnical Commission
IT-SiBe	IT-Sicherheitsbeauftragte
StGB	Strafgesetzbuch
RFC	Request for Comments
VSA	Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital·Sicher·BSI·

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Dienststellen der obersten Bundesbehörden

ITZ Bund (ISB)

Landes-CISOs über Geschäftsstelle der AG InfoSic

- per E-Mail -

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 228 99 9582 [redacted]
Fax +49 228 99 10 9582 [redacted]

mindeststandards@bsi.bund.de

www.bsi.bund.de

Betreff: Mindeststandard des BSI gem. § 8 Abs. 1 BSIG
hier: Nutzung externer Cloud-Dienste, Version 2.1

Bezug: Mein Schreiben BL35 – 750 07 vom 08.07.2021
RESSORTKONSULTATION
Geschäftszeichen: 750 04 01
Datum: 19.12.2022

Anlage:
1. Mindeststandard des BSI zur Nutzung externer Cloud Dienste, Version 2.1
2. Hilfsdokument / Umsetzungshinweise, Version 2.1
3. Referenztabelle zum Mindeststandard, Version 2.1

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den Mindeststandard zur Nutzung externer Cloud-Dienste aktualisiert. Die Aktualisierung umfasst verschiedene Korrekturen, Ergänzungen und Begriffsanpassungen. Ebenso wurden das dazugehörige Hilfsdokument und die Referenztabelle aktualisiert.

Die neue Version des Mindeststandards ist ab Veröffentlichung gültig und ersetzt die alte Version.

Die neue Version 2.1 des Mindeststandards, eine Übersicht über die durchgeführten Anpassungen, das Hilfsdokument und die Referenztabelle werden auch unter https://www.bsi.bund.de/mindeststandards zur Verfügung gestellt.

Ich möchte Sie bitten, diesen Mindeststandard und die zugehörigen Dokumente in Ihrem Bereich entsprechend bekannt zu geben. Rückfragen und Anregungen nehme ich über das zentrale Postfach mindeststandards@bsi.bund.de gerne entgegen.

Mit freundlichen Grüßen
Im Auftrag

Samsel

Umgang mit der Referenztabelle

Zu jeder Version eines Mindeststandards wird eine Referenztabelle erstellt. Eine Referenztabelle ist
aufgelistet wird. Sollte es zu einer Sicherheitsanforderung einen korrespondierenden IT-Grundschut
zu einer Sicherheitsanforderung mehrere korrespondierende IT-Grundschutzbausteine geben, so w
Die Referenztabelle kann als Hilfsmittel zur Bearbeitung und Dokumentation der Erfüllung der Siche
angepasst werden.

Hinweis:
Die Referenztabelle dient der Arbeitserleichterung beim Umgang mit den Mindeststandards. Das
Aktualität und der Vollständigkeit der Sicherheitsanforderungen liegt in der Zuständigkeit des jew

: eine Excel-Tabelle, in der jede Sicherheitsanforderung eines Mindeststandards
tz-Baustein geben, so wird dieser der Sicherheitsanforderung zugewiesen. Sollte es
ird die Sicherheitsanforderung mehrfach aufgelistet.
erheitsanforderungen eines Mindeststandards dienen. Sie kann je nach Bedarf

verbindliche Dokument ist der Mindeststandard selbst. Die Prüfung der
veiligen Anwenders.

N	Be eichnung	Ab atz	Si he hei san o de ung MST-NCD V21)	IT G undschut - Kompendium 2022
NCD 2 1 01	t a egie ü d e C oud-Nu zung	a	Die E n chtung MUSS eine St a egie ü d e Cloud Nutzung na h OPS 2 2 A1 E te lung e ne St ate ie ü d e Cloud Nu zung e s el en	OPS 2 2 A1
NCD 2 1 01	t a egie ü d e C oud-Nu zung	b	Die E n chtung MUSS in di se St ate ie ü d e Cloud Nu zung e t egen wie s e m t Ris ken bei de Nut ung e te e Cloud Diens e umgeht Hie zu MUSS e ne Rich l nie zu R s koana yse e te lt we den	
NCD 2 1 01	t a egie ü d e C oud-Nu zung	c	Die E n chtung MUSS p ü en ob ein exte ne C oud-Di nst g u dsät l ch m t den in ih e St ate ie ü d e Cloud Nutzung de in e en Z el n Chancen und Ri iken ve einba st D e E n ch ung DAR einen ex e nen Cloud Dien t NUR nu zen wenn iese d e in de St a egie ü d e Cloud-Nutzu g de in e en ie e Chancen und Ri iken an emes en u te tüt t	
NCD 2 1 01	t a egie ü d e C oud-Nu zung	d	Die E n chtung MUSS vo de Nut ung ines ex e nen Clou -Dien tes e ne R s koana yse gemäß	
NCD 2 1 02	iche hei s cht nie ü ex e ne Cloud D ens e	a	Die E n chtung MUSS eine S che h its cht in e ü ex e ne Clo d-Dien te nach OPS 2 2 A2 E te lung e ne Si he he ts i ht in e ü die C oud-Nut ung e ste l n	OPS 2 2 A2
NCD 2 1 02	iche hei s cht nie ü ex e ne Cloud D ens e	b	Die E n chtung MUSS in di se S che he ts cht in e m ndestens d e Umse zung und Ein al ung de Ba isk i e en ach dem Cl ud Comput ng Comp i nce C te a Cata ogue – C5 (K i e enkat log C oud Comput ng) a s spez el e Si he he ts n o de ungen an den loud-Dien teanb ete es legen	
NCD 2 1 02	iche hei s cht nie ü ex e ne Cloud D ens e	c	Die E n chtung MUSS die I -S che eit beau t a ten bei de E ste lung de iche hei s ch l nie bete l gen und eben a ls - o e n bet o en - die zu tänd gen D tens hutz- nd Geheims hutzbe u t ag en	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	a	Die E n chtung MUSS ein S che he t konzept ü den exte nen C oud-D enst na h OPS 2 2 A7 E te lung e nes Si he he ts onzeptes ü die C oud-Nut ung e ste len	OPS 2 2 A7
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	b	Die E n chtung MUSS in dem S che hei skonze t die ak uel en Ve ö ent ichun en des B I zu Cl ud-S che h it be ücks ch igen	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	c	Die E n chtung MUSS die I -S che eit beau t a ten bei de E ste lung des S che hei skonz ptes bete l gen und eben a ls – so e n bet o en – d e ust ndigen Da enschu z- und	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	d	Die E n chtung MUSS sämt iche d enst che D ten iden i iz e en die kün tig n em exte nen Cl ud-Die st ve a be tet we den so len	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	e	Kommt d e in ich ung zu dem E ebnis dass n dem exte nen C oud-D enst ke ne dien t ichen Daten ve a be tet we den h ndelt es ich n cht um e ne Nu zung ode Mit utzung ex e ne Cl ud-Die ste im Sinne d eses M ndes st nda ds In di sen äl en KANN die E n chtung d e S che he t an o de ungen des Minde ts anda s umse zen	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st		Die E n chtung MUSS die i enti i ie ten dien t ich n Da en den na h o genden Katego ien zuo dnen – K tego ie 1 P i at- Diens - Bet ebs- und Gesc ä sgehe mn sse gemäß St a ge etzbu h (S GB) §§ 203 und 353b – K tego ie 2 pe sonenbe ogene Daten gemäß D tens hutz G undve o dnung D GVO) A t 4 N 1 – K tego ie 3 Ve sch us sachen gemäß Ve s hlu ssa henanweisu g - VSA – K tego ie 4 ons ige Daten wede K tego ie 1 noch 2 och 3)	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	g	Die E n chtung KANN ie iden i iz e en diens l chen Daten den Ka ego en 1 2 und 3 g ei hzei ig zuo dnen	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	h	a ls Da en den Ka ego en 1 2 ode 3 zugeo dnet wu den D e in ch ung MUSS ü die id nti i ie ten dien t ichen Da en d ese K tego ien die Gehe m- und Date schu zaspe te ow e An o de ungen h ns cht i h P iv t- D enst Bet ieb - und Ge chä tsgeh imnis e e m t eln und aus di sen gg en s ehende we te e An o de ngen ble ten	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	h i	Die E n chtung MUSS Ri iken ie aus de kün t gen Nu zung des exte nen Cloud Diens es ent tehen können um ssend e mi te n u d bewe en Die Ein i htung MUSS ie e mi te ten Ri iken gemäß de in de St a egie ü die Clou -Nutzu g est eleg en ich l nie zu R s koana yse	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	h i	Die E n chtung DAR den exte nen Cloud Dienst NUR nut en wenn a le e m tt lten R s ken gemäß de in de St at gie ü d e Cloud N tzung gena nten Ri htl n e u Ris koan lyse wi ksam ve m eden ode hin eiche d eduz e t ode n Übe ein t mmung m t den R s koak eptan k te en	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	h i	Die E n chtung DAR den exte nen Cloud Dienst NUR nut en wenn a le e m tt lten R s ken gemäß de in de St at gie ü d e Cloud N tzung gena nten Ri htl n e u Ris koan lyse wi ksam ve m eden ode hin eiche d eduz e t ode n Übe ein t mmung m t den R s koak eptan k te en bei de C oud-Nu zung get agen we den können	
NCD 2 1 03	iche hei skonz pt ü den xte nen C oud-Die st	i	Die E n chtung MUSS p ü en ob sie wei e en An o de ungen (z B aus Ges tzen Ve o dnun en Bes hlüs en o e ande en Quel en) unte l egt d e hin ich l ch de Clo d-Nutz ng ele ant s nd Die e An o de ungen MUSS d e E n ch ung einha ten ie we den im Üb ig n du ch die en M ndes st nda d n cht be üh t	
NCD 2 1 04	Not a l- und Kont nui ätsmanagement	a	Die E n chtung MUSS bewe ten we che Bedeutung de e te ne C oud-D enst n Not ä len und K sen itu t onen e nnehmen wü e	
NCD 2 1 04	Not a l- und Kont nui ätsmanagement	b	Die E n chtung MUSS p ü en ob sie n Not ä len und K sens tua ionen wei e au den exte nen	
NCD 2 1 04	Not a l- und Kont nui ätsmanagement	c	Die E n chtung MUSS die zu tänd gen Not a lb au t ag en en sp echend einb nden D ese MÜ SEN p ü en ob s ch die C oud-Nut ung au M ßnahmen die Not äl en nd K is nsi uat onen p vent v nd ode e kt v entgegenwi ken uswi kt und nwie e n die e Maßnahmen gg anzup ssen s nd Die E n chtu g MUSS die e Ände ungen vo de C oud-Nut ung umse zen	OPS 2 2 A11
NCD 2 2 01	Umset ung de iche hei san o de ungen	a	Die E n chtung MUSS vo Ve t ag absc luss bewe en nw e e n de exte ne C oud-D enst d e n ih e S che he ts cht in e es gele ten Si he he ts n o de ungen (iehe NCD 2 1 02 Buch tabe a) e ül t	
NCD 2 2 01	Umset ung de iche hei san o de ungen	b	Die E n chtung MUSS die E ül ung die e S che he t an o de ungen be eits n de e stu gsbes h e bung des exte nen C oud-D ens es ein o de n	OPS 2 2 A8
NCD 2 2 01	Umset ung de iche hei san o de ungen	c	Die E n chtung MUSS die Angaben und Nachwei e des C oud-D ens eanbie e s zu Buch tabe a hi si ht ich nhalt Auss gek a t Na hvol z ehba eit Aktua i ät nacht i ige Re elungen sow e M twi kung p ich en und Maßnahmen auswe en Dazu SO E de eit aden mit Che kl ste zu Auswe ung eine Be i hte ta tung nach BSI C5 ve wendet we den	
NCD 2 2 01	Umset ung de iche hei san o de ungen	d	Die E n chtung MUSS s ch ie ege m ßige Vo age von Si he he ts achwei en vom Cloud-Dien teanb ete us che n assen	
NCD 2 2 01	Umset ung de iche hei san o de ungen	e	Die e iche hei sna hwe se SO T N minde tens – die angemes ene und wi ksame E ü ung de Bas sk te ien nach C5 – die ak uel e Do umen at on de Sys embe ch e bung – die Aktu l tät von ve t agl ch zuge ic e ten Ze ti z e ungen und Be chte s at ungen ow e – die o dn ngsgemäße Du ch üh ung von Date si he ungen und e p obten Rück ic e ungen um as en und KÖNNEN vom Cloud Diens eanb ete du ch die ege mäßige Be ei ste lung e ne ak uel en 5-Be ich e tat ung vom Ty 2 e b a ht we den	
NCD 2 2 01	Umset ung de iche hei san o de ungen		Die E n chtung MUSS die S che he t nachwei e des C oud-D ens eanbi te s au we ten und even uel en Un la hei en und nsbesonde e da n usgewie ene Abwe chungen in gee gnete o m nachgeh n Hie bei MUSS d e Ein ich ung auch abwägen ob und inw e e n e n R s ko ent teht und wie m t d esem umzugehen i t	
NCD 2 2 01	Umset ung de iche hei san o de ungen	g	In besonde e MÜSSEN Ze i ik te P ü be ch e und Nachwe se den eit aum in dem d e E n chtung den Cl ud-Die st nut t ewe ls ol stä dig abdec en und DÜR EN KEINE ze t i hen ü ken en ha ten ode ent tehen l ssen D es MUSS d e in ich ung in ih e	
NCD 2 2 01	Umset ung de iche hei san o de ungen	h	Die E n chtung MUSS s ch ie Einh l ung o ge ehene und ve e nba e P o esse sowie d e Du h üh ng on Aud ts Si he he tsp ü ungen Penet at onst sts und Schwac ste len naly en	
NCD 2 2 01	Umset ung de iche hei san o de ungen	i	Die E n chtung MUSS e mi te te Ri iken d e ni ht be e ts du h B si k te ien nach C5 abgede kt s nd übe zu ät l che An o de ungen d e vom C oud-D enstea bie e zu e ü l n s nd abd cken ode d ese Ris ken t ans e e en ode akze tie en und MU S d es ent p echend dokument e en	
NCD 2 2 01	Umset ung de iche hei san o de ungen	i i	Die E n chtung MUSS die wei e en An o de ungen nach NCD 2 1 03 Bu hst be i in h e S che he t an o de ungen au nehmen Soweit d e in ch ung diese wei e en An o de ung n nu gemein am m t dem C oud-D ens eanbie e e ül en kann MUSS die Ein i htung d ese in die e stu gsbes h e bung bzw in das Ve t ag ve h lt is mit dem C oud-D ens eanbie e au nehmen	
NCD 2 2 01	Umset ung de iche hei san o de ungen	i ii	ü d e usä zl chen An o de ungen MUSS die E n i htung mit dem loud D ens eanb ete ve einba en dass d ese egelmäß g geeig ete N chweise h e an emes enen und wi ksamen Um etzung vo le t a s d e An o e ungen nu gemein am e ül t we den können e st ecken s ch die Nachwei e nu au den An eil de vom Cloud Dien teanb ete umgese zt wi d	
			Die E n chtung SO TE s ch eigene P ü e hte ve t ag i h us che n assen	
NCD 2 2 01	Umset ung de iche hei san o de ungen	j i	Die E n chtung MUSS die P ü e hte so ausge ta ten d ss die E n chtung h e weite en An o de ungen z B aus Ge etzen Ve o dnun en Bes hlüs en ode ande en Quel en) e ül t	
NCD 2 2 01	Umset ung de iche hei san o de ungen	j ii	Die E n chtung MUSS die P ü e hte so ausge ta ten d ss s e na h A t und Um ng e ne Bewe ung des om Cloud Dien teanb ete ü den bet achte en Cloud Dienst ebotenen In o mat ons iche hei sn veaus e mög i hen und d e E n ch ung selb t ode D t e n h em Au t ag (z B ande e te len e te ne T-Rev s on Wi scha t p ü e de) die P ü ec te wah nehmen können	
NCD 2 2 01	Umset ung de iche hei san o de ungen	j i i	So e n de Cloud Dien teanb ete einen P ü be cht na h C5 vo legen kann MUSS s ch die E n chtung vom Cloud Diens eanb ete da u be ech igen l ssen d e P ü ung n ch C5 du ch D t e se bst beau t agen zu können	
NCD 2 2 01	Umset ung de iche hei san o de ungen	j iv	Au g und de E ge nis e a s de D tenka ego s e ung und Ri iko naly e KANN die E n chtung n beg ündeten ä len au e gene P ü ech e e z cht n soweit we te e An o de un en z B us Gese zen Ve o dnungen esch üssen ode ande en Que l n) nich entgegen tehen	
NCD 2 2 02	Umgang m t Un e au t gnehme n und ande en xte nen D t en	a	Die E n chtung MUSS s ch om Clo d-Dien teanb ete ol st ndig benennen l ssen we che se ne Unte au t agne me gemäß C5 als Subd ens le s ungsun e nehmen anz sehen sind und au wel he A t und in we chem Um ng e iese n d e e e ts el ung des Cloud Diens es ei bezieht	OPS 2 2 A9
NCD 2 2 02	Umgang m t Un e au t gnehme n und ande en xte nen D t en	b	Die E n chtung MUSS m t dem C oud-D enste nbie e ve e nba en dass e de in ch ung beabs ch ig e Ände ungen an ve t ag i hen Ve ein a ungen mit Subd ens le st ngsunte nehmen die n d e Be e ts el ung des Cloud Dien tes in olv e t ind un e zü l ch sch i l ch ode pe E-	
NCD 2 2 02	Umgang m t Un e au t gnehme n und ande en	b i	Die e Mi te lung SO TE ze tl ch vo Umset ung de Ände ung e ol en	
NCD 2 2 02	Umgang m t Un e au t gnehme n und ande en xte nen D t en	b i	De Cl ud-Die steanb ete MUSS de E n chtu g nsbe onde e m t ei en wenn e estehende Ve t ag ve hä tn s e beendet de neue Ve t agsve hä tni se m t Subd enst e stung unte nehmen e ngeht Ve t agsve hä tn sse in d esem S nne sch ießen a le m t el enden Dok men e und Rege ungen wie z B e stun ssche ne D enst üteve einba ungen ode A lgemeine Ges hä s- und Ein au sb dingun en e n	
NCD 2 2 02	Umgang m t Un e au t gnehme n und ande en xte nen D t en	c	Die e Mi te lun en KANN e Cloud Diens eanb ete z B übe nte ne po ale ode Pu h-Benach i ht gungen be e t tel en wenn die E n chtung d ese An o de ungen a s e ü l ans eht	
NCD 2 2 02	Umgang m t Un e au t gnehme n und ande en xte nen D t en	d	a ls de C oud-D ens eanbie e Subd enst e stung unte nehmen e nbez eht ode ande we t g wesent i he ei e de ntwi klung ode Be ei ste l ng des C oud-D ens es an Un e au t agnehme aus age t MUSS si h d e Ein i htung vom C oud-D ens eanbie e zu iche n as en dass - die Subd enst ei tung unte nehmen und Unte au t agnehme d e w schen de E n ch ung u d dem C oud-D enst anbie e ve t a l ch es gele ten Vo gaben eben al s e ül en u d - si h d e P ü ech e die de C oud-D enst anbie e de E n chtung zu esi he t hat au h au d e Subd enst e stung unte nehmen und Unte au t agnehme des C oud-D enste nbie e s bez ehen	
NCD 2 2 03	Ge ich sba eit	a	Die E n chtung SO TE zu Abs che ung de Ve ü ba ke t a s Teil de In o mat onss che heit Ve e nba ngen ussc l eßl ch nach deut chem Re ht und deu sch m Ge cht stand und ohne ob iga o sch vo ab u bet e bende Sch ich ungs e h en absc l eßen	
NCD 2 2 03	Ge ich sba eit	b	Die E n chtung MUSS be ü ksi ht gen da s bei gegebenen al s notwend gem Rech ss hutz bez ehungswe se Eil e hts chutz Ze tve lu te eint e en önnen in besonde e du ch eine E na be tung n emde Re htso dnungen ode e n Au t eten vo ent e nt g legenen Ge ch en	
NCD 2 2 03	Ge ich sba eit	c	Die E n chtung MUSS beim Ve hande n des Ve t ages s che te len d ss s e ha dlungs äh g ble bt	
NCD 2 2 04	okat on de Da enve a bei ung	a	Die E n chtung MUSS p ü en ob die dien t ich n Da en n den ve t gl ch zuge iche ten ok ti nen ve a b ite we den dü en H e u MUSS die E n chtung d e E gebn sse de Daten atego i ie ung nd de R s koana yse d s mög i he R s ko eines emdsta tl chen Zug i s (z B du h Na h chtend ens e ode E mi tungsbehö den) sowie wei e e An o de ungen (z B aus Gese zen Ve o dnungen Besch üssen ode an e en Q el en) bewe ten	
NCD 2 2 04	okat on de Da enve a bei ung	b	Die E n chtung MUSS sämt iche o at onen an denen de Clou -Dien teanb ete m t dem Clou -Dien t dien t iche Da en peic e t und ve a be tet ve t ag i h est egen Dabe MUSS d e E n chtung au h Da ens che u gen be ück ich i en da die e gg an D t loka ionen du chge üh t we den	OPS 2 2 A9
NCD 2 2 05	Mel ep icht s che eits e evante Vo ä le	a	Die E n chtung MUSS die P i hten des Clo d-Dien teanb ete s iche hei s elevan e Vo ä e (ow e gg nde e Vo äl e) gegenübe de Ein ich ung zu me den ve t agl ch ege n	
NCD 2 2 05	Mel ep icht s che eits e evante Vo ä le	a i	Die E n chtung MUSS beim est egen von Ve t ags t a en und Ha t ngs agen au e n angemess nes Ve hä tn s um e m tte ten Sch tzbeda de mit dem C oud D enst e a bei eten di nst i hen Da en achten	
NCD 2 2 05	Mel ep icht s che eits e evante Vo ä le	a i	Be m es legen von Ve t ag st a en und Ha ungs egelun en ind die aus echt i he Si ht zu äss gen G en en u be ücks ch igen Die Ein i htung SO TE ei de Anse zung von %	
NCD 2 2 06	Bee digung des Ve t agsve häl nisses	a	Die E n chtung MUSS dem Anwendungs al angem ssene Künd gungs sten e t egen	OPS 2 2 A9
NCD 2 2 06	Bee digung des Ve t agsve häl nisses	b	Soweit ech l ch mög i h MUSS d e Ein ich ung ku z s ige e nsei i e Künd gung - ode Zu ückbeha tungs ech e an den e s ungen zu as en de Ein ic tung aus chl eßen	
NCD 2 2 07	Reg lung de D ten ü kgabe u d Daten öschung	a	Die E n chtung MUSS m t dem C oud-D enste nbie e ve t ag i h ege n w e die e die m t dem Cl ud-Die st ve a be teten d enst chen D ten nach Beend gung de Nutzung an d e E n ch ung übe ibt z B i ten Da en o mat Datent ä e P otoko le)	
NCD 2 2 07	Reg lung de D ten ü kgabe u d Daten öschung	b	Die E n chtung MUSS m t dem C oud-D enste nbie e ve t ag i h ege n w lche Maßnahmen di se zu öschung de d enst chen D ten du h üh t Dabei MUSS die E n chtung iche st l en dass d e Maßn hmen dem zu o e mi te ten Schu zbeda entsp echen	OPS 2 2 A9
NCD 2 3 01	inb ndung n d s SMS	a	Die E n chtung MUSS den xte nen C oud-D enst n h e genes In o mat onss che hei s-m nagements stem I MS) e nbin en	OPS 2 2 A12
NCD 2 3 01	inb ndung n d s SMS	b	Die E n chtung MUSS die im C5-Be i ht genann en ko e pondie enden Kont o en ü Cloud-Kunden n ih em I MS ein i hten D e in ich ung SO TE da übe h naus die im C5 esch iebenen ko espond e end n K i e en ü Kunden be üc si ht gen	
NCD 2 3 02	Au we tung von Siche hei snachwe sen	a	Die E n chtung MUSS die Nachwei e u d s nst ge Be chte des C oud-D enstea bie e s	OPS 2 2 A13
NCD 2 3 02	Au we tung von Siche hei snachwe sen	a i	Die e DÜR N übe den Nutzu gsze t aum KE NE ei l chen ücken en hal en	
NCD 2 3 02	Au we tung von Siche hei snachwe sen	b	Die E n chtung MUSS p ü en ob es ges el ten Unkla he ten du ch Wah nehmung de zuge i he ten P ü - und Kont oll e hte nachzu ehen st	
NCD 2 3 03	P ü ung de e stungs äh gkeit	a	Die E n chtung MUSS m ndes ens jäh l ch die e st ngs higke ten h e genen IT In a t u tu wie Pe o mance de Netz nbindung und - e b ndungen vo dem Hinte g nd de Nu zung des Cl ud-Die stes beu te len	
NCD 2 3 03	P ü ung de e stungs äh gkeit	b	Die E n chtung MUSS gg au t ete de Abwei hungen bewe ten und au d ese du ch gee gnete Annas ungen an de eigenen T- n ast uktu u d Net anbi dung eag e en	
NCD 2 3 03	P ü ung de e stungs äh gkeit	c	Die E n chtung MUSS m ndes ens jäh l ch die e st ngs higke ten des C oud-D enste nbie e s und des Cloud Dien tes sowie de Net ve b ndung zum C oud-D ens eanbi te beu tei en	OPS 2 2 A12
NCD 2 3 04	n o ma ion p ich en	a	Die E n chtung MUSS nachha ten dass de C oud-D enste nbie e se nen ve t ag ichen In o mat onsp l ch en tets na hkommt Dies g lt nsbe onde e bei - eine E ng iede ung des Cloud Diens eanb ete s n ein ande es U te nehmen ode ei en ande en Kon e n ode n s nst gen äl en des Wec sels des wi t cha l chen E gentums an ihm - einem Au tau ch von Un e au t agnehme n ode D t en sie e h e zu au h NCD 2 2 02)	
NCD 2 3 04	n o ma ion p ich en	b	Die E n chtung MUSS Me dungen des Clou -Dien teanb ete s übe e evan e S ö un en und Cybe -Ang i e dokumen ie en und au diese gemäß de ve e nba ten M twi kungsp l ch en n ch NCD 2 2 01 Buch tabe c eag e en	
NCD 2 3 05	Mul i- ak o -Au hent sie ung	a	Bi tet de ex e ne Clo d-Dien t eine Mul i- akto -Au hent sie ung ü Anmeldun en v n Benut enden (og in) n SO E d e Ein ic tung die e nu zen	
NCD 2 3 05	Mul i- ak o -Au hent sie ung	b	Bi tet de ex e ne Clo d-Dien t eine Mul i- akto -Au hent sie ung ü Anmeldun en v n Benut enden m t p vi eg e ten Re hten (o -i) wie bspw zu Adm nist a ion an MU S d e E n chtung d ese nutz n	
NCD 2 4 01	Da en üc gabe bei Beend gung	a	Die E n chtung MUSS p ü en ob de Cloud Dien teanb ete a le d enst chen D ten in de	OPS 2 2 A14
NCD 2 4 01	Da en üc gabe bei Beend gung	a	Die E n chtung MUSS p ü en ob de Cloud Dien teanb ete a le d enst chen D ten in de ve einba ten o m zu ü k he gehen hat	OPS 2 2 A15
NCD 2 4 02	Da enlö chung bei Bee digung	a	Die E n chtung MUSS s ch om Clo d-Dien teanb ete ie gem NCD 2 2 07 e o gte ös hung al e di nst i hen Da en e nsch ieß i h o handene Da ens che ungen bes ät gen la sen Dies um as t die Bes ät gung d ss die d enst i hen Da en gemäß de ve t ag ich ve einba ten Ve ah en ge öscht wu den	OPS 2 2 A14
NCD 2 4 02	Da enlö chung bei Bee digung	b	Die Bes ät gung nach Buch tabe a MUSS au h D ten und Da ens che ungen ei mög chen Unte au t agn hme n z B Su diens le s ungsun e nehmen) und ande en ex e nen D tten um as en	OPS 2 2 A14
NCD 2 4 02	Da enlö chung bei Bee digung	c	Die E n chtung MUSS die du h den C oud-D enste nbie e bes ät gte Daten ös hung	OPS 2 2 A14
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	a	Die E n chtung MUSS s che te len da s die M tnu zung mit de e genen St ate ie ü d e C oud-Nutzu g s ehe NCD 2 1 01) ve ein a i t	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	b	Die E n chtung MUSS die S che he t an o de ungen na h NCD 2 1 03 B chs aben d b s i umset en und e nhal en	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	c	Die E n chtung MUSS e mi te n an we chen ok ti nen mit dem exte nen loud D enst di nst i he Da en e a bei et we den D es sch ießt au h D tens che ungen sowie o e n gegeben Unte u t agnehme und Subdie st ei te des C oud-D enste nbie e s ein	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	c i	Die E n chtung MUSS bewe ten ob d e diens l chen Daten an d esen oka ionen ve a be tet	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	c i	ü d ese Bewe tung MUSS die E n chtung nsbesonde e die E ebnis e de D tenka ego s e ung sowie so e n egeben wei e e An o de ungen z B aus Ge etzen Ve o dnun en Bes hlüs en ode ande en Que len he anz ehen	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	d	Die E n chtung MUSS e mi te n w lche Rech e an den d enst i hen D ten dem C oud-Dien teanb ete o e D i ten du h d s A zept e en de vom Cloud Diens eanb ete vo gegebenen Al gem inen Geschä t bedingu gen AGB) Da enschu ze klä ung ode sons i en	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	d i	Die E n chtung MUSS bewe ten ob d ese Rech e mit d n e genen Si he he ts n o e ungen d e s e n de Si he he ts i ht in e und dem e genen S che he t konzept de in e t h t ve einba sind	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	d i	Die E n chtung MUSS in besonde e d e Nu zungsb dingun en und d e Da enschu ze klä ung des Cl ud-Die steanb ete s auswe en	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	e	Die E n chtung MUSS bewe ten ob und wie die d enst chen D ten im xte nen C oud-D enst ve sch üsse t zu spe che n s nd ü d e ansch i ßende Bewe tung SO E d e Ein ic tung die id nti i ie ten Ri iken mit de e genen St ateg e ü d e C oud-Nu zung (iehe NCD 2 1 1)	OPS 2 2 A17
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	e i	Die E n chtung MUSS dann bewe ten b d e Ve sch üs elung mit den An o de ungen aus den E ebni sen de Datenk tego is e ung ve einba ist	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	e i	I t die vom C oud-D ens eanb te e ngese zte Ve chlü se ung n chtig eignet MU S d e E n chtung d e n ob n an de e ande e [illegible]	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste		Die E n chtung MUSS e hebe n w e und wann Daten du [illegible]	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	g	Die E n chtung MUSS e mi te n ob ü d e Mi nutz ng [illegible]	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	g i	Die E n chtung MUSS bewe ten ob d e [illegible]	
NCD 2 5 01	Mi nut ung ex e ne C oud-D enste	g i	I t ein Zug i [illegible]	