Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundeskanzlei BK
IKT-Standarddienste und Supportprozesse
SD Büroautomation/UCC

Rechtliche Grundlagen

Cloud-Enabling Büroautomation

Hermes

Inhalt

1 Ausgangslage 3
1.1 Grundsatz der geteilten Verantwortlichkeit 3
2 Rechtliche Grundlagen 4
2.1 Einsatz von Informations- und Kommunikationstechnik (IKT) 4
2.2 Sicherheitsvorgaben für IKT-Projekte 4
2.3 Datenschutz 5
2.3.1 Revision des schweizerischen Datenschutzrechts 5
2.3.2 Datenbearbeitung durch Bundesorgane 5
2.3.3 Outsourcing in eine Cloud 8
2.3.4 Datensicherheit 11
2.4 Informationssicherheit und Geheimhaltungspflichten 11
2.4.1 Informationsschutz durch Klassifizierung 11
2.4.2 Amtsgeheimnis 12
3 Bevorstehende Änderungen der Rechtsgrundlagen 12
3.1 Totalrevision Datenschutzgesetz und -verordnung 12
3.2 Teilrevision Cyberrisikenverordnung (CyRV) 13
3.3 Teilrevision der Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV) 13
3.4 Inkrafttreten BG über die Informationssicherheit beim Bund (ISG) 13
3.4.1 Grundsätzliche Neuerungen des ISG 13
3.4.2 Auswirkungen des ISG ab Inkraftsetzung für Cloud-Anwendungen 14
3.5 Vernehmlassung BG über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben 15
4 Fazit 15

1 Ausgangslage

Die Büroautomation unterstützt die Verwaltungstätigkeit mit geeigneten IKT-Mitteln, wie den Arbeitsplatzsystemen inkl. zugehörigen Kommunikations- und Kollaborationsservices, Smartdevices und Drucker.

Bei der Erarbeitung der neuen Strategie zur Büroautomation wurde schnell ersichtlich, dass die Möglichkeiten der Cloud-Nutzung von grosser Bedeutung für die Neuausrichtung der Büroautomation sind. Es wurde das Projekt Cloud Enabling Büroautomation (CEBA) gestartet. Im Rahmen dieses Projekts ist vorgesehen, sämtliche cloudbasierten Dienste von Microsoft 365 als Ergänzung zur bestehenden On-Premises Büroautomation den Verwaltungseinheiten zugänglich zu machen.

Die beschaffungsrechtlichen Grundlagen für eine Büroautomation mit Cloudnutzung wurde im März 2020 geschaffen. Die aktuellen Lizenzverträge laufen bis 31. Dezember 2022, mit einer Verlängerungsoption von 2 Jahren.

Die vorliegende Analyse widerspiegelt die Rechtslandschaft im Januar 2023. Sie wird bei Bedarf angepasst oder erweitert.

1.1 Grundsatz der geteilten Verantwortlichkeit

Der Bereich DTI der Bundeskanzlei und die Departemente teilen sich die Verantwortlichkeit in Bezug auf Datenschutz und Datensicherheit. Der Bereich DTI der Bundeskanzlei stellt dabei die standardisierten und zentralisierten IKT-Grundleistungen des digitalen Arbeitsplatzes mit den dazugehörigen Betriebs- und Supportprozessen und den IT-Grundschutz sicher.

Die Departemente und Verwaltungseinheiten (Leistungsbezüger) kennen die Daten, die Geschäftsprozesse sowie die Risiken und sie sind vertraut mit den für die jeweiligen Bereiche geltenden Gesetzen und Vorgaben. Sie sind für die Daten verantwortlich und müssen daher selber den Schutzbedarf der bestimmen. Die Verwaltungseinheiten bleiben auch bei Auslagerung der Datenverarbeitung bzw. durch Nutzung der Microsoft Services für ihre Daten sowie für den ausreichenden Schutz der Daten bei der Datenverarbeitung verantwortlich. Als Dateneigner müssen die einzelnen Verwaltungseinheiten durch angemessene Massnahmen den Schutz von Personendaten und anderen Informationen sicherstellen. Diese treffen die erforderlichen Regelungen unter Berücksichtigung der für den jeweiligen Bereich geltenden Gesetze und Vorgaben. Insbesondere muss dem Schutz von Personendaten und anderen schutzwürdigen Informationen Beachtung geschenkt werden. Die Verwaltungseinheiten prüfen nach eigenem Ermessen, ob die Sicherheitsmassnahmen des Standartdienstes Büroautomation für die von ihnen zu verantwortenden Daten ausreichen. Sollten die Verwaltungseinheiten zum Schluss kommen, dass eine Datenschutzfolgenabschätzung durchgeführt werden muss, sind die verwaltungsinternen Richtlinien einzuhalten. Sie können zusätzliche technische Massnahmen einsetzen sowie organisatorische Massnahmen umsetzen.

Die vorliegende Rechtsgrundlagenanalyse fokussiert sich somit nicht auf Daten, die mit Microsoft 365 theoretisch in der Cloud bearbeitet werden können. Dies ist aufgrund der geteilten Verantwortlichkeit Sache der Departemente und Verwaltungseinheiten. CEBA nimmt diese jedoch mit der Einsatzrichtlinie Microsoft 365 (E 031[1]) in die Pflicht, ihre Verantwortungen entsprechend wahrzunehmen.

[1] Link auf E 031, wenn in Kraft.

2 Rechtliche Grundlagen

2.1 Einsatz von Informations- und Kommunikationstechnik (IKT)

Gestützt auf Art. 43 und 47 RVOG[2] werden die Aufgaben und Zuständigkeiten bei der Steuerung und Führung des Einsatzes von Informations- und Kommunikationstechnik (IKT) in der Bundesverwaltung in der Bundesverwaltung (VDTI[3]) geregelt. Die Übergangsbestimmungen der VDTI sehen vor, dass für Stellen, die sich vor Inkrafttreten der VDTI durch Vereinbarung mit dem ISB gemäss Art. 2 Abs. 2 BinfV verpflichtet haben, die Bestimmungen der BinfV noch bis zum 31. Dezember 2023 weitergelten. Auch die IKT-Weisungen des Bundesrates, des Eidgenössischen Finanzdepartements und des ISB behalten ihre Gültigkeit, soweit sie der VDTI nicht widersprechen (Art. 36 Abs. 1 und 3 VDTI).

Nach dem Legalitätsprinzip setzt der Einsatz der IKT in der Bundesverwaltung voraus, dass hinreichende Rechtsgrundlagen bestehen oder geschaffen werden. Die Anforderungen an die Rechtsgrundlagen sind dabei davon abhängig, ob und welche Eingriffe in die Rechte des Bürgers damit verbunden sind.

Beim vorliegenden Projekt handelt es sich um die Weiterentwicklung der Büroautomation (BA), welche die Erfüllung von Bundesaufgaben unterstützt und für eine wirtschaftliche und nachvollziehbare Verwaltungstätigkeit notwendig ist. Mit dem Betrieb der BA sind keine Eingriffe in die Rechte Einzelner verbunden. Unter diesen Umständen kann für den Betrieb der BA direkt auf die Übertragung der entsprechenden Verwaltungsaufgaben abgestellt werden. Eine explizite Rechtsgrundlage ist damit nicht notwendig; dies gilt auch für die Auslagerung der BA in die Public Cloud. Bei der Auslagerung der Bearbeitung in die Public Cloud handelt es sich um eine Auftragsdatenbearbeitung (Microsoft ist Auftragsbearbeiter) im Sinne der Datenschutzgesetzgebung. Entsprechend sind die Datenschutzbestimmungen zu erfüllen. Die Rechtliche Grundlage für die Bearbeitung der Daten durch die Bundesverwaltung ergeben sich aus Artikel 57h RVOG. Die Datenschutzbestimmungen werden mit den Ergänzungen zu SCC und Anerkennung der CH DSG erfüllt.

2.2 Sicherheitsvorgaben für IKT-Projekte

Inhaltlich sieht die CyRV vor, dass für alle IKT-Schutzobjekte (Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der IKT) die minimalen Sicherheitsvorgaben (IKT-Grundschutz[4]) umzusetzen und eine Schutzbedarfsanalyse (Schuban)[5] durchzuführen ist (Art. 14b und 14c CyRV). Das ISDS-Konzept legt die nötigen Angaben zur Erhaltung und Verbesserung der Informationssicherheit und des Datenschutzes fest. Für die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen wird im Rahmen des ISDS ein Bearbeitungsreglement erstellt[6]. Falls sich im Rahmen der Schuban ein erhöhter Schutzbedarf zeigt, so sind zusätzliche Sicherheitsanforderungen zu ergreifen, d.h. es ist ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) mit Risikoanalyse zu erstellen[7] und/oder ein RINA-Prozess[8] zu durchlaufen (Art. 14d CyRV). Bei einem Schutzobjekt, das kritische Geschäftsprozesse unterstützt, ist zudem ein Notfallkonzept zu entwickeln[9]. Die Sicherheitsdokumentationen haben eine Gültigkeit von höchstens fünf Jahren (Art. 14e CyRV). Diese Vorschriften zur IKT-Sicherheit in der

[2] Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG; SR 172.010).
[3] Verordnung vom 25. November 2020 über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (Verordnung über die digitale Transformation und die Informatik, VDTI; SR 172.010.58).
[4] IT-Grundschutz in der Bundesverwaltung (NCSC).
[5] Beurteilung des Schutzbedarfs (NCSC).
[6] Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) (NCSC) | Bearbeitungsreglement
[7] Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) (NCSC)
[8] RINA = Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung.
[9] Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) | Notfallkonzept

Bundesverwaltung werden künftig teilweise im Informationssicherheitsgesetz (ISG), das derzeit noch nicht in Kraft ist (siehe dazu 3.4), verankert werden[10].

Gemäss der unterzeichneten Schuban des Projekts CEBA gibt es keinen erhöhten Schutzbedarf, da keine besonders schützenswerten Personendaten in der Public Cloud bearbeitet oder gespeichert werden. Die Bearbeitung solcher Daten erfolgt mit dem lokal installierten M365 und die Speicherung wird nach wie vor On-Premises sein. Das Projekt CEBA erstellte dennoch ein ISDS Konzept und eine Risikoanalyse.

In Bezug auf die Cybersicherheit enthält die Cyberrisikenverordnung weitere rechtliche Vorgaben, die auch für das Cloud Enabling Büroautomation massgebend sind. Grundsätzlich gilt, dass die Verwaltungseinheiten für die Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen in Bezug auf die Cybersicherheit in ihren Sektoren verantwortlich sind (Art. 14 Abs. 7 CyRV). Die Beschaffungskonferenz des Bundes (BKB) hat für Beschaffungen im IT-Bereich Musterklauseln der BKB betreffend Cyberrisiken verfasst[11]. Der Delegierte für Cybersicherheit hat gestützt auf Art. 11 Abs. 1 lit. e CyRV Vorgaben zur Netzwerksicherheit in der Bundesverwaltung[12] erlassen, die die Modalitäten für den Zugriff auf die Netzwerke festlegen.

Zur Umsetzung der Vorgaben zur IKT-Sicherheit wurde eine Schuban erstellt; das ISDS-Konzept wurde in der Phase Konzept durch den PAS CEBA abgenommen. Die IKT-Vorgaben des Bundes werden eingehalten, zu notwendigen Ausnahmen betreffend Netzwerkkommunikation werden Ausnahmen erstellt.

2.3 Datenschutz

2.3.1 Revision des schweizerischen Datenschutzrechts

Die 2017 eingeleitete Totalrevision des Datenschutzgesetzes hatte zum Ziel, das schweizerische Datenschutzrecht an das Niveau der EU (DSVGO) anzupassen und die modernisierte Datenschutzkonvention des Europarates (SEV 108) - dessen Änderungsprotokoll (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten) von der Schweiz am 30. Oktober 2019 unterzeichnet wurde - umzusetzen. Der Gesetzesentwurf wurde im September 2020 vom Parlament verabschiedet. Das revDSG tritt nach Überarbeitung der Verordnungen am 1. September 2023[13] in Kraft.

Im Zuge der Totalrevision des Datenschutzgesetzes wurde das Regelungskonzept des geltenden Erlasses beibehalten. Gleichzeitig wurden zahlreiche terminologische und inhaltliche Anpassungen an die DSGVO vorgenommen. Da die Grundsätze des geltenden Datenschutzgesetzes[14] im Wesentlichen ins revDSG überführt wurden, bilden die nachfolgend zitierten Bestimmungen des DSG weiterhin die massgebenden Leitlinien; auf abweichende Regelungen des revDSG wird punktuell hingewiesen.

2.3.2 Datenbearbeitung durch Bundesorgane

Organe des Bundes dürfen Personendaten bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Dabei ist die erforderliche Normstufe (Gesetz oder Verordnung) abhängig von der Art der bearbeiteten Daten (Art. 17 Abs. 1 DSG; Art. 34 revDSG). Als Personendaten

[10] Das ISG unterteilt in Anlehnung an die geltenden Regelungen drei Sicherheitsstufen, die fast gleich bezeichnet werden («Grundschutz», «hoher Schutz» und «sehr hoher Schutz»; Art. 17 ISG), siehe BBL 2020 9975.
[11] Mustervertragsklausel der BKB betreffend Cyberrisiken (PDF, 385 kB, 31.08.2020) (admin.ch).
[12] IT-Grundschutz in der Bundesverwaltung (NCSC).
[13] Totalrevision des Bundesgesetzes über den Datenschutz (DSG) (Bundesamt für Justiz)
[14] Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

gelten gemäss Art. 3 Bst. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

Bei der Bearbeitung von besonders schützenswerten Personendaten sind die Anforderungen an die erforderliche Normstufe erhöht und es braucht in aller Regel ein Bundesgesetz (Art. 17 Abs. 2 DSG). Besonders schützenswerte Personendaten gemäss Artikel 3 Buchstabe c DSG (Art. 5 Bst. d revDSG) sind Daten über:

- religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
- die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse o-der Ethnie,
- genetische Daten,
- biometrische Daten, die eine natürliche Person eindeutig identifizieren,
- verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
- Massnahmen der sozialen Hilfe.

Als *Datenbearbeitung* gilt jeder Umgang mit (besonders schützenswerten) Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren, Löschen) oder Vernichten von Daten (Art. 4 DSG). Datenbearbeitungen, die bisher erlaubt waren, werden grundsätzlich auch mit dem Inkrafttreten des revDSG erlaubt sein (vgl. Art. 6 revDSG).

Mit Art. 57h RVOG[15] wurde eine gesetzliche Grundlage für die Datenbearbeitung mit Geschäftserfassungssystemen innerhalb der Bundesverwaltung geschaffen. Gestützt auf Art. 57h Abs. 3 RVOG hat der Bundesrat die GEVER-Verordnung[16] zur Regelung der elektronischen Geschäftsverwaltung erlassen. Nach der GEVER-Verordnung ist jede Verwaltungseinheit für den Datenschutz in Bezug auf ihr Geschäftsverwaltungssystem verantwortlich. Die Geschäftsverwaltungssysteme müssen Zugriffe auf Informationen, Druck und Versand von Informationen sowie Änderungen an der Klassifizierung oder an den Zugriffsberechtigungen protokollieren (Art. 12 und 13 Gever-Verordnung).

Microsoft bearbeitet Metadaten, die im Rahmen der Nutzung von Microsoft 365 generiert werden. Dabei ist Microsoft als unabhängiger Datenverantwortlicher für die Nutzung und als solcher verantwortlich für die Einhaltung aller geltenden Gesetze und Verpflichtungen eines Datenverantwortlichen. Der Umfang sowie die Verwendung personenbezogener Daten hat Microsoft im Rahmen der Datenschutzbestimmungen festgehalten. Die Datenbearbeitung durch Microsoft erfolgt jedoch stets im Rahmen von Artikel 57h RVOG und den weiteren rechtlichen Grundlagen, eine weitergehende Bearbeitung ist Microsoft untersagt.

Microsoft führt regelmässig Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Rechenzentren, die Microsoft zur Verarbeitung von Kundendaten, Professional Services-Daten und personenbezogenen Daten nutzt, durch. Jede Prüfung wird entsprechend den Standards und Regeln der Aufsichts- oder Akkreditierungsstellen für die jeweils anwendbaren Kontrollstandards oder Rahmenbestimmungen durchgeführt. Jede Prüfung wird von qualifizierten, unabhängigen dritten Sicherheitsprüfern durchgeführt, die von Microsoft ausgewählt werden und für die Microsoft die Kosten trägt. Jede Prüfung führt zur Erstellung eines Prüfungsberichts („Microsoft-Prüfungsbericht“), den Microsoft unter https://servicetrust.microsoft.com/ oder an einem anderen von Microsoft angegebenen Ort zur Verfügung stellt. Der Microsoft-Prüfungsbericht ist eine vertrauliche Information von Microsoft und legt alle wesentlichen Feststellungen des Prüfers eindeutig offen. Microsoft behebt umgehend alle in einem Microsoft-Prüfbericht festgestellten Probleme zur Zufriedenheit

[15] Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (RVOG; SR 172.010).
[16] Verordnung vom 3. April 2019 über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung; SR 172.010.441).

des Prüfers. Auf Verlangen des Kunden stellt Microsoft dem Kunden jeden Microsoft-Prüfbericht zur Verfügung. Der Microsoft-Prüfbericht unter-liegt den Vertraulichkeits- und Verteilungseinschränkungen, von Microsoft und dem Prüfer.

Die Ergebnisse der Prüfungen werden durch die Bundesverwaltung geprüft und bei Bedarf Massnahmen ergriffen. Die Identitäts- und Zugriffsverwaltung Bund (IAM Bund) sorgt dafür, dass die richtigen Personen und Anwendungen zum richtigen Zeitpunkt den richtigen Zugriff auf Ressourcen der Bundesverwaltung erhalten. Die Datenbearbeitung im Rahmen der Identitätsverwaltungs-Systeme, der Verzeichnisdienste und des zentralen Identitätsspeichers wird in der IAM-Verordnung[17] geregelt, die sich neben der RVOG auch auf das Bundespersonalgesetz[18] stützt. Das IAM-System prüft als vorgelagertes System die Identität und bestimmte berechtigungsrelevante Eigenschaften von Personen, Maschinen und Systemen, die auf ein nachgelagertes System zugreifen wollen, und übermittelt das Resultat der Überprüfung an das nachgelagerte Informationssystem, damit dieses die Berechtigungen ermitteln kann. Der Verzeichnisdienst erfasst Informationen über Benutzerinnen und Benutzer von Infrastrukturen des Bundes, um damit die Personen zu identifizieren und die ihnen zugeordneten Geräte, Anschlüsse, Kontaktangaben und dergleichen zu verwalten (Art. 3 ff. IAMV). In den IAM-Systemen, den Verzeichnisdiensten und dem zentralen Identitätsspeicher dürfen Personendaten bearbeitet werden (Art. 11 Abs. 1 IAMV). Wird ein Informationssystem des Bundes von einem externen Betreiber im Auftrag des Bundes betrieben oder müssen für die Bundesverwaltung tätige Personen auf fremde Informationssysteme zugreifen, so dürfen die dazu notwendigen Personendaten aus Personalinformationssystemen, dem zentralen Identitätsspeicher oder IAM-Systemen automatisiert dem externen Betreiber bekanntgegeben werden (Art. 17 IAMV).Die bei der Nutzung der elektronischen Infrastruktur durch das Bundespersonal anfallenden Personendaten und deren Bearbeitung wird in Art. 57i ff. RVOG geregelt. Gestützt auf Art. 57q Abs. 1 RVOG hat der Bundesrat in der sog. Randdatenverordnung[19] die Zugriffsberechtigung, Aufbewahrungsdauer, Vernichtung sowie Auswertung dieser Personendaten geregelt. Bei der Aufbewahrungsdauer wird zwischen bewirtschafteten und nicht bewirtschafteten Daten unterschieden (Art. 4 f.); letztere sind im Prinzip rasch zu vernichten. Verantwortlich für Aufbewahrung und Vernichtung der Personendaten sind die Betreiberin der elektronischen Infrastruktur (in der Regel das BIT) sowie das Bundesorgan, das für den Datenschutz zuständig ist (Datenschutzberater/in) bzw. die Geräte nutzt (Art. 6).

Die notwendigen gesetzlichen Grundlagen bestehen, damit die Bundesorgane im Rahmen der Büroautomation Personendaten bearbeiten dürfen.

Mit Inkrafttreten des revDSG müssen Bundesorgane:
-Verzeichnisse über die Bearbeitungstätigkeiten führen, die sie via Datenschutzberater dem EDÖB melden (Art. 12 revDSG; Art. 7, 27 E-VDSG).
- das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten bei der automatisierten Bearbeitung von Personendaten protokollieren und die Protokolle 1 Jahr aufbewahren (Art. 4 E-VDSG; vgl. Art. 10 VDSG)[20].

Besonders schützenswerten Personendaten dürfen in der Public Cloud nicht bearbeitet oder gespeichert werden. Die Bearbeitung solcher Daten erfolgt mit dem lokal installierten M365 und die Speicherung wird nach wie vor On-Premises sein.

[17] Verordnung vom 19. Oktober 2016 über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV; SR 172.010.59).
[18] Bundespersonalgesetz vom 24. März 2000 (BPG; SR172.220.1).
[19] Verordnung vom 22. Februar 2012 über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442).
[20] Die Beschränkung der Protokollierungspflicht nur auf Fälle, wo trotz Massnahmen noch ein hohes Risiko für die Persönlichkeit/Grundrechte der betroffenen Personen besteht, gilt nur für private Verantwortliche. Bundesorgane müssen neu gemäss Art. 5 Abs. 2 E-VDSG generell *alle* automatisierten Bearbeitungen protokollieren.

2.3.3 Outsourcing in eine Cloud

Im Rahmen des Projektes Cloud-Enabling Büroautomation (CEBA) ist vorgesehen, BA-Services aus der Microsoft 365-Cloud bereitzustellen. Dazu werden Daten der Identitätsverwaltungssysteme und der Verzeichnisdienste an einen durch Microsoft betriebenen Dienst in der Cloud übergeben, der gegebenenfalls auf Servern im Ausland gespeichert wird.

Das Auslagern von Datenbearbeitungen in eine Cloud stellt eine Datenbearbeitung durch Dritte dar[21]. Nach Art. 10a Abs. 1 DSG kann das Bearbeiten von (besonders schützenswerten) Personendaten durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte, der Auftragnehmer die Sicherheit der Daten gewährleistet und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet[22].Die Auftragsbearbeitung durch den Anbieter einer Cloudlösung ist auch für Daten zulässig, die vom Amts-, Geschäfts- oder Berufsgeheimnis bzw. der beruflichen Schweigepflicht erfasst sind[23], sofern die Geheimhaltungs- und Schweigepflichten in Spezialgesetzen nicht enger umschrieben und eine Auslagerung an Dritte ausgeschlossen werden. Auftragsbearbeiter sind in der Regel als Hilfspersonen zur Wahrung des Amtsgeheimnisses verpflichtet und werden bei einer Verletzung entsprechend strafbar; die Wahrung von Geheimhaltungs- und Schweigepflichten ist durch vertragliche Regelungen sowie technische und organisatorische Massnahmen sicherzustellen.

Der Bund als Auftraggeber bleibt für die Rechtmässigkeit der Datenbearbeitung durch den beauftragten Anbieter einer Cloudlösung verantwortlich und hat sich zu vergewissern, dass der Beauftragte die Datensicherheit gewährleistet und Daten nur soweit bearbeitet, wie dies dem Bund gestattet wäre. Will der Anbieter der Cloudlösung für die Datenbearbeitung Subunternehmer beiziehen, besteht im revDSG künftig – entsprechend Art. 28 Ziff. 2 DSGVO – ein Genehmigungsvorbehalt.[24] In der Praxis wird die Genehmigung einer Veto-Lösung entsprechen, d.h. es reicht aus, dass der Bund als Verantwortlicher vorgängig über den Beizug informiert wird und nicht widerspricht[25].

Die Einhaltung von Gegenstand, Umfang und Grenzen der Datenbearbeitung sind durch vertragliche Vereinbarungen und/oder technische Massnahmen sicherzustellen[26]. Die Einhaltung der Datenschutzgrundsätze wird in der Regel durch Zertifizierungen nachgewiesen.

Die Datenübermittlung ins Ausland erfolgt unter Anwendung der Standardvertragsklauseln mit Schweizer Adaptierung. Dies bedeutet, dass neben der DSVGO auch das Schweizer DSG zur Anwendung kommt. Zusätzlich gibt es auch eine Zusatzvereinbarung zur Geheimhaltungsverpflichtung.

Das revidierte Datenschutzrecht hat auf die Nutzung von Cloudlösungen insbesondere folgende Auswirkungen:

- Verträge mit Auftragsbearbeitern (z.B. Anbietern von Cloud Lösungen) sind dem Datenschutzberater des Departements in Kopie zuzustellen (Art. 9 E-VDSG).

[21] Es ist denkbar, dass die Cloudlösung vom Unternehmen A angeboten wird und auf einer Cloud läuft, die vom Unternehmen B betrieben wird. Sofern das Unternehmen B ebenfalls Zugriff auf die Daten hat, die in der Cloudlösung vom Unternehmen A bearbeitet werden, liegt eine zweifache Auftragsdatenbearbeitung vor.

[22] Erläuterungen des EDÖB zum Cloud Computing (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html, zuletzt besucht am 21.10.20); Privatim: Merkblatt Cloud-spezifische Risiken und Massnahmen (Stand 17.12.2019); ISB, Sicherheitsempfehlungen für Leistungsbezüger / Projektleiter bei der Nutzung von Cloud-Diensten vom 1. März 2017 (Stand 1. Februar 2018).

[23] Vgl. Art. 22 BPG, Art. 320 StGB, Art. 35 DSG bzw. Art. 62 revDSG.

[24] Zur Information: Die Unterauftragsverarbeiter sind im Dokument "Microsoft Cloud Services Subpro-cessors List" aufgeführt. Das Dokument kann im Service Trust Portal geladen werden: https://servicetrust.microsoft.com/DocumentPage/e380d830-a35d-421b-971c-531ff90151e8.

[25] David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. August 2020, Rz. 50; David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020 N 59 ff.

[26] Zum Vertragsinhalt im Einzelnen Ursula Widmer, Gutachten "Klärung und Analyse der rechtlichen Grundlagen für die Integration von Platform-as-a-Service und Software-as-a-Service in der öffentlichen Verwaltung", Ziff. 5.2.1

- Der Beizug von Subunternehmen durch Auftragsbearbeiter ist von den Bundesorganen zu genehmigen (Art. 9 Abs. 3 revDSG, vgl. Art. 28 DSGVO).
- Die Auftragsbearbeiter müssen im Verzeichnis über die Bearbeitungstätigkeiten z.B. Angaben zur Datensicherheit und den Garantien bei Bekanntgabe ins Ausland machen (Art. 12 Abs. 3 revDSG).
- Auftragsbearbeiter müssen Verletzungen der Datensicherheit dem Verantwortlichen so rasch als möglich melden (Art. 24 Abs. 3 revDSG; vgl. Art. 33 DSGVO).

Die Nutzung von Cloud Services, die von Servern im Ausland betrieben werden oder für deren Support ein Fernzugriff (Remote Access) aus dem Ausland vorgesehen ist, gilt als Datenbekanntgabe ins Ausland (Art. 6 Abs. 1 DSG). Nicht als Bekanntgabe ins Ausland gilt die Übermittlung von verschlüsselten, pseudonymisierten oder anonymisierten Personendaten, solange der Empfänger keine Informationen erhält, mit denen er einen Bezug zu bestimmten Personen (z.B. durch Entschlüsselung) herstellen kann[27]. Sofern die Daten bei einer Nutzung von Clouddiensten mit einem hinreichenden Sicherheitsniveau verschlüsselt werden und der Schlüssel ausschliesslich bei der Bundesverwaltung bleibt, bestehen keine datenschutzrechtlichen Einschränkungen für die Bekanntgabe ins Ausland.

Es werden keine Daten auf Systeme ausserhalb der Schweiz bzw. der europäischen Union gespeichert, auch ein Ausfall des Verzeichnisdienstes (Azure AD) wird nicht auf einen Server ausserhalb erfolgen. Dies gilt auch für Verrechnungs- und Supportdaten (bis Ende 2022 umgesetzt). Es werden einzig für die Sicherheitsanalyse zeitlich beschränkt Daten in die USA anonymisiert übermittelt. Entsprechend der EU Boundary Massnahmen von Microsoft, wird Microsoft dazu Anfang nächsten Jahres eine Zusammenstellung machen, welche Daten übermittelt werden.

Die entsprechenden vertraglichen Vereinbarungen sind bereits abgeschlossen oder liegen vor Inbetriebnahme vor. Gemäss Art. 6 Abs. 1 DSG dürfen (besonders schützenswerte) Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich, weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte führt eine Liste der Länder[28], deren Gesetzgebung ein angemessenes Datenschutzniveau gewährleistet. Mit Inkrafttreten des revDSG wird der Bundesrat diese Aufgabe vom EDÖB übernehmen (vgl. Art. 16 revDSG).

Bei einer Bekanntgabe von (besonders schützenswerten) Personendaten in Länder, die gemäss der EDÖB-Liste ein angemessenes Datenschutzniveau haben, wird vermutet, dass keine schwerwiegende Persönlichkeitsgefährdung zu befürchten ist. Die für eine Auslagerung in eine ausländische Cloud im Vordergrund stehenden europäischen Länder, so namentlich Polen, Niederlande, Deutschland und Irland, fungieren alle auf der EDÖB-Liste.

Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn hinreichende Garantien bestehen, insbesondere durch Vertrag, die einen angemessenen Schutz im Ausland bieten können (Art. 6 Abs. 2 DSG)[29].

Für eine Datenbearbeitung in den USA ist grundsätzlich Vorsicht geboten. Mit Urteil vom 16. Juli 2020 («Schrems II») hat der EuGH den Angemessenheitsbeschuss zum Privacy Shield

[27] Matthias Bossardt, in: Datenschutzrecht, Nicolas Passadelis, David Rosenthal, Hanspeter Thür [Hrsg.], 2015, S. 808.
[28] https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2017/04/staatenliste.pdf.download.pdf/staatenliste.pdf
[29] Werden keine anerkannten Standardverträge verwendet („Swiss Transborder Data Flow Agreement“, EU Standardvertragsklauseln) müssen die vertraglichen Garantien mindestens den Anforderungen des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SR 0.235.1; Europarat Übereinkommens STE 108) und dem Zusatzprotokoll vom 8. November 2001 zum genannten Übereinkommen bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (SR 0.235.11; Zusatzprotokoll zum Europarat Übereinkommen STE 108) genügen.

EU-USA für ungültig erklärt, da das Privacy Shield Abkommen keinen gleichwertigen Datenschutz zum Unionsrecht biete[30]. Das Urteil entfaltet keine direkte Wirkung für die Schweiz, hat aber Auswirkungen für schweizerische Unternehmen mit Bezug zur EU. Obschon noch kein schweizerisches Urteil zum Datenschutzniveau des Privacy Shield Abkommens CH-USA ergangen ist und dieses Abkommen weiterhin gilt, hat der EDÖB mit Stellungnahme vom 8. September 2020 das Datenschutzniveau der USA auf der von ihm geführten Liste als ungenügend eingestuft[31]. Nach seiner Einschätzung sind auch Standardklauseln oder sog. «Binding Corporate Rules» als vertragliche Garantien (Art. 6 Abs. 2 lit. a DSG) nicht geeignet, Transparenz und Rechtsschutz gegen den Zugriff von US-Behörden zu garantieren. Diese neue Entwicklung betrifft somit auch Unternehmen, die sich dem Privacy Shield CH-USA unterstellt haben[32].

Falls eine Cloud oder ein Cloud Service von einem Unternehmen mit Bezugspunkten zu den USA betrieben wird - und zwar unabhängig von seinem Sitz, den Serverstandorten oder dem Bezugsort der Cloudlösung -, besteht zudem die Gefahr, dass dieses Kundendaten gestützt auf den CLOUD-Act[33] an die amerikanischen Strafverfolgungsbehörden herausgeben muss, selbst wenn dies schweizerisches Recht verletzt (Art. 271, 320 StGB). Voraussetzung dafür ist jedoch, dass diese Daten im Zusammenhang mit einem Verbrechen stehen.[34]

Neben dem US Cloud-Act ist der Foreign Intelligence Surveillance Act (FISA) von Bedeutung. Dieser regelt die nachrichtendienstliche Ausspähung von amerikanischen Geheimdiensten. Er sollte bei der Risikobeurteilung jedoch nicht mehr ins Gewicht fallen, als das allgemeine Risiko der nachrichtendienstlichen Ausspähung.

Aufgrund der geteilten Verantwortlichkeit ist es an den Departementen und Verwaltungseinheiten im Einzelfall das Risiko bezüglich Datenbekanntgabe an die USA aufgrund ihrer Daten abzuschätzen. Die vorliegende Rechtsgrundlagenanalyse weist allgemein auf das bestehende Risiko hin. Die Einsatzrichtlinie E 031[35] definiert welche Daten in die Cloud bearbeitet werden dürfen und welche nicht.

Zu beachten ist bei einer Auslagerung ins Ausland, dass die Durchsetzung von vertraglichen Vereinbarungen zur Sicherstellung der korrekten Datenbearbeitung (vgl. vorne Ziff. 1.2.3) im Ausland erschwert sein kann. Mit der Mitteilung vom 27. August 2021 anerkennt der EDÖB die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäss der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (gem. Durchführungsbeschluss 2021/914/EU) als Grundlage für Personendatenübermittlungen in ein Land ohne angemessenes Datenschutzniveau (z.B. USA), sofern die für eine Verwendung unter Schweizer Datenschutzrecht notwendigen Anpassungen und Ergänzungen vorgenommen werden.

Die Bundesverwaltung übermittelt die Daten an Microsoft in der EU (Irland), ein Land mit angemessenen Datenschutzniveau gemäss Staatenliste, basierend auf den Standardvertragsklauseln mit Ergänzung, dass auch das CH-DSG gültig ist. Entsprechend der EU Boundary Massnahmen werden sämtliche Daten in EU/CH-Rechenzentren gehalten.

---

[30] Siehe Pressemitteilung EuGH mit Link zum Urteil.
[31] Stellungnahme des EDÖB vom 8. September 2020.
[32] Nach Abschluss des Privacy Shield Abkommens CH-USA im Januar 2017 beurteilte der EDÖB das Datenschutzniveau der USA als angemessen, sofern die Daten empfangenden Unternehmen dem Privacy Shield beigetreten und auf der Liste des U.S. Department of Commerce verzeichnet waren (wie z.B. die Microsoft Corporation oder Google LLC).
[33] Der CLOUD Act steht für “Clarifying Lawful Overseas Use of Data Act” (https://www.congress.gov/bill/115th-congress/senate-bill/2383/text) und ergänzt den “Stored Communications Act” (SCA). Der CLOUD Act erlaubt den US-Strafbehörden, auf Daten zuzugreifen, die sich in Besitz, Obhut oder Kontrolle von US-Unternehmen oder ihren ausländischen Tochtergesellschaften befinden, ohne dafür den Rechthilfeweg zu beschreiten. Dem CLOUD Act unterstehende Cloud-Anbieter – wie beispielsweise die Microsoft Corporation - müssen US-Behörden auch dann Zugriff auf gespeicherte Daten gewährleisten, wenn die Speicherung nicht in den USA, sondern z.B. in einem EU-Mitgliedstaat oder in der Schweiz erfolgt. Das US-amerikanische Justizministerium hat ein Whitepaper zum US CLOUD Act veröffentlicht.
[34] Siehe hierzu auch den Bericht des BJ zum US CLOUD-Act: 2021-09-17-us-cloud-act-d.pdf.
[35] Siehe hierzu E 031, 2.6 Umgang mit Geschäftsdaten.

Eine Auslagerung von Datenbearbeitungen in eine Cloudlösung mit Support und Serverstandort in den genannten europäischen Ländern ist datenschutzrechtlich zulässig.
Bei einer Cloudlösung mit Server- oder Supportstandort in den USA ist eine Datenbearbeitung dagegen nur ins Auge zu fassen, wenn im Einzelfall festgestellt werden kann, dass hinreichende Garantien vertraglicher oder technischer/organisatorischer Art bestehen, die einen angemessenen Datenschutz gewährleisten.
Das Risiko eines «lawful access» der US-Stafverfolgungsbehörden gestützt auf den CLOUD Act, d.h. einer nach Schweizer Recht unzulässigen Datenbekanntgabe des Cloud Betreibers an US-Strafverfolgungsbehörden, kann durch Vereinbarung einer hohen Konventionalstrafe - sowie der Strafandrohung für fehlbare Mitarbeitende in der Schweiz - gesenkt werden.

2.3.4 Datensicherheit

Art. 7 Abs. 1 DSG verlangt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Die Vertraulichkeit, Verfügbarkeit und Integrität der Daten sind zu gewährleisten.

Werden die IKT-Vorgaben des Bundes eingehalten, kann davon ausgegangen werden, dass die Datensicherheit im Sinne dieser Bestimmungen gewahrt ist. Gegenüber einem Cloud Provider als Auftragsbearbeiter ist vertraglich sicherzustellen, dass die Vorgaben zur Datensicherheit kontrolliert werden können (z.B. mit Audits) und bei mangelnder Datensicherheit Handlungsmöglichkeiten bestehen (z.B. Konventionalstrafen, Kündigung). Die Datensicherheit ist auch bei Rechtsstreitigkeiten mit dem Anbieter, Insolvenz und neuen Vorschriften anderer Staaten zu gewährleisten.

Dies ist vertraglich bereits geregelt. Microsoft verpflichtet sich zur Einhaltung der Bestimmungen zu Datenschutz und Datensicherheit gemäss den Bestimmungen in den anwendbaren Vertragswerken von Microsoft. Microsoft lässt zu, dass Bezugsberechtigte ihre Daten verschlüsseln können.

2.4 Informationssicherheit und Geheimhaltungspflichten

2.4.1 Informationsschutz durch Klassifizierung

Gewisse Informationen der Bundesbehörden oder der Armee sind vor Veränderung, Verlust und Zugriff unberechtigter Dritter durch besondere Massnahmen zu schützen. Solche schutzwürdigen Informationen werden zur Wahrung der Landesinteressen klassifiziert. Die Informationsschutzverordnung[36] - sowie künftig auch Art. 13 des Informationssicherheitsgesetzes (siehe dazu 3.4) - unterscheidet je nach konkretem Schutzbedarf für die jeweiligen Informationen drei Klassifizierungsstufen: INTERN, VERTRAULICH und GEHEIM. Im Grundsatz gilt für alle klassifizierten Informationen, dass die Erstellung, die Bekanntgabe und das Zugänglichmachen auf ein Minimum zu beschränken ist (Art. 13). Klassifizierte Informationen unterliegen - wie alle anderen nicht öffentlich bekannten Daten - dem Amtsgeheimnis; für Übermittlung, Aufbewahrung und Bearbeitung gelten besondere Bestimmungen (Anhang ISchV). Die Vorgaben der ISchV werden bei der Nutzung der Cloud eingehalten, wenn:

- Informationen der Stufe INTERN auf einem geschützten Übertragungsweg übermittelt werden und nur berechtigten Personen zugänglich sind.
- Informationen der Stufe VERTRAULICH mit einer für diese Stufe freigegebenen kryptographischen Verfahren verschlüsselt werden und die Schlüssel ausschliesslich durch den Bund verwaltet werden.

[36] Informationsschutzverordnung vom 4. Juli 2007 (ISchV; SR 510.411).

Der EDÖB hat eine Konkordanztabelle für die Schutzniveaus im Informationsschutz (klassifizierte Informationen, die aus Sicht Landesinteresse geschützt werden müssen) und im Datenschutz (Schutz der Persönlichkeit und der Grundrechte des Individuums) erstellt[37].

Auf der M365 Cloud der Bundesverwaltung werden nur Daten bis Schutzniveau INTERN bearbeitet. Für höher klassifizierte Daten und besonders schützenswerte Personendaten werden wie heute On-Premises Datenspeicher benutzt und Verschlüsselungstools eingesetzt.

2.4.2 Amtsgeheimnis

Informationen, die Bundesangestellte in ihrer dienstlichen Tätigkeit erfahren, fallen unter das Amtsgeheimnis, wenn sie nur einem beschränkten Personenkreis bekannt sind und der Geheimnisherr an ihrer Geheimhaltung ein berechtigtes Interesse hat (Art. 320 StGB[38] i.V.m. Art. 22 BPG[39]). Bundesangestellte unterstehen neben dem Amtsgeheimnis auch Berufs- und Geschäftsgeheimnissen (Art. 22 BPG, Art. 94 BPV[40]). Mit dem revidierten Artikel 320 StGB werden neu auch Hilfspersonen strafrechtlich sanktioniert. Da sich externe IKT-Leistungserbringer als solche qualifizieren ist eine Weitergabe von Informationen an Auftragsdatenbearbeiter zulässig. Der revidierter Artikel 320 StGB ist am 1. Januar 2023 in Kraft getreten.

Bei der Nutzung von Cloud Services soll der Anbieter vertraglich zur Geheimhaltung zu verpflichtet werden. Durch vertragliche Regelungen ist ferner sicherzustellen, dass er diese Geheimhaltungspflichten auch auf beigezogene Dritte überbindet. Die Durchsetzbarkeit von Geheimhaltungspflichten ist erschwert, wenn in den jeweiligen Verträgen ein ausländischer Gerichtsstand vereinbart und ein ausländisches Recht anwendbar erklärt wurde.

Gemäss dem CLOUD Act können US-Strafverfolgungsbehörden Cloud Betreiber mit Bezug zum US-Markt verpflichten, ihnen Kundendaten herauszugeben, selbst wenn sie damit Schweizer Recht und vertragliche Geheimhaltungspflichten verletzen. Voraussetzung dafür ist jedoch, dass die Daten in Zusammen mit einem Verbrechen stehen.[41] Diesem Risiko ist bei der Auswahl der Cloud Betreiber Rechnung zu tragen.

Die Wahrung der Vertraulichkeit von Daten (Amtsgeheimnis, Informationsschutz) durch Anbieter von Cloud Services und durch von ihnen beigezogene Dritte ist vertraglich zu regeln und abzusichern. Hat der Anbieter von Cloud Services oder der Cloud Provider (bzw. eine Entität des Konzerns) einen Bezug zum US-Markt, stellt der CLOUD Act ein zusätzliches Risiko für die Wahrung von Geheimhaltungspflichten dar.

Daten, deren Vertraulichkeit erhöht ist, sollen nicht in der M365 Cloud abgespeichert werden, sondern wie heute auf On-Premises Datenablagen der Bundesverwaltung. Dies wird durch technische und organisatorische Massnahmen unterstützt.

3 Bevorstehende Änderungen der Rechtsgrundlagen

3.1 Totalrevision Datenschutzgesetz und -verordnung

Die 2017 eingeleitete Totalrevision des Datenschutzgesetzes hatte zum Ziel, das schweizerische Datenschutzrecht an das Niveau der DSVGO und der Datenschutzkonvention des Eu-

[37] Leitfaden EDÖB «Technische und Organisatorische Massnahmen Datenschutz TOM».
[38] Strafgesetzbuch vom 21. Dezember 1937, SR 311.0.
[39] Bundespersonalgesetz vom 24. März 2000 (BPG; SR 172.220.1).
[40] Bundespersonalverordnung vom 3. Juli 2001 (BPV; SR 172.220.111.3).
[41] Siehe hierzu auch den Bericht des BJ zum US CLOUD-Act: 2021-09-17-us-cloud-act-d.pdf.

roparates anzupassen. Der Gesetzesentwurf wurde im September 2020 vom Parlament verabschiedet; die Referendumsfrist ist am 14. Januar 2021 unbenutzt abgelaufen[42]. Das totalrevidierte Datenschutzgesetz[43] wird voraussichtlich 2022 in Kraft treten. Die wesentlichen Änderungen betreffen hauptsächlich den Ausbau von Governance-Pflichten. Die Ämterkonsultation der totalrevidierten Verordnung zum revDSG erfolgte anfangs Februar 2021.

3.2 Teilrevision Cyberrisikenverordnung (CyRV)

Es steht aktuell zur Diskussion, ob die Cyberrisikenverordnung per 1. April 2023 ausser Kraft gesetzt wird. Die relevanten Artikel würden dann in die Informationssicherheitsverordnung (ISV) aufgenommen, die am voraussichtlich am 1. April 2023 in Kraft tritt.

3.3 Teilrevision der Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV)

Die IAMV wird gegenwärtig revidiert und soll mit dem ISG am 1. April 2023 in Kraft treten. Die Änderungen haben keinen Einfluss auf das vorliegende Projekt.

3.4 Inkrafttreten BG über die Informationssicherheit beim Bund (ISG)

Das Informationssicherheitsgesetz (ISG), das vom Parlament am 18. Dezember 2020 verabschiedet wurde, soll die sichere Bearbeitung von Informationen sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten[44]. Es bildet die formell-gesetzliche Grundlage für die Informationsschutzverordnung (ISchV), die bislang die wesentlichen Regelungen zur Informationssicherheit enthielt. Das ISG soll am 1. April 2023 in Kraft treten.

3.4.1 Grundsätzliche Neuerungen des ISG

Das ISG soll die sichere Bearbeitung aller Informationen, für die der Bund zuständig ist (auch die nicht-klassifizierten Informationen) hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit gewährleisten und ebenfalls neu den sicheren Einsatz von Informatikmittel des Bundes gewährleisten. Gemäss der Legaldefinition nach Artikel 5 Bst. a ISG werden als Informatikmittel «Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen» bezeichnet, worunter auch jegliche Arten der Cloud-Anwendung fallen.

Um die Informationssicherheit beim Einsatz von Informatikmitteln zu gewährleisten, insb. beim Bezug von Informatikdienstleistungen bei externen Leistungserbringern, sind neu die Bestimmungen zur «Sicherheit beim Einsatz von Informatikmitteln» nach Artikel 16-19 ISG massgebend (ISG 16-19 ersetzen die Artikel 14b -14e CyRV).

Gemäss den Ausführungsbestimmungen zum neuen ISG soll die Schwelle der Klassifizierungsstufen (INTERN, VERTRAULICH, GEHEIM) angehoben werden: Das heutige VERTRAULICH wird in der Tendenz das morgige INTERN. Die Klassifizierungskriterien werden künftig in der Informationssicherheitsverordnung im Detail festgelegt (vgl. VE-ISV Art. 17 ff.) Es wird neu die «sicherheitsempfindliche Tätigkeit» eingeführt (Art. 5 Bst. b ISG), die neu für die Durchführung von Personensicherheitsprüfungen (PSP) und von Betriebssicherheitsver-

[42] BBl 2020 7639
[43] Bundesgesetz über den Datenschutz vom 25. September 2020 (Datenschutzgesetz, DSG; SR 235.1).
[44] BBL 2020 9975.

fahren (BSV; ehemals Geheimschutzverfahren) massgebend ist. Sie umfasst die Bearbeitung von VERTRAULICH und GEHEIM klassifizierten Informationen (Art. 13 Abs. 2 und 3 ISG), die Verwaltung, den Betrieb, die Wartung und die Überprüfung von Informatikmitteln mit hohem und sehr hohem Schutz (Art. 17 ISG) sowie den Zugang zu Sicherheitszonen 2 und 3 einer Anlage nach der Gesetzgebung über den Schutz militärischer Anlagen. Die Informationssicherheit soll sich künftig an internationalen Standards ausrichten, wobei ein Informationssicherheitsmanagementsystem (ISMS) samt Ambitionsniveau der Sicherheit sowie entsprechende Massnahmen definiert werden. Mit dem ISMS wird der minimal erforderliche Schutz der Information und Informatikmittel im Vergleich zu den heutigen Anforderungen nach CyRV und ISchV angehoben.

3.4.2 Auswirkungen des ISG ab Inkraftsetzung für Cloud-Anwendungen

Das ISG regelt zwei Faktoren, die für den Einsatz einer Cloud-Lösung in seinem Geltungsbereich massgeblich sind: Erstens von den darin zu bearbeitenden Informationen (klassifizierte vs. nicht-klassifizierte Information) und zweitens vom Resultat des Sicherheitsverfahrens bzw. ob ein Informatikmitten der Sicherheitsstufe «Grundschutz», «hoher Schutz» oder «sehr hoher Schutz» gemäss Artikel 17 ISG zuzuordnen ist.

Insbesondere werden folgende Punkte zu prüfen sein:

- *Klassifizierung*: Nach ISchV klassifizierte Informationen müssen mit der Inkraftsetzung des ISG an die neuen Klassifizierungsvorschriften angepasst werden (vgl. Art. 11-15 ISG i.V.m. der künftigen Informationssicherheitsverordnung (ISV)), sobald diese Informationen das erste Mal bearbeitet (bspw. gespeichert, angepasst, gelöscht etc.) werden (vgl. Art. 90 Abs. 1 ISG);
- Die *Informatikmittel* (vgl. Art. 5 Bst. a ISG) müssen innerhalb von zwei Jahren nach Inkraftsetzung des ISG nach den neuen Bestimmungen des ISG eingestuft werden (vgl. Art. 16-19 ISG i.V.m. der künftigen Informationssicherheitsverordnung). Technische Massnahmen zur Gewährleistung der Informationssicherheit müssen hingegen erst innerhalb von sechs Jahren nach Inkraftsetzung des ISG umgesetzt werden (vgl. Art. 90 Abs. 2 ISG). Als Informatikmittel gilt auch eine Cloud-Anwendung, womit das ISG und alle entsprechenden Ausführungsbestimmungen auf für Cloud-Projekte zur Anwendung gelangen;
- *Personensicherheitsprüfungen (PSP)*: Nach bisherigem Recht ausgestellte Sicherheits- und Risikoerklärungen sind fünf Jahre ab deren Ausstellung gültig. D.h. die Projektleitung hat hins. bestehender Prüfungen nichts zu unternehmen. Anders aber hins. neuer Mitarbeitenden im Projekt: Hier hat die Projektleitung i.Z.m. dem Auftraggeber das Recht, dass die PSP für die neuen Mitarbeitenden nach den neuen Bestimmungen des ISG erfolgen;
- *Betriebssicherheitsverfahren (BSV)*: Nach bisherigem Recht ausgestellte Betriebssicherheitserklärungen (BSE) sind fünf Jahre ab deren Ausstellung gültig; d.h. die Projektleitung muss bei sicherheitsempfindlichen Aufträgen sicherstellen, dass der Anbieter über eine gültige BSE verfügt, ggf. unter Hinzuziehung der Fachstelle Betriebssicherheitsverfahren (vgl. Verfahren nach der VBSV). Wenn noch gar keine BSE ausgestellt wurde, ist eine entsprechende zu besorgen bzw. dies zu prüfen (vgl. Verfahren nach der BSVV). Neu sind auch Auftraggeber und Auftraggeberinnen der zivilen Bundesverwaltung gehalten, das BSV anzustossen (und nicht mehr nur das VBS gemäss der ehemaligen Geheimschutzverordnung).

3.5 Vernehmlassung BG über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

Das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG), dessen Vernehmlassung am 11. Dezember 2020 eröffnet wurde, hat zum Ziel, die Rechtsgrundlagen für einen wirkungsvollen Einsatz elektronischer Mittel in der Bundesverwaltung im Zusammenhang mit dem Angebot digitalisierter Behördenleistungen zu schaffen[45]. Das EMBAG könnte Auswirkungen auf die BA haben, falls der Bundesrat entsprechende Standards definiert. Zurzeit ist das EMBAG im Parlament hängig.

4 Fazit

Mit den mit Microsoft abgeschlossenen Verträgen hat die Bundesverwaltung die Grundlagen geschaffen, mit Einhaltung der rechtlichen Rahmenbedingungen die Nutzung von M365 zuzulassen. Für den Einsatz ist eine Einsatzrichtlinie zu schaffen, damit Daten mit höherem Schutzbedarf nicht in der Cloud abgelegt werden. Im Rahmen des ISDS Konzepts wurde eine Risikoanalyse erstellt, die Restrisiken wurden darin ausgewiesen und sind bekannt.

[45] Vorentwurf EMBAG: https://www.admin.ch/ch/d/gg/pc/documents/3175/Vorentwurf_de.pdf, Erläuternder Bericht zum EMBAG vom 11.12.20: https://www.admin.ch/ch/d/gg/pc/documents/3175/Erl.-Bericht_de.pdf.