UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Institut für Europarecht
Institut de droit européen

Verfassungs- und völkerrechtliche Vorgaben der Bekanntgabe von Personendaten ins Ausland im Rahmen einer Auftragsbearbeitung

Rechtsgutachten im Auftrag des Rechtsamtes
der Direktion für Inneres und Justiz des Kantons Bern

Prof. Dr. Astrid Epiney, LL.M.
Dr. Nula Frei

Oktober 2023

Inhaltsverzeichnis

Executive Summary

Die **wichtigsten Ergebnisse der Untersuchung** können stichwortartig wie folgt zusammengefasst werden:

1. Bei einer **Datenbearbeitung im Auftrag einer Behörde** erfolgt **keine Datenbekanntgabe an den Auftragnehmer**, da die Behörde verantwortlich bleibt. Dessen ungeachtet sind aufgrund der Vorgaben für die Zulässigkeit einer Datenbearbeitung im Auftrag im Falle einer Bearbeitung im Ausland oder der Anwendbarkeit ausländischen Rechts auf die entsprechende Auftragsbearbeitung oder den Auftragsbearbeiter die strengeren **Voraussetzungen für die Datenbekanntgabe ins Ausland sinngemäss anwendbar**.

2. Der Rückgriff durch eine Behörde auf eine ***Cloud*-Lösung** eines US-Anbieters ist nach aktueller Rechtslage sowie nach Art. 12 Abs. 1 lit. a E-KDSG **unzulässig**, **es sei denn die Personendaten sind verschlüsselt und das Schlüsselmanagement bleibt bei der Behörde**. Dies gilt auch, wenn sich die Server in der Schweiz befinden, weil US-Behörden gestützt auf den *US Cloud Act* auch auf solche Daten Zugriff erlangen können. Denn eine Auftragsbearbeitung ist nur zulässig, wenn gewährleistet ist, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie es die Behörde selbst tun dürfte.

3. Diese Unzulässigkeit ergibt sich aus der **Ausgestaltung der Gesetzeslage** in den USA, die es mit sich bringt, dass der Auftragsbearbeiter verpflichtet werden kann, die Daten in einer Weise zu bearbeiten, wie die Behörde dies nicht tun dürfte. Damit kann die Behörde nicht darlegen, dass grundsätzlich sichergestellt ist bzw. davon auszugehen ist, dass der Auftragsbearbeiter die Daten nur so bearbeiten darf, wie es die Behörde selbst tun dürfte. Für eine **Risikoanalyse** in dem Sinn, dass es darauf ankäme, mit welcher Wahrscheinlichkeit eine solche Bearbeitung tatsächlich erfolgen könnte, bleibt vor diesem Hintergrund **kein Raum**. Denn ob das Recht eingehalten wird oder nicht, ist keine Frage des Risikos, sondern eine Rechtsfrage, die im Übrigen wegen der Grundrechtsbindung der staatlichen Behörden für diese anders zu beantworten sein kann als für Private.

4. Die vom Kanton Bern in die Vernehmlassung geschickte **Variante 2** ist völker- und verfassungsrechtlich **unzulässig**. Überdies wäre sie «nutzlos», soweit sie die Bearbeitung im Auftrag durch *US-Cloud*-Anbieter ermöglichen soll.

§ 1 Einleitung und Problemstellung

1. Die **Digitalisierung** bringt Transformationen der Arbeitsweise und -instrumente auch im Bereich der **öffentlichen Verwaltung** mit sich. Neue Formen der Datenbearbeitung sowie geänderte Arbeitsformen wie mobiles Arbeiten und damit einhergehende Kommunikationsbedürfnisse oder Zusammenarbeitsformen stellen die öffentliche Verwaltung vor bedeutsame Fragen, namentlich in der IT-Beschaffung. Dabei hat sich die Nutzung neuer IT-Instrumente selbstverständlich an den einschlägigen **verfassungs- und völkerrechtlichen rechtlichen Vorgaben** zu orientieren bzw. die Einhaltung derselben zu gewährleisten. Soweit natürliche oder juristische Personen von der Nutzung der Digitalisierung durch öffentliche Organe betroffen sind, kommt den **Grundrechten** eine besondere Bedeutung zu.

2. Dabei werden immer häufiger auch von öffentlichen Organen Informatiklösungen von Drittanbietern in Betracht gezogen, bei denen entweder **Daten im Ausland bearbeitet** werden (etwa weil sie vom Drittanbieter auf ausländischen Servern gelagert werden) oder bei denen die Drittanbieter zumindest teilweise **ausländischem Recht unterstehen**, etwa weil sie mit Hauptsitz im Ausland domiziliert sind. Dies wirft für öffentliche Organe des Bundes wie auch der Kantone besondere (datenschutz-)rechtliche Fragen auf, die sich auch von denjenigen Fragen unterscheiden, mit denen Private konfrontiert sind, welche solche Informatiklösungen ebenfalls nutzen, insbesondere wenn der Sitzstaat des Drittanbieters nicht über ein dem Schweizer Datenschutzrecht angemessenes Datenschutzniveau verfügt.

3. Auch der **Kanton Bern** ist mit diesen Fragen konfrontiert, die sich im Rahmen der geplanten Totalrevision des kantonalen Datenschutzgesetzes erneut akzentuiert haben. Um die Nutzung insbesondere von *US-Cloud*-Lösungen wie Microsoft 365[1] durch die kantonalen öffentlichen Organe zu ermöglichen, hat der Regierungsrat eine Variante im Entwurf für das kantonale Datenschutzgesetz in die Vernehmlassung geschickt, welche als eigenen Ausnahmetatbestand vom Grundsatz, dass Datenbekanntgaben ins Ausland nur im Falle eines angemessenen Schutzniveaus zulässig sind, formuliert, dass eine solche Bekanntgabe auch erfolgen darf, wenn die Datenbekanntgabe zum Zweck der Bearbeitung im Auftrag erfolgt und deren Voraussetzungen erfüllt sind. Dabei stellt sich die Frage, ob die vorgesehene Variante mit dem übergeordneten Recht vereinbar ist.

> Die in die Vernehmlassung gesandte Variante enthält somit eine zusätzliche Ausnahme von dem Grundsatz, dass eine Datenbekanntgabe ins Ausland nur im Falle eines angemessenen Schutzes zulässig ist, welche die «Bekanntgabe zum Zweck der Bearbeitung im Auftrag» erlaubt, wobei deren Voraussetzungen erfüllt sein müssen (vgl. Art. 15 Abs. 3 lit. d E-KDSG).

4. Vor diesem Hintergrund erörtert die vorliegende Untersuchung die **verfassungs- und völkerrechtliche Zulässigkeit** einer **Datenbekanntgabe ins Ausland** (insbesondere mit Blick auf die Nutzung von in den USA basierten *Cloud*-Lösungen, bei denen

---

[1] Vgl. zum Begriff des *Cloud Computing* sowie den damit verbundenen Risiken, m.w.N., SCHEFER/GLASS, Gutachten zum grundrechtskonformen Einsatz von M365, 22 ff.; BLONSKI, SJZ 2023, 991 (993 f.).

Personendaten in die USA übermittelt werden) im Rahmen von Auftragsbearbeitungen: Auf der Grundlage einer Skizzierung der für die Auftragsdatenbearbeitung sowie die Datenübermittlung ins Ausland geltenden Grundsätze im Völker-, Europa- und nationalen Recht (§ 2), wird der Frage nachgegangen, ob und ggf. unter welchen Voraussetzungen eine Übermittlung von Personendaten ins Ausland zum Zweck der Bearbeitung im Auftrag zulässig ist (§ 3). Der Beitrag schliesst mit einer Zusammenfassung der wichtigsten Ergebnisse, an welche sich eine kurze Schlussbetrachtung anschliesst (§ 4).

Die vorliegende Untersuchung geht auf ein Gutachten zurück, welches die Verfasserinnen im Auftrag des Rechtsamts der Direktion für Inneres und Justiz des Kantons Bern erstellten. Inhaltlich handelt es sich um eine unabhängige Arbeit: Die Verfasserinnen wurden um eine unabhängige Klärung der sich stellenden Fragen gebeten. Dabei wurden die zu erörternden Rechtsfragen wie folgt formuliert:

«Vor dem Hintergrund der geplanten Totalrevision des Datenschutzgesetzes des Kantons Bern soll das Rechtsgutachten die Frage klären, ob und ggf. unter welchen Voraussetzungen eine Datenbekanntgabe ins Ausland (insbesondere mit Blick auf die Nutzung von in den USA basierten *Cloud*-Lösungen, bei welchen Personendaten in die USA übermittelt werden) verfassungs- und völkerrechtlich zulässig ist. Berücksichtigt werden soll auch die Rechtslage in der Europäischen Union, sowohl soweit die grundrechtlichen Garantien betroffen sind als auch die einschlägige Regelung in der Datenschutzgrundverordnung (DSGVO). Nicht Gegenstand des Gutachtens sind Einzelheiten der in den USA geltenden Regeln und die dortige behördliche Praxis des Zugriffs auf in die USA im Rahmen der Nutzung von *Cloud*-Lösungen übermittelte Daten. Ebensowenig werden die „technischen" Aspekte des Rückgriffs auf *Cloud*-Lösungen erörtert.»

Dem Rechtsamt der Direktion für Inneres und Justiz des Kantons Bern, insbesondere Frau *Anna Bäumlin* und Frau *Sarah Hostettler*, sei an dieser Stelle für das entgegengebrachte Vertrauen und die sehr angenehme Zusammenarbeit gedankt.

§ 2 Datenübermittlung ins Ausland im Rahmen der Bearbeitung im Auftrag: Grundsätze

5. Die Frage nach der Zulässigkeit der Datenübermittlung ins Ausland im Rahmen einer Auftragsbearbeitung ist notwendigerweise auf der Grundlage der einschlägigen **völker- und verfassungsrechtlichen Vorgaben** zu beantworten, welche daher nachfolgend zunächst allgemein erörtert werden sollen (I.), bevor auf die sich hieraus ergebenden **spezifischen Vorgaben** für die in dieser Untersuchung im Vordergrund stehende Thematik eingegangen wird (II.).

Im Rahmen der Erörterung der spezifischen Vorgaben soll auch rechtsvergleichend auf das Datenschutzgesetz des Bundes, welches ebenfalls die genannten völker- und verfassungsrechtlichen Vorgaben zu beachten hat, hingewiesen werden, auch wenn dieses für die kantonalen Behörden rechtlich nicht bindend ist, da es nur auf Bundesbehörden und Privatpersonen anwendbar ist, nicht aber auf kantonale Behörden. Ebenso soll ein Seitenblick auf die Regelungen anderer Kantone zur Bekanntgabe von Personendaten ins Ausland geworfen werden.

I. Verfassungs- und völkerrechtliche Vorgaben

6. Ausgangspunkt für die Beantwortung der einleitend skizzierten Rechtsfragen bildet das **Grundrecht auf Datenschutz** (1.), das sich völkerrechtlich in Art. 8 EMRK verankert findet (wobei die parallele Rechtsprechung des EuGH zu Art. 7, 8 Grundrechtecharta (GRCh) herangezogen werden kann, sich der EuGH auch an der Rechtsprechung des EGMR orientiert) und das zudem in der Bundesverfassung in Art. 13 Abs. 2 BV zu verorten ist. Weiter seien nachfolgend im Überblick die völkerrechtlich verbindlichen Regelwerke, die dieses Grundrecht konkretisieren, erörtert, nämlich das Übereinkommen des Europarats zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (**Konvention 108+**) sowie die **Richtlinie (EU) 2016/680** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung[2] (2., 3.).

1. Das Grundrecht auf Datenschutz[3]

a) EMRK

7. Von zentraler Bedeutung ist auf völkerrechtlicher Ebene der Schutz des Privatlebens gemäss **Art. 8 EMRK** sowie die hierzu ergangene **Rechtsprechung des EGMR**. Aus dem Recht auf Privatleben, einem der Teilgehalte des Art. 8 EMRK, leitet der EGMR

---

[2] ABl. 2016 L 119, 89. Diese Richtlinie ist für die Schweiz aufgrund der Schengen-/Dublin-Assoziierung der Schweiz verbindlich, vgl. allgemein zur Relevanz bzw. Verbindlichkeit unionsrechtlicher Vorgaben für die Schweiz EPINEY/NÜESCH/ROVELLI, Datenschutzrecht in der Schweiz, 59 ff.

[3] Die Ausführungen in den nachfolgenden Abschnitten dieses Kapitels beruhen teilweise auf früheren Untersuchungen, vgl. insbesondere EPINEY/NÜESCH/ROVELLI, Datenschutzrecht in der Schweiz, 7 ff.; EPINEY/FREI, in: Bieri/Powell, OFK-DSG, Völker- und Europarecht, N 6 ff.

auch einen Anspruch auf Schutz der persönlichen Daten ab. M.a.W. ist Datenschutz bzw. das Recht der Einzelnen darauf, dass sie betreffende Daten (vorbehaltlich einer Rechtfertigung) nicht bearbeitet werden, als spezifischer Ausfluss bzw. Teilbereich des Rechts auf Achtung der Privatsphäre (Art. 8 EMRK) zu sehen.

8. **Eingriffe** in das aus Art. 8 Abs. 1 EMRK fliessende Recht auf Datenschutz sind nur zulässig, wenn sie **gerechtfertigt** werden können, wobei sie den eng auszulegenden Anforderungen des Art. 8 Abs. 2 EMRK entsprechen müssen:

- Erstens muss die staatliche Massnahme «**gesetzlich vorgesehen**» sein. M.a.W. ist für jede Einschränkung eine innerstaatliche gesetzliche Grundlage erforderlich.
- Zweitens muss die staatliche Massnahme einen der in Art. 8 Abs. 2 EMRK genannten **legitimen Zwecke** verfolgen. Den Vertragsstaaten kommt dabei ein weites Ermessen zu; die Zwecke bzw. zulässigen Rechtfertigungsgründe sind allerdings abschliessend geregelt. Im Fall datenschutzrechtlich relevanter Massnahmen kommen unterschiedliche Zwecke in Betracht, darunter namentlich die Wahrung der nationalen oder öffentlichen **Sicherheit**, die Aufrechterhaltung der **Ordnung**, die Verhütung von **Straftaten** sowie der Schutz der **Rechte und Freiheiten** anderer.
- Schliesslich muss die Massnahme gemäss Art. 8 Abs. 2 EMRK auch «**in einer demokratischen Gesellschaft notwendig**» sein. Diese Vorgabe nimmt auf den Grundsatz der Verhältnismässigkeit Bezug. Gemäss der Rechtsprechung des EGMR ist insbesondere von Bedeutung, dass staatliche Eingriffe einem dringenden Bedürfnis der Gesellschaft («*pressing social need*») entsprechen und im Hinblick auf den verfolgten Zweck erforderlich und angemessen sind. Die konkreten, sich aus dem Grundsatz der Verhältnismässigkeit ergebenden Anforderungen hängen weitgehend vom Einzelfall und insbesondere von der Art und Schwere des Eingriffs ab, wobei den Mitgliedstaaten in diesem Zusammenhang – insbesondere was die Wahl der Mittel betrifft – ein weiter Ermessensspielraum zukommt.

9. Auch die **Bekanntgabe von Personendaten an ausländische Behörden** stellt einen Eingriff in das Recht auf Datenschutz gemäss Art. 8 Abs. 1 EMRK dar. In der Rechtssache *Centrum för rättvisa gegen Schweden*[4] konkretisierte der EGMR die skizzierten Anforderungen an die Rechtfertigung eines solchen Eingriffs, wobei u.a. die Konventionskonformität des Austauschs von durch Massenüberwachung gewonnenen Erkenntnissen zwischen dem schwedischen Nachrichtendienst und ausländischen Staaten und internationalen Organisationen im Vordergrund stand. Der EGMR hielt in diesem Punkt fest, dass die Übermittlung von solchem Material gewissen Garantien unterliegen muss. Namentlich

- müssen die Voraussetzungen der Übermittlung im **nationalen Recht** klar festgelegt sein;
- muss der übermittelnde Staat sicherstellen, dass der empfangende Staat über **Garantien** verfügt, die geeignet sind, Missbrauch und unverhältnismässige Eingriffe zu verhindern (insbesondere Gewährleistung einer sicheren Speicherung und Beschränkung der Weitergabe des Materials), ohne dass jedoch insgesamt ein vergleichbarer Schutz oder eine Zusicherung vor jeder Übermittlung notwendig wäre;

---

[4] EGMR, Centrum för rättvisa gegen Schweden [Grosse Kammer], Nr. 35252/08, Urteil vom 25.05.2021.

- sind verstärkte **Sicherheitsvorkehrungen** erforderlich, wenn klar ist, dass Material, das besonderer Vertraulichkeit bedarf (wie etwa vertrauliches journalistisches Material) übermittelt wird;
- und muss die Übermittlung von Material an ausländische nachrichtendienstliche Partner einer **unabhängigen Kontrolle** unterliegen.

10. In diesem Zusammenhang von Interesse ist auch das Recht der **Europäischen Union**, namentlich das **Grundrecht auf Datenschutz** in Art. 7 (Achtung des Privat- und Familienlebens) und Art. 8 (Schutz personenbezogener Daten) GRCh. Nicht nur sind diese selbständig zu beachten, sondern es ist auch sämtliches Sekundärrecht, namentlich die DSGVO und die Richtlinie 2016/680, am Massstab dieser beiden Grundrechte zu messen. Diese Praxis der EU bzw. das EU-Recht ist im vorliegenden Zusammenhang insbesondere vor dem Hintergrund von Bedeutung, dass der EuGH Art. 7, 8 GRCh gemäss Art. 52 GRCh im Lichte des Art. 8 EMRK auslegt, so dass die Rechtsprechung des EuGH insofern auch für die Interpretation dieser Bestimmung hoch relevant ist.

11. Inzwischen sind denn auch rund **30 Urteile des EuGH** zu verzeichnen, in welchen es zumindest auch bzw. meist schwerpunktmässig um die Vereinbarkeit von Sekundärrecht, mitgliedstaatlichen Durchführungsakten oder völkerrechtlichen Abkommen mit **Art. 7, 8 GRCh** oder um die Auslegung dieser Bestimmungen im Zusammenhang mit der primärrechtskonformen Auslegung ging. Insgesamt nimmt der EuGH in dieser Rechtsprechung eine **sehr detaillierte Grundrechtsprüfung** vor und prüft im Einzelnen insbesondere die Verhältnismässigkeit, dies mit einer **hohen Prüfdichte**, wobei er auch zahlreiche, eher detaillierte Vorgaben für den Unionsgesetzgeber formuliert und dem Grundrechtsschutz in der gesamten einschlägigen Rechtsprechung einen sehr hohen Stellenwert einräumt.[5] Dadurch ergibt sich, dass der Verfolgung durchaus legitimer öffentlicher oder privater Interessen durch den grundrechtlich garantierten Persönlichkeitsschutz Grenzen gesetzt sind, so dass diese «nicht um jeden Preis» verfolgt werden dürfen. Insofern wohnt den Grundrechten ein gewisser «Absolutheitsanspruch» inne, was nicht nur für die Gewährleistung des Kerngehalts der Grundrechte, sondern auch für die übrigen Anforderungen gilt, wobei gleichzeitig nicht zu verkennen ist, dass auch die datenschutz- bzw. grundrechtlichen Vorgaben eine Verfolgung wichtiger (insbesondere öffentlicher) Interessen keineswegs verunmöglichen, sofern die vom EuGH aufgestellten Vorgaben bzw. Schranken beachtet werden.

> Die Bestimmung des **Kerngehalts** der Art. 7, 8 GRCh im Zusammenhang mit der Verarbeitung von Personendaten ist noch nicht abschliessend geklärt. Aus der bisherigen Rspr. ergibt sich aber immerhin, dass dieser jedenfalls in den Fällen, in denen in Bezug auf einen nicht näher eingegrenzten Personenkreis auf Kommunikationsinhalte zurückgegriffen werden kann, berührt ist.[6] Auch dürfte der Kerngehalt immer dann betroffen sein, wenn umfassend (fast) alle Aspekte des Privatlebens betroffen sind und die Nutzung ohne eine präzise Umschreibung des Zwecks erfolgen darf. Sodann dürfte der Kerngehalt der Art. 7, 8 GRCh i.V.m. Art. 21 GRCh (Nichtdiskriminierung) ebenfalls berührt sein, wenn es um die Verarbeitung besonders sensibler Daten (wie z.B. Rasse oder Religion) geht und die Annahme

---

5 Vgl. die Auflistung der einschlägigen Urteile bei EPINEY, sic 2022, 575, 580; s. auch schon die Skizzierung wichtiger Urteile bei EPINEY/FREI, in: Epiney/Rovelli (Hrsg.), DSGVO, 2 ff., ein Beitrag, worauf die nachfolgenden Ausführungen teilweise zurückgreifen.

6 Vgl. EuGH, Rs. C-293/12 (*Digital Rights Ireland*), ECLI:EU:C:2014:238; EuGH, Rs. C-362/14 (*Schrems*), ECLI:EU:C:2015:650.

zugrunde gelegt wird, dass ein solches Merkmal unabhängig von konkreten Anhaltspunkten im Verhalten des Betroffenen für die öffentliche Sicherheit relevant sein könnte.[7]

12. In der Rs. C-362/14[8] (*Schrems*) setzte sich der Gerichtshof spezifisch mit der Zulässigkeit der **Übermittlung von Daten in einen Drittstaat** auseinander: Diese sei nur dann zulässig, wenn im Zielstaat ein hohes Schutzniveau gewährleistet sei, das zwar nicht identisch mit demjenigen der RL 95/46[9] sein, jedoch einen **gleichwertigen Schutz** bieten müsse. In den **USA** könne das Konzept des *Safe Harbour* kein solches angemessenes Schutzniveau gewährleisten. Auch der Nachfolgebeschluss 2016/1250, mit welchem die Kommission die Angemessenheit des Datenschutzniveaus in den USA aufgrund des im Anschluss an die Rs. C-362/14 eingerichteten sog. *privacy shield* feststellte, wurde in der Rs. C-311/18 (*Schrems II*) für ungültig erklärt,[10] dies im Wesentlichen aufgrund paralleler Erwägungen wie in der Rs. C-362/14: Auch auf der Grundlage des neuen Beschlusses werde den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts letztlich allgemein Vorrang eingeräumt. Insbesondere verstiessen die vorgesehenen Überwachungsprogramme gegen Art. 7, 8 GRCh, da der Grundsatz der Verhältnismässigkeit nicht beachtet sei. Es sei nämlich jedenfalls in Bezug auf bestimmte Überwachungsprogramme nicht erkennbar, dass für den Datenzugriff Einschränkungen bestünden. Auch stünden den Betroffenen keine ausreichenden Rechtsschutzmöglichkeiten zur Verfügung (womit der Wesensgehalt des Art. 47 GRCh verletzt werde), woran auch die durch den *privacy shield* eingerichtete Ombudsstelle nichts ändere. Allerdings seien die im Beschluss 2010/87 vorgesehenen Standardvertragsklauseln zulässig.

Inzwischen wurde ein neuer Angemessenheitsbeschlusses der Kommission, der *EU-US Data Privacy Framework*, gefasst.[11] Danach gewährleisten die USA Staaten ein angemessenes Schutzniveau – vergleichbar mit dem der Europäischen Union – für personenbezogene Daten, welche innerhalb des neuen Rahmens aus der EU an US-Unternehmen (soweit diese sich dem Datenschutzrahmen angeschlossen haben, was die Verpflichtung zur Einhaltung detaillierter datenschutzrechtlicher Vorgaben voraussetzt) übermittelt werden. Im Übrigen wird der Zugriff von US-Nachrichtendiensten auf ein «notwendiges und verhältnismässiges Mass» beschränkt und eine (quasi-) gerichtliche Überprüfung vorgesehen. Der Beschluss soll der eben skizzierten Rechtsprechung des EuGH Rechnung tragen, wobei aber fraglich ist, ob er einer Überprüfung durch den EuGH standhalten wird.[12]

In der Schweiz hat sich an der Rechtslage jedoch (noch) nichts geändert; der Bundesrat wird über die Angemessenheit des Datenschutzniveaus in den USA auf der Grundlage des am 1. September 2023 in Kraft getretenen Datenschutzgesetzes entscheiden müssen und damit auch darüber, ob die USA in die Liste derjenigen Staaten mit einem angemessenen Schutzniveau aufgenommen wird.

---

7 EuGH, Gutachten 1/15 (*Abkommen EU-Kanada betreffend Übermittlung von Fluggastdatensätzen*), ECLI:EU:C:2017:592.

8 EuGH, Rs. C-362/14 (*Schrems)*, ECLI:EU:C:2015:650.

9 RL 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31. Diese Richtlinie wurde inzwischen durch die sog. Datenschutzgrundverordnung (VO 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. 2016 L 119, 1) abgelöst.

10 EuGH, Rs. C-311/18 (*Schrems II)*, ECLI:EU:C:2020:559.

11 COM(2023) 4745 final.

12 Hierzu GLOCKER, ZD 2023, 189 ff.

b) Bundesverfassung

13. Art. 13 BV verankert neben dem Anspruch auf Achtung des Privatlebens (einschliesslich der Wohnung) sowie des Brief-, Post- und Fernmeldeverkehrs auch allgemein einen Anspruch jeder Person auf «**Schutz vor Missbrauch ihrer persönlichen Daten**».

> Damit wird – wie schon in Art. 8 GRCh – der Schutz personenbezogener Daten vom Schutz der Privatsphäre losgelöst und unabhängig von dem Vorliegen eines Eingriffs in dieselbe als eigenständiges Schutzgut definiert. Insofern kann man hier von einer zweiten Generation datenschutzrechtlicher Regelungen sprechen, die – im Gegensatz zu der etwa in Art. 8 EMRK zum Ausdruck gekommenen ersten Generation – Datenschutz als eigenständiges Ziel unabhängig von einem Eingriff in die Privatsphäre versteht. Daran schliesst sich die dritte Generation datenschutzrechtlicher Regelungen an, die auch den Schutz von Daten, die nicht einer bestimmten identifizierbaren Person zugeordnet werden können, zum Gegenstand hat, ein Ansatz, der sich bislang insbesondere in der RL 2002/58 (Datenschutzrichtlinie für elektronische Kommunikation bzw. dem Entwurf für den Nachfolgerechtsakt der E-Privacy-Verordnung[13]) niedergeschlagen hat.

14. Der Schutzbereich des Art. 13 Abs. 2 BV umfasst – was in der etwas missglückten Formulierung nicht wirklich zum Ausdruck kommt – nach der hier vertretenen und auch vom Bundesgericht[14] geteilten Ansicht tatsächlich ein **Grundrecht auf informationelle Selbstbestimmung**, so dass jeder Umgang mit personenbezogenen Daten erfasst ist und der Einzelne grundsätzlich bestimmen können muss, ob und zu welchem Zweck ihn betreffende Daten bearbeitet werden. Allerdings kann dieses Grundrecht unter Wahrung der Vorgaben des Art. 36 BV (gesetzliche Grundlage, öffentliches Interesse oder Schutz von Grundrechten Dritter, Verhältnismässigkeit sowie Wahrung des Kerngehalts) **eingeschränkt** werden.

> Damit wird der Datenschutz auf verfassungsrechtlicher Stufe verankert, so dass er – ein wichtiger Aspekt – nur unter den verfassungsrechtlich geregelten Voraussetzungen eingeschränkt werden darf und insofern nicht zur Disposition des Gesetzgebers steht.
>
> Zur Tragweite von Art. 13 Abs. 2 BV stellen sich insbesondere Abgrenzungsfragen zum Recht auf persönliche Freiheit gemäss Art. 10 Abs. 2 BV sowie zum Recht auf Schutz des Privat- und Familienlebens gemäss Art. 13 Abs. 1 BV. In Bezug auf das Verhältnis zu Art. 10 Abs. 2 BV geht es insbesondere darum, ob die beiden Grundrechte nebeneinander und damit unabhängig voneinander Bestand haben oder ob Art. 13 BV gewissermassen als *lex specialis* zu Art. 10 Abs. 2 BV fungiert. Fraglich ist überdies, ob sich die Schutzbereiche der beiden Grundrechte überschneiden oder ob der Schutzbereich von Art. 10 Abs. 2 BV vielmehr um den von Art. 13 BV tangierten Bereich «gekürzt» sein soll. Auch das Verhältnis zwischen Art. 13 Abs. 1 und Art. 13 Abs. 2 BV ist insoweit unklar. Das Bundesgericht erachtet den verfassungsrechtlichen Datenschutz gemäss Art. 13 Abs. 2 BV als Teilgehalt des in Art. 13 Abs. 1 BV verankerten Schutzes der Privat- und Geheimsphäre und führt überdies aus, dass Art. 13 Abs. 2 BV damit auch als Präzisierung einer der in Art. 13 Abs. 1 BV genannten Teilaspekte – namentlich des dort verankerten Schutzes der Privatsphäre – anzusehen sei. Zum Verhältnis zur persönlichen Freiheit gemäss Art. 10 Abs. 2 BV betont das Bundesgericht überdies, dass Art. 13 Abs. 1 BV

---

13 COM(2017) 10 final.

14 Vgl. BGE 144 II 77, E. 5.2.; BGE 142 II 340, E. 4.2.

im Verhältnis zu dieser Bestimmung als Spezialgarantie anzusehen sei und sich die beiden Schutzbereiche überdies überschnitten.[15]

c) Grundrecht auf Datenschutz und Datenschutzgesetze

15. Insbesondere der EGMR, aber auch das Bundesgericht, haben aus Art. 8 EMRK und Art. 13 Abs. 2 BV zahlreiche Gewährleistungen bzw. Rechte abgeleitet und den Schutzbereich somit mit Blick auf die Effektivität des Rechts auf Datenschutz eher weit gefasst. Sowohl das Datenschutzgesetz des Bundes (DSG) als auch die kantonalen Datenschutzgesetze greifen diese Garantien auf und präzisieren sie in verschiedener Hinsicht. Insofern stellt die **Datenschutzgesetzgebung** in weiten Teilen **konkretisiertes Verfassungsrecht** dar, wie auch das Bundesgericht mit Bezug zum Datenschutzgesetz des Bundes explizit betont.[16] Von Bedeutung ist dieser «materiell-verfassungsrechtliche Gehalt» der Datenschutzgesetzgebung insbesondere bei der Auslegung sowohl der Datenschutzgesetzgebung als auch spezialgesetzlicher Regelungen mit Bezug zum Datenschutz.

Vor diesem Hintergrund ist immer (auch) danach zu fragen, ob und inwieweit die jeweiligen datenschutzrechtlichen Bestimmungen (auf kantonaler Ebene oder auf Bundesebene) tatsächlich Art. 8 EMRK oder Art. 13 Abs. 2 BV konkretisieren und welchen Teilgehalten der Datenschutzgesetzgebung damit aus materiell-rechtlicher Sicht **verfassungsrechtlicher Rang** zukommt. Dies zeitigt sodann Auswirkungen auf das Verhältnis der Datenschutzgesetzgebung zu anderen spezialgesetzlichen Erlassen mit datenschutzrechtlichen Bestimmungen, denn soweit Bestimmungen des DSG konkretisiertes Verfassungsrecht darstellen, sind diese auch im Verhältnis zu anderen gesetzlichen Vorgaben vorrangig zu berücksichtigen bzw. die Spezialgesetze sind auch vor dem Hintergrund der Garantien der Datenschutzgesetzgebung auszulegen. Vorbehalten bleibt selbstredend die Konstellation, dass gemäss Verfassungsrecht eine vom DSG abweichende Lösung ebenfalls zulässig ist.[17]

2. Völkerrechtliche Konkretisierung des Grundrechts auf Datenschutz: Konvention 108+ zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten

16. Das Übereinkommen des Europarats zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108) stammt ursprünglich aus dem Jahr 1981 und stellt nach wie vor das **einzige rechtsverbindliche völkerrechtliche Instrument** im Bereich des Datenschutzes dar. Im Jahr 2018 nahmen die Vertragsstaaten ein **Protokoll zur Modernisierung des Übereinkommens** Nr. 108 an (SEV 223), welches zum Ziel hatte, das Übereinkommen angesichts des technologischen Fortschrittes zu modernisieren und die Kohärenz mit dem zeitgleich sich weiterentwickelndem Unionsrecht sicherzustellen.[18] Das Protokoll befindet sich derzeit in der Ratifikationsphase und ist noch nicht in Kraft. Das Übereinkommen Nr. 108 in seiner aktuellen sowie dereinst

---

15 Vgl. BGE 138 I 331, E. 5.1.; BGE 137 I 167, E. 3.2.; BGE 126 I 7, E. 2.a; BGE 128 II 259, E. 3.2. Vgl. zu diesen hier nicht näher zu vertiefenden Fragen des Verhältnisses der verschiedenen Grundrechtsgarantien zueinander z.B. SCHWEIZER/STRIEGEL, in: Ehrenzeller u.a. (Hrsg.), SGK-BV, Art. 13 N 96 ff.

16 Vgl. BGE 143 1 257, E. 3.3.

17 Vgl. BGE 126 II 126.

18 Vgl. zum Protokoll im Einzelnen DE TERWANGNE, in: Epiney/Rovelli (Hrsg.), DSGVO, 39 ff.

seiner modernisierten Form sind für die Vertragsstaaten **verbindlich**. Zwar untersteht es nicht der richterlichen Aufsicht des EGMR, wurde jedoch in dessen Rechtsprechung im Zusammenhang mit Art. 8 EMRK berücksichtigt.

17. Die **Schweiz** hat das Protokoll am 8. September 2023 **ratifiziert**.[19] Dessen Inhalt ist auch bereits davor in die Totalrevision des DSG eingeflossen.[20] Die Ratifizierung des Änderungsprotokolls durch die Schweiz ist **auch für die Kantone verbindlich**. Die Bestimmungen dieses Rechtsakts müssen, soweit erforderlich, gemäss der im innerstaatlichen Recht vorgesehenen verfassungsmässigen Kompetenzverteilung umgesetzt werden.[21]

18. Die modernisierte Konvention enthält Regelungen sowohl zur **Auftragsdatenbearbeitung** als auch zur **Datenbekanntgabe ins Ausland**. Diese werden untenstehend ausführlicher erörtert.[22]

3. Richtlinie 2016/680 zum Datenschutz bei der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung

19. Die sekundärrechtlichen Regeln zum Datenschutz in der Europäischen Union wurden im Jahr 2016 grundlegend überarbeitet. Die 2016 erlassene und seit 2018 massgebliche **Datenschutzgrundverordnung** (VO 2016/679, DSGVO)[23], welche die aus dem Jahr 1995 stammende Datenschutzrichtlinie (RL 95/46[24]) ablöste, stellt das Herzstück dieser Revision dar. Sie ist – anders als die RL 95/46 – nicht Teil des Schengen-Acquis und somit für die Schweiz nicht verbindlich,[25] entfaltet aber in gewissen – hier vorliegend nicht relevanten – Bereichen auch Wirkungen für Drittstaaten.[26]

20. Für die Schweiz im Bereich der Schengen-Assoziierung verbindlich ist hingegen die **Richtlinie (EU) 2016/680** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung** sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses

---

19 S. Medienmitteilung des EDÖB vom 8.9.2023, https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/convention108.html (zuletzt besucht am 20.9.2023).

20 Vgl. Botschaft Konvention 108+, BBl 2020 588 ff.; Botschaft nDSG, BBl 2017 6993 ff.

21 Botschaft Konvention 108+, BBl 2020 594.

22 N 33 ff., 53 ff.

23 VO 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. 2016 L 119, 1.

24 RL 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31.

25 Vgl. hierzu EPINEY, sic! 2022, 575 (579).

26 S. hierzu, m.w.N., EPINEY/NÜESCH/ROVELLI, Datenschutzrecht in der Schweiz, S. 59 ff.; EPINEY, sic! 2022, 575 (578 ff.).

2008/977/JI des Rates[27] (im Folgenden: Richtlinie zum Datenschutz in der Strafverfolgung; RL 2016/680), welche – gewissermassen als kleines Geschwister der DSGVO – deren hürdenreichen Gesetzgebungsprozess «mitgemacht» hat.

21. Inhaltlich **bezweckt** die Richtlinie einerseits den Schutz natürlicher Personen bei der Verarbeitung von Daten im Bereich der Strafverfolgung, der Strafvollstreckung und der Abwehr von Gefahren für die öffentliche Sicherheit und damit zusammenhängend den Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen (Art. 1 Abs. 1 und Abs. 2 lit. a RL 2016/680), zum anderen soll der Austausch personenbezogener Daten in diesen Bereichen zwischen den zuständigen Behörden innerhalb der EU ermöglicht werden.[28]

22. Die Richtlinie ist anwendbar auf die Datenbearbeitung durch zuständige Behörden zu den Zwecken der **Verhütung, Ermittlung, Aufdeckung** oder **Verfolgung von Straftaten, Strafvollstreckung** sowie des **Schutzes vor** und der **Abwehr von Gefahren für die öffentliche Sicherheit** (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 RL 2016/680). Im Unterschied zur Vorgängerregelung fallen nunmehr auch präventive und repressive Massnahmen im Rahmen des polizeilichen Handelns in den Anwendungsbereich der Richtlinie.[29] Von der Richtlinie erfasst sind sowohl **grenzüberschreitende** als auch rein **innerstaatliche Datenbearbeitungsvorgänge** zu den Zwecken der Richtlinie (Art. 2 Abs. 1 RL 2016/680). In persönlicher Hinsicht wurde der Anwendungsbereich von eigentlichen Behörden in den genannten Bereichen auf Stellen oder Einrichtungen ausgeweitet, denen gestützt auf nationales Recht die Ausübung öffentlicher Gewalt oder hoheitlicher Befugnisse für die Zwecke der Richtlinie übertragen wurde (Art. 2 Abs. 1 i.V.m. Art. 3 Ziff. 7 lit. b RL 2016/680). Damit gelangt der Regelungsrahmen der Richtlinie auch auf private Akteure, welche mit justiziellen oder polizeilichen Aufgaben betraut wurden, zur Anwendung.

23. Eine Richtlinie ist für die Mitgliedstaaten hinsichtlich des zu erreichenden **Ziels** verbindlich, überlässt ihnen jedoch die Wahl der Form und der **Mittel** (Art. 288 Abs. 3 AEUV), so dass Richtlinien einer innerstaatlichen Umsetzung bedürfen. Mit der RL 2016/680 erfolgte eine **Mindestharmonisierung** im Anwendungsbereich des Rechtsakts, indem den Mitgliedstaaten ein datenschutzrechtlicher Mindeststandard vorgegeben wird, für den jedoch Abweichungsmöglichkeiten zugunsten des mitgliedstaatlichen Rechts vorgesehen sind, und über den die Mitgliedstaaten gegebenenfalls auch hinausgehen können.

24. Die Richtlinie ist für die Schweizer **Kantone** von besonderer Bedeutung, da die in ihren Anwendungsbereich fallenden Staatsaufgaben zum grössten Teil kantonale Kompetenzen sind. Für die kantonalen Polizei-, Strafverfolgungs- sowie -vollzugsbehörden ist

---

27 ABl. 2016 L 119, 89.

28 Zum Ganzen: EPINEY/KERN, in: Epiney/Nüesch (Hrsg.), Revision des Datenschutzes in Europa, 39 (59 ff.), worauf die folgenden Ausführungen teilweise zurückgreifen.

29 EPINEY/FREI, in: Bieri/Powell, OFK-DSG, Völker- und Europarecht, N 32.

die Richtlinie somit massgebend, was bei der Revision kantonaler Datenschutzgesetze zu berücksichtigen ist.[30]

II. Zu den Vorgaben für die Datenübermittlung ins Ausland im Rahmen der Bearbeitung im Auftrag

25. Die hier interessierende Problematik wirft datenschutzrechtlich Fragen in zwei Bereichen auf: Einerseits werden im Rahmen von *Cloud-Computing* Daten durch einen **Auftragnehmer** bearbeitet (1.). Andererseits könnte es sein, dass **Personendaten ins Ausland bekanntgegeben** werden, wofür die entsprechenden Voraussetzungen erfüllt sein müssen (2.). Nachfolgend werden die einschlägigen Regelungen *in abstracto* erörtert, bevor sie in einem zweiten Schritt (§ 3) auf die in dieser Untersuchung im Vordergrund stehende Problematik angewendet werden.

26. Neben den einschlägigen und für die Schweiz verbindlichen bzw. relevanten völkerrechtlichen Vorgaben werden auch das **Datenschutzgesetz des Bundes** sowie die Rechtslage in ausgewählten **Kantonen** berücksichtigt:

- Zwar ist das **Datenschutzgesetz des Bundes** auf kantonale Behörden nicht anwendbar. Gleichwohl sind seine Regelungen für die vorliegende Thematik von Interesse, da sie dort herangezogen werden können, wo eine Parallelität der Regelungen besteht und auf kantonaler Ebene jedenfalls keine bewusste Abweichung gesucht wurde. Es ist nämlich angesichts gemeinsamer übergeordneter Vorgaben (Völkerrecht, Bundesverfassung) davon auszugehen, dass die Bundesgesetzgebung ebenso wie die kantonalen Gesetze diesen Vorgaben Rechnung tragen sollen, so dass erstere auch für die Auslegung kantonaler Regelungen rechtsvergleichend herangezogen werden kann. Insofern hat das DSG für die Konkretisierung der völker- und verfassungsrechtlichen Vorgaben schweizweit eine harmonisierende Wirkung.[31]
- In rechtsvergleichender Hinsicht, namentlich im Rahmen der systematischen Auslegung, sind auch die Datenschutzgesetze anderer **Kantone** von Interesse. Einige von ihnen werden deshalb nachfolgend ebenfalls berücksichtigt.

1. Bearbeitung im Auftrag

a) Vorbemerkung: Zur Rechtsnatur der Auftragsdatenbearbeitung

27. **Zweck** der Regelungen zur Datenbearbeitung im Auftrag durch Dritte («*outsourcing*», Auftragsbearbeitung) ist es, eine solche Auslagerung der Datenbearbeitung an Dritte zu ermöglichen, ohne dadurch den **Datenschutz** zu relativieren und damit die Rechtsstellung der Betroffenen zu gefährden.[32]

---

30 BLONSKI, in: Epiney/Moser/Rovelli (Hrsg.), Revision des Datenschutzgesetzes, 89 ff.; POWELL, Jusletter vom 31. Mai 2021, N 1 ff.

31 BELSER/NOUREDDINE, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 8 N 10.

32 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10 N 34.

28. Die **Rechtsnatur** der Datenbearbeitung im Auftrag ist allerdings nicht vollends geklärt. Fraglich ist insbesondere, ob es sich dabei um eine **Datenbekanntgabe** (i.S. der Schweizer Terminologie nach Art. 5 lit. e DSG) bzw. eine Offenlegung durch Übermittlung (i.S. der Terminologie von Art. 4 Ziff. 2 DSGVO und Art. 3 Ziff. 2 Richtlinie 2016/680) handelt, oder ob eine solche Bekanntgabe bzw. Offenlegung gerade nicht stattfindet. Die Antwort auf diese Frage könnte insbesondere **Auswirkungen auf internationale Auftragsbearbeitungsverhältnisse** entfalten: Liegt keine Bekanntgabe bzw. Offenlegung durch Übermittlung vor, so folglich auch keine Bekanntgabe bzw. Übermittlung ins Ausland, was bedeutet, dass die Vorgaben zur Auslandsbekanntgabe in diesen Fällen möglicherweise nicht beachtet werden müssten.

29. Im Rahmen der **DSGVO** ist sich die (Kommentar-) Literatur[33] weitgehend einig, dass die Auftragsverarbeitung normativ privilegiert ist, da der Auftragsverarbeiter nicht «Dritter» ist (vgl. Art. 4 Nr. 10 DSGVO: «ausser […] dem Auftragsverarbeiter»)[34] und dass entsprechend der Datenaustausch zwischen ihm und dem Verantwortlichen keine Übermittlung von Daten i.S.v. Art. 4 Nr. 2 DSGVO darstellt. Aus diesem Grund bedarf der Datenaustausch keiner (gesonderten) Verarbeitungsgrundlage aus Art. 6 DSGVO und ist damit unter vereinfachten Voraussetzungen zulässig bzw. privilegiert.[35] Ein weiterer Beleg für diese beabsichtigte Privilegierung ergibt sich daraus, dass ein Auftragsverarbeiter, der entgegen seiner Rolle selbst über Zweck und Mittel einer Verarbeitung befindet, gemäss Art. 28 Nr. 10 DSGVO nicht mehr als Auftragsverarbeiter, sondern selbst als Verantwortlicher anzusehen ist.[36] Alternative Erklärungsversuche, um trotz fehlender Privilegierung die entsprechenden Rechtswirkungen der Auftragsverarbeitung zu begründen, werden als nicht überzeugend verworfen.[37]

30. In der **Schweiz** wurde diese Frage bislang nur vereinzelt diskutiert, wobei die Ansichten und Ansätze divergieren:

- Teilweise wird vertreten, dass eine Auftragsbearbeitung **keine Datenbekanntgabe im datenschutzrechtlichen Sinne** beinhalte, da die Datenherrschaft beim Verantwortlichen verbleibe und gerade nicht auf den Auftragsbearbeiter übertragen werde, was auch für Datenbearbeitungen im Ausland gelte.[38]

---

33 Soweit ersichtlich wurde diese Frage in der Rechtsprechung des EuGH noch nicht aufgeworfen bzw. geklärt.

34 S. insoweit auch klar GOLA, in: Gola/Heckmann (Hrsg.), DSGVO/BDSG, Art. 4 DSGVO N 98 f.; JAHNEL, DSGVO, Art. 28 N 3; KLUG, in: Gola/Heckmann (Hrsg.), DSGVO/BDSG, Art. 28 DSGVO N 4; ZIEBARTH, in: Sydow/Marsch (Hrsg.), DSGVO/BDSG, Art. 4 DSGVO N 161.

35 JAHNEL, DSGVO, Art. 28 N 5; MARTINI, in: Paal/Pauly (Hrsg.), DSGVO, Art. 28 DSGVO N 8a; GABEL/LUTZ, in: Taeger/Gabel (Hrsg.), DSGVO/BDSG/TTDSG, Art. 28 DSGVO N 8 ff.

36 HARTUNG, in: Kühling/Buchner (Hrsg.), DSGVO/BDSG, Art. 28 DSGVO N 18.

37 HARTUNG, in: Kühling/Buchner (Hrsg.), DSGVO/BDSG, Art. 28 DSGVO N 20.

38 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 10 f.; besonders deutlich BLONSKI, SJZ 2023, 991 (992); MÉTILLE, in: Métille/Meier (Hrsg.), CR-LPD, Art. 9 N 18, vertritt unter Verweis auf BAERISWYL ebenfalls die Ansicht, dass keine Bekanntgabe stattfinde, setzt sich aber nicht mit den Gründen für diese Argumentation auseinander und hält in der übernächsten Randnote fest, dass bei Auftragsbearbeitern aus dem Ausland die Vorgaben von Art. 9 und Art. 16 DSG kumulativ zu beachten seien, ohne darauf einzugehen, warum trotz fehlender Bekanntgabe eine Bekanntgabe ins Ausland vorliegen soll.

- Auf der anderen Seite wird davon ausgegangen, dass bei der Auftragsbearbeitung zwar eine **Datenbekanntgabe** stattfinde, diese aber **nicht die Rechtsfolgen einer Datenbekanntgabe** an Dritte nach sich ziehe,[39] wobei die Gründe für diese in sich nicht ganz widerspruchsfreie Position nicht klar werden.
- In Bezug auf **Auftragsdatenbearbeitungen mit Auslandsbezug** wird wohl mehrheitlich vertreten, dass die Vorgaben für die Bekanntgabe ins Ausland zusätzlich (im Verhältnis zu den Anforderungen an eine Auftragsbearbeitung) zu berücksichtigen seien,[40] womit – allerdings ohne Diskussion dieser impliziten Vorannahmen – davon ausgegangen wird, dass eine Datenbekanntgabe stattfinde. Auch der EDÖB hat in seiner Stellungnahme zur Datenschutz-Risikobeurteilung der Suva zum Projekt *Digital Workplace* «M365» die (nicht weiter begründete) Auffassung vertreten, dass sowohl der vom Bearbeitungsverantwortlichen gewollte als auch der von ihm missbilligte Export von Personendaten eine «grenzüberschreitende Bekanntgabe» i.S. der Datenschutzgesetzgebung darstelle, weshalb die Bestimmungen von Art. 16 ff. DSG auf entsprechende Sachverhalte und somit auch Auslagerungen von Personendaten in eine vom US Konzern Microsoft in der Schweiz betriebene *Cloud* Anwendung fänden.[41]

31. U.E. sprechen jedenfalls in Bezug auf das Datenschutzgesetz des Bundes **gute Gründe** für die Rechtsauffassung, dass zwischen Verantwortlichem und Auftragsverarbeiter ein Art **Bekanntgabeprivileg**[42] besteht, so dass die «**Datenbekanntgabe» im Rahmen einer Auftragsbearbeitung** gerade **keine Datenbekanntgabe** im Sinn des Art. 5 lit. e DSG darstellt, sondern der Auftragsbearbeiter der «Sphäre» des Verantwortlichen zugeordnet ist. Zwar handelt es sich dabei um eine rechtliche Fiktion (denn in Wirklichkeit gelangen ja durchaus Daten von einem Akteur zu einem anderen); jedoch dürfte sich dieser Ansatz bereits aus dem Wortlaut der einschlägigen gesetzlichen Bestimmungen ergeben und wird durch zahlreiche Anhaltspunkte in der Systematik sowie den Zielsetzungen des Gesetzes im Allgemeinen und der Regelung der Auftragsbearbeitung im Besonderen gestützt:

- Der Gesetzeswortlaut in Art. 9 DSG spricht von «übertragen» und nicht von «bekanntgeben», und die Legaldefinition der Datenbekanntgabe in Art. 5 lit. e DSG umfasst «das Übermitteln oder Zugänglichmachen von Personendaten», nicht jedoch das «Übertragen».
- Sodann betont bereits die Botschaft zum (total revidierten) Datenschutzgesetz, dass der Auftragsbearbeiter ab dem Zeitpunkt, an dem er seine vertragliche Tätigkeit im Auftrag des Verantwortlichen beginnt, kein «Dritter» mehr sei,[43] was sich in Art. 9 Abs. 3 DSG niedergeschlagen hat, wo Auftragsbearbeiter und Dritte nebeneinander genannt werden[44] und was insofern folgerichtig ist, als der Auftragsbearbeiter eben

---

39 ROSENTHAL/JÖHRI, HK-DSG, Art. 10a N 26.

40 So u.a. LEZZI, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 9 N 19; MÉTILLE, in: Métille/Meier (Hrsg.), CR-LPD, Art. 9 N 20; i.Erg. ebenso DRITTENBASS, Regulierung von autonomen Robotern, N 227.

41 EDÖB, Stellungnahme SUVA, 2022, Rz. 14.

42 EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10 N 51.

43 Botschaft DSG, BBl 2017 7023.

44 Dies im Zusammenhang mit der Übertragung der Bearbeitung durch den Auftragsbearbeiter an einen «Dritten».

im Auftrag und damit statt des Verantwortlichen, aber für ihn, Daten bearbeitet. Insofern ist es auch stimmig, dass der Auftragsbearbeiter die Daten nur so behandeln darf, wie es der Verantwortliche tun dürfte (Art. 9 Abs. 1 lit. a DSG) und er dieselben Rechtfertigungsgründe für die Bearbeitung gelten machen kann wie der Verantwortliche (Art. 9 Abs. 4 DSG).

- Daher benötigt der Auftragsbearbeiter auch keine spezifische gesetzliche Grundlage oder einen Rechtfertigungsgrund für die Vornahme von Datenbearbeitungen; ebensowenig ist eine spezifische gesetzliche Grundlage für die «Datenbekanntgabe» des öffentlichen Organs an den Auftragsbearbeiter notwendig, wie es für eine «normale» Datenbekanntgabe notwendig wäre, und die betroffenen Personen sind auch nicht involviert (wie etwa bei Art. 17 Abs. 1 lit. a DSG). Nur wenn der Auftragsbearbeiter Daten zu eigenen Zwecken bearbeiten würde, müsste der Verantwortliche eine diesbezügliche Rechtsgrundlage oder einen Rechtfertigungsgrund anführen können.[45]
- Schliesslich ist die Beziehung zwischen Behörde und Auftragsbearbeiter auch strafrechtlich privilegiert in dem Sinne, dass eine Übertragung von Daten an einen Auftragsbearbeiter kein Offenbaren eines Amtsgeheimnisses darstellt.[46] In der Literatur wird hierfür das Bild einer «Käseglocke» verwendet, unter welche die Behörde und ihre Hilfspersonen in Bezug auf den Geheimnisschutz stehen.[47]

Auch das **kantonale Datenschutzgesetz des Kantons Bern** steht dieser Auffassung nicht entgegen; die Begriffsdefinition des «Bekanntmachens» in Art. 2 Abs. 1 lit. e E-KDSG nennt den Vorgang des «Übertragens» (der im Zusammenhang mit der Auftragsbearbeitung in Art. 12 E-KDSG verwandt wird) nicht. Allerdings dürfte der in die Vernehmlassung geschickte Art. 15 Abs. 3 lit. d E-KDSG davon ausgehen, dass im Falle der Auftragsbearbeitung jedenfalls die Weitergabe der Daten an den Auftragsbearbeiter im Ausland als eine Bekanntgabe ins Ausland angesehen wird.[48]

32. Dessen ungeachtet ist nicht zu verkennen, dass die Verneinung des Vorliegens einer Bekanntgabe von Personendaten im Falle der Auftragsbearbeitung auch in den Fallgestaltungen, in welchen die (Auftrags-) Datenbearbeitung dann im Ergebnis im Ausland stattfindet, dazu führt, dass die strengen Voraussetzungen der Zulässigkeit einer **Datenbekanntgabe ins Ausland** unterlaufen werden könnten,[49] so dass **Sinn und Zweck** derselben sowie eine verfassungskonforme Auslegung für ihre zumindest sinngemässe Einschlägigkeit sprechen. Zwar ist dem Vorliegen einer Datenbearbeitung ins Ausland im Rahmen einer Auftragsbearbeitung bei der Frage nach deren Zulässigkeit Rechnung zu tragen;[50] jedoch ist nicht zu verkennen, dass die Voraussetzungen in Bezug auf die Datenbekanntgabe ins Ausland jedenfalls im Datenschutzgesetz des Bundes, aber auch in zahlreichen Kantonen,[51] deutlich präziser formuliert sind und häufig auch engere Grenzen setzen. Insofern besteht das Problem des «Unterlaufens» dieser Vorgaben sehr wohl, es

---

45 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 10 f.

46 S. noch unten N 43.

47 So das Bild bei DZAMKO, in: Métille (Hrsg), L'informatique en nuage, 83 (93).

48 S. insoweit auch noch die Ausführungen unten N 81 f.

49 Vor diesem Hintergrund dürfte denn auch der Ansatz von MÉTILLE, in: Métille/Meier (Hrsg.), CR-LPD, Art. 9 N 20, zu sehen sein, der in solchen Fällen Art. 9 und Art. 16 DSG kumulativ für anwendbar und massgeblich erachtet.

50 S. insoweit noch unten N 33 ff., 84 ff.

51 S. insoweit noch unten N 42 ff.

sei denn, man gehe davon aus, dass die Verpflichtung des Auftragsbearbeiters, die Daten nur so zu bearbeiten, wie es auch die Behörde tun dürfte, impliziere, dass eine Bekanntgabe ins Ausland durch den Auftragsbearbeiter nur – wie bei Behörden – unter Beachtung der diesbezüglichen spezifischen Anforderungen erfolgen dürfte (wofür übrigens gute Gründe sprechen).[52] Diesfalls aber wären bzw. sind im Ergebnis diese Vorgaben eben doch zu beachten, was der hier vertretenen Auffassung entspricht.

> Insoweit sei bereits an dieser Stelle darauf hingewiesen, dass bereits die bei Auftragsbearbeitungen in der Regel zum Zuge kommende Anforderung, dass die Daten durch den Auftragsbearbeiter nur so bearbeitet werden dürfen, wie dies die Behörde selbst tun dürfte, letztlich ein angemessenes Schutzniveau im Ausland (soweit eine Auslandsbearbeitung vorliegt) impliziert.[53] Insofern sollte die praktische Relevanz der Antwort auf die hier thematisierte dogmatische Frage nicht überschätzt werden.[54]

b) Auftragsbearbeitung in der Konvention Nr. 108+

33. Die ursprüngliche Konvention Nr. 108 des Europarats enthielt keine Regelungen zur Auftragsverarbeitung. In **Parallelität zu den Rechtsentwicklungen in der Europäischen Union**, an welche sich die Revisionsbestrebungen der Konvention eng anlehnten bzw. mit welchen sie eng koordiniert waren, wurde in die modernisierte Konvention Nr. 108+ neu auch der Begriff des «Auftragsverarbeiters» aufgenommen. Gemäss Art. 2 lit. f. der modernisierten Konvention ist darunter «eine natürliche oder juristische Person, eine Behörde, ein Dienst, eine Einrichtung oder jede andere Stelle, die beziehungsweise der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet», zu verstehen.

34. Anders als die DSGVO, die RL 2016/680 und das DSG sowie kantonale Datenschutzgesetze regelt die Konvention Nr. 108+ die Voraussetzungen der Auslagerung von Datenbearbeitungen an Auftragsbearbeiter jedoch nicht im Detail. Lediglich gewisse **Pflichten des Auftragsverarbeiters** sind in den Art. 7 und 10 der modernisierten Konvention formuliert. Demgemäss müssen sowohl der Verantwortliche als auch der Auftragsverarbeiter die **Datensicherheit** wahren und diesbezüglich geeignete Sicherheitsvorkehrungen treffen, um Risiken wie unbeabsichtigten oder unbefugten Zugang zu oder Vernichtung, Verlust, Verwendung, Veränderung oder Offenlegung von personenbezogenen Daten vorzubeugen (Art. 7 Abs. 1 Konvention 108+).

35. Art. 10 Konvention 108+ regelt zudem gewisse **Mindestverpflichtungen**, welche sowohl Verantwortliche wie auch Auftragsverarbeiter zu beachten haben. Die Mitgliedstaaten können diese in ihrer Umsetzungsgesetzgebung modifizieren, um der Art oder dem Umfang der Verarbeitung Rechnung zu tragen. Demgemäss müssen auch die Auftragsverarbeiter alle Massnahmen treffen, um die Verpflichtungen nach der Konvention in allen Phasen der Datenverarbeitung einzuhalten und über diese Massnahmen gegebenenfalls auch **Rechenschaft** ablegen zu können. Sie sind zudem verpflichtet, eine **Datenschutzfolgenabschätzung** durchzuführen und Datenschutzüberlegungen so früh wie möglich in den Datenbearbeitungsprozess einfliessen zu lassen (***privacy by design***).[55]

---

52 S. insoweit noch unten N 87 ff.
53 S.u. N 89 ff.
54 S. insoweit noch unten N 109 ff.
55 S. dazu Erläuternder Bericht zur Konvention 108+, 2018, Ziff. 89.

c) Auftragsbearbeitung in der Richtlinie 2016/680 und in der Datenschutzgrundverordnung

36. Die Richtlinie 2016/680 regelt die Auftragsdatenverarbeitung in Kapitel IV und schreibt vor, dass eine Auftragsverarbeitung nur zulässig ist, wenn der Auftragsverarbeiter **hinreichende Garantien** (namentlich mittels geeigneter technischer und organisatorischer Vorkehrungen) für die Einhaltung des Datenschutzes nach der Richtlinie bietet (Art. 22 Abs. 1 RL 2016/680). In einem **schriftlichen Vertrag** zwischen dem Verantwortlichen und dem Auftragsverarbeiter muss u.a. vorgesehen sein, dass der Auftragsverarbeiter ausschliesslich auf Weisung des Verantwortlichen handelt, dass seine Mitarbeitenden zur Vertraulichkeit verpflichtet sind, dass er den Verantwortlichen mit geeigneten Mitteln bei der Einhaltung des Datenschutzes unterstützt, und dass alle Personendaten nach Abschluss des Auftrags zurückgegeben oder gelöscht werden (Art. 22 Abs. 3 RL 2016/680).

37. Dabei folgt die Richtlinie dem Verständnis, dass der Auftragsverarbeiter nicht selbständig über die **Zwecke und Mittel der Verarbeitung** bestimmen kann, sondern dass diese ausschliesslich durch den Verantwortlichen vorgegeben werden. Art. 22 Abs. 5 RL 2016/680 hält denn auch ausdrücklich fest, dass ein Auftragsverarbeiter, der unter Verstoss gegen die Richtlinie die Zwecke und Mittel der Verarbeitung selbst bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher gilt. Eine Subdelegation an einen weiteren Auftragsbearbeiter bedarf einer vorherigen **Genehmigung** durch den Verantwortlichen (Art. 22 Abs. 2 RL 2016/680).

38. Die Richtlinie 2016/680 steht in engem Zusammenhang mit der Datenschutzgrundverordnung. Gemäss Art. 2 Abs. 2 lit. d DSGVO gilt die Richtlinie als *lex specialis* zur Verordnung; der Anwendungsbereich der DSGVO reduziert sich um diese Ausweitungen des Anwendungsbereichs der Richtlinie. Inhaltlich gesehen ist das Verhältnis zwischen Richtlinie und Verordnung durch **zahlreiche Parallelitäten der Begrifflichkeiten, Konzepte und Instrumente** gekennzeichnet. Die inhaltlichen Übereinstimmungen wurden im Zuge des Gesetzgebungsprozesses im Vergleich zum Kommissionsentwurf eher noch etwas verstärkt, so beispielsweise mit der Verankerung des Instruments der Datenschutz-Folgenabschätzung auch im Anwendungsbereich der Richtlinie (Art. 27 RL 2016/680). Gleichzeitig bestehen zwischen den beiden Regelungsinstrumenten jedoch auch beträchtliche Unterschiede, zumeist im Sinne grösserer mitgliedstaatlicher Gestaltungsspielräume im Rahmen der Richtlinie im Vergleich zur Datenschutzgrundverordnung. Dennoch ist nicht zu verkennen, dass die strukturelle, konzeptuelle und begriffliche Verschränkung der beiden Instrumente dazu führt, dass die DSGVO gewissermassen als naheliegender Vergleichsstandard für die Richtlinie herangezogen und diese folglich am – relativ weitgehenden – Schutzniveau der Grundverordnung gemessen werden sollte,[56] so dass jedenfalls immer dann, wenn sich aus der RL 2016/680 nicht explizit anders lautende materielle Vorgaben entnehmen lassen, für ihre Auslegung und damit zur Bestimmung ihrer rechtlichen Tragweite auch auf die Vorgaben der DSGVO zurückgegriffen werden kann.

---

56 EPINEY/FREI, in: Bieri/Powell, OFK-DSG, Völker- und Europarecht, N 33.

39. Die **DSGVO** regelt die Auftragsbearbeitung in ihrem Kapitel IV.[57] Diese ist – wie nach der Richtlinie – nur zulässig, wenn der Auftragsverarbeiter hinreichende Garantien für die **Einhaltung des Datenschutzes** bietet (Art. 28 Abs. 1 DSGVO); hierfür können auch z.B. genehmigte Verhaltensregeln oder ein Zertifizierungsverfahren (Art. 40, 42 DSGVO) ausreichen. Der Auftrag muss auf einem schriftlichen Vertrag basieren, welcher Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen regelt. In Bezug auf den Auftragsverarbeiter muss im Vertrag u.a. geregelt sein, dass die Daten nur auf Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland – verarbeitet werden dürfen, dass die Mitarbeitenden zur Vertraulichkeit verpflichtet sind, dass der Auftragsverarbeiter die Datensicherheit gewährleistet, den Verantwortlichen bei berechtigten Anträgen der Betroffenen (z.B. Auskunftsersuchen) unterstützt, und die Daten nach Beendigung des Auftrags zurückgibt oder löscht (Art. 28 Abs. 3 DSGVO). Der Vertrag kann auch teilweise aus genehmigten Standardvertragsklauseln bestehen (Art. 28 Abs. 6 DSGVO).

40. Auch die DSGVO hält fest, dass ein Auftragsverarbeiter, der unter Verstoss gegen die DSGVO die **Zwecke und Mittel** der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher gilt (Art. 28 Abs. 10 DSGVO). Wie in der Richtlinie ist zudem die Hinzuziehung von Dritten durch den Auftragsverarbeiter von einer vorherigen **Genehmigung** des Verantwortlichen abhängig; dieser muss zudem auch im Einzelfall über die beabsichtigte Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter informiert werden (Art. 28 Abs. 2 DSGVO).

41. Ist der Auftragsverarbeiter nicht in der Union niedergelassen, so hat auch er – gleich wie ein aussereuropäischer Verantwortlicher – einen **Vertreter** in der Union zu benennen (Art. 27 DSGVO), ausser es handelt sich um eine nur gelegentliche Verarbeitung oder generell um eine ausländische Behörde oder öffentliche Stelle.

d) Rechtsvergleich: DSG und kantonale Regelungen

aa) Datenschutzgesetz des Bundes

42. Im **Datenschutzgesetz des Bundes** ist die Datenbearbeitung durch Auftragsbearbeiter in Art. 9 sowie in der Datenschutzverordnung (DSV) geregelt. Es gelten zwei grundsätzliche Voraussetzungen für die Zulässigkeit einer Auslagerung der Datenbearbeitung an Dritte:

- Erstens darf der Auftragsbearbeiter die Daten nur so bearbeiten, **wie der Verantwortliche es tun dürfte** (Art. 9 Abs. 1 DSG). Das bedeutet auch, dass der Auftragsbearbeiter die Personendaten nicht zu eigenen Zwecken, sondern nur zu den vom Verantwortlichen festgelegten Zwecken und nach dessen Weisung bearbeiten darf.[58] Art. 9 DSG geht denn auch davon aus, dass bei jeglicher Art der Datenbearbeitungen durch einen Auftragsbearbeiter der Auftraggeber verantwortlich bleibt.[59]

---

57 Vgl. zu den Regeln über die Auftragsbearbeitung in der DSGVO die einschlägigen, im Literaturverzeichnis zitierten Kommentare.

58 LEZZI, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 9 N 4 und 7.

59 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 2.

Zudem hält Art. 9 Abs. 1 Abs. 1 lit. a DSG explizit fest, dass die Daten nur so bearbeitet werden dürfen, wie es der Verantwortliche selbst tun dürfte, was wohl auch impliziert, dass letzterer durch das Ergreifen geeigneter Massnahmen sicherstellen muss, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie er es selbst tun dürfte.[60] Der Auftragsdatenbearbeiter muss sämtliche Datenschutzgrundsätze ebenfalls einhalten, also die Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckbindung, Transparenz, Datenrichtigkeit, und Datensicherheit (zur Datensicherheit auch ausdrücklich Art. 9 Abs. 2 DSG). Eine Übertragung an weitere Dritte darf der Auftragsbearbeiter nur mit vorgängiger Genehmigung des Verantwortlichen vornehmen (Art. 9 Abs. 3 DSG; Art. 7 DSV).

- Zweitens dürfen keine gesetzlichen oder vertraglichen **Geheimhaltungspflichten** der Übertragung entgegenstehen. Als Geheimhaltungspflichten kommen das Amtsgeheimnis (Art. 320 StGB), die Berufsgeheimnisse nach Art. 321, 321bis und 321ter StGB sowie weitere spezialgesetzliche Berufsgeheimnisse[61] in Frage. Neben dem Amtsgeheimnis kennen verschiedene Gesetze auch **Spezialgeheimnisse** (z.B. Art. 110 DBG im Bereich der direkten Bundessteuer, Art. 33 ATSG im Bereich der Sozialversicherungen, Art. 11 Abs. 1 OHG im Bereich der Opferhilfe; parallele Bestimmungen finden sich zudem in kantonalen Steuer- und Sozialhilfegesetzen). Diese dienen der Sicherstellung des Vertrauensverhältnisses zwischen den Bürgerinnen und Bürgern und den betroffenen öffentlichen Organen. Sie **gelten absolut**, soweit nicht eine gesetzliche Grundlage die Weitergabe von Informationen erlaubt. Darüber hinaus stellt im Übrigen auch das Datenschutzgesetz die vorsätzliche Verletzung der beruflichen Schweigepflicht durch Offenbaren von Personendaten unter Strafe (Art. 62 DSG).

Strafbar macht sich, wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner Stellung als Hilfsperson wahrgenommen hat (Art. 320 StGB). Der objektive Tatbestand des **Offenbarens eines Geheimnisses** ist erfüllt, wenn das Geheimnis an unbefugte Dritte bekannt gegeben oder zugänglich gemacht wird. Nach überwiegender Ansicht ist der Tatbestand erfüllt, wenn die Kenntnisnahme Dritter ermöglicht wird (Tätigkeitsdelikt), ohne dass das Geheimnis auch tatsächlich durch einen Dritten eingesehen wird (Erfolgsdelikt).[62] Wenn eine technische Lösung, z.B. eine **Pseudonymisierung** der Daten durch den Verantwortlichen oder eine **Verschlüsselung** der Daten mit dem Schlüsselmanagement beim Verantwortlichen, das Offenbaren von Informationen und Daten unter einem Geheimnis an den Auftragsbearbeiter ausschliesst, ist der Tatbestand nicht erfüllt.[63] Für die Erfüllung des **subjektiven Tatbestands** ist eine vorsätzliche Offenbarung des Geheimnisses notwendig, wobei **Eventualvorsatz** genügt.

43. Im vorliegenden Zusammenhang ist insbesondere zu betonen, dass die **Weitergabe von Daten an eine Hilfsperson** kein strafrechtlich relevantes Offenbaren eines Geheimnisses darstellt. Der datenschutzrechtliche Auftragsdatenbearbeiter ist eine Hilfsperson

---

60 Wenn es auch natürlich keine «absoluten» Garantien dafür geben kann, dass sich der Auftragsbearbeiter hieran hält; es geht also um nach den Umständen angemessene und grundsätzlich geeignete Massnahmen.

61 Namentlich das sog. Bankgeheimnis (Art. 47 BankG).

62 Für ein Tätigkeitsdelikt: BGE 142 IV 68 E. 5.1; MÉTILLE, in: Métille/Meier (Hrsg.), CR-LPD, Art. 9 N 56; für ein Erfolgsdelikt hingegen DZAMKO, in: Métille (Hrsg), L'informatique en nuage, 2022, 83 (109); SCHWANINGER/MERZ, Jusletter vom 21.6.2021, Rz. 21.

63 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 49 und 52; MÉTILLE, in: Métille/Meier (Hrsg.), CR-LPD, Art. 9 N 67; MÉTILLE, ALP 2019, 609 (614).

i.S.v. Art. 320 StGB, somit entsteht durch die (gesetzeskonforme) Auslagerung der Bearbeitung keine Strafbarkeit. Gibt der Auftragsdatenbearbeiter jedoch **geheimnisgeschützte Daten an Dritte bekannt** – selbst wenn er dazu von einer ausländischen Behörde gezwungen wird –, macht er sich selbst gem. Art. 320 StGB strafbar.[64] Datenschutzrechtlich handelt es sich dabei um eine Datenbekanntgabe, die einen eigenen Rechtfertigungsgrund braucht und von der Auslagerung abzugrenzen ist.[65] Dabei trifft die auftraggebende Behörde eine Sorgfaltspflicht bei der Auswahl, Instruktion und Überwachung des Auftragsbearbeiters, analog zur Geschäftsherrenhaftung gem. Art. 55 OR (*cura in eligendo, in instruendo, in custodiendo*).

> Die strafrechtliche Qualifizierung des Auftragsbearbeiters als Hilfsperson und die damit einhergehende rechtliche Fiktion, dass hierbei keine Geheimnisoffenbarung stattfindet, ist ein Element, das dafür spricht, dass die Auftragsdatenbearbeitung eine privilegierte Rechtsbeziehung darstellt, bei welcher **keine «Bekanntgabe»** im datenschutzrechtlichen Sinne stattfindet.[66]

44. Das Offenbaren eines Geheimnisses kann **gerechtfertigt** werden, wenn die betroffene Person eingewilligt hat (beim Berufsgeheimnis) oder wenn die vorgesetzte Behörde ihre Einwilligung gegeben hat (beim Amts- wie beim Berufsgeheimnis). Hierfür ist eine Einwilligung im jeweils konkreten Fall notwendig, eine Pauschaleinwilligung der vorgesetzten Behörde nach Art. 320 Abs. 2 StGB kann diese nicht ersetzen.[67]

bb) Kantonale Datenschutzgesetze

45. Die meisten **Kantone** haben ihr kantonales Datenschutzgesetz in den vergangenen Jahren revidiert, um den Rechtsentwicklungen auf europäischer Ebene (namentlich die Pflicht zur Umsetzung der Richtlinie 2016/680) Rechnung zu tragen.[68] Nachfolgend werden einige kantonale Regelungen zur Bearbeitung im Auftrag dargestellt, wobei der Akzent auf denjenigen Vorgaben bzw. kantonalen Regelungen liegt, welche besondere Anforderungen für die Auftragsbearbeitung formulieren.

46. Im Kanton **Aargau** verlangt § 18 IDAG-AG[69], dass bei der Datenbearbeitung durch Dritte der Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sichergestellt werden muss. Das öffentliche Organ bleibt für die Einhaltung des Datenschutzes verantwortlich; die Rechte der Betroffenen sind ihm gegenüber geltend zu machen.

47. Im Kanton **Appenzell Innerrhoden** ist Voraussetzung für die «Übertragung an Dritte», dass dafür eine generell-abstrakte oder schriftliche vertragliche Regelung besteht, dass der Auftrag klar umschrieben ist und die Einhaltung der gesetzlichen Vorgaben

---

64 MÉTILLE, in: Métille/Meier (Hrsg.), CR-LPD, Art. 9 DSG N 66.
65 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 30.
66 Oben N 31.
67 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 56.
68 Zum aktuellen Stand der Revisionen in den Kantonen s. die Übersichtswebsite von *privatim*, www.privatim.ch (zuletzt besucht am 20.9.2023).
69 Gesetz [des Kantons Aargau] über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen vom 24.10.2006 (IDAG), SAR 150.700.

durch geeignete Massnahmen sichergestellt ist (Art. 6 DIAG-AI[70]). Das öffentliche Organ bleibt «mitverantwortlich».

48. In den Kantonen **Basel-Landschaft** und **Basel-Stadt** darf die Datenbearbeitung an einen Auftragsdatenbearbeiter übertragen werden, wenn keine rechtlichen oder vertraglichen Bestimmungen entgegenstehen und wenn sichergestellt ist, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte (§ 7 Abs. 1 IDG-BL[71] und wortlautgleicher § 7 Abs. 1 IDG-BS[72]). Das öffentliche Organ bleibt für den Umgang mit Informationen verantwortlich.

49. Der Kanton **Freiburg** enthält im kantonalen Datenschutzgesetz eine besonders ausführliche Regelung zur «Auslagerung» der Datenbearbeitung. Personenbezogene Daten, einschliesslich besonders schützenswerter Daten, dürfen nur ausgelagert werden, wenn die Daten «jederzeit auf dem Gebiet der Schweiz oder auf dem Gebiet eines Staates, der einen gleichwertigen Datenschutz gewährleistet, bearbeitet werden» (Art. 12b Abs. 2 DSchG-FR[73]). Das öffentliche Organ bleibt für den Schutz der Personendaten, insbesondere für die Vertraulichkeit und die Kontinuität ihrer Aufbewahrung und Nutzung, verantwortlich und muss diesbezüglich Massnahmen ergreifen (Art. 12c DSchG-FR). So muss es bei der Wahl, Weisungserteilung und Aufsicht des Auftragsbearbeiters Vorsichtsmassnahmen ergreifen und einen Vertrag mit diesem abschliessen, der den Schutz und die Sicherheit der Daten und deren eigenen Informationssysteme gewährleistet, wobei das Gesetz für den Vertrag gewisse Mindestinhalte vorschreibt; u.a. muss das öffentliche Organ den Auftragsbearbeiter verpflichten, den Verantwortlichen der Datensammlung unverzüglich zu informieren, wenn er aufgrund eines ausländischen Gesetzes oder eines richterlichen Entscheids die Daten einer ausländischen Behörde bekanntgeben muss oder Gefahr läuft, dass er es tun muss (Art. 12c Abs. 1 lit. b Ziff. 6 DSchG-FR). Betrifft die Auslagerung mehrere Organe desselben Gemeinwesens, so muss ein hauptverantwortliches Organ bezeichnet werden (Art. 12c Abs. 2 DSchG-FR). Das Gesetz schreibt Sicherheitsmassnahmen vor, welche die kantonalen Behörden umzusetzen haben, wenn sie Datenbearbeitungen auslagern; namentlich müssen sie die Unversehrtheit, die Authentizität, die Verfügbarkeit und die Vertraulichkeit der Personendaten, die von einer Auslagerung betroffen sind, sowie deren ständige Aufbewahrung und Verwendung mit geeigneten, dem Stand der Technik entsprechenden, organisatorischen und technischen Massnahmen sicherstellen (Art. 12d Abs. 1 DSchG-FR). Diese Sicherheitsmassnahmen sind basierend auf einer Risikoabwägung zu definieren: Das kantonale Organ muss die Gefahren, die das Bearbeiten der fraglichen Daten für die Persönlichkeit und die Grundrechte der betroffenen Personen mit sich bringt, berücksichtigen (Art. 12d Abs. 2 DSchG-FR); zudem muss ein angemessenes Dispositiv für den Fall eines «Zwischenfalls» getroffen

---

70 Datenschutz-, Informations- und Archivgesetz [des Kantons Appenzell-Innerrhoden] vom 28.04.2019 (DIAG), GS 172.800.

71 Gesetz [des Kantons Basel-Landschaft] vom 10. Februar 2011 über die Information und den Datenschutz, SGS 162.

72 Gesetz [des Kantons Basel-Stadt] vom 10. Juni 2010 über die Information und den Datenschutz, SG 153.260.

73 Gesetz [des Kantons Freiburg] vom 25. November 1994 über den Datenschutz (DSchG), SGF 17.1.

werden, wenn die Auslagerung Daten betrifft, die für den Betrieb der Verwaltung unbedingt nötig sind. Wird die Bearbeitung von besonders schützenswerten Personendaten ausgelagert, so sind besondere Vorkehrungen zu treffen: Unterliegen diese Daten einer gesetzlichen oder vertraglichen Geheimhaltungspflicht und besteht ein konkretes Risiko, dass gegen das Recht der betroffenen Personen verstossen wird, so darf diese Bearbeitung nur ausgelagert werden, wenn die Vertraulichkeit gegenüber dem Auftragsbearbeiter sichergestellt ist, so dass dieser auf deren Inhalt keinen Zugriff hat (Art. 12e Abs. 1 DSchG-FR); zu denken ist hier insbesondere an Verschlüsselung der Daten. Muss der Auftragsbearbeiter aus technischen Gründen unbedingt Zugriff auf die Daten haben, so müssen im Auslagerungsvertrag besondere Anforderungen bezüglich des Bearbeitens solcher besonders schützenswerter Personendaten festgelegt werden, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis des öffentlichen Organs auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen (Art. 12e Abs. 2 DSchG-FR). Schliesslich ist der Staatsrat des Kantons Freiburg verpflichtet, dem Kantonsparlament in regelmässigen Abständen über die Auslagerung Bericht zu erstatten (Art. 12b Abs. 4 DschG-FR).

> Das kantonale Datenschutzgesetz im Kanton Freiburg wurde totalrevidiert; der Grosse Rat verabschiedete das Gesetz im Oktober 2023, und es wird am 1. Januar 2024 in Kraft treten. Die erwähnten Bestimmungen über die Auftragsbearbeitung werden weitgehend unverändert in Art. 18 ff. DSchG n.F. übernommen.

50. Die Regelungen anderer Kantone sind wesentlich knapper, so schreibt etwa das Gesetz im **Kanton Solothurn** lediglich vor, dass eine Behörde, die Personendaten durch Dritte bearbeiten lässt, den Datenschutz durch Vereinbarungen, Auflagen oder in anderer Weise sicherzustellen hat (§ 17 InfoDG-SO[74]). Ähnliche Regelungen finden sich auch z.B. in den Kantonen **Schwyz** (§ 20 ÖDSG-SZ[75]), **Thurgau** (§ 12 DSG-TG[76]) oder **Wallis** (Art. 29 GIDA-VS[77]).

51. Im **Kanton Zürich** bestand bis anhin ebenfalls eine eher knappe Regelung, wonach die Übertragung von Daten zur Bearbeitung durch Dritte zulässig ist, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht, und das öffentliche Organ verantwortlich bleibt (§ 6 IDG-ZH[78]). Das IDG wird derzeit revidiert, die vom Regierungsrat im Sommer 2023 nach Abschluss der Vernehmlassung an den Kantonsrat überwiesene Vorlage[79] sieht für die «Informationsbearbeitung durch Dritte» zusätzlich

---

74 Informations- und Datenschutzgesetz [des Kantons Solothurn] vom 21. Februar 2001 (InfoDG), BGS 114.1.

75 Gesetz [des Kantons Schwyz] über die Öffentlichkeit der Verwaltung und den Datenschutz vom 23. Mai 2007, SRSZ 140.410.

76 Gesetz [des Kantons Thurgau] über den Datenschutz vom 09. November 1987 (TG DSG), RB 170.7.

77 Gesetz [des Kantons Wallis] über die Information der Öffentlichkeit, den Datenschutz und die Archivierung vom 9.10.2008 (GIDA), neue Version in Kraft ab 01.01.2024, SGS 170.2.

78 Gesetz [des Kantons Zürich] vom 12. Februar 2007 über die Information und den Datenschutz, LS 170.4.

79 Antrag 5923 des Regierungsrates vom 5. Juli 2023: Gesetz über die Information und den Datenschutz (IDG), https://www.zh.ch/de/politik-staat/gesetze-beschluesse/beschluesse-des-regierungsrates/rrb/regierungsratsbeschluss-878-2023.html (zuletzt besucht am 20.9.2023).

zur bisherigen Regelung vor, dass die Dritten die Informationssicherheit gewährleisten müssen, Informationen nur so bearbeiten dürfen, wie es das öffentliche Organ selbst tun darf, und die Bearbeitung erst nach Bewilligung durch das öffentliche Organ an weitere Dritte übertragen dürfen (§ 9 Abs. 2 eIDG-ZH).

2. Bekanntgabe ins Ausland

52. Ähnlich wie bei der Datenbearbeitung im Auftrag bezwecken die Regeln zur Bekanntgabe von Personendaten ins Ausland das Verhindern einer Relativierung des Datenschutzrechts durch die Weitergabe von Daten. Anders als bei der Auftragsdatenbearbeitung, welche im Grundsatz nur so vorgenommen werden darf, wie der Verantwortliche es dürfte, gilt bei einer Datenbekanntgabe ins Ausland ein anderer Standard. Dieser Standard ist in der Regel derjenige der «**Angemessenheit**»; m.a.W. muss am Zielort ein «angemessenes», jedoch kein identisches Datenschutzniveau herrschen wie am Ausgangsort der Daten, wobei es hiervon einige eng gefasste Ausnahmen gibt. Zudem dürfen die Daten, anders als bei der Auftragsdatenbearbeitung, nach der Entgegennahme durch den ausländischen Dritten und sofern die entsprechenden Voraussetzungen, namentlich Rechtfertigungsgründe, erfüllt sind, auch zu anderen Zwecken und mit anderen Mitteln bearbeitet werden, als dies der «einheimische» Verantwortliche tut.

Diese Grundsätze werden in den verschiedenen einschlägigen Rechtsakten etwas unterschiedlich formuliert bzw. konkretisiert.

a) Konvention Nr. 108+ des Europarates

53. Eine der Neuerungen der modernisierten Konvention 108+ betrifft auch den **grenzüberschreitenden Verkehr** personenbezogener Daten. Art. 14 der modernisierten Konvention unterscheidet zwischen der Weitergabe personenbezogener Daten in andere Vertragsstaaten der Konvention und der Weitergabe in Nichtvertragsparteien. Während die Weitergabe an Empfänger, die der Hoheitsgewalt einer anderen Vertragspartei unterstehen, grundsätzlich nicht verboten oder einer Genehmigung unterstellt werden darf, es sei denn, es bestünde eine tatsächliche und ernsthafte Gefahr, dass dies zu einer Umgehung des durch die Konvention vorgesehenen Schutzes führen würde (Art. 14 Abs. 1 Konvention 108+), ist eine Weitergabe in eine Nichtvertragspartei nur zulässig, wenn ein **angemessenes Schutzniveau** vorliegt (Art. 14 Abs. 2 Konvention 108+). Ein solches kann sichergestellt werden durch das nationale Recht des Nichtvertragsstaats, durch einen völkerrechtlichen Vertrag oder durch entsprechende *ad hoc*- oder standardisierte Garantien, sofern sie rechtlich bindend und durchsetzbar sind (Art. 14 Abs. 3 lit. a und b Konvention 108+).

54. Von den erwähnten Regeln für die Weitergabe personenbezogener Daten in andere Staaten darf gemäss Art. 14 Abs. 4 Konvention 108+ in folgenden Fällen **abgewichen** werden:

- Es liegt eine **Einwilligung** der oder des Betroffenen vor (lit. a), wobei die Einwilligung ausdrücklich, für den konkreten Fall, freiwillig und informiert erfolgen muss.
- Die Weitergabe ist im Einzelfall wegen **spezifischer Interessen des Betroffenen** erforderlich (lit. b).

- Es liegen **überwiegende berechtigte Interessen** vor, insbesondere **wichtige öffentliche Interessen**, die gesetzlich vorgesehen sind und die eine Weitergabe der Daten als eine in einer demokratischen Gesellschaft notwendige und verhältnismässige Massnahme erscheinen lassen (lit. c).
- Die Weitergabe ist im Hinblick auf die **Meinungsfreiheit** notwendig und verhältnismässig (lit. d).

55. Erfolgt eine Weitergabe in einen anderen Staat gestützt auf geeignete Garantien (Art. 14 Abs. 3 lit. b Konvention 108+), spezifische Interessen des Betroffenen (Art. 14 Abs. 4 lit. b Konvention 108+) oder überwiegender berechtigter Interessen (Art. 14 Abs. 4 lit. c Konvention 108+), so müssen die Verantwortlichen der zuständigen **nationalen Aufsichtsbehörde** alle sachdienlichen Informationen hinsichtlich dieser Datenweitergaben zur Verfügung stellen (Art. 14 Abs. 5 Konvention 108+). Das Vorliegen überwiegender berechtigter Interessen muss zudem nachgewiesen werden können, und die Aufsichtsbehörde muss eine solche Datenweitergabe verbieten, aussetzen oder an Bedingungen knüpfen können (Art. 14 Abs. 6 Konvention 108+).

b) Richtlinie 2016/680 und Seitenblick auf die Datenschutzgrundverordnung

56. Kapitel V der Richtlinie 2016/680 regelt die **Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen**. Die Regelung ist wesentlich umfassender als noch unter der Vorgängerregelung (der Rahmenbeschluss 2008/977/JI), wobei sich das neue Regime in seinem grundsätzlichen Aufbau an jenes der Datenschutzgrundverordnung anlehnt. Ausgeweitet wird zunächst der Anwendungsbereich der Regelung, der sich auf sämtliche Datenübermittlungen an Drittländer erstreckt, während sich das Regime des Rahmenbeschlusses lediglich auf Daten bezog, welche die nationalen Behörden von den Behörden anderer Mitgliedstaaten erhalten haben.

57. Zur Übermittlung erforderlich ist zunächst das Vorliegen von **drei allgemeinen Voraussetzungen** (Art. 35 Abs. 1 RL 2016/680):
- Die Übermittlung muss zur Erreichung der **Richtlinienzwecke** erforderlich sein (Art. 35 Abs. 1 lit. a RL 2016/680).
- Beim Empfänger muss es sich grundsätzlich um eine im Sinne der Richtlinie zuständige **Behörde** handeln (Art. 35 Abs. 1 lit. b RL 2016/680). M.a.W. dürfen personenbezogene Daten zu Richtlinienzwecken nur an ausländische Behörden, die in der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, der Strafvollstreckung, sowie dem Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit tätig sind, übermittelt werden. Handelt es sich um andere Empfänger, ist Art. 39 RL 2016/680 einschlägig.[80]
- Es muss eine **Genehmigung** des betreffenden Mitgliedstaats vorliegen, wenn Daten übermittelt werden sollen, die **ursprünglich aus einem anderen Mitgliedsstaat stammen**. Vorbehalten sind Fälle unmittelbarer und ernsthafter Gefahr für die öffentliche Sicherheit (Art. 35 Abs. 1 lit. c und Art. 35 Abs. 2 RL 2016/680).

---

[80] S. hierzu unten N 59.

58. Überdies muss ein **Erlaubnistatbestand** gegeben sein (Art. 35 Abs. 1 lit. d sowie Art. 36 ff. RL 2016/680). Überblickt man den hiermit geschaffenen Regelungsrahmen, so wird der erste Eindruck einer vergleichsweise restriktiven Ausformung der Übermittlungsvoraussetzungen dadurch relativiert, dass im Rahmen der Erlaubnistatbestände eher weit gefasste Ausnahmeklauseln bestehen:

- Mit dem **Angemessenheitsbeschluss** bestätigt die Kommission im Rahmen eines Durchführungsrechtsakts, dass ein Drittland bzw. eine internationale Organisation ein angemessenes Schutzniveau bietet, wobei der Richtlinie Vorgaben zu den hierfür heranzuziehenden Kriterien (Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten etc.) zu entnehmen sind (Art. 36 RL 2016/680).
- **Geeignete Garantien** können als Grundlage für eine Übermittlung herangezogen werden, wenn sie entweder in einem rechtsverbindlichen Instrument verankert sind oder der Verantwortliche gestützt auf eine umfassende Abwägung zum Schluss gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten vorliegen (Art. 37 RL 2016/680).
- Schliesslich kann sich die Übermittlungserlaubnis gestützt auf die vorgesehenen **Ausnahmebestimmungen** ergeben, wenn die Übermittlung erforderlich ist, um lebenswichtige Interessen einer Person zu schützen, rechtlich geschützte berechtigte Interessen der betroffenen Person zu wahren, eine unmittelbare oder ernsthafte Gefahr für die öffentliche Sicherheit abzuwenden oder im Einzelfall die Zwecke der Richtlinie zu erreichen oder Rechtsansprüche im Zusammenhang mit diesen Zwecken geltend zu machen oder auszuüben (Art. 38 Abs. 1 RL 2016/680).

59. Ferner können auch personenbezogene Daten an **weitere Empfänger in Drittländern** übermittelt werden, die nicht in den engen Kreis von «im Sinne der Richtlinie zuständigen Behörden» im Drittland (Art. 35 Abs. 1 lit. b RL 2016/680) fallen, sofern die übrigen Bestimmungen der Richtlinie eingehalten werden und die Voraussetzungen von Art. 39 RL 2016/680 erfüllt sind:

- Die Übermittlung erfolgt ausschliesslich im **speziellen Einzelfall** (Art. 39 Abs. 1 RL 2016/680).
- Die Übermittlung ist für die Ausübung der Richtlinienzwecke **unbedingt erforderlich** (Art. 39 Abs. 1 lit. a RL 2016/680).
- Die **Grundrechte und Grundfreiheiten** der betroffenen Person überwiegen das öffentliche Interesse an der Übermittlung nicht (Art. 39 Abs. 1 lit. b RL 2016/680).
- Die Übermittlung an eine gem. Art. 35 Abs. 1 lit. b RL 2016/680 zuständige Behörde wäre im konkreten Fall **wirkungslos oder ungeeignet** (Art. 39 Abs. 1 lit. c RL 2016/680).
- Die zuständige Behörde wird unverzüglich **unterrichtet**, sofern dies nicht wirkungslos oder ungeeignet ist (Art. 39 Abs. 1 lit. d RL 2016/680).
- Dem Empfänger werden die **festgelegten Zwecke der Datenbearbeitung** mitgeteilt (Art. 39 Abs. 1 lit. e RL 2016/680).

60. Aufgrund der inhaltlichen Parallelitäten lohnt sich auch ein Blick auf die Vorschriften der **Datenschutzgrundverordnung** zur Übermittlung personenbezogener Daten an

Drittländer, welche sich in den Artikeln 44 bis 50 DSGVO finden.[81] Übermittlungen an Drittländer sind im Grundsatz nur zulässig, wenn ein **Angemessenheitsbeschluss** der EU-Kommission vorliegt, welcher gestützt auf eine Reihe von in der DSGVO festgelegten Kriterien (Art. 45 Abs. 2 DSGVO) festhält, dass der betreffende Drittstaat ein angemessenes Schutzniveau bietet (Art. 45 Abs. 3 DSGVO).

> Nachdem der EuGH in der Rs. C-311/18 (*Schrems II*) festgestellt hatte, dass der sog. *EU-US privacy shield* kein angemessenes Schutzniveau gewährleisten kann, bestand für die USA während mehrerer Jahre kein Angemessenheitsbeschluss der Kommission. Am 10. Juli 2023 hat die Kommission auf der Grundlage des neu verhandelten ***EU-US Data Privacy Framework*** einen neuen Angemessenheitsbeschluss verabschiedet.[82]

61. Falls kein Angemessenheitsbeschluss vorliegt, kann eine Datenübermittlung stattfinden, sofern **geeignete Garantien** vorliegen und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 Abs. 1 DSGVO). Solche Garantien sind:

- ein **Abkommen** zwischen den betreffenden Behörden oder öffentlichen Stellen (Art. 46 Abs. 2 lit. a DSGVO);
- von der zuständigen Aufsichtsbehörde genehmigte verbindliche **interne Datenschutzvorschriften** (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DSGVO);
- **Standarddatenschutzklauseln** (Art. 46 Abs. 2 lit. d DSGVO);
- genehmigte **Verhaltensregeln** (Art. 46 Abs. 2 lit. e DSGVO);
- ein genehmigter **Zertifizierungsmechanismus** in Verbindung mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des im Drittland ansässigen Verantwortlichen (Art. 46 Abs. 2 lit. f DSGVO);
- genehmigte **Vertragsklauseln** (Art. 46 Abs. 3 lit. a DSGVO);
- in **Verwaltungsvereinbarungen** zwischen Behörden aufgenommene Bestimmungen (Art. 46 Abs. 3 lit. b DSGVO).

62. Von diesen Vorschriften für die Datenübermittlung in Drittstaaten kann abgewichen werden, sofern eine der folgenden **Ausnahmen** vorliegt:

- Die betroffene Person hat eingewilligt, wobei die **Einwilligung** ausdrücklich, für den konkreten Fall, freiwillig, und informiert erfolgen muss (Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO).
- Die Übermittlung dient dem **Abschluss oder der Erfüllung eines Vertrags** (Art. 49 Abs. 1 UAbs. 1 lit. b und c DSGVO).
- Die Übermittlung ist aus **wichtigen Gründen des öffentlichen Interesses** notwendig (Art. 49 Abs. 1 UAbs. 1 lit. d DSGVO); das öffentliche Interesse muss im Unionsrecht oder im nationalen Recht anerkannt sein (Art. 49 Abs. 4 DSGVO).
- Die Übermittlung ist erforderlich zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** (Art. 49 Abs. 1 UAbs. 1 lit. e DSGVO).
- Sie ist erforderlich zum Schutz **lebenswichtiger Interessen** der betroffenen Person, sofern diese keine Einwilligung geben kann (Art. 49 Abs. 1 UAbs. 1 lit. f DSGVO).

---

81 Vgl. zu den Regeln über die Datenbekanntgabe an Drittstaaten die einschlägigen, im Literaturverzeichnis zitierten Kommentare.

82 C(2023) 4745 final. S. insoweit schon oben N 12.

- Es handelt sich um ein **öffentliches Register** (Art. 49 Abs. 1 UAbs. 1 lit. g DSGVO).
- Die Übermittlung ist im Einzelfall und für eine begrenzte Zahl von betroffenen Personen notwendig für die Wahrung **zwingender berechtigter Interessen** des Verantwortlichen und sofern die Interessen und Rechte der betroffenen Person nicht überwiegen (Art. 49 Abs. 1 UAbs. 2 DSGVO).

63. Mitgliedstaatliche **Behörden, die in Ausübung ihrer hoheitlichen Befugnisse** tätig sind, können sich nur auf die Ausnahmetatbestände der wichtigen Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d DSGVO), der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e DSGVO), des Schutzes lebenswichtiger Interessen der betroffenen Person (Art. 49 Abs. 1 UAbs. 1 lit. f DSGVO) sowie der öffentlichen Register (Art. 49 Abs. 1 UAbs. 1 lit. g DSGVO) berufen, nicht jedoch auf die anderen aufgezählten Ausnahmetatbestände (Art. 49 Abs. 3 DSGVO).

c) Rechtsvergleich: DSG und kantonale Regelungen

aa) Datenschutzgesetz des Bundes

64. Gemäss Art. 16 DSG dürfen Personendaten nur ins Ausland bekanntgegeben werden, wenn ein Entscheid des Bundesrats über die **Angemessenheit** des Schutzes personenbezogener Daten im betreffenden Staat vorliegt (Art. 16 Abs. 1 DSG). In Abwesenheit eines solchen Entscheides, kann ein geeigneter Datenschutz auch durch eine der folgenden **Garantien** gewährleistet werden:

- ein **völkerrechtlicher Vertrag** (Art. 16 Abs. 2 lit. a DSG);
- **vertragliche Datenschutzklauseln** (Art. 16 Abs. 2 lit. b DSG);
- **spezifische Garantien** des zuständigen Bundesorgans (Art. 16 Abs. 2 lit. c DSG);
- vom EDÖB genehmigte **Standarddatenschutzklauseln** (Art. 16 Abs. 2 lit. d DSG);
- verbindliche, vom EDÖB oder einer anderen ausländischen Behörde genehmigte **unternehmensinterne Datenschutzvorschriften** (Art. 16 Abs. 2 lit. e DSG);
- vom EDÖB genehmigte **Verhaltenskodizes oder Zertifizierungen**, welche mit einer verbindlichen und durchsetzbaren Verpflichtung des Verantwortlichen oder Auftragbearbeiters im Drittstaat verbunden sind, die darin enthaltenen Massnahmen anzuwenden (Art. 16 Abs. 3 DSG i.V.m. Art. 12 DSV).

Analog zum *EU-US Data Privacy Framework* und dem entsprechenden Angemessenheitsbeschluss der EU ist die Schweiz ebenfalls daran, mit den USA Gespräche zur Erstellung eines entsprechenden Rahmenwerks (**Swiss-US Data Privacy Framework**) zu führen. Solange der Bundesrat keinen Beschluss darüber trifft, die USA in die Liste der Staaten mit angemessenem Datenschutz aufzunehmen, gilt die USA aktuell weiterhin als Staat ohne angemessenen Schutz.[83]

65. **Ausnahmen** von den genannten Voraussetzungen für die Bekanntgabe von Personendaten ins Ausland sind in Art. 17 DSG geregelt. Liegt weder eine Angemessenheits-

---

83 S. insoweit bereits oben N 12.

entscheidung noch eine andere geeignete Garantie i.S.v. Art. 16 DSG vor, so dürfen Bundesorgane und Privatpersonen Personendaten ins Ausland bekanntgeben, wenn eine der folgenden Ausnahmetatbestände vorliegt:

- ausdrückliche **Einwilligung** der betroffenen Person in die Bekanntgabe (Art. 17 Abs. 1 lit. a DSG);
- unmittelbarer Zusammenhang der Bekanntgabe mit dem **Abschluss oder der Abwicklung eines Vertrags** (Art. 17 Abs. 1 lit. b Ziff. 1 und 2 DSG);
- Notwendigkeit der Bekanntgabe für die Wahrung eines **überwiegenden öffentlichen Interesses** (Art. 17 Abs. 1 lit. c Ziff. 1 DSG);
- Notwendigkeit der Bekanntgabe für die Feststellung, Ausübung oder Durchsetzung von **Rechtsansprüchen** vor einem Gericht oder einer ausländischen Behörde (Art. 17 Abs. 1 lit. c Ziff. 2 DSG);
- Notwendigkeit der Bekanntgabe zum **Schutz des Lebens oder der körperlichen Unversehrtheit** der betroffenen Person oder eines Dritten (Art. 17 Abs. 1 lit. d DSG);
- allgemeines **Zugänglichmachen** der Daten durch die betroffene Person (Art. 17 Abs. 1 lit. e DSG);
- Herkunft der Personendaten aus einem **öffentlichen Register** (Art. 17 Abs. 1 lit. f DSG).

66. Der Ausnahmetatbestand der **überwiegenden öffentlichen Interessen** entspricht demjenigen in Art. 49 Abs. 1 lit. d DSGVO.[84] Es genügt dabei sowohl ein überwiegendes öffentliches Interesse der Schweiz als auch eines ausländischen Staates, dieses muss jedoch konkret nachgewiesen und darf nicht bloss hypothetisch sein.[85] Als öffentliche Interessen, die (ggf.) überwiegen können, werden etwa die innere Sicherheit, Betrugsbekämpfung, Kampf gegen Geldwäscherei und Terrorismus, oder das Interesse an der Beilegung diplomatischer Streitigkeiten, wie etwa dem sog. Steuerstreit, genannt.[86] Die Datenbekanntgabe muss zur Wahrung dieses Interesses notwendig sein (m.a.W. **unerlässlich**[87]); die Gerichtspraxis zum altrechtlichen Ausnahmetatbestand des überwiegenden öffentlichen Interesses ist diesbezüglich **äusserst streng**.[88]

67. Schliesslich sei daran erinnert, dass der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter sich zwar auf Art. 17 Abs. 1 lit. c Ziff. 1 DSG berufen kann, um personenbezogene Daten in einen Staat zu übermitteln, der kein angemessenes Schutzniveau gewährleistet, dass aber dennoch die **Einhaltung der allgemeinen Grundsätze des Datenschutzrechts** sichergestellt werden muss.[89]

---

84 KUNZ, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 17 N 15.

85 Vgl. BGer 4A_83/2016 v. 22.09.2016, E. 3.3.4.

86 HUSI-STÄMPFLI, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 17 N 13; KUNZ, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 17 N 17.

87 Das Bundesgericht hat mehrfach festgestellt, dass die Datenübermittlung zur Wahrung des öffentlichen Interesses «absolument nécessaire», respektive «unerlässlich» («indispensable») sein muss, s. BGer 4A_452/2018 v. 1.10.2018, E. 3.2.3; BGer 4A_83/2016 v. 22.09.2016, E. 3.3.4; BGer 4A_73/2017 v. 26.07.2017, E. 3.1; BGer 4A_390/2017 v. 23.11.2017 E. 4.3.2.

88 KUNZ, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 17 N 10.

89 FISCHER, in: Métille/Meier (Hrsg.), CR-LPD, Art. 17 N 32.

bb) Kantonale Datenschutzgesetze

68. Im **Kanton Zürich** sieht das IDG derzeit vor, dass Personendaten an Staaten, die der Europarats-Konvention Nr. 108 nicht unterstehen, nur bekanntgegeben werden dürfen, wenn (a) im Empfängerstaat ein angemessener Schutz für die Datenübermittlung gewährleistet ist, (b) eine gesetzliche Grundlage dies erlaubt, um bestimmte Interessen der betroffenen Person oder überwiegende öffentliche Interessen zu schützen, oder (c) vom öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen werden (§ 19 IDG). Das IDG wird derzeit revidiert; die vom Regierungsrat im Sommer 2023 nach Abschluss der Vernehmlassung an den Kantonsrat überwiesene Vorlage ist im Bereich der Datenübermittlung ins Ausland weitgehend unverändert (§ 36 E-IDG).

69. Im **Kanton Glarus** dürfen Personendaten ins Ausland bekannt gegeben werden, wenn im Empfängerland ein angemessener Datenschutz gewährleistet ist (Art. 24 Abs. 1 IDAG-GL[90]). Zudem sind die folgenden Ausnahmetatbestände im Gesetz vorgesehen: völkerrechtliche Verpflichtung zur Bekanntgabe; Einwilligung der betroffenen Person; allgemein zugängliche Personendaten oder öffentliche Register und amtliche Veröffentlichungen; Notwendigkeit der Bekanntgabe für die Wahrnehmung schutzwürdiger Interessen oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht; unmittelbarer Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags (Art. 24 Abs. 2 IDAG-GL).

70. Im **Kanton St. Gallen** richtet sich die Bekanntgabe von Personendaten ins Ausland sinngemäss nach den Bestimmungen der Bundesgesetzgebung über den Datenschutz (Art. 16 Abs. 1 DSG-SG[91]); es sind also sowohl die Regelungen im Grundsatz wie auch die Ausnahmetatbestände des Bundesdatenschutzgesetzes anwendbar. Will eine kantonale Behörde Personendaten in einen Staat bekanntgeben, der nicht auf der vom EDÖB veröffentlichten Liste der Staaten mit angemessener Datenschutzgesetzgebung aufgeführt ist, so hat sie zusätzlich die zuständige kantonale Fachstelle für Datenschutz zu informieren (Art. 16 Abs. 2 DSG-SG).

71. Demgegenüber ist die Regelung im **Kanton Schwyz** relativ einfach: Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet (§ 18g des kantonalen Gesetzes über die Öffentlichkeit der Verwaltung und den Datenschutz[92]).

72. Im **Kanton Uri** sieht das revidierte Gesetz über den Schutz von Personendaten[93] vor, dass Personendaten in Länder der Europäischen Union sowie in Vertragsstaaten des

---

90 Gesetz [des Kantons Glarus] über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 05.09.2021, GS I F/1.

91 Datenschutzgesetz [des Kantons St. Gallen] vom 20.01.2009 (DSG), sGS 142.1.

92 Gesetz [des Kantons Schwyz] über die Öffentlichkeit der Verwaltung und den Datenschutz vom 23.05.2007, SRSZ 140.410.

93 Gesetz [des Kantons Uri] über den Schutz von Personendaten (Kantonales Datenschutzgesetz, KDSG) vom 24.05.2023.

Übereinkommens 108 des Europarats bekannt gegeben werden dürfen, wenn die Voraussetzungen erfüllt sind, die für die Bekanntgabe von Daten im Inland erfüllt sein müssen (Art. 10b) Abs. 1 KDSG-UR). Bekanntgaben in Drittländer richten sich grundsätzlich nach den Erlaubnistatbeständen von Art. 16 DSG; zusätzlich sind die folgenden Ausnahmen im kantonalen Datenschutzgesetz vorgesehen: Notwendigkeit der Bekanntgabe für die Wahrung eines überwiegenden öffentlichen Interesses bzw. für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde; zum Schutz des Lebens oder der körperlichen Unversehrtheit der betroffenen Person oder einer Drittperson, sofern keine Einwilligung eingeholt werden kann; allgemeine Zugänglichmachung der Daten; öffentliche Register (Art. 10b) Abs. 3 KDSG-UR).

73. Das jüngst teilrevidierte Datenschutzgesetz[94] des **Kantons Wallis** sieht vor, dass Personendaten ins Ausland bekannt gegeben werden dürfen, wenn der Empfänger der Gerichtsbarkeit von Staaten oder Organisationen unterliegt, die ein angemessenes Schutzniveau für die beabsichtigte Übermittlung von Personendaten gewährleisten (Art. 25 Abs. 1 GIDA-VS). Ein solches Schutzniveau wird durch hinreichende, insbesondere vertragliche Garantien gewährleistet, welche vom kantonalen Beauftragten genehmigt, ausgestellt oder anerkannt werden müssen (Art. 25 Abs. 1bis GIDA-VS). Ausnahmsweise können Personendaten bekannt gegeben werden, wenn die betroffene Person eingewilligt hat, die Bekanntgabe zur Wahrung eines überwiegenden öffentlichen Interesses, für die Feststellung, die Ausübung oder die Verteidigung eines Rechtes vor Gericht oder für den Schutz des Lebens oder der körperlichen Integrität der betroffenen Person oder einer Drittperson unerlässlich ist, oder wenn die Bekanntgabe in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht (Art. 25 Abs. 2 GIDA-VS).

74. Der **Kanton Waadt** sieht im kantonalen Datenschutzgesetz[95] vor, dass eine Datenübermittlung ins Ausland nur stattfinden darf, wenn der betreffende Drittstaat über ein angemessenes Datenschutzniveau verfügt (Art. 17 Abs. 1 LPrD-VD). Als Ausnahmetatbestände sind die Folgenden vorgesehen: Einwilligung der betroffenen Person; Notwendigkeit für den Abschluss oder die Abwicklung eines Vertrags; Unerlässlichkeit für die Wahrung eines öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht; Erforderlichkeit zum Schutz des Lebens oder der körperlichen Integrität der betroffenen Person; öffentliche Register, oder Vorliegen hinreichender Garantien, namentlich vertraglicher Art (Art. 17 Abs. 2 LPrD-VD).

75. Im **Kanton Zug** gilt die Regelung, dass Personendaten nicht bekanntgegeben werden dürfen, wenn dadurch die Persönlichkeit der betroffenen Person gefährdet wird, was insbesondere bei Fehlen einer Gesetzgebung vorliegt, die einen angemessenen Schutz gewährleistet (§ 10a Abs. 1 DSG-ZG[96]). Liegt keine solche Gesetzgebung vor, muss zwingend einer der folgenden Ausnahmetatbestände erfüllt sein: hinreichende Garantien,

---

94 Gesetz [des Kantons Wallis] über die Information der Öffentlichkeit, den Datenschutz und die Archivierung vom 9.10.2008 (GIDA), neue Version in Kraft ab 01.01.2024, SGS 170.2.

95 Loi [du Canton de Vaud] sur la protection des données personnelles du 11 septembre 2007 (LPrD), 172.65.

96 Datenschutzgesetz [des Kantons Zug] vom 28.09.2000 (DSG), BGS 157.1.

insbesondere vertraglicher Art, über welche die kantonale Datenschutzstelle informiert wurde; Einwilligung der betroffenen Person; Unerlässlichkeit im Einzelfall für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht oder Erforderlichkeit, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen (§ 10a Abs. 2 DSG-ZG).

3. Weitere Vorgaben

76. Am Rande sei noch darauf hingewiesen, dass ggf. sektorspezifische Vorgaben zur Datenbearbeitung im Auftrag existieren können, welche die Kantone beim Vollzug von Bundesrecht zu berücksichtigen haben.

77. So schreibt etwa die Verordnung über das **elektronische Patientendossier**[97] in Art. 12 Abs. 5 ausdrücklich vor, dass sich die Datenspeicher in der Schweiz befinden und dem Schweizer Recht unterstehen müssen.

78. Im Bereich der **direkten Bundessteuer** bestimmt Art. 112a Abs. 1 DBG dass die Eidgenössische Steuerverwaltung zur Erfüllung der gesetzlichen Aufgaben ein Informationssystem betreiben soll, welches besonders schützenswerte Personendaten über administrative und strafrechtliche Sanktionen enthalten kann, die steuerrechtlich wesentlich sind. Die Personendaten und zur Bearbeitung verwendeten Einrichtungen sind vor unbefugtem Verwenden, Verändern oder Zerstören zu schützen.[98]

79. Für den Bund (nicht aber die Kantone) verpflichtend sind die Regelungen in der Verordnung über die **elektronische Geschäftsverwaltung in der Bundesverwaltung** (GEVER-Verordnung, SR 172.010.441), wo u.a. (Art. 11 ff. GEVER-Verordnung) einschlägige Informations- und Datenschutzvorgaben, wie z.B. die Verschlüsselungspflicht für «vertraulich» klassifizierte Informationen formuliert sind. Die ebenfalls das RVOG ausführende Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung[99] erlaubt in Art. 11 ausdrücklich, nicht allgemein zugängliche Daten externen Leistungserbringern zugänglich zu machen, wenn gewisse Voraussetzungen erfüllt sind; dazu gehören die Erforderlichkeit für die Leistungserbringung, die Zustimmung der verantwortlichen Behörde oder der vorgesetzten Stelle und angemessene vertragliche, organisatorische und technische Vorkehrungen, um eine weitere Verbreitung der Daten zu verhindern.

---

97 Verordnung über das elektronische Patientendossier (EPDV) vom 22. März 2017, SR 816.11.

98 Dazu DZAMKO, in: Métille (Hrsg), L'informatique en nuage, 83 (93).

99 Verordnung vom 25. November 2020 über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (VDTI), SR 172.010.58.

§ 3 Zur Zulässigkeit der Übermittlung von Personendaten ins Ausland zum Zweck der Bearbeitung im Auftrag, insbesondere im Rahmen von sog. *Cloud-Computing*

80. Nachdem in § 2 die verfassungs- und völkerrechtlichen Grundlagen sowie deren Konkretisierungen in völker- und unionsrechtlichen Instrumenten und in den Datenschutzgesetzen des Bundes und der Kantone dargelegt wurden, geht es im Folgenden darum, diese Grundlagen auf die vorliegend interessierende Problematik anzuwenden. Namentlich ist danach zu fragen, ob innerhalb des vom übergeordneten Recht vorgegebenen Rahmens Raum besteht für eine kantonale Regelung, welche die **Datenbekanntgabe ins Ausland** auch in **Staaten ohne angemessenes Datenschutzniveau** zulässt, wenn sie zum Zweck der **Bearbeitung im Auftrag** erfolgt und deren Voraussetzungen erfüllt sind (Art. 15 Abs. 3 lit. d VE-KDSG).

Diese Frage wird vor dem Hintergrund bearbeitet, dass Ziel dieser Regelung ist, die Nutzung von US-basierten *Cloud*-Lösungen durch öffentliche Organe im Kanton Bern zu ermöglichen, bei denen Datenübermittlungen in die USA erfolgen. Nicht eigens thematisiert wird, auf welche anderen möglichen Konstellationen diese Regelung allenfalls anwendbar wäre und welche möglichen Konsequenzen sich daraus ergeben würden. Dieser Aspekt ist aber für die grundsätzliche Zulässigkeit des Art. 15 Abs. 3 lit. d E-KDSG bzw. seine Vereinbarkeit mit übergeordnetem Recht durchaus von Bedeutung.

Nicht näher dargestellt werden allfällige spezialgesetzliche Vorgaben für die Zulässigkeit der Auslagerung von Datenbearbeitungen an *Cloud*-Dienstleister, wie sie etwa in der Verordnung über das elektronische Patientendossier oder im Gesetz über die Direkte Bundessteuer enthalten sind.

81. Ausgangspunkt der Untersuchung ist die Frage, ob im Rahmen von **Auftragsbearbeitungsverhältnissen** überhaupt eine **«Bekanntgabe» von Personendaten** stattfindet. Hierzu besteht, wie oben ausgeführt,[100] eine Rechtsunsicherheit, wobei u.E. zwar **gute Gründe** dafür sprechen, dass auch bei einer «Datenbekanntgabe» ins Ausland im Rahmen einer Auftragsbearbeitung keine Bekanntgabe im Sinne des Gesetzes vorliegt, da es sich beim Auftragsdatenbearbeitungsverhältnis um eine privilegierte Rechtsbeziehung handelt, bei welcher sich Verantwortlicher und Auftragsdatenbearbeiter gewissermassen unter derselben «Käseglocke» befinden und somit weder eine strafrechtliche Geheimnisverletzung noch eine datenschutzrechtliche Bekanntgabe stattfindet, solange der Auftragsbearbeiter ausschliesslich auf Weisung und an Stelle des Verantwortlichen die Daten bearbeitet.

82. Dessen ungeachtet legen es aber Hintergrund und Sinn und Zweck der (strengen) Regelungen der Zulässigkeit einer Datenbekanntgabe ins Ausland sowohl im Datenschutzgesetz des Bundes als auch in den kantonalen Datenschutzgesetzen nahe, dass im Falle einer Auftragsbearbeitung durch Anbieter im Ausland oder durch Anbieter, welche

---

100 N 27 ff.

die Datenbearbeitung im Ausland vornehmen, neben den Vorgaben für die Auftragsbearbeitung auch diejenigen für die **Bekanntgabe der Personendaten ins Ausland massgeblich** sind.[101]

Das **kantonale Datenschutzgesetz des Kantons Bern** ist in Bezug auf die Frage, ob im Falle einer Auftragsbearbeitung eine Bekanntgabe vorliegt, nicht ganz klar, jedenfalls soweit es um eine Auftragsbearbeitung im Ausland geht:[102] Die Begriffsdefinition des «Bekanntmachens» in Art. 2 Abs. 1 lit. e E-KDSG nennt den Vorgang des «Übertragens» (der im Zusammenhang mit der Auftragsbearbeitung in Art. 12 E-KDSG verwandt wird) nicht, was dafür spricht, dass bei der Auftragsbearbeitung eben gerade keine Bekanntgabe erfolgt. Allerdings dürfte die in die Vernehmlassung geschickte Variante (Art. 15 Abs. 3 lit. d E-KDSG) davon ausgehen, dass im Falle der Auftragsbearbeitung die Weitergabe der Daten an den Auftragsbearbeiter – jedenfalls soweit die Daten ins Ausland gelangen – eine Bekanntgabe im Sinne des Art. 2 Abs. 1 lit. e E-KDSG vorliegt, da hier von «Bekanntgabe zum Zweck der Bearbeitung im Auftrag» die Rede ist.

Jedenfalls ist festzuhalten, dass es nicht gegen übergeordnetes Recht verstiesse, im Falle einer Auftragsbearbeitung keine Datenbekanntgabe und damit auch keine Datenbekanntgabe ins Ausland anzunehmen. Das übergeordnete Recht, namentlich die Richtlinie 2016/680 sowie die Konvention 108+, stehen dieser Auslegung nämlich nicht entgegen respektive stützen sie (vgl. Art. 22 Abs. 5 RL 2016/680); zudem ist das Bearbeitungsprivileg im Rahmen der DSGVO anerkannt.[103] Ggf. wäre aus Gründen der Rechtssicherheit zu erwägen, diese Auslegung an geeigneter Stelle (z.B. in Art. 2 oder Art. 12 E-KDSG) im Gesetz zu verankern.

83. Vor diesem Hintergrund wird bei der nachfolgenden Analyse davon ausgegangen, dass im Falle einer **Auftragsbearbeitung durch Anbieter im Ausland oder durch Anbieter, welche die Datenbearbeitung im Ausland** vornehmen, neben den Vorgaben für die Auftragsbearbeitung auch diejenigen für die **Bekanntgabe der Personendaten ins Ausland** zu beachten sind (II.). Dies ändert freilich nichts daran, dass es in jedem Fall um eine **Auftragsbearbeitung** geht, so dass die diesbezüglichen Vorgaben jedenfalls einzuhalten sind, auch bei einer Nutzung von ausländischen *Cloud*-Lösungen im Rahmen einer Auftragsdatenbearbeitung (I.).

Der Klarheit halber sei in diesem Zusammenhang daran erinnert, dass sich die hier aufgeworfenen Rechtsfragen selbstredend nur dann stellen, wenn es um die Auftragsbearbeitung von **Personendaten** geht. Werden dem Auftragsbearbeiter nur **verschlüsselte Daten** übermittelt und bleibt der Schlüssel bei der auftraggebenden Behörde, so geht es bei den an den Auftragsbearbeiter weitergegebenen Daten nicht um Personendaten, so dass die Vorgaben des Datenschutzrechts diesbezüglich nicht anwendbar sind.[104]

I. Zulässigkeit der Auftragsbearbeitung

84. Wird davon ausgegangen, dass im Rahmen der Auftragsbearbeitung keine Datenbekanntgabe stattfindet und entgegen der hier vertretenen Auffassung die Voraussetzungen einer Bekanntgabe ins Ausland auch nicht sinngemäss zu beachten sind, so sind bzw. wären für die Zulässigkeit einer Auftragsbearbeitung ausschliesslich die Voraussetzun-

101 S. auch schon oben N 32.
102 S. auch schon N 31.
103 N 29.
104 S. nur KUNZ, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 16 N 12.

gen der Auftragsdatenbearbeitung massgeblich, ohne dass die zusätzlichen Voraussetzungen der Datenbekanntgabe ins Ausland (soweit die Datenbearbeitung selbst ins Ausland verlagert wird) zu prüfen wären.

> Eine Bekanntgabe ins Ausland läge in diesem Fall erst dann vor, wenn eine eigentliche Bekanntgabe an Dritte im Ausland erfolgte, so z.B., wenn ein *Cloud-Service*-Betreiber aufgrund des *US Cloud Acts* von den US-amerikanischen Behörden dazu gezwungen würde, Daten aus der Schweiz abzuliefern (in diesem Falle läge eine zweckwidrige Bearbeitung durch den Auftragnehmer vor, welche den Rahmen des Auftragsverhältnisses sprengt und eines eigenen Rechtfertigungsgrundes bedürfte sowie die Vorgaben von Art. 15 Abs. 3 lit. d i.V.m. Art. 12 E-KDSG einhalten müsste).

85. Gemäss **Art. 12 E-KDSG** – der übrigens weitgehend Art. 9 DSG entspricht – kann die Behörde die Bearbeitung von Personendaten an Dritte übertragen und damit eine Auftragsbearbeitung veranlassen, wenn die in dieser Bestimmung formulierten Anforderungen erfüllt sind. Dabei ist zwischen der Übertragung von Daten, die einer gesetzlichen Geheimhaltungspflicht unterliegen, und solchen, die keiner Geheimhaltungspflicht unterliegen, zu unterscheiden:

- Bei **nicht geheimnisgeschützten Daten** gilt als Voraussetzung für die Zulässigkeit einer Übertragung zwecks Bearbeitung im Auftrag, dass die Daten nur so bearbeitet werden, **wie die Behörde es selbst tun dürfte**, und dass **keine Gesetzesbestimmungen** oder vertragliche Pflichten entgegenstehen (Art. 12 Abs. 1 E-KDSG). Zudem muss sich die Behörde insbesondere vergewissern, dass die beauftragten Dritten die **Datensicherheit** gewährleisten (Art. 12 Abs. 3 E-KDSG). Schliesslich dürfen die beauftragten Dritten Daten nur mit **vorgängiger Genehmigung** der verantwortlichen Behörde an weitere Dritte übertragen (Art. 12 Abs. 4 E-KDSG).[105]
- Unterliegen Daten einer **gesetzlichen Geheimhaltungspflicht**, so gilt zusätzlich zu den vorgenannten Voraussetzungen, dass durch die Auftragsbearbeitung erstens diese Geheimhaltungspflicht nicht verletzt werden darf (was sich letztlich aus der Anforderung der Rechtmässigkeit der Datenbearbeitung ergibt), und dass zweitens technische oder organisatorische Massnahmen den Zugang der Auftragsbearbeiter auf die Daten auf das notwendige Minimum beschränken müssen (Art. 12 Abs. 2 E-KDSG).

86. Zentral sind somit die Anforderungen, dass die Bearbeitung nur so erfolgen darf, wie sie die Behörde selbst vornehmen dürfte (1.) und die Beachtung des gesetzlichen Rahmens (2.). Daneben ist noch auf weitere Verpflichtungen einzugehen (3.), bevor ein kurzes Zwischenfazit gezogen wird (4.).

1. Bearbeitung in gleicher Weise

87. Grundlegende Voraussetzung für die Zulässigkeit einer Übertragung zwecks Bearbeitung im Auftrag ist, dass die Daten durch den Auftragnehmer nur so bearbeitet werden dürfen, wie die **Behörde es selbst tun dürfte** (Art. 12 Abs. 1 lit. a E-KDSG). Das bedeutet, dass der Auftragsbearbeiter die Personendaten **nicht zu eigenen Zwecken**, sondern

---

105 Dies entspricht auch den Vorgaben des übergeordneten Rechts, namentlich der Konvention 108+ sowie der Richtlinie 2016/680, s.o. N 33 ff., N 36 ff.

nur zu den vom Verantwortlichen festgelegten Zwecken und nach dessen Weisung bearbeiten darf.[106]

> Diese Voraussetzung ist vor dem Hintergrund zu sehen, dass die Behörde verantwortlich bleibt und die Betroffenen in ihren Rechten nicht deshalb schlechter gestellt werden sollen, weil die Datenbearbeitung ausgelagert wird. Dieser Gedanke spricht im Übrigen dafür, dass bei einer Auftragsbearbeitung die Datenbearbeitung im Ausland nur dann erfolgen darf, wenn die diesbezüglichen Voraussetzungen, die auch sonst für die Behörde in Bezug auf Datenbekanntgaben ins Ausland gelten, was im Ergebnis zu einer (sinngemässen) Massgeblichkeit dieser Vorgaben führt.[107]

88. Insbesondere darf ein *Cloud*-Dienstleister die ihm übertragenen Daten **nicht** zu eigenen Zwecken, wie z.B. **Nutzungsanalyse zwecks Verbesserung des Angebots oder Profilbildung für Werbezwecke**, bearbeiten. Zudem muss er sämtliche Datenschutzgrundsätze ebenfalls einhalten, also namentlich die im kantonalen Gesetz verankerten Grundsätze der Rechtmässigkeit, Zweckbindung, Verhältnismässigkeit, Datenrichtigkeit sowie Datensicherheit (vgl. Art. 4-11 E-KDSG).

89. Die in Art. 12 Abs. 1 lit. a E-KDSG – übrigens im Passiv – formulierte Anforderung bezieht sich auf die Datenbearbeitung durch den Auftragsbearbeiter. Sie impliziert aber entsprechende **Vorkehrungen** durch die Behörde bei der **Entscheidung über die Übertragung und der Übertragung** selbst: Diese muss den Umständen angemessene Massnahmen ergreifen, damit auch sichergestellt ist, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie es die Behörde selbst tun dürfte. Welche Massnahmen hier genau notwendig sind, ist im Einzelfall zu ermitteln, dies insbesondere in Abhängigkeit von den zu bearbeitenden Daten, dem Auftragsbearbeiter selbst sowie der Art der Datenbearbeitung.

> Notwendig ist jedenfalls ein **Vertrag**, welcher die wesentlichen Elemente regelt.[108] Die Gesamtheit der Umstände muss im Übrigen so ausgestaltet sein, dass vernünftigerweise davon ausgegangen werden kann, dass der Anforderung des Art. 12 Abs. 1 lit. a E-KDSG Rechnung getragen wird. Dies impliziert – da es hier keine «absolute» Garantie geben kann – eine **Risikoanalyse**, in deren Rahmen nachgewiesen wird, dass grundsätzlich sichergestellt bzw. davon auszugehen ist, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie es die Behörde tun darf. M.a.W. geht es hier um eine Sorgfaltspflicht der Behörde, und der Auftraggeber muss analog der Geschäftsherrenhaftung des Obligationenrechts (Art. 55 OR) alle gebotene Sorgfalt aufwenden, um Verstösse des Auftragsbearbeiters gegen das Datenschutzgesetz zu verhindern. Diese Sorgfaltspflicht bezieht sich auf die sorgfältige Auswahl und Instruktion sowie ein angemessenes «Programm» zur prospektiven, fortwährenden und retrospektiven Überwachung des Vorgangs.[109]

90. Bei der Beantwortung der Frage, ob zu erwarten ist, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie es die Behörde tun dürfte, ist ebenfalls zu berücksichtigen, ob der **Auftragsdatenbearbeiter im Ausland** ansässig ist bzw. einer ausländischen Rechtsordnung unterworfen ist oder die **Datenbearbeitung im Ausland** erfolgt und insbesondere, um welchen Staat es sich hier handelt: Denn nur wenn die Datenbearbeitung

---

106 LEZZI, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 9 DSG, N 4 und 7.

107 S. insoweit schon oben N 32 sowie die Präzisierungen unten N 90 ff.

108 Zu diesen z.B. LEZZI, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 9 N 22; EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10 N 42. Die Notwendigkeit eines Vertrags auch hervorhebend BLONSKI, SJZ 2023, 991 (998 f.).

109 S. schon EPINEY/FASNACHT, in: Belser/Epiney/Waldmann, Datenschutzrecht, § 10 N 42 ff. Vgl. die Präzisierungen für die Auslagerung in eine *Cloud* bei BLONSKI, SJZ 2023, 991 (998).

in einem «vertretbaren juristischen Umfeld»[110] stattfindet, in welchem davon ausgegangen werden kann, dass der Auftragsbearbeiter auch tatsächlich in der Lage ist, die durch ihn aufgrund des Art. 12 Abs. 1 lit. a E-KDSG zu beachten, können die Anforderungen dieser Vorschrift als erfüllt angesehen werden.[111]

91. Insofern ist die Frage, ob im betreffenden Staat ein **angemessenes Datenschutzniveau** gewährleistet ist, auch im Rahmen der Auftragsbearbeitung von Belang, sofern der Auftragsdatenbearbeiter im Ausland ansässig ist bzw. einer ausländischen Rechtsordnung unterworfen ist oder die Datenbearbeitung im Ausland stattfindet: Denn grundsätzlich kann nur dann davon ausgegangen werden, dass die Daten in einem anderen Staat so bearbeitet werden (können), wie dies die Behörde selbst tun dürfte, wenn in dem betreffenden Staat ein angemessenes Schutzniveau im Sinn des Art. 15 Abs. 1, 2 E-KDSG bzw. des Art. 8 EMRK und der Konvention 108+[112] oder allenfalls sonstige effektive und durchsetzbare Garantien bestehen.

92. Damit erweist sich eine Datenbearbeitung im Auftrag einer Behörde, im Rahmen derselben der Auftragsdatenbearbeiter im Ausland ansässig ist bzw. einer ausländischen Rechtsordnung unterworfen ist oder die Datenbearbeitung im Ausland stattfindet (wo kein angemessenes Schutzniveau gewährleistet ist), jedenfalls dann als **unzulässig**, wenn der ausländische Staat keine **hinreichenden rechtsstaatlichen Strukturen** kennt. Denn diesfalls ist davon auszugehen, dass auch vertragliche Zusicherungen des Auftragsbearbeiters nicht durchgesetzt werden können bzw. ein erhebliches Risiko besteht, dass der Auftragsbearbeiter dies nicht gewährleisten kann.

> Bei einem im Ausland domizilierten Auftragsbearbeiter ist damit zu prüfen, ob eine Durchsetzung der vertraglichen Vereinbarungen in einem rechtsstaatlichen Verfahren möglich ist, da insbesondere in Ländern, wo kein gleichwertiger Datenschutz besteht, die datenschutzrechtlichen Vorgaben vertraglich zu überbinden sind, analog wie bei einer Datenbekanntgabe ins Ausland.[113]

93. Selbst wenn aber in einem Staat rechtsstaatliche Strukturen bestehen, ist es gleichwohl denkbar, dass weder allgemein ein angemessenes Datenschutzniveau besteht noch andere hinreichende Garantien (z.B. vertragliche Zusicherungen) möglich bzw. effektiv durchsetzbar sind. Dies war nach Ansicht des EuGH bei den USA der Fall, wie der Gerichtshof in verschiedenen Urteilen festgestellt hat.[114] Inzwischen wurde zwar ein neuer Angemessenheitsbeschlusses der Kommission, der *EU-US Data Privacy Framework*[115], gefasst, wobei jedoch offen ist, ob dieser tatsächlich den Anforderungen des Unionsrechts Rechnung trägt.[116] Festzuhalten ist jedenfalls, dass bislang noch kein entsprechender schweizerischer Angemessenheitsbeschluss mit diesbezüglichen Vorgaben gefasst

---

110 S. diesen Ausdruck bei BLONSKI, SJZ 2023, 991 (998).
111 Ebenso BLONSKI, SJZ 2023, 991 (998).
112 S. insoweit die Ausführungen oben N 7 ff., 16 ff., 53 ff.
113 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 68 f.
114 EuGH, Rs. C-362/14 (*Schrems)*, ECLI:EU:C:2015:650; EuGH, Rs. C-311/18 (*Schrems II)*, ECLI:EU:C:2020:559. S.o. N 12.
115 COM(2023) 4745 final.
116 Oben N 12.

wurde, so dass für die Situation in der **Schweiz** davon auszugehen ist, dass in den **USA kein angemessenes Datenschutzniveau** gewährleistet ist.

Dies beruht insbesondere darauf, dass das ausländische Recht eine allfällige vertragliche Übereinkunft übersteuern könnte: Der ***US Cloud Act*** *(Clarifying Lawful Overseas Use of Data Act)* ist global auf Daten bei amerikanischen Unternehmen anwendbar, unabhängig davon, wo diese gespeichert sind. Er erlaubt es amerikanischen Behörden, für strafrechtliche Zwecke auch ohne Rückgriff auf internationale Rechtshilfeabkommen Auskunftsbegehren betreffend Personendaten zu stellen, welche sich im Besitz, in Gewahrsam oder unter Kontrolle eines in den USA domizilierten Unternehmens befinden. Die betroffenen Unternehmen können dabei explizit zur Verschwiegenheit bei solchen Zugriffen verpflichtet werden.[117] Das Verfahren und der Zugriff auf Daten nach dem *Cloud Act* sind als solche kaum mit dem schweizerischen und europäischen Datenschutzrecht vereinbar;[118] insbesondere stehen auch diverse Bestimmungen des *Cloud Act* (so der Grundsatz der Transparenz sowie der Zweckbindung bei einem Zugriff auf Daten des Auftragsbearbeiters) nicht in Einklang mit den Bearbeitungsgrundsätzen des schweizerischen Rechts.[119] Etwas anderes könnte aber dann gelten, wenn die Schweiz mit den USA ein gesondertes Abkommen abschliesst, welches (im Ansatz vergleichbar mit dem erwähnten *EU-US Data Privacy Framework*) den Bedenken Rechnung trägt.

Sind die Daten darüber hinaus auch **auf amerikanischen Servern** gespeichert, besteht die Möglichkeit, dass amerikanische Behörden von ihren Kompetenzen Gebrauch machen, die Internetprovider zu verpflichten, ihnen Zugang zu Internetverkehrsflüssen zu geben, um diese zu kopieren und zu filtern (wobei sie sowohl Zugriff auf die Metadaten als auch auf den Inhalt der betreffenden Kommunikation nehmen können), sowie Daten mittels Zugriffs auf die am Grund des Atlantiks verlegten Seekabel einzusehen.[120]

94. Vor diesem Hintergrund ist derzeit davon auszugehen, dass eine Datenbearbeitung im **Auftrag** einer staatlichen Behörde, welche die Nutzung von **US-basierten *Cloud*-Lösungen** vorsieht, **nicht mit Art. 12 Abs. 1 lit. a E-KDSG vereinbar** wäre.

Ergänzend ist darauf hinzuweisen, dass im Falle der USA der behördliche Zugriff auf Personendaten im Ergebnis die Vorgaben der **internationalen Rechtshilfe** aushebelt, so dass gute Gründe dafür sprechen, hierin einen Verstoss gegen den *ordre public* der Schweiz anzunehmen, dies mit der Folge, dass eine Auftragsdatenbearbeitung unter der Nutzung einer US-basierten *Cloud*-Lösung schon aus diesem Grund rechtswidrig wäre (und damit gegen den nachfolgend zu erörternden Art. 12 Abs. 1 lit. b E-KDSG sowie das allgemein geltende Legalitätsprinzip verstiesse).[121]

95. Dieser Schluss ist nach dem Gesagten dadurch begründet, dass die **Gesetzeslage** in den USA so ausgestaltet ist, dass der Auftragsbearbeiter verpflichtet werden kann, die Daten in einer Weise zu bearbeiten, wie die Behörde dies nicht tun dürfte; auch ganz allgemein entsprechen die in den USA vorgesehenen Verfahren und der Zugriff nicht den

---

117 Vgl. SCHWANINGER/MERZ, Jusletter vom 21.6.2021, Rz. 19; BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 70; SCHEFER/GLASS, Gutachten zum grundrechtskonformen Einsatz von M365, 28.

118 Bundesamt für Justiz, Bericht zum US CLOUD Act, 46 f.; BLONSKI, SJZ 2023, 991 (993); SCHEFER/GLASS, Gutachten zum grundrechtskonformen Einsatz von M365, 28.

119 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 70; SCHEFER/GLASS, Gutachten zum grundrechtskonformen Einsatz von M365, 28.

120 S. die Zusammenfassung der Kompetenzen der amerikanischen Sicherheitsbehörden in EuGH, Rs. C-311/18 (*Schrems II*), ECLI:EU:C:2020:559, Rz. 61-65.

121 S. so mit ausführlicher Begründung BLONSKI, SJZ 2023, 991 (993).

im schweizerischen Datenschutzrecht geltenden Grundsätzen,[122] welche ihrerseits (weitgehend) konkretisiertes Verfassungsrecht darstellen.[123] Damit ergibt sich schon aus der Rechtslage in den USA, dass ein diesem Recht unterworfener Auftragsbearbeiter nicht gewährleisten kann, dass er die in Art. 12 Abs. 1 lit. a E-KDSG formulierte Anforderungen einhalten kann. Dass ein effektiver Zugriff auf die Daten des Auftragsbearbeiters möglicherweise nur in sehr wenigen Fällen erfolgen würde, ändert hieran nichts: Die auch im Rahmen des Art. 12 Abs. 1 lit. a E-KDSG durchaus vorzunehmende Risikoanalyse nimmt ja keinen Bezug darauf, ob ein bestimmtes Ereignis tatsächlich eintritt oder ein Rechtsunterworfener sich in einer bestimmten Weise verhält; vielmehr geht es darum, ob die Behörde darlegen kann, dass grundsätzlich sichergestellt bzw. davon auszugehen ist, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie es die Behörde tun darf; diese Anforderung ist aber von vornherein nicht erfüllt, wenn der Auftragsbearbeiter aufgrund gesetzlicher Vorgaben zu einem Verhalten verpflichtet werden kann, welches gerade nicht mit dem für die Behörde zur Anwendung kommenden datenschutzrechtlichen Vorgaben in Einklang steht. Ob und ggf. mit welcher Wahrscheinlichkeit dieses «Risiko» dann eintritt, muss vor diesem Hintergrund unerheblich sein. Für eine **Risikoanalyse** gleich welcher Art bleibt daher hier **kein Raum**.[124]

> Es ist insofern auch daran zu erinnern, dass es vorliegend um Datenbearbeitungen durch staatliche Behörden geht; diese haben – was gerade auch bei Grundrechtseingriffen von grosser Bedeutung ist – ausgehend vom Legalitätsprinzip bestimmte Anforderungen zu beachten, wobei diese eben beachtet sind oder nicht.[125] Insofern unterscheiden sich denn auch die datenschutzrechtlichen Vorgaben für Private und öffentliche Organe: Bei ersteren bleibt im Zusammenhang mit der Interessenabwägung wohl deutlich mehr Raum für eine gewisse «Risikoabwägung» (vgl. insoweit Art. 30 ff. DSG), wenn auch die Frage, wie die Zulässigkeit des Rückgriffs auf *US-Cloud*-Lösungen durch Private zu beurteilen wäre, hier aber offen gelassen werden soll. Im Übrigen ist zu betonen, dass die Intensität einer Grundrechtsgefährdung nicht nur von der Wahrscheinlichkeit des Eintritts einer Grundrechtsverletzung abhängt, sondern auch davon, wie viele Personen betroffen sind und wie schwer der Grundrechtseingriff ist. Daher kann auch eine sehr geringe Wahrscheinlichkeit des Eintritts einer Grundrechtsverletzung eine hohe Intensität in Bezug auf die Grundrechtsgefährdung aufweisen, wenn sehr viele Personen betroffen sind und es um schwerwiegende Verletzungen geht.[126]

2. Keine entgegenstehenden gesetzlichen Bestimmungen

96. Entsprechend dem schon verfassungsrechtlich geltenden Legalitätsprinzip (Art. 5 Abs. 1 BV) dürfen nach Art. 12 Abs. 1 lit. b E-KDSG einer Auftragsbearbeitung keine

---

122 S. N 93.

123 S. N 15, 26.

124 Diesem Umstand – Unzulässigkeit der Auftragsbearbeitung, weil bereits aufgrund der Gesetzeslage nicht gewährleistet ist, dass die Daten nur so bearbeitet werden, wie es die Behörde selbst tun dürfte – wird von ROSENTHAL, Jusletter vom 10.8.2020, *passim*, und insbesondere N 82 ff., wohl nicht Rechnung getragen.

125 S. insoweit auch die treffende Formulierung von BLONSKI, SJZ 2023, 991 (993): «Rechtmässige Datenbearbeitung heisst, dass das Recht bei der Datenbearbeitung eingehalten wird. Ob das Recht eingehalten ist oder nicht, ist keine Risikofrage – Recht ist eingehalten oder nicht.»

126 S. insoweit ebenso SCHEFER/GLASS, Gutachten zum grundrechtskonformen Einsatz von M365, 29 ff., die nach ausführlicher Begründung folgern, dass «die Bearbeitung bzw. Speicherung von (…) Personendaten in der Cloud eines US-Anbieters wie Microsoft unabhängig von dem mit einem möglichen Zugriff auf solche Daten verbundenen Gefährdungseingriff für sich bereits einen schweren Grundrechtseingriff» darstelle.

gesetzlichen Bestimmungen entgegenstehen (s. insoweit auch Art. 6 Abs. 1 DSG). Zu beachten ist dabei die gesamte Rechtsordnung, wobei nachfolgend besonders auf gesetzliche Geheimhaltungspflichten hingewiesen wird (a), bevor an die sonstigen zu beachtenden Vorgaben erinnert wird (b).

a) Geheimhaltungspflichten

97. Als einer Auslagerung potentiell entgegenstehende gesetzliche Bestimmungen (Art. 12 Abs. 1 lit. b E-KDSG) kommen insbesondere das **Amtsgeheimnis** sowie **spezialgesetzliche Geheimnisse** (z.B. im Steuer- oder Sozialversicherungsbereich) in Frage. Durch die Auslagerung an einen *Cloud*-Dienstleister wird die Geheimhaltungspflicht grundsätzlich an sich nicht verletzt, solange dieser seine Hilfstätigkeit im Rahmen seines Auftrags wahrnimmt, das heisst, die Daten ausschliesslich zu den vom Verantwortlichen festgelegten Zwecken und nach dessen Weisung bearbeitet. Allerdings ist jeweils im Einzelnen die zur Debatte stehende Geheimhaltungspflicht zu analysieren und auszulegen, um ihre Tragweite zu eruieren.[127]

98. Gibt der *Cloud*-Dienstleister hingegen **Daten an weitere Dritte bekannt**, unabhängig davon ob dies «freiwillig» oder basierend auf der Anordnung einer ausländischen Behörde erfolgt, so macht er sich wegen Geheimnisverletzung strafbar (es sei denn es liege ein Rechtfertigungsgrund vor, namentlich eine schriftliche Einwilligung der übergeordneten Behörde, vgl. Art. 320 Abs. 2 StGB).

> Ob der Strafanspruch im Einzelfall **durchgesetzt** werden könnte – schliesslich handelt es sich um ein Antragsdelikt – wird in der Literatur bezweifelt.[128]

99. Die Behörde hat diesbezüglich eine aus Art. 12 Abs. 1 lit. b E-KDSG fliessende Sorgfaltspflicht: Sie darf nur dann Daten zur Bearbeitung im Auftrag an einen bestimmten Dritten (z.B. einen *Cloud*-Dienstleister) übertragen, wenn sie sich **vergewissert** hat, dass dieser **keine (eventual-)vorsätzliche Geheimnisverletzung begehen wird**. Diese Vergewisserung stellt eine Rechtmässigkeitsvoraussetzung für die Auslagerung dar und ist zu unterscheiden von der Pflicht zur (risikoabhängigen) Gewährleistung der Datensicherheit gemäss Art. 12 Abs. 3 E-KDSG, welche eine Rechtsfolge des Entscheids zur Auslagerung an einen bestimmten Anbieter darstellt. Sie wird analog zur Geschäftsherrenhaftung (Art. 55 OR) ausgelegt; namentlich muss Sorgfalt bei der Auswahl, der Instruktion wie auch der Kontrolle des Auftragnehmers ausgeübt werden (*cura in eligendo, instruendo, custodiendo*);[129] insoweit besteht eine Parallelität zur im Rahmen des Art. 12 Abs. 1 lit. a E-KDSG bestehenden Pflicht der Behörde, sich zu vergewissern, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie sie es selbst tun dürfte.[130]

100. In Bezug auf diese **Sorgfaltspflicht** stellt sich die Frage, ob und unter welchen Voraussetzungen die Behörde durch eine Risikoabwägung (unabhängig von der dazu verwendeten «Methode») ihrer Sorgfaltspflicht nachkommen bzw. diese respektiert werden

---

127 Vgl. insoweit die instruktiven Ausführungen bei BLONSKI, SJZ 2023, 991 (995 ff.).
128 BAERISWYL, digma 2019, 118 (121).
129 Botschaft DSG, BBl 2017 7032; LEZZI, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 9 N 14.
130 N 89 ff.

kann, selbst wenn nicht ausgeschlossen werden kann, dass der Auftragnehmer die Daten ins Ausland übermittelt oder übermitteln könnte.

U.E. kann es dabei nicht nur auf die (hypothetische) Frage ankommen, ob eine Behörde sich durch eine Auslagerung an einen *Cloud*-Anbieter strafbar machen würde, m.a.W., ob Eventualvorsatz ausgeschlossen werden kann, indem die Behörde eine Risikoabwägung vornimmt, wie dies teilweise in der Doktrin vertreten wird.[131] Da eine Strafbarkeit nur für Individuen besteht, ist diese Frage ohnehin rein hypothetisch. Ausschlaggebend ist u.E., ob der Sorgfaltspflicht bei der Auswahl, Instruktion und Überwachung des Auftragsbearbeiters nachgekommen wurde, was keinen strafrechtlichen, sondern einen (staats-)haftungsrechtlichen Massstab beinhaltet.

101. Angesichts der Unsicherheit der Kalkulationsbasis der derzeit verfügbaren Risikoberechnungsmodelle ist u.E. bei solchen Modellen im Bereich des hoheitlichen Staatshandelns **grosse Vorsicht** geboten; dies gilt umso mehr, wenn (auch) besonders schützenswerte Personendaten bearbeitet werden, insbesondere da die gesetzlichen Geheimhaltungspflichten absolut gelten.[132] Insbesondere erschiene es unzulässig, allein aufgrund der (möglicherweise anzunehmenden) geringen Wahrscheinlichkeit etwa eines staatlichen Zugriffs auf einem Geheimnisschutz unterliegende Personendaten – trotz bestehender gesetzlich vorgesehener Zugriffsmöglichkeiten – davon auszugehen, dass der Sorgfaltspflicht Rechnung getragen werde. Vielmehr dürfte jedenfalls bei Auftragsdatenbearbeitungen, welche aufgrund des «Auslandsbezugs» die **Anwendbarkeit gesetzlich vorgesehener Rückgriffsmöglichkeiten auf dem Geheimnisschutz unterliegende Daten** nach sich ziehen (wie dies bei der Nutzung von US-basierten *Cloud*-Lösungen der Fall ist), grundsätzlich eine Verletzung der Geheimhaltungspflichten anzunehmen sein. Denn auch hier gilt, dass die Möglichkeit der Verletzung der Geheimhaltungspflichten bereits aus der Gesetzeslage folgt, so dass für eine Risikoabwägung kein Raum bleibt.[133]

102. Für die Auslegung der Anforderungen an die Ausübung der Sorgfaltspflicht ist zudem zu beachten, dass der Entwurf für das kantonale Datenschutzgesetz vorsieht, dass bei Daten, die einer Geheimhaltungspflicht unterliegen, technische oder organisatorische Massnahmen getroffen werden müssen, die den **Zugang** des Auftragsbearbeiters zu diesen Daten **auf ein Minimum** beschränken (Art. 12 Abs. 2 E-KDSG). Diese Bestimmung lässt keinen Raum für eine Risikoabwägung, sondern gibt eine absolute Grösse («Minimum») vor.

Denkbar ist beispielsweise, in Anlehnung an die Regelung im Kanton Freiburg, dass die betreffenden Daten verschlüsselt sind, und der Auftragsbearbeiter nur dann Zugriff erhält, wenn dies aus technischen Gründen unbedingt notwendig ist.[134] Für diesen Fall müssten im Auslagerungsvertrag[135] besondere Anforderungen bezüglich des Bearbeitens solcher besonders schützenswerter Personendaten festgelegt werden, insbesondere die Verpflichtung des Auftragsbearbeiters, nur mit ausdrücklichem Einverständnis des öffentlichen Organs auf den Inhalt der Daten zuzugreifen, und die Pflicht, ein Zugriffsjournal zu führen (vgl. Art. 12e Abs. 2 DSchG-FR).

---

131 DZAMKO, in: Métille (Hrsg), L'informatique en nuage, 83 (110), mit Verweis auf ROSENTHAL, Jusletter vom 10.8.2020, N 82 ff.

132 S.o. N 97.

133 S.o. N 93 ff.

134 S.o. N 49.

135 S. auch. N 89.

103. In Anbetracht dieser Erwägungen ist u.E. der Sorgfaltspflicht nur dann Rechnung getragen, wenn die in der *Cloud* abgelegten geheimnisgeschützten Daten **verschlüsselt** werden, wobei in diesem Fall das Schlüsselmanagement ausschliesslich bei der auftraggebenden Behörde und nicht beim *Cloud-Service*-Provider liegen darf.[136] Ausnahmen können mit dem Auftragsbearbeiter für technisch unabdingbare Zugriffe (z.B. Wartungsarbeiten, die auf unverschlüsselte Daten angewiesen sind) vereinbart werden.

104. Sämtliche erwähnten Voraussetzungen sind in der Regel mittels eines **Vertrags** dem Auftragsbearbeiter vorzuschreiben. Im Anwendungsbereich der Richtlinie 2016/680 muss es sich um einen schriftlichen Vertrag handeln (Art. 22 Abs. 4 RL 2016/680). Hierbei ist zu unterscheiden zwischen in der Schweiz und im Ausland domizilierten Auftragsbearbeitern. Ein in der Schweiz domizilierter Auftragsbearbeiter ist in das schweizerische Rechtssystem und das Datenschutzrecht eingebunden. Ein bestehendes Amts- oder Spezialgeheimnis lässt sich in diesem Fall mit dem Auftragsbearbeiter vertraglich absichern; zudem stellen sich in Bezug auf die Durchsetzung des Strafanspruchs bei einer Verletzung des Amtsgeheimnisses durch den Auftragsbearbeiter keine besonderen Fragen. Bei einem im Ausland domizilierten Auftragsbearbeiter ist zu prüfen, ob eine Durchsetzung der vertraglichen Vereinbarungen in einem rechtsstaatlichen Verfahren möglich ist, da insbesondere in Ländern, wo kein gleichwertiger Datenschutz besteht, die datenschutzrechtlichen Vorgaben vertraglich zu überbinden sind, analog wie bei einer Datenbekanntgabe ins Ausland; insoweit stellen sich parallele Fragen wie im Rahmen des Art. 12 Abs. 1 lit. a E-KDSG.[137]

105. Kann der Auftragsbearbeiter somit vertraglich nicht zusichern, dass die auftraggebende Behörde bei einem Datenzugriff informiert wird oder dass sie Teil des Verfahrens wird, sind die Voraussetzungen von Art. 12 Abs. 1 lit. a, b E-KDSG (Bearbeitung nur so, wie der Verantwortliche dies dürfte sowie keine entgegenstehende Geheimhaltungspflicht) **nicht erfüllt.** In diesen Fällen dürfen dem Auftragsbearbeiter **keine Daten**, die einem **Spezialgeheimnis** unterliegen, zur Bearbeitung übertragen werden.[138]

> Eine Übertragung ist auch nicht zulässig mit dem Argument, ein tatsächlicher Zugriff einer US-Behörde auf die Daten sei sehr unwahrscheinlich.[139] Wie bereits oben ausgeführt,[140] haben die kantonalen Behörden die Grundrechte der betroffenen Personen nämlich stets so zu gewährleisten, wie wenn sie die Daten selbst bearbeiten würden (Art. 12 Abs. 1 lit. a E-KDSG); hinzu kommt die Verpflichtung, Geheimhaltungspflichten einzuhalten. Kann eine kantonale Behörde dies nicht gegenüber dem Auftragsdatenbearbeiter durch rechtliche Vereinbarungen erwirken oder bietet das Rechtsumfeld des Auftragsbearbeiters keinen dem schweizerischen «Ordre public» entsprechenden Schutz der Daten vor staatlichen Zugriffen, ist auf eine Übertragung dieser Daten zu verzichten.[141]

---

136 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 74.

137 So dass auf die obigen Ausführungen verwiesen werden kann, vgl. N 89 ff.

138 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 71.

139 Vgl. EDÖB, Stellungnahme SUVA, 2022, Rz. 25 ff.

140 N 89 ff.

141 BAERISWYL, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG, Art. 9 N 77. S. insoweit schon oben N 89 ff., N 100.

Zu prüfen ist allenfalls, ob mit technischen Massnahmen, z.B. einer Verschlüsselung, ein Offenbaren dieser Daten gegenüber dem Auftragsbearbeiter ausgeschlossen werden kann.[142]

b) Weitere gesetzliche Vorgaben

106. Neben Geheimhaltungspflichten ist an mögliche weitere gesetzliche Vorgaben zu erinnern, welche einer Auftragsbearbeitung entgegen stehen könnten oder für diese spezifische (weitere) Anforderungen vorsehen.[143] Auf hier allenfalls einschlägige Bestimmungen soll im Rahmen dieser Untersuchung jedoch nicht weiter eingegangen werden.

3. Weitere Verpflichtungen des Dritten: Datensicherheit, Unterauftragsnehmer

107. Die auftraggebende Behörde muss sich vergewissern, dass der Dritte die **Datensicherheit** gewährleistet (Art. 12 Abs. 3 E-KDSG). Zur Datensicherheit schreibt Art. 10 E-KDSG vor, dass mit geeigneten technischen und organisatorischen Massnahmen für eine dem Risiko angemessene Datensicherheit zu sorgen ist. Diese Bestimmung lässt Raum für **Risikoabwägungen**: Je geringer die Wahrscheinlichkeit für den Eintritt und je weniger gravierend die Auswirkungen einer Gefährdung der Datensicherheit (z.B. durch Zugriffe ausländischer Regierungen) eingeschätzt werden, desto niedriger sind die Anforderungen an die zu treffenden technischen und organisatorischen Massnahmen. Allerdings besteht auch dort keine *de-minimis*-Regelung: Eine kleine Menge an besonders schutzwürdigen Daten erlaubt nicht einen tieferen Grad an Datensicherheit als eine grosse Menge.[144]

108. Schliesslich darf der Dritte die Bearbeitung nur mit vorgängiger Genehmigung der Behörde **an weitere Dritte übertragen** (Art. 12 Abs. 4 E-KDSG). Gemeint ist hier eine Subdelegation der Auftragsdatenbearbeitung; der Dritte darf also nicht wie ein Verantwortlicher selber darüber entscheiden, ob er die ihm anvertrauten Daten wiederum durch Dritte bearbeiten lässt, selbst wenn sich diese, bildhaft gesprochen, ebenfalls unterhalb derselben «Käseglocke» befinden würden, sondern muss die Datenherrschaft der verantwortlichen Behörde wahren, indem er eine vorgängige (allgemeine oder spezifische) Genehmigung für solche Unteraufträge einholt.

Nicht anwendbar ist diese Vorschrift auf sonstige Datenbekanntgaben an Dritte, worunter auch Zugriffe ausländischer Behörden fallen würden. Solche sind *per se* datenschutzrechtswidrig, da es ihnen an einem Rechtfertigungsgrund fehlt.

4. Zwischenfazit

109. Im Ergebnis ist damit festzuhalten, dass eine Datenbearbeitung im Auftrag einer Behörde, im Rahmen derselben der Auftragsdatenbearbeiter im Ausland ansässig ist bzw. einer ausländischen Rechtsordnung unterworfen ist oder die Datenbearbeitung im Ausland stattfindet (wo kein angemessenes Schutzniveau gewährleistet ist), jedenfalls dann

---

142 Vgl. Bundeskanzlei, Bericht Public Cloud, 24.
143 S. insoweit bereits oben N 76 ff. sowie BLONSKI, SJZ 2023, 991 (997).
144 GORDON/EGLI, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 8 N 7.

unzulässig ist, wenn der ausländische Staat keine **hinreichenden rechtsstaatlichen Strukturen** kennt. Darüber hinaus ist eine Unzulässigkeit auch dann anzunehmen, wenn der Auftragsbearbeiter aufgrund des im Ausland geltenden Rechts nicht gewährleisten kann, dass die Daten nur so bearbeitet werden, wie es die Behörde selbst tun dürfte. Dies ist insbesondere dann der Fall, wenn **weitgehende staatliche Zugriffsmöglichkeiten** bestehen und keine hinreichenden Garantien für ihre Beschränkung gegeben sind (was auch dann der Fall sein kann, wenn der Server in der Schweiz steht), wie dies im Verhältnis der Schweiz zu den USA der Fall ist. Insoweit ist jedenfalls im Ergebnis auch im Rahmen des Art. 12 Abs. 1 lit. a E-KDSG danach zu fragen, ob im betreffenden Staat, in welchem der Auftragsbearbeiter ansässig ist oder dessen Rechtsordnung die Datenbearbeitung unterworfen werden kann, ein angemessenes Schutzniveau angenommen werden kann, womit letztlich parallele Erwägungen wie im Rahmen des Art. 15 Abs. 1, 2 E-KDSG zum Zuge kommen.

110. Vor diesem Hintergrund erweist sich eine Datenbearbeitung im **Auftrag** einer staatlichen Behörde, welche die Nutzung von **US-basierten *Cloud*-Lösungen** vorsieht, als **nicht mit Art. 12 Abs. 1 lit. a E-KDSG vereinbar.** Im Übrigen dürfte in aller Regel auch ein Verstoss gegen **Art. 12 Abs. 1 lit. b E-KDSG** vorliegen, soweit es auch um Personendaten geht, welche einer **gesetzlichen Geheimhaltungspflicht** unterliegen.

111. Die Einführung des Art. 15 Abs. 3 lit. d E-KDSG in der vorgesehenen Form würde daher – im Gegensatz zur Absicht des Gesetzgebers – die Nutzung von **US-basierten *Cloud*-Lösungen** im Rahmen einer Auftragsbearbeitung gar nicht erlauben, da eine solche nicht mit Art. 12 Abs. 1 E-KDSG vereinbar wäre, auf den Art. 15 Abs. 3 lit. d E-KDSG verweist.

II. Bekanntgabe ins Ausland im Rahmen von Auftragsbearbeitungsverhältnissen

112. Wird entsprechend der hier vertretenen Ansicht davon ausgegangen, dass eine Datenbearbeitung im Auftrag mit einer Datenbekanntgabe von der verantwortlichen Behörde an den Auftragsbearbeiter einhergeht, so sind bei Auftragsbearbeitungen mit Auslandsbezug **zusätzlich** zu den Anforderungen von Art. 12 E-KDSG auch die Voraussetzungen von Art. 15 E-KDSG zu beachten. Eine Bekanntgabe ins Ausland liegt vor, wenn die Daten effektiv im Ausland bearbeitet werden, d.h. den Hoheitsbereich der Schweiz verlassen und unter die Jurisdiktion einer ausländischen Rechtsordnung fallen.[145] Bei *Cloud-Computing* ist dies insbesondere dann der Fall, wenn sich die *Cloud*-Infrastruktur, namentlich die Server, im Ausland befindet.[146]

113. Eine Bekanntgabe ins Ausland ist nur zulässig, wenn die im Inland bestehenden datenschutzrechtlichen Vorgaben dadurch nicht unangemessen relativiert werden.[147] Im Entwurf des (neuen) Datenschutzgesetzes des Kantons Bern ist diesbezüglich vorgeschrieben, dass kantonale Behörden Personendaten nur ins Ausland bekanntgeben dürfen,

---

145 KUNZ, in: Bieri/Powell (Hrsg.), OFK-DSG, Art. 17 N 3.
146 S. etwa *privatim*, Merkblatt Cloud-spezifische Risiken und Massnahmen, Ziff. 2.2.
147 S.o. N 27.

wenn das Grundrecht auf Datenschutz der betroffenen Person angemessen geschützt ist, wobei die **Angemessenheit des Schutzes** festgestellt werden kann durch einen völkerrechtlichen Vertrag, einen Feststellungsbeschluss des Bundesrats oder «andere hinreichende Garantien» (Art. 15 Abs. 1 und 2 E-KDSG). Dies entspricht den übergeordneten Vorgaben der Konvention 108+ und der Richtlinie 2016/680.

114. Datenbekanntgaben ins Ausland können zunächst in einen Staat mit angemessenen Schutzniveau erfolgen (1.). Ist das Schutzniveau in dem betreffenden Staat nicht «angemessen», so können Personendaten ins Ausland bekanntgegeben werden, sofern ein **Ausnahmetatbestand** greift (2.a). Auf den im kantonalen Entwurf für ein Datenschutzgesetz vorgesehenen, auf *Cloud-Computing* ggf. anwendbaren Ausnahmetatbestand wird gesondert eingegangen (2.b), bevor ein Zwischenfazit gezogen wird (3.).

1. Bekanntgabe in einen Staat mit angemessenem Datenschutzniveau

115. Liegen die Server in einem **Staat mit angemessenem Datenschutzniveau** (oder der Schweiz, wobei in diesem Fall in der Regel keine Datenbekanntgabe ins Ausland stattfindet), ist die Zulässigkeit der Nutzung von *Cloud-Services* (zusätzlich zu den oben erwähnten Vorgaben der Auftragsbearbeitung) grundsätzlich zu bejahen (vgl. Art. 15 Abs. 2 lit. b E-KDSG). Sie wäre auch mit übergeordnetem Recht vereinbar (Art. 36 RL 2016/680, Art. 14 Abs. 2 Konvention 108+).

Die in die Vernehmlassung geschickte «Variante 2» wäre für diesen Sachverhalt nicht notwendig.

116. Jedoch kann es auch in diesen Fällen zu einem **Datenzugriff durch die US-Behörden** kommen, da diese gemäss des *US Cloud Act* US-Unternehmen verpflichten können, Daten herauszugeben, unabhängig davon, ob die Daten in den USA oder im Ausland gespeichert sind. Rechtlich handelt es sich dabei um eine die Grenzen des Auftragsverhältnisses überschreitende – rechtswidrige – Bekanntgabe durch den Auftragsbearbeiter, und ggf. um ein (strafbares) Offenbaren eines Geheimnisses durch eine Hilfsperson. Hierfür ist auf die obigen Ausführungen zu verweisen.[148]

2. Bekanntgabe in einen Staat ohne angemessenes Datenschutzniveau

117. Werden in der *Cloud* abgelegte Daten auf Servern in einem Staat ohne angemessenes Datenschutzniveau – wozu aktuell auch die Vereinigten Staaten gehören[149] – bekannt gegeben, so muss sich die Datenübermittlung auf einen **Ausnahmetatbestand** stützen können. Das **übergeordnete Recht** normiert als Ausnahmetatbestände namentlich die Folgenden:[150]

- **Einwilligung** der oder des Betroffenen, wobei die Einwilligung ausdrücklich, für den konkreten Fall, freiwillig und informiert erfolgen muss (Art. 14 Abs. 4 lit. a Konvention 108+);

---

148 N 89 ff.
149 N 12, 64.
150 Ausführlich hierzu bereits oben N 52 ff.

- Erforderlichkeit im Einzelfall wegen **spezifischer Interessen der betroffenen Person** (Art. 14 Abs. 4 lit. b Konvention 108+);
- überwiegende berechtigte Interessen, insbesondere **überwiegende, wichtige öffentliche Interessen**, die gesetzlich vorgesehen sind und die eine Weitergabe der Daten als eine in einer demokratischen Gesellschaft notwendige und verhältnismässige Massnahme erscheinen lassen (Art. 14 Abs. 4 lit. c Konvention 108+);
- Notwendigkeit und Verhältnissmäsigkeit der Weitergabe im Hinblick auf die **Meinungsäusserungsfreiheit** (Art. 14 Abs. 4 lit. d Konvention 108+);
- unbedingte Erforderlichkeit für Zwecke der **Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung** im speziellen Einzelfall, sofern diese Zwecke die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 39 Abs. 1 RL 2016/680).

118. Der Entwurf des (revidierten) Datenschutzgesetzes des Kantons **Bern** sieht demgegenüber drei respektive (gem. Variante 2) vier Ausnahmetatbestände vor:
- Notwendigkeit der Bekanntgabe im Einzelfall für die Wahrung eines **überwiegenden öffentlichen Interessens** (Art. 15 Abs. 3 lit. a E-KDSG);
- ausdrückliche **Einwilligung** der betroffenen Person im Einzelfall oder allgemeine Zugänglichmachung durch die betroffene Person (Art. 15 Abs. 3 lit. b E-KDSG);
- Notwendigkeit der Bekanntgabe zum **Schutz des Lebens oder der körperlichen oder geistigen Unversehrtheit** der betroffenen Person oder eines Dritten, sofern nicht innert angemessener Frist eine Einwilligung eingeholt werden kann (Art. 15 Abs. 3 lit. c E-KDSG);
- Bekanntgabe zum Zweck der **Bearbeitung im Auftrag**, sofern deren Voraussetzungen erfüllt sind (Art. 15 Abs. 3 lit. d E-KDSG; «Variante 2»).

119. Fraglich ist zunächst, ob die Ausnahmetatbestände geeignet sind, auf grossangelegte, **regelmässige** Datenbekanntgaben – wie im Rahmen von *Cloud Computing* – angewendet zu werden, oder ob diese jeweils nur im **Einzelfall** zum Tragen kommen können. Für die meisten Ausnahmetatbestände präzisieren die Rechtsgrundlagen kongruent, dass diese nur im Einzelfall angewendet werden dürfen (so namentlich im Falle der Einwilligung, der spezifischen Interessen der betroffenen Person respektive dem Schutz ihres Lebens oder ihrer körperlichen oder geistigen Unversehrtheit sowie zum Zweck der Strafverhütung- und -verfolgung), was auch vor dem Hintergrund des Charakters einer Ausnahme von der grundsätzlichen Regel, die ja den Grundrechtsschutz gewährleisten soll, begründet erscheint. Auch rechtsvergleichend (Datenschutzgesetze des Bundes und anderer Kantone) ist zu konstatieren, dass die genannten Ausnahmetatbestände nur im speziellen Einzelfall zur Anwendung kommen dürfen. Diese scheiden somit als Rechtsgrundlagen für eine Datenübermittlung ins Ausland im Rahmen von *Cloud Computing* von vornherein aus.

120. Keine ausdrückliche Einschränkung auf den Einzelfall enthalten die Ausnahmetatbestände der «**überwiegenden, wichtigen öffentlichen Interessen**» in der Fassung der Konvention 108+ sowie der «**Bearbeitung im Auftrag**» gemäss dem Entwurf für das kantonale Datenschutzgesetz. Auf die Modalitäten und die Rechtmässigkeit dieser beiden Ausnahmetatbestände im Zusammenhang mit *Cloud* Computing wird im Folgenden näher eingegangen.

a) Bekanntgabe aufgrund überwiegender öffentlicher Interessen

121. Eine Bekanntgabe von Personendaten an die USA im Rahmen der Nutzung von *Cloud*-Diensten könnte somit möglicherweise auf den Ausnahmetatbestand der «überwiegenden wichtigen öffentlichen Interessen» (Art. 14 Abs. 4 lit. c Konvention 108+) gestützt werden, ein Ausnahmetatbestand, den Art. 15 Abs. 3 lit. a E-KDSG teilweise aufgreift.

122. Der Konventionstext äussert sich nicht dazu, ob dieser Ausnahmetatbestand auch auf **massenhafte, wiederholte oder routinemässige Bekanntgaben** anwendbar ist. Ein Blick in die EU-DSGVO, welche die Ausarbeitung der Konvention stark prägte, zeigt jedoch, dass diese die Ausnahmetatbestände auch für «eine Reihe von Übermittlungen» zulässt und somit nicht nur im Einzelfall.[151] Eine Abstützung der Datenbekanntgabe ins Ausland im Rahmen der Nutzung von *Cloud*-Diensten auf den Ausnahmetatbestand der «überwiegenden öffentlichen Interessen» wäre somit völkerrechtlich nicht ausgeschlossen, sofern es sich dabei tatsächlich um überwiegende Interessen handelt und die Verhältnismässigkeit gegeben ist.

> Allerdings ist zu konstatieren, dass der Kanton Bern in der **aktuellen Fassung** von Art. 15 Abs. 3 lit. a E-KDSG den Ausnahmetatbestand des überwiegenden öffentlichen Interesses nur im **Einzelfall** zur Anwendung zulässt.

123. Damit ist entscheidend, ob an der **Nutzung von *Cloud*-Diensten**, bei denen Daten in Staaten ohne angemessenes Datenschutzniveau übermittelt werden, ein überwiegendes öffentliches Interesse besteht, das gesetzlich vorgesehen ist und das eine Weitergabe der Daten als eine in einer demokratischen Gesellschaft notwendige und verhältnismässige Massnahme erscheinen lässt (Art. 14 Abs. 4 lit. c Konvention 108+), was im Folgenden zu untersuchen ist.

aa) Gesetzlich vorgesehenes öffentliches Interesse

124. Als überwiegendes öffentliches Interesse an einer Nutzung von *Cloud*-Diensten kommt in erster Linie das Anliegen, auf ein sehr **leistungsfähiges Instrument** zurückgreifen zu können, in Betracht, was mit Blick auf die **Qualität der Dienstleistungen der Verwaltung** sowie deren **Effizienz und Effektivität** von Vorteil sein dürfte. So wird vom Regierungsrat des Kantons Bern als öffentliches Interesse mit Blick auf die Nutzung von *US-Cloud*-Software die «raschere, kostengünstigere und kundenfreundlichere» Erreichung der behördlichen Digitalisierungsziele angeführt. Im Einzelnen geht es gemäss dem Vortrag des Regierungsrats des Kantons Bern um

> «die grossen praktischen öffentlichen Interessen an der Nutzung der weltweit besten *Cloud*-Lösungen: Mit ihnen können die Behörden ihre Digitalisierungsziele viel rascher, kostengünstiger und kundenfreundlicher erreichen als mit konventioneller, nicht cloudbasierter Software. Tiefer gewichtet werden

---

151 Vgl. SCHRÖDER, in: Kühling/Buchner (Hrsg.), DSGVO/BDSG, Art. 49 DSGVO N 11a.

die gegebenenfalls erleichterten Zugriffe ausländischer Strafbehörden oder Nachrichtendienste auf Daten oder die eingeschränkten Möglichkeiten, sich gerichtlich gegen Datenschutzverletzungen im Ausland zu wehren.»[152]

125. Derartige Effizienz- und Effektivitätserwägungen müssten somit als **legitimes öffentliches Interesse** gelten können.

Der **Begriff des öffentlichen Interesses** – der in der Verfassung (zu Recht) nicht definiert wird – zeichnet sich durch eine gewisse **Offenheit** aus,[153] wobei den Wertentscheidungen der Verfassung bei der Frage, ob es um ein öffentliches Interesse geht, jedoch eine zentrale Bedeutung zukommt. Aus diesen lässt sich insbesondere die grosse Bedeutung der Grundrechte ableiten; sie enthalten aber auch eine Reihe von Zielsetzungen (z.B. Sozialziele oder das Ziel der Nachhaltigen Entwicklung), deren Verwirklichung zweifellos als öffentliches Interesse anzusehen ist. Auf der anderen Seite ist es aber nicht notwendig, dass ein Anliegen in irgendeiner Form in der Verfassung Niederschlag gefunden haben muss, damit es als öffentliches Interesse qualifiziert werden kann; einen irgendwie gearteter *Numerus clausus* öffentlicher Interessen gibt es nicht. Dies drängt sich schon deshalb auf, weil es grundsätzlich **Sache des Gesetzgebers** ist, die öffentlichen Interessen zu definieren, und diese im Übrigen auch einem gewissen Wandel unterworfen sind bzw. sein können.[154]

Vor diesem Hintergrund und angesichts der Tatsache, dass es in einer Demokratie keinen grundsätzlichen Gegensatz zwischen staatlichen und gesellschaftlichen Interessen gibt (was aber nicht bedeutet, dass Staat und Gesellschaft in jeder Beziehung gleichzusetzen wären), können öffentliche Interessen sowohl solche des Staates als solchem (wie z.B. fiskalische Interessen) als auch solche primär der Gesellschaft (wie das Anliegen ausreichender Kinderbetreuungsmöglichkeiten) sein.[155]

Als von öffentlichem Interesse gelten mithin ausschliesslich solche, die im Prozess der **demokratischen Rechtsetzung** als Belange des Gemeinwesens ausgewiesen wurden. Dazu gehören insbesondere der Schutz der Polizeigüter sowie die mit den einzelnen Staatsaufgaben zu verfolgenden Anliegen, wie sie in den Aufgabennormen der Verfassung und in den Ziel- und Zweckartikeln der Aufgabengesetze zum Ausdruck kommen.[156] Schliesslich schreibt auch die Konvention 108+ vor, dass das öffentliche Interesse gesetzlich vorgesehen sein muss (Art. 14 Abs. 4 lit. c Konvention 108+).

126. Die Digitalisierung der öffentlichen Verwaltung kann im Kanton Bern als **öffentliches Interesse** qualifiziert werden: Mit dem vom Grossen Rat am 3. März 2022 verabschiedeten Gesetz über die digitale Verwaltung (DVG)[157] hat der Kanton auf demokratischem Wege Digitalisierungsziele für die öffentliche Verwaltung von Kanton und Gemeinden festgelegt.

Selbst wenn man dieser Einschätzung kritisch gegenüberstehen kann (schliesslich ist die Digitalisierung der öffentlichen Verwaltung für sich allein kein Selbstzweck), so kann zumindest das dahinter liegende Interesse der «**Effizienzsteigerung**» als öffentliches Interesse angesehen werden.[158]

---

152 Regierungsrat des Kantons Bern, Vortrag KDSG, S. 33.

153 DUBEY, in: Martenet/Dubey (Hrsg.), CR Cst., Art. 5 N 73.

154 DUBEY, in: Martenet/Dubey (Hrsg.), CR Cst., Art. 5 N 74 ff.; EPINEY, in: Waldmann/Belser/Epiney (Hrsg.), BSK-BV, Art. 5 N 63.

155 EPINEY, in: Waldmann/Belser/Epiney (Hrsg.), BSK-BV, Art. 5 N 64.

156 TSCHANNEN, Staatsrecht, § 7 Rz. 364.

157 Gesetz [des Kantons Bern] vom 7. März 2022 über die digitale Verwaltung (DVG), BSG 109.1.

158 BGE 147 I 346 E. 5.4.2. S. insoweit auch DUBEY, in: Martenet/Dubey (Hrsg.), CR Cst., Art. 5 N 83.

bb) Notwendigkeit und Verhältnismässigkeit in einer demokratischen Gesellschaft

127. Fraglich ist, ob dieses Interesse (hinreichend) «wichtig» und «überwiegend» ist, d.h. ob es die Weitergabe der Daten als eine in einer demokratischen Gesellschaft notwendige und verhältnismässige Massnahme erscheinen lässt, so dass sie den Interessen der betroffenen Personen am Schutz ihrer personenbezogenen Daten vorgehen kann. Zu fragen ist dabei nach der **Erforderlichkeit** der Datenbekanntgabe zur Erreichung dieser Ziele, also danach, ob keine alternativen *Cloud*-Lösungen zur Verfügung stehen, welche mit weniger Gefahren für die Grundrechte der betroffenen Personen einhergehen, und nach der **Verhältnismässigkeit** im engeren Sinne, also einer Abwägung zwischen den öffentlichen und den privaten Interessen.[159]

128. Der Konventionstext verlangt ein **«wichtiges»** öffentliches Interesse. Dies geht über ein blosses normales öffentliches Interesse hinaus, wie übrigens auch die Doktrin zu Art. 49 DSGVO betont.[160] Allerdings ist mit dem Hinweis auf die «Wichtigkeit» noch nicht allzu viel gewonnen, da diese selbstredend sehr unterschiedlich beurteilt werden kann und sich die diesbezüglichen Einschätzungen durchaus auch wandeln können. Insofern geht es bei den hier in Frage stehenden Anliegen zwar sicherlich nicht um überragende öffentliche Interessen (wie der Schutz von Leib und Leben sowie der öffentlichen Sicherheit); nichtsdestotrotz kann nicht von vornherein ausgeschlossen werden, dass es sich bei den vorgebrachten Effizienz- und Effektivitätserwägungen für die Verwaltung und die Bürger um hinreichend «wichtige» öffentliche Interessen handelt.

129. Damit ist entscheidend, ob diese Interessen auch **«überwiegend»** sind. Da es sich bei der Frage, ob das öffentliche Interesse im Kontext der Nutzung von *Cloud*-Lösungen überwiegt, um eine abstrakte Abwägung für eine unbestimmte Vielzahl von Fällen handelt, kann u.E. für diese Beurteilung mit gewissen «Vereinfachungen» operiert werden, etwa einer **umfassenden Risikokalkulation**, welche sowohl die Art und Schwere als auch die Eintrittswahrscheinlichkeit und voraussichtliche Häufigkeit von Grundrechtsverletzungen, die mit der beabsichtigen Datenbekanntgabe ins Ausland einhergehen, einbezieht. Von Bedeutung ist insbesondere, dass dabei nicht nur die Eintrittswahrscheinlichkeit einer Grundrechtsverletzung (z.B. das Risiko eines unbefugten Zugriffs einer ausländischen Behörde), sondern auch die Auswirkungen auf die betroffenen Personen, inklusive ihrer Möglichkeiten, sich gegen eine Verletzung ihrer Grundrechte zu wehren, und die Schwere der Verletzung mit in die Kalkulation einbezogen werden müssen. Je schwerer die potenzielle Grundrechtsverletzung wiegt, desto geringere Anforderungen sind an ihre Eintrittswahrscheinlichkeit und -häufigkeit zu stellen, und *vice versa*. Nach der Rechtsprechung des Bundesgerichts vermag allerdings die Datensicherheit allein (im Sinne einer statistisch geringen Risikoeintrittswahrscheinlichkeit) den Umstand, dass die Datenbearbeitung an sich unverhältnismässig ist, nicht aufzuwiegen. Andernfalls käme

---

159 Sehr instruktiv zu dieser «*pondération*» DUBEY, in: Martenet/Dubey (Hrsg.), CR Cst., Art. 5 N 86 ff.

160 SCHRÖDER, in: Kühling/Buchner (Hrsg.), DSGVO/BDSG, Art. 49 DSGVO N 24; PAULY, in: Paal/Pauly (Hrsg.), DSGVO, Art. 49 DSGVO N 18 ff.; SCHANTZ, in: Spiecker et al. (Hrsg.), GDPR, Art. 49 N 28.

dem Grundsatz der Erforderlichkeit immer dann keine Bedeutung mehr zu, wenn die datenbearbeitende Instanz beweisen kann, dass sie genügend Schutzvorkehrungen getroffen hat.[161] Zu beachten ist auch, dass eine Verletzung des **Kerngehalts eines Grundrechts** durch kein öffentliches Interesse gerechtfertigt werden kann.[162]

In Bezug auf die Nutzung von *US-Cloud*-Dienstleistungen besteht aber genau dieses Risiko: So ist der EuGH in der Rs. C-311/18 (*Schrems II*)[163] zum Schluss gekommen, dass die Rechtslage in den USA und insbesondere die Überwachungsprogramme, welche auf alle in den USA gelagerten Daten anwendbar sind, den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts letztlich allgemein Vorrang einräumen und integral gegen Art. 7, 8 GRCh verstossen, da in Bezug auf bestimmte Überwachungsprogramme nicht erkennbar sei, dass für den Datenzugriff Einschränkungen bestünden und den Betroffenen keine ausreichenden Rechtsschutzmöglichkeiten zur Verfügung stünden, womit der **Wesensgehalt des Art. 47 GRCh verletzt** werde.

130. Eine abschliessende und allgemeingültige Einschätzung kann an dieser Stelle nicht gegeben werden, da die notwendige umfassende Risikokalkulation zahlreiche Elemente umfasst, die einer spezifischen Betrachtung des jeweiligen *Cloud*-Auftragsbearbeitungsverhältnisses bedürften. Klar dürfte aber sein, dass es **nicht (allein) auf eine statistische Berechnung des Eintrittsrisikos** ankommt, sondern auch auf die **Schwere** der Grundrechtsverletzungen und die Gefahr einer **Kerngehaltsverletzung**.

Diese Faktoren werden bei gewissen öffentlich verfügbaren, ausserhalb des Grundrechtekontextes erstellten Risikokalkulationsinstrumenten soweit ersichtlich **nicht berücksichtigt**.

131. Allerdings dürfte vor dem Hintergrund der obigen Ausführungen gerade bei Datenübermittlungen in Staaten mit ausgedehnten Überwachungsprogrammen, wo tendenziell im Falle selbst eines unwahrscheinlichen Zugriffs eine Kerngehaltsverletzung droht, das öffentliche Interesse an einer rascheren und kostengünstigeren Erreichung der Digitalisierungsziele die Grundrechte grundsätzlich **nicht überwiegen**, womit der Ausnahmetatbestand von Art. 14 Abs. 4 lit. c Konvention 108+ nicht als Grundlage für eine Datenübermittlung in Staaten ohne angemessenen Datenschutz im Rahmen von *Cloud*-Auftragsdatenbearbeitung dienen könnte. Zu einem anderen Abwägungsergebnis dürfte man hingegen kommen, wenn die in der *Cloud* abgelegten Daten **verschlüsselt** werden, wobei in diesem Fall das Schlüsselmanagement ausschliesslich bei der auftraggebenden Behörde und nicht beim *Cloud-Service*-Provider liegen dürfte.

Zu berücksichtigen ist, dass auch bei Bejahung eines überwiegenden Interesses an der massenhaften, routinemässigen Bekanntgabe von Personendaten in Staaten ohne angemessenes Datenschutzniveau zwecks Erreichung der kantonalen Digitalisierungsziele die Voraussetzungen der **Auftragsdatenbearbeitung erfüllt** sein müssen. Diese dürften jedoch grundsätzlich einer solchen Auftragsdatenbearbeitung entgegen stehen, soweit nicht sichergestellt werden kann, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie dies auch die Behörde dürfte, eine Voraussetzung, welche bei einer Bekanntgabe in Staaten ohne angemessenes Datenschutzniveau in der Regel nicht gegeben sein dürfte.[164]

---

161 BGE 147 I 346 E. 5.5.3.

162 Art. 36 Abs. 4 BV, s. dazu EPINEY, in: Waldmann/Belser/Epiney (Hrsg.), BSK-BV, Art. 36 BV N 61. Gleiches gilt im Kanton Bern: Art. 28 Abs. 4 KV-BE.

163 EuGH, Rs. C-311/18, *Schrems II*, ECLI:EU:C:2020:559.

164 Oben N 89 ff.

b) Bekanntgabe zwecks Bearbeitung im Auftrag

132. Abschliessend ist zu fragen, inwiefern der vom Regierungsrat des Kantons Bern vorgeschlagene Ausnahmetatbestand (Art. 15 Abs. 3 lit. d, **«Variante 2»**) der Bekanntgabe zwecks Bearbeitung im Auftrag als Grundlage für die Nutzung von *US-Cloud*-Dienstleistungen dienen kann. Im Vordergrund steht dabei – abgesehen von den Voraussetzungen der Zulässigkeit der Auftragsdatenbearbeitung als solche[165] – die **Vereinbarkeit mit übergeordnetem Recht**.

133. Ein Ausnahmetatbestand wie der vorgeschlagene, wonach in Abwesenheit eines angemessenen Datenschutzniveaus Daten zwecks Bearbeitung im Auftrag ins Ausland bekannt gegeben werden dürfen, befreit die Auftragsdatenbearbeitung mit Auslandsbezug gänzlich von den für internationale Datentransfers vorgesehenen Voraussetzungen. Eine solche Möglichkeit ist im übergeordneten Recht, namentlich in der Konvention 108+ und in der Richtlinie 2016/680, nicht vorgesehen. Da die Ausnahmekataloge dieser beiden Rechtsquellen mangels anderslautender Hinweise abschliessend zu verstehen sind, ist die vom Regierungsrat in die Vernehmlassung geschickte Variante 2 **nicht mit dem übergeordneten Recht vereinbar**.

> Würde sie als zulässig erachtet, so müssten lediglich die Voraussetzungen der **Auftragsdatenbearbeitung**, nicht jedoch diejenigen der Bekanntgabe von Daten ins Ausland erfüllt werden. Für die Zulässigkeit der Nutzung von *US-Cloud*-Dienstleistungen stellen sich aber auch unter diesem Gesichtspunkt zahlreiche Fragen, und die Zulässigkeit einer solchen Auftragsdatenbearbeitung dürfte im Ergebnis zu verneinen sein.[166]

134. Nur am Rande sei in diesem Zusammenhang darauf hingewiesen, dass Art. 15 Abs. 3 lit. d E-KDSG auch ausgesprochen weit formuliert und keineswegs auf Auftragsdatenbearbeitungen mit *US-Cloud*-Lösungen beschränkt ist. Eine **Bekanntgabe ins Ausland** käme nach dem Wortlaut ganz **allgemein** unter den genannten Voraussetzungen in Betracht, so nicht nur in die USA, sondern auch in alle anderen Staaten mit einem nicht angemessenen Schutzniveau. Eine solche «Generalermächtigung» stünde auch kaum mit den erörterten grundrechtlichen Vorgaben (Art. 8 EMRK und Art. 13 Abs. 2 BV)[167] in Einklang.

3. Zwischenfazit

135. Im Ergebnis ist somit festzuhalten, dass eine **Datenbekanntgabe ins Ausland** im Rahmen der Nutzung von *Cloud*-Lösungen bei Auftragsbearbeitungen zwar *a priori* durch die Wahrung eines überwiegenden öffentlichen Interesses gerechtfertigt werden (Art. 14 Abs. 4 lit. c Konvention 108+) gerechtfertigt werden könnte. Allerdings dürfte bei Datenübermittlungen in Staaten mit ausgedehnten Überwachungsprogrammen, wo tendenziell im Falle selbst eines unwahrscheinlichen Zugriffs eine Kerngehaltsverletzung droht, das öffentliche Interesse an einer rascheren und kostengünstigeren Erreichung der Digitalisierungsziele die Grundrechte **nicht überwiegen**, womit der Ausnahmetatbestand

---

165 S.o. N 84 ff.
166 N 89 ff.
167 Zu diesen oben N 7 ff.

von Art. 14 Abs. 4 lit. c Konvention 108+ nicht als Grundlage für eine Datenübermittlung in Staaten ohne angemessenen Datenschutz im Rahmen von *Cloud*-Auftragsdatenbearbeitung dienen könnte. Zu einem anderen Abwägungsergebnis dürfte man hingegen kommen, wenn die in der *Cloud* abgelegten Daten **verschlüsselt** werden, wobei in diesem Fall das Schlüsselmanagement ausschliesslich bei der auftraggebenden Behörde und nicht beim *Cloud-Service*-Provider liegen dürfte.

136. Ein Ausnahmetatbestand wie **Art. 15 Abs. 3 lit. d E-KDSG**, wonach in Abwesenheit eines angemessenen Datenschutzniveaus Daten zwecks Bearbeitung im Auftrag ins Ausland bekannt gegeben werden dürfen, befreite die Auftragsdatenbearbeitung mit Auslandsbezug gänzlich von den für internationale Datentransfers vorgesehenen Voraussetzungen. Eine solche Möglichkeit wäre weder mit den völkerrechtlichen Vorgaben noch mit der Verfassung vereinbar.

§ 4 Zusammenfassung und Fazit

137. Die Ergebnisse der vorliegenden Untersuchung können folgendermassen zusammengefasst werden:

- Die **Bearbeitung von Personendaten** durch **öffentliche Behörden** muss mit den **verfassungs- und völkerrechtlichen Vorgaben** vereinbar sein. Von Bedeutung sind hier in erster Linie Art. 8 EMRK, Art. 13 Abs. 2 BV und die Konvention 108+ des Europarates. Zu beachten ist weiter die RL 2016/680 (im Bereich der Strafverfolgung und der Strafvollstreckung), und die Datenschutzgrundverordnung gibt wichtige Hinweise auf die Tragweite der Konvention 108+.
- Insbesondere die **Konvention 108+** enthält bedeutende Präzisierungen in Bezug auf die Anforderungen an eine Datenbekanntgabe ins Ausland und die Zulässigkeit von Auftragsbearbeitungen, welche zwingend zu beachten sind.
- Das **Datenschutzgesetz des Bundes** und die **Datenschutzgesetze der (anderen) Kantone** greifen die erwähnten völkerrechtlichen Vorgaben auf und konkretisieren sie, wobei der diesbezügliche Präzisierungsgrad jedoch variiert. Festzuhalten ist aber, dass eine Bestimmung wie Art. 15 Abs. 3 lit. d E-KDSG weder im Datenschutzgesetz des Bundes noch in einem (anderen) kantonalen Datenschutzgesetz zu finden ist.
- Im Falle einer **Auftragsdatenbearbeitung** liegt grundsätzlich **keine Datenbekanntgabe an Dritte** vor, da die Datenherrschaft beim Verantwortlichen verbleibt und gerade nicht auf den Auftragsbearbeiter übertragen wird; insofern befindet sich letzterer in der «Sphäre» der verantwortlichen Behörde. Dies muss auch für Auftragsbearbeitungen im Ausland gelten. Dessen ungeachtet sprechen Ziel und Zweck der Vorgaben der Datenbekanntgabe ins Ausland dafür, dass in den Fallgestaltungen, in welchen die (Auftrags-) Datenbearbeitung dann im Ergebnis im Ausland stattfindet, die Vorgaben für die **Datenbekanntgabe ins Ausland** sinngemäss (zusätzlich) zu beachten sind.
- Daher ist auch die Nutzung von *US-Cloud*-Lösungen im Rahmen einer Auftragsbearbeitung nur zulässig, wenn die **völker- und verfassungsrechtlichen Vorgaben für eine Auftragsbearbeitung** beachtet werden, die in Art. 12 E-KDSG konkretisiert sind. Von besonderer Bedeutung ist dabei Art. 12 Abs. 1 lit. a E-KDSG, wonach die Daten nur so bearbeitet werden dürfen, wie es die auftraggebende Behörde selbst tun dürfte. Darüber hinaus ist das Legalitätsprinzip zu beachten (Art. 12 Abs. 1 lit. b E-KDSG):
  - Im Rahmen des Art. 12 Abs. 1 lit. a E-KDSG ist danach zu fragen, ob im betreffenden Staat, in welchem der Auftragsbearbeiter ansässig ist oder dessen Rechtsordnung die Datenbearbeitung unterworfen werden kann, ein **angemessenes Schutzniveau** angenommen werden kann, womit letztlich parallele Erwägungen wie im Rahmen des Art. 15 Abs. 1, 2 E-KDSG zum Zuge kommen.
  - Eine Datenbearbeitung im Auftrag einer Behörde, im Rahmen derselben der Auftragsdatenbearbeiter im Ausland ansässig ist bzw. der Rechtsordnung eines ausländischen Staates unterworfen ist oder die Datenbearbeitung im Ausland stattfindet (wo kein angemessenes Schutzniveau gewährleistet ist), ist jedenfalls dann **unzulässig**, wenn der ausländische Staat keine **hinreichenden rechtsstaatlichen Strukturen** kennt.

- Darüber hinaus ist eine Unzulässigkeit auch dann anzunehmen, wenn der Auftragsbearbeiter aufgrund des im Ausland geltenden Rechts nicht gewährleisten kann, dass die Daten nur so bearbeitet werden, wie es die Behörde selbst tun dürfte. Dies ist insbesondere dann der Fall, wenn **weitgehende staatliche Zugriffsmöglichkeiten** bestehen und keine hinreichenden Garantien für ihre Beschränkung gegeben sind (was auch dann der Fall sein kann, wenn der Server in der Schweiz steht), wie dies im Verhältnis der Schweiz zu den USA auf der Grundlage der derzeit geltenden Rechtslage (welche sich freilich mit einem Angemessenheitsbeschluss des EDÖB und den damit einhergehenden Garantien ändern kann) anzunehmen ist. Diese Unzulässigkeit ergibt sich aus der **Ausgestaltung der Gesetzeslage** in den USA, die es mit sich bringt, dass der Auftragsbearbeiter verpflichtet werden kann, die Daten in einer Weise zu bearbeiten, wie die Behörde dies nicht tun dürfte. Damit kann die Behörde nicht darlegen, dass grundsätzlich sichergestellt ist bzw. davon auszugehen ist, dass der Auftragsbearbeiter die Daten nur so bearbeiten darf, wie es die Behörde selbst tun dürfte. Für eine **Risikoanalyse** in dem Sinn, dass es darauf ankäme, mit welcher Wahrscheinlichkeit eine solche Bearbeitung tatsächlich erfolgen könnte, bleibt vor diesem Hintergrund **kein Raum**.
- Vor diesem Hintergrund erweist sich eine Datenbearbeitung im **Auftrag** einer staatlichen Behörde, welche die Nutzung von **US-basierten *Cloud*-Lösungen** vorsieht, als **nicht mit Art. 12 Abs. 1 lit. a E-KDSG vereinbar.** Im Übrigen dürfte in aller Regel auch ein Verstoss gegen **Art. 12 Abs. 1 lit. b E-KDSG** vorliegen, soweit es auch um Personendaten geht, welche einer **gesetzlichen Geheimhaltungspflicht** (wie z.B. das Amtsgeheimnis) unterliegen.

- Eine **Datenbekanntgabe ins Ausland** im Rahmen der Nutzung von *Cloud*-Lösungen bei Auftragsbearbeitungen könnte *a priori* durch die Wahrung eines überwiegenden öffentlichen Interesses gerechtfertigt werden (Art. 14 Abs. 4 lit. c Konvention 108+). Allerdings dürfte bei Datenübermittlungen in Staaten mit ausgedehnten Überwachungsprogrammen, wo tendenziell eine Kerngehaltsverletzung droht (auch wenn der Zugriff unwahrscheinlich sein sollte), das öffentliche Interesse an einer rascheren und kostengünstigeren Erreichung der Digitalisierungsziele die Grundrechte **nicht überwiegen**, womit der Ausnahmetatbestand von Art. 14 Abs. 4 lit. c Konvention 108+ nicht als Grundlage für eine Datenübermittlung in Staaten ohne angemessenen Datenschutz im Rahmen von *Cloud*-Auftragsdatenbearbeitung dienen könnte. Zu einem anderen Abwägungsergebnis dürfte man hingegen kommen, wenn die in der *Cloud* abgelegten Daten **verschlüsselt** werden, wobei in diesem Fall das Schlüsselmanagement ausschliesslich bei der auftraggebenden Behörde und nicht beim *Cloud-Service*-Provider liegen dürfte.
- Ein **Ausnahmetatbestand** wie **Art. 15 Abs. 3 lit. d E-KDSG**, wonach in Abwesenheit eines angemessenen Datenschutzniveaus Daten zwecks Bearbeitung im Auftrag ins Ausland bekannt gegeben werden dürfen, befreite die Auftragsdatenbearbeitung mit Auslandsbezug gänzlich von den für internationale Datentransfers vorgesehenen Voraussetzungen. Eine solche Möglichkeit ist im übergeordneten Recht, namentlich in der Konvention 108+ und in der Richtlinie 2016/680, nicht vorgesehen. Da die Ausnahmekataloge dieser beiden Rechtsquellen mangels anderslautender Hinweise abschliessend zu verstehen sind, ist die vom Regierungsrat in die Vernehmlassung geschickte Variante 2 auch aus diesem Grund **nicht mit**

dem übergeordneten Recht vereinbar. Ebensowenig dürfte sie mit Art. 8 EMRK und Art. 13 Abs. 2 BV in Einklang stehen.

138. Insgesamt konnte die Untersuchung somit die sehr **engen Grenzen** für die Nutzung von *Cloud*-Lösungen im Rahmen von Auftragsbearbeitungen aufzeigen, dies soweit der Auftragsbearbeiter in einem Staat, ansässig ist, der über kein angemessenes Datenschutzniveau im Sinn der Konvention 108+ (und des Art. 15 Abs. 1, 2 E-KDSG) verfügt. Gleiches gilt für die Konstellation, dass die Datenbearbeitung in einem solchen Staat erfolgt, oder die Datenbearbeitung des Auftragsbearbeiters dessen Rechtsordnung unterworfen werden kann. Im Ergebnis dürfte eine solche Auftragsbearbeitung grundsätzlich nicht mit den völker- und verfassungsrechtlichen Vorgaben (und ihrer Konkretisierung in Art. 9, 16 DSG und in Art. 12, 15 Abs. 1-3 E-KDSG) vereinbar sein.

139. Bemerkenswert ist dabei, dass auch auf der Grundlage des **Art. 15 Abs. 1 lit. d E-KDSG** eine solche Auftragsbearbeitung als **unzulässig** anzusehen wäre. Denn diese Bestimmung nimmt auf die Rechtmässigkeitsvoraussetzungen der Auftragsbearbeitung Bezug. Aus diesen ergibt sich aber ebenfalls die Unzulässigkeit einer derartigen Auftragsbearbeitung, da in einer solchen Konstellation gerade nicht sichergestellt werden kann, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie dies auch die Behörde selbst tun dürfte (Art. 12 Abs. 1 lit. a E-KDSG). Denn diese Anforderung dürfte in der Regel nur dann erfüllt sein, wenn im Falle einer Auftragsbearbeitung im Ausland die entsprechende ausländische Rechtsordnung ein angemessenes Datenschutzniveau gewährleistet. Insofern decken sich die Anforderungen des Art. 12 Abs. 1 lit. a E-KDSG zumindest teilweise mit denjenigen des Art. 15 Abs. 1, 2 E-KDSG.

140. Die Einführung des Art. 15 Abs. 3 lit. d E-KDSG in der vorgesehenen Form würde daher – im Gegensatz zur Absicht des Gesetzgebers – die Nutzung von **US-basierten *Cloud*-Lösungen** im Rahmen einer Auftragsbearbeitung gar nicht erlauben, da eine solche nicht mit Art. 12 Abs. 1 E-KDSG vereinbar wäre, auf den Art. 15 Abs. 3 lit. d E-KDSG verweist. Vor diesem Hintergrund erwiese sich eine Bestimmung wie **Art. 15 Abs. 1 lit. d E-KDSG** jedenfalls insoweit als «nutzlos», als sie den Rückgriff auf *US-Cloud*-Lösungen ermöglichen soll. Daher drängte es sich auch aus diesem Grund – abgesehen davon, dass die Bestimmung im Widerspruch zu den völkerrechtlichen Vorgaben der Konvention 108+ steht – auf, auf ihre **Einführung zu verzichten**.

Literaturverzeichnis

BAERISWYL, Bruno/PÄRLI, Kurt/BLONSKI, Dominika (Hrsg.), Stämpfli Handkommentar Datenschutzgesetz, Bern 2023 (zit. VERFASSER/IN, in: Baeriswyl/Pärli/Blonski (Hrsg.), SHK-DSG).

BAERISWYL, Bruno, Wenn die Rechtsauslegung «nebulös» wird, digma 2019, 118 ff.

BELSER, Evamaria/EPINEY, Astrid/WALDMANN, Bernhard, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011 (zit. VERFASSER/IN, in: Belser/Epiney/Waldmann, Datenschutzrecht).

BIERI, Adrian/POWELL, Julian (Hrsg.), Orell Füssli Kommentar Datenschutzgesetz, Zürich 2023 (zit. VERFASSER/IN, in: Bieri/Powell (Hrsg.), OFK-DSG).

BLONSKI, Dominika, Was bedeutet die Revision für die kantonalen Datenschutzgesetze?, in: Astrid Epiney/Sophie Moser/Sophia Rovelli (Hrsg.), Die Revision des Datenschutzgesetzes des Bundes, Zürich 2022, 89 ff.

BLONSKI, Dominika, Cloud – alles Risiko? Rechtliche Vorgaben für die Auslagerung von Datenbearbeitungen in die Cloud, SJZ 2023, 991 ff.

DE TERWANGNE, Cécile, La Convention 108+ du Conseil de l'Europe, in: Astrid Epiney/Sophia Rovelli (Hrsg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen, Zürich 2020, 39 ff.

DRITTENBASS, Joel, Regulierung von autonomen Robotern – angewendet auf den Einsatz von autonomen Medizinrobotern: eine datenschutzrechtliche und medizinprodukterechtliche Untersuchung, Zürich/Baden-Baden 2021.

DZAMKO, Daniel, Überlegungen zu Recht und Risiko bei behördlicher Cloudnutzung in: Sylvain Métille (Hrsg), L'informatique en nuage, Bern 2022, 83 ff.

EHRENZELLER, Bernhard/EGLI, Patricia/HETTICH, Peter/HONGLER, Peter/SCHINDLER, Benjamin/SCHMID, Stefan G./SCHWEIZER, Rainer J. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 4. Aufl., St. Gallen 2023 (zit. VERFASSER/IN, in: Ehrenzeller u.a. (Hrsg.), SGK-BV).

EPINEY, Astrid, Datenschutz in der EU und die Schweiz, sic 2022, 575 ff.

EPINEY, Astrid/FREI, Nula, Die Datenschutzgrundverordnung: Grundsätze und ausgewählte Aspekte, in: Astrid Epiney/Sophia Rovelli (Hrsg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen, Zürich 2020, 2 ff.

EPINEY, Astrid/KERN, Markus, Zu den Neuerungen im Datenschutzrecht der Europäischen Union, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Die Revision des Datenschutzes in Europa und die Schweiz, Zürich 2016, 39 ff.

EPINEY, Astrid/NÜESCH, Daniela/ROVELLI, Sophia, Datenschutzrecht in der Schweiz, Bern 2023.

GLOCKER, Felix, EU-US Data Privacy Framework: Update des Privacy Shield mit Augenmass. Entwurf des Angemessenheitsbeschlusses der EU-Kommission und seine Erfolgsaussichten vor dem EuGH, ZD 2023, 189 ff.

GOLA, Peter/HECKMANN, Dirk (Hrsg.), Datenschutz-Grundverordnung / Bundesdatenschutzgesetz, Kommentar, 3. Aufl., München 2022 (zit. VERFASSER/IN, in: Gola/Heckmann (Hrsg.), DSGVO/BDSG).

JAHNEL, Dieter, Kommentar zur Datenschutz-Grundverordnung (DSGVO), Wien 2022.

KÜHLING, Jürgen/BUCHNER, Benedikt (Hrsg.), Kommentar Datenschutz-Grundverordnung, BDSG, 3. Auflage München 2020 (zit. VERFASSER/IN, in: Kühling/Buchner (Hrsg.), DSGVO/BDSG).

MARTENET, Vincent/DUBEY, Jacques (Hrsg.), Commentaire romand. Constitution fédérale, 2 Bände, Basel 2021 (zit.: VERFASSER/IN, in: Martenet/Dubey (Hrsg.), CR Cst.).

MÉTILLE, Sylvain, L'utilisation de l'informatique en nuage par l'administration publique, AJP/PJA 2019, 609 ff.

MÉTILLE, Sylvain/MEIER, Philippe (Hrsg.), Commentaire Romand Loi sur la protection des données, Basel 2023 (zit. VERFASSER/IN, in: Métille/Meier (Hrsg.), CR-LPD).

PAAL, Boris/PAULY, Daniel (Hrsg.), Kommentar Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Auflage München 2021 (zit. VERFASSER/IN, in: Paal/Pauli (Hrsg.), DSGVO).

POWELL, Julian, Die Revision der kantonalen Datenschutzgesetze, Jusletter vom 31. Mai 2021.

ROSENTHAL, David, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, Jusletter vom 10. August 2020.

ROSENTHAL, David/JÖHRI, Yvonne, Handkommentar zum Datenschutzgesetz, Zürich 2021.

SCHEFER, Markus/GLASS, Philip, Gutachten zum grundrechtskonformen Einsatz von M365 durch die Gemeinden im Kanton Zürich, 6. Juli 2023.

SCHWANINGER, David/MERZ, Michelle, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke 2.0., Jusletter vom 21. Juni 2021.

SPIECKER GEN. DÖHMANN, Indra/PAPAKONSTANTINOU, Vagelisi/HORNUNG, Gerrit/DE HERT, Paul (Hrsg.), General Data Protection Regulation. Article-by-Article Commentary, Oxford/Baden-Baden 2023 (zit. VERFASSER/IN, in: Spiecker et al. (Hrsg.), GDPR).

SYDOW, Gernot/MARSCH, Nikolaus (Hrsg.), DS-GVO/BDSG, Handkommentar, 3. Aufl., Baden-Baden 2022 (zit. VERFASSER/IN, in: Sydow/Marsch (Hrsg.), DSGVO/BDSG).

TAEGER, Jürgen/GABEL, Detlev (Hrsg.), DSGVO – BDSG – TTDSG, Kommentar, Frankfurt 2022 (zit. VERFASSER/IN, in: Taeger/Gabel (Hrsg.), DSGVO/BDSG/TTDSG).

TSCHANNEN, Pierre, Staatsrecht der Schweizerischen Eidgenossenschaft, 5. Auflage Bern 2021.

WALDMANN, Bernhard/BELSER, Eva Maria/EPINEY, Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015 (zit. VERFASSER/IN, in: Waldmann/Belser/Epiney (Hrsg.), BSK-BV).

Materialien

Bundesrat, Botschaft zur Genehmigung des Protokolls vom 10. Oktober 2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, BBl 2020 565 (zit. Botschaft Konvention 108+).

Bundesrat, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 (zit. Botschaft DSG).

Bundesamt für Justiz, Bericht zum US CLOUD Act, 17. September 2021 (zit. US Cloud Act).

Bundeskanzlei, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung. Bericht in Umsetzung vom Meilenstein 5 der Cloud-Strategie des Bundesrates, 31. August 2022 (zit. Bericht Public Cloud).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Stellungnahme zur Datenschutz Risikobeurteilung der Suva zum Projekt Digital Workplace «M365» unter besonderer Berücksichtigung des von der Suva thematisierten Zugriffs von US-amerikanischen Behörden auf Personendaten, die das Unternehmen in eine von der Firma Microsoft betriebene Cloud auslagert, Bern, 13. Mai 2022 (zit. EDÖB, Stellungnahme SUVA, 2022).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final vom 10.1.2017.

Europäische Kommission, Durchführungsbeschluss (EU) 2023/1795 vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ABl. L 231 vom 20.9.2023, 118.

Europarat, Erläuternder Bericht zum Modernisierten Übereinkommens zum Schutz des Menschen bei automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108) vom 8. Mai 2018 (zit. Erläuternder Bericht zur Revision der Datenschutzkonvention des Europarates).

privatim, Merkblatt Cloud-spezifische Risiken und Massnahmen.

Regierungsrat des Kantons Bern, Vortrag zum Datenschutzgesetz, 21. Juni 2023 (zit. Regierungsrat des Kantons Bern, Vortrag KDSG).

Abkürzungsverzeichnis

a.M.	anderer Meinung
Abs.	Absatz
AJP	Aktuelle juristische Praxis
Art.	Artikel
Aufl.	Auflage
BBl	Bundesblatt
BGE	Entscheidungen des Schweizerischen Bundesgerichts (Amtliche Sammlung)
Bst.	Buchstabe
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101)
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
DSG	Bundesgesetz über den Datenschutz vom 25. September 2020, SR 235.1
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. 2016 L 119, 1
DSV	Verordnung über den Datenschutz vom 31. August 2022, SR 235.11
DVBl	Deutsches Verwaltungsblatt
E/Erw.	Erwägung
ECLI	European Case Law Identifier
EGMR	Europäischer Gerichtshof für Menschenrechte
E-KDSG	Entwurf für ein kantonales Datenschutzgesetz des Kantons Bern
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (SR 0.101)
Erw.	Erwägung
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
f. / ff.	folgende / fortfolgende
ggf.	gegebenenfalls

GRCh	Grundrechtecharta
i.e.S.	im engeren Sinne
i.V.m.	in Verbindung mit
ID	(elektronische) Identität
ISKE	three-level IT baseline security system
lit.	litera
m.a.W.	mit anderen Worten
m.w.N.	mit weiteren Nachweisen
N	Randnote
Nr.	Nummer
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PKI	Public Key Infrastructure
RIA	Information system authority (Estland)
RJD	Recueil juridique Dalloz
RL 2016/680	Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehrs und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl 2016 L 119, 89
Rz.	Randziffer
s.	siehe
sog.	sogenannt(en)
u.E.	unseres Erachtens
vgl.	vergleiche
VPB	Verwaltungspraxis der Bundesbehörden
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
Ziff.	Ziffer
zit.	zitiert