Strategische Initiative SI-4 Hybrid Multi Cloud
WTO-20007 Beschaffung Public Clouds

Aktueller Stand Umsetzung Befunde des EDÖB aus dem Review zu den Ausschreibungsunterlagen WTO-20007 Beschaffung Public Clouds Bund in der weiteren Umsetzung der Cloud-Strategie 2022 ff.

Ausgabe: 10. Januar 2022 (Stand Ende 2021)

1 Abkürzungsverzeichnis

DSG	Datenschutzgesetz
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
IAM	Identity and Access Management
IEC	International Electrotechnical Commission
ISDS	Informationssicherheits- und Datenschutzkonzept
ISMS	Information Security Management System
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
RZ	Rechenzentrum
SCHUBAN	Schutzbedarfsanalyse
SOC	Service Organization Control

2 Ausgangslage

In einer ersten Phase wurden mit der WTO-20007 Beschaffung Public Clouds Bund die beschaffungsrechtlichen Grundlagen gelegt, damit die Bundesverwaltung in Erfüllung der Cloud-Strategie des Bundesrates Zugang zu den neuesten Technologien gem. Anforderungen erlangt. Um sicherzustellen, dass für die aktuellen und zukünftigen Bedürfnisse der Bundesverwaltung moderne Cloud-Technologie erschlossen wird, wurden gemäss einer von GARTNER (G00352196) abgeleiteten Definition 24 von 32 möglichen Funktionalitäten verlangt (siehe auch Technische Spezifikation TS05 der Ausschreibung).

Die Beschaffung stellt einen Rahmen dar, in dem unter gewissen Bedingungen Leistungen bezogen werden können. Zu diesen Bedingungen gehören insbesondere auch Anforderungen an die Kritikalität und den Datenschutz. Diese sollen beispielsweise mittels Datenschutzfolgeabschätzung vor dem Bezug umgesetzt werden.

Im Rahmen der Prüfung zur Erstellung der Ausschreibungsunterlagen WTO-20007 Beschaffung Public Clouds Bund gab es sieben Befunde des EDÖB.

Da im gesamten Themenkomplex Public Clouds die Themen Sicherheit und Datenschutz äusserst wichtig sind, werden die Massnahmen aufgrund der Befunde des EDÖB regelmässig getrackt. Diese Massnahmen sind technischer, organisatorischer und vertraglicher Natur und werden in den weiteren iterativen Projektphasen umgesetzt. Diese drei Massnahmentypen unterstützen die geordnete und sichere Nutzung von Public Clouds und helfen, allfällige Risiken zu mitigieren.

3 Befunde

3.1 Nachweis Scope der Verifzierung

Befund des EDÖB:
Nachweis des Scope der Zertifizierung wichtig!

Änderungsvorschlag des EDÖB:
Nachweis: Der Zertifizierungsbereich (Scope) der Zertifizierung

Aktueller Stand:
Mit dem Eignungskriterium EK04 wurden in den Ausschreibungsunterlagen die folgenden Zertifizierungen (oder äquivalente) für einen Teil des Serviceangebotes verlangt:

i. SOC 1 Type II
ii. ISO/IEC 27001 (ISMS)
iii. ISO/IEC 27017 (Cloud Security)
iv. ISO/IEC 27018 (Cloud Privacy)

Ein Nachweis einer pauschalen Zertifizierung über sämtliche Dienste eines Anbieters (Hyperscaler) wird nach wie vor als unrealistisch und sehr komplex eingeschätzt. Dies vor allem auch aufgrund der Tatsache, dass je nach Anbieter, das Serviceangebot aus ca. 210 bis 270 Services besteht.

Anforderungen sind daher in konkreten Umsetzungsprojekten der jeweiligen Verwaltungseinheiten im Vorfeld aufzunehmen. Wird dabei ein spezifisches Zertifikat für einen spezifischen Service verlangt, so ist dies bspw. in der Lösungsarchitektur entsprechend zu berücksichtigen.

3.2 Anforderungskatalog: Privacy gemäss NIST

Befund des EDÖB:
Privacy gemäss NIST aufnehmen: Cloud-Anbieter sollten die gesicherte, ordnungsgemäße und konsistente Sammlung, Verarbeitung, Kommunikation, Nutzung und Disposition persönlicher Daten (PI) und personenbezogener Daten (PII) im Cloud-System schützen.

Änderungsvorschlag des EDÖB:
Security and Compliance

1. Audit Trail
2. Identity & Access Management (IAM)
3. Security
4. **Privacy**
5. Vulnerability Assessment

Aktueller Stand:
Die Rückmeldungen des EDÖB für die Abschnitte 3.2, 3.4, 3.5 und 3.6 bedürfen Massnahmen in der weiteren Umsetzung der Cloud-Strategie der Bundesverwaltung. Diese Massnahmen können organisatorischer-, technischer und/oder vertraglicher Art sein.

Der vorliegende Stand gilt zusammenfassend für die thematisch überlappenden Rückmeldungen unter Abschnitt 3.4, 3.5 und 3.6.

Die Sicherstellung des Datenschutzes ist, je nach Liefermodell, in geteilter Verantwortung zwischen dem Cloud Nutzer und dem Cloud Anbieter (Shared Responsibility Model für die Cloud Liefermodelle IaaS, PaaS und SaaS).

Der Punkt «Privacy» wurde bereits in den Ausschreibungsunterlagen mittels Eignungskriterium EK04 als Muss-Kriterium und somit mit höchster Priorität verankert.

Damit verbundene Vorgaben und zu treffende Massnahmen auf Seiten Cloud Nutzung in der Bundesverwaltung werden im Rahmen der weiteren Umsetzung der Cloud-Strategie erarbeitet.

Weitergehende Arbeitspakete / Streams (vertragliche-, technische- und organisatorische Massnahmen) sind vorgesehen und geplant:

i. Rahmenvertragsverhandlungen (= vertragliche Massnahmen)
ii. Cloud Operating Model und Cloud Service Broker der Bundesverwaltung (= organisatorische Massnahmen)
iii. Sourcing Kriterien beim Bezug, d.h. Kriterien wenn Leistungen intern erbracht werden und wenn Leistungen outgesourct werden (= organisatorische Massnahmen)
iv. Bereitstellung von z.B. Landing Zones, SCHUBAN / ISDS, Lösungsmuster, Lösungsarchitekturen, etc (= technische Massnahmen) durch die Cloud Service Broker
v. Abrufprozess, von Leistungen durch die Leistungsbezüger inkl. Datenschutzfolgeabschätzung (= Vorgaben)
vi. Verabschiedung von Cloud-Prinzipien (= Vorgaben)
vii. Bericht zu Rechtsklarheiten und Rechtssicherheit

3.3 Datenschutzverordnung aufnehmen

Befund des EDÖB:
Datenschutzverordnung bitte noch aufnehmen

Änderungsvorschlag des EDÖB:
Bundesgesetz und Verordnung über den Datenschutz (DSG, SR 235.1 und VDSG SR 235.11) und die Datenschutz-Grundverordnung der Europäischen Union (DSGVO)

Aktueller Stand:
In den Ausschreibungsunterlagen wurde bereits mit dem Zuschlagskriterium ZK03 verankert, dass das «Swiss Transborder Data Flow Agreement for outsourcing of data processing» Vertragsbestandteil ist respektive unterschrieben wird.

Ob die genannten Bundesgesetze und Verordnungen bspw. im Mechanismus des Abrufprozesses von Leistungen als Muss-Kriterium verankert werden könnten, wird im Rahmen des Arbeitspaketes «Abrufprozess» geprüft.

Der Abrufprozess wird als mögliches Instrument in Betracht gezogen, um die Konformität zu Bundesgesetzen und Verordnungen zu gewährleisten. Weitere Instrumente könnten dabei auch sein:

i. Sourcing Kriterien (siehe 3.2)
ii. Bereitstellung von Landing Zones (siehe 3.2)
iii. Cloud Prinzipien (siehe 3.2)

Das geeignete Instrument wird in den weiteren Arbeiten geprüft. Denkbar ist auch eine Kombination aus den genannten Instrumenten.

3.4 Serviceskatalog: Privacy gemäss NIST

Befund des EDÖB:
Privacy gemäss NIST aufnehmen: Cloud-Anbieter sollten die gesicherte, ordnungsgemässe und konsistente Sammlung, Verarbeitung, Kommunikation, Nutzung und Disposition persönlicher Daten (PI) und personenbezogener Daten (PII) im Cloud-System schützen.

Änderungsvorschlag des EDÖB:
Zeile "Privacy" hinzufügen unterhalb Zeile "Security"

Aktueller Stand:
Siehe Abschnitt 3.2.

3.5 Serviceskatalog: Privacy gemäss NIST

Befund des EDÖB:
Privacy gemäss NIST aufnehmen: Cloud-Anbieter sollten die gesicherte, ordnungsgemässe und konsistente Sammlung, Verarbeitung, Kommunikation, Nutzung und Disposition persönlicher Daten (PI) und personenbezogener Daten (PII) im Cloud-System schützen.

Änderungsvorschlag des EDÖB:
Der Anbieter verfügt über Services, die es ermöglichen, Datenschutzregeln des Bedarfsträgers zu überprüfen und bei Abweichungen vom erforderlichen Zustand Aktionen (z.B. Notifikationen) auszulösen

Der Anbieter bietet die Möglichkeit, Kontrollrechte des Bedarfsträgers sowie unabhängiger Aufsichtsbehörden zu definieren

Der Anbieter ist in der Lage, regelmässige Kontrollen seiner Cloud-Infrastruktur nach internationalen Audit Standards vorzunehmen und die Prüfberichte dem Bedarfsträger und der zuständigen Datenschutzaufsichtsbehörde auf Verlangen vorzulegen.

Aktueller Stand:
Siehe Abschnitt 3.2.

3.6 Begriffserklärung: Privacy gemäss NIST

Befund des EDÖB:
Privacy gemäss NIST aufnehmen: Cloud-Anbieter sollten die gesicherte, ordnungsgemässe und konsistente Sammlung, Verarbeitung, Kommunikation, Nutzung und Disposition persönlicher Daten (PI) und personenbezogener Daten (PII) im Cloud-System schützen.

Änderungsvorschlag des EDÖB:
Title:
Privacy

Description:
Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use, and disposition of personal information (PI) and personally identifiable information (PII) in the cloud system. PII is the information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Aktueller Stand:
Siehe Abschnitt 3.2.

3.7 Nutzen einer RZ Verteilung auf 3 Kontinente

Befund des EDÖB:
Was bringt der Bundesverwaltung eine Verteilung der RZ auf min. 3 Kontinente? Das schliesst möglicherweise Anbieter aus.

Änderungsvorschlag des EDÖB:
Der Anbieter verfügt über verteilte und redundante Rechenzentren an mindestens drei verschiedenen Standorten (inkl. Europäischem Wirtschaftsraum) und stellt seine Public Cloud Services darüber einer internationalen Kundschaft zur Verfügung.

Aktueller Stand
Die Schweiz ist im Ausland mit Botschaften, Generalkonsulaten und Kooperationsbüros sowie Missionen bei internationalen Organisationen präsent. Für diese weltweiten Vertretungen und Aufgaben sind Leistungen aus Rechenzentren ausserhalb Europas weiterhin ein Muss-Kriterium.

Eine Diversifizierung von Rechenzentren nach Wirtschaftsräumen o.ä. gilt es aufgrund der hohen Komplexität von Multi-Provider-Management auch weiterhin zu vermeiden.

Ferner muss es im Kontext ausserordentlicher Lagen (Pandemie, überregionaler Stromausfall grosser Stromnetze etc) und damit verbundenem Business Continuity Management und Disaster Recovery möglich sein, Leistungen und Betrieb auf mehrere Kontinente zu verteilen.