Die Sicherheit persönlicher Daten beim Outsourcing der Datenbearbeitung an Dritte

Fabia Stöcklin*

SCHLAGWÖRTER Outsourcing – Datenbearbeitung – Dritte – Bekanntgabeprivileg – Cloud-Dienst

ZUSAMMENFASSUNG Der folgende Beitrag widmet sich der Frage, wie sicher Personendaten sind, welche von Privatpersonen an Dritte zur Bearbeitung weitergegeben werden. Dafür müssen sowohl die rechtlichen Voraussetzungen gemäss Art. 10a DSG als auch die Möglichkeiten der vertraglichen Ausgestaltung beleuchtet werden. Besonders bei einer Verlagerung der Datenbearbeitung ins Ausland oder der Nutzung eines Cloud-Dienstes sind ausserdem zusätzliche sicherheitsrelevante Aspekte zu beachten.

RÉSUMÉ Le présent article est consacré à la question de la sécurité des données personnelles transmises par des personnes privées à des tiers pour traitement. Pour ce faire, il convient d'examiner aussi bien les conditions légales selon l'article 10a LPD que les possibilités d'aménagement contractuel. En particulier en cas de transfert du traitement des données à l'étranger ou d'utilisation d'un service en nuage, il convient en outre de tenir compte d'aspects supplémentaires liés à la sécurité.

ABSTRACT The following article addresses the issue of security regarding personal data which is passed on by private individuals to third parties for processing. For this purpose, both the legal requirements according to art. 10a FADP and the possibilities of contractual arrangements must be examined. Particularly when data processing is transferred abroad or a cloud service is used, additional security-relevant aspects must also be taken into account.

I. Einleitung

Täglich werden über jeden von uns unzählige Daten erfasst und verarbeitet. Immer häufiger wird die Bearbeitung solcher Daten von den Personen, welche die Daten ursprünglich sammeln, an Dritte übertragen – selbst bei sensiblen und infolgedessen besonders schützenswerten Personendaten. Dies kann beispielsweise vorkommen, wenn ein Arzt eine externe Abrechnungsstelle beauftragt,[1] Anwälte externe Server für die Speicherung von Mandantendaten nutzen,[2] Banken Kontoauszüge extern erstellen lassen[3] oder bereits bei einer alltäglichen, weit verbreiteten Auslagerung von Akten.[4] Besonders aktuell wird das Thema Datenschutz im Zusammenhang mit dem neuen E-Justice-Gesetz, das mittels Anpassungen der Prozessordnungen ein Obligatorium für eine elektronische Übermittlung vorsieht.[5] Doch wie sicher sind die Personenda-

* LL.M. (Edinburgh), wissenschaftliche Mitarbeiterin am Lehrstuhl von Frau Prof. Dr. iur. Corinne Zellweger-Gutknecht, Universität Basel.

Dieser Beitrag ist lizenziert unter Creative Commons Lizenz CC BY-NC-ND. DOI dieses Artikels: 10.3256/978-3-03929-024-6_04

1 Schweizerische Akademie der Medizinischen Wissenschaften / Verbindung der Schweizer Ärztinnen und Ärzte, Rechtliche Grundlagen im medizinischen Alltag, Ein Leitfaden für die Praxis, Bern 2020, 130 ff.

2 Ausführlicher dazu Daniel Hürlimann/Martin Steiger, Auf dem Weg zur digitalen Anwaltskanzlei trotz Berufsgeheimnis und Datenschutz, Anwaltsrevue 5/2021, 199 ff.

3 Leo Rusterholz, The Impact of the revised Data Protection Act on Outsourcings by Swiss Financial Institutions, Swiss Capital Markets Law vom 7. Juni 2022.

4 Fabian Baumgartner, Zürcher Behörde lagert Akten mit heiklen Daten aus, NZZ vom 5. Oktober 2015, 15.

5 Vorentwurf vom 11. September 2020 zu einem Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ). Insbesondere interessant sind die Vorentwürfe für die neuen Art. 47a Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968 (VwVG; SR 172.021), Art. 38c Bundesgesetz über das Bundesgericht vom 17. Juni 2005 (BGG; SR 173.110), Art. 128c Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (ZPO; SR 272), Art. 103c Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO; SR 312.0), Art. 2c Bundesgesetz über den ausserprozessualen Zeugenschutz vom 23. Dezember 2011 (ZeugSG; SR 312.2), Art. 8c Bundesgesetz über die Hilfe an Opfer von Straftaten vom 23. März 2007 (Opferhilfegesetz, OHG; SR 312.5), Art. 31c Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (VStrR; SR 313.0) und Art. 37c Militärstrafprozess vom 23. März 1979 (MStP; SR 322.1) (alle mit dem Titel «Obligatorische elektronische Übermittlung») sowie einen neuen Art. 37a Bundesgesetz über das Verwaltungsgericht vom 17. Juni 2005 (VGG; SR 173.32) («Elektronische Übermittlung») und einen neuen Art. 8 Abs. 1 Bst. e Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte vom 23. Juni 2000 (Anwaltsgesetz, BGFA; SR 935.61)

ten, welche von Privatpersonen an (teilweise unbekannte) Dritte zur Bearbeitung weitergegeben werden?

Der folgende Beitrag widmet sich dieser Fragestellung, indem zuerst aufgezeigt wird, wann eine Auslagerung der Datenbearbeitung rechtlich überhaupt zulässig ist, bevor auf die vertraglich zu vereinbarenden Rechte und Pflichten der beteiligten Parteien eingegangen wird. Ein besonderer Fokus wird dabei auf Cloud-Dienste und die Verlegung der Datenbearbeitung ins Ausland gelegt.

II. Die rechtmässige Datenübertragung an einen Dritten

A. Voraussetzungen

Personendaten dürfen nur bearbeitet werden, wenn dabei die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzt wird.[6] Sofern die betroffene Person die Daten nicht selbst allgemein zugänglich macht,[7] ist grundsätzlich jede Bearbeitung widerrechtlich, sofern sie nicht durch eine Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder durch ein Gesetz gerechtfertigt wird.[8] Eine Weitergabe von Personendaten an einen Dritten zur Datenbearbeitung (sog. Outsourcing) untersteht ebenfalls dieser Regelung.[9]

Das Bearbeiten von Personendaten kann gemäss Art. 10a Abs. 1 DSG[10] vertraglich oder qua Gesetz an Dritte übertragen werden. Damit dies zulässig ist, dürfen Dritte die Daten nur so bearbeiten, wie der Auftraggeber, der die Daten gesammelt hat, es selbst tun dürfte (lit. a) und falls keine gesetzliche oder vertragliche Geheimhaltungspflicht dies verbietet (lit. b). Gesetzliche Geheimhaltungspflichten können sich beispielsweise aus dem Bankgeheimnis, dem Fernmeldegeheimnis oder dem Strafrecht ergeben.[11] Daraus ergeben sich weiterführende Fragen, wie beispielsweise, ob eine Datenauslagerung eine Verletzung des Berufsgeheimnisses für Anwältinnen und Anwälte darstellen kann.[12] Vor einer Auslagerung ist der Auftraggeber verpflichtet, sich zu vergewissern, dass der Dritte die Datensicherheit gewährleistet.[13] Für gewisse Branchen existieren zusätzlich spezialgesetzliche Regelungen, so unter anderem für Versicherungen und Banken.[14] Die Bestimmung in Art. 10a DSG gilt aufgrund der Gesetzessystematik sowohl bei einem Outsourcing durch Private wie auch durch Bundesbehörden.

Dritte sind grundsätzlich alle vom Auftraggeber verschiedene externe Personen. Nicht dazu zählen demzufolge die eigenen Arbeitnehmer des Auftraggebers.[15] Was simpel klingt, kann zum Beispiel in einem Konzern bereits zu Abgrenzungsfragen führen.[16]

B. Das Bekanntgabeprivileg

Sind die Voraussetzungen von Art. 10a DSG erfüllt, handelt es sich um eine gehörige Datenbearbeitung durch Dritte. Die Konsequenz ist das sogenannte Bekanntgabeprivileg. Der Auftragnehmer gilt nicht mehr als Dritter im Sinne des DSG, obwohl es sich bei ihm und dem Auftraggeber weiterhin um zwei unterschiedliche Rechtssubjekte handelt.[17] Es muss demzufolge sprachlich unterschieden werden zwischen einem Dritten, welcher die gesetzlichen Voraussetzungen für ein Outsourcing gemäss Art. 10a DSG nicht erfüllt, und einem Auftragnehmer, welcher die

(Zustelladresse auf der E-Justiz-Plattform als Voraussetzung für den Anwaltsregistereintrag).

6 Art. 12 Abs. 1 Bundesgesetz über den Datenschutz vom 19. Mai 1992 (DSG; SR 235.1). Siehe für einen generellen Überblick statt vieler Lukas Morscher/Leo Rusterholz, Outsourcing: Switzerland Overview, Thomson Reuters Practical Law vom 1. Mai 2021.

7 Art. 12 Abs. 3 DSG.

8 Art. 13 Abs. 1 DSG.

9 Neu soll dies auch explizit in Art. 9 Abs. 4 revDSG festgehalten werden.

10 Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

11 Zur Auswirkung des Berufsgeheimnisses auf den Datenschutz vgl. Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Schriften zum Datenrecht (digma), Bd. 9, Zürich 2016, 3 ff.; zum Strafrecht siehe Christian Schwarzenegger et al., Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte / Utilisation des services de cloud par les avocates et avocats, Center for Information Technology Society and Law (ITSL) 4/2019, 15 ff.

12 Vertiefend Schwarzenegger (Fn. 11), 15 ff.

13 Art. 10a Abs. 2 DSG.

14 Rundschreiben 2018/3 der FINMA betreffend Outsourcing – Auslagerungen Banken, Versicherungsunternehmen und ausgewählten Finanzinstituten nach FINIG vom 4. November 2020.

15 Diese Unterscheidung kann bspw. im Strafrecht relevant werden. Siehe dazu Urteil Bezirksgericht ZH GG 150233 (18. November 2015), E. II.2.5.5; Schwarzenegger (Fn. 11), 22 ff. Grundsätzlich zu den rechtlichen Neuerungen für Unternehmen Adrian Bieri/Julian Powell, Die Totalrevision des Bundesgesetzes über den Datenschutz, Jusletter vom 16. November 2020.

16 Sandro Germann, Übermittlung von Personendaten im Konzern, AJP 2021, 336 ff.; Clara-Ann Gordon, Crossborder-Outsourcing und Datenschutz, in: Europa Institut, Seminar Crossborder Outsourcing – Rechtsfragen und Lösungen vom 28. September 2016, 7.

17 HK DSG-Rosenthal, Art. 10a N 24 f.

Daten auftragsgemäss und rechtlich zulässig bearbeitet.[18] Die Qualifizierung als Auftragnehmer bedeutet unter anderem, dass für die Bekanntgabe besonders schützenswerter Personendaten oder Persönlichkeitsprofile an den Auftragnehmer kein Rechtfertigungsgrund im Sinne von Art. 12 Abs. 2 lit. c DSG notwendig ist und Datensammlungen privater Personen nicht ausschliesslich aufgrund regelmässiger Datenbekanntgabe an den Auftragnehmer angemeldet werden müssen.[19]

C. Aufklärung der betroffenen Personen über den Auftragnehmer

Nicht abschliessend geklärt ist, wie detailliert die Auftraggeber die betroffenen Personen über den Auftragnehmer informieren müssen. Konkret stellt sich die Frage, ob ein Auftragnehmer namentlich genannt werden muss (z.B. in den AGB) oder ob es genügt, wenn in genereller Weise ein Auftragsverhältnis bekannt gegeben wird. Zur Beantwortung dieser Frage muss wohl auf die rechtliche Einordnung der gesammelten Personendaten abgestellt werden. Wenn eine Privatperson besonders schützenswerte Personendaten sammelt, muss den betroffenen Personen der Inhaber der Datensammlung mitgeteilt werden.[20] Die besonders schützenswerten Personendaten werden in Art. 3 lit. c DSG abschliessend aufgelistet und umfassen Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten (Ziff. 1), die Gesundheit, die Intimsphäre und die Rassenzugehörigkeit (Ziff. 2), Massnahmen der sozialen Hilfe (Ziff. 3) und administrative oder strafrechtliche Verfolgungen und Sanktionen (Ziff. 4). Beim Outsourcing solcher Daten müsste der Auftragnehmer den betroffenen Personen namentlich bekannt gegeben werden. Bei der Sammlung von nicht besonders schützenswerten Personendaten gibt es keine solche gesetzliche Vorschrift, womit von der Zulässigkeit eines generellen Hinweises auf die Datenbearbeitung durch einen Dritten auszugehen ist.[21]

III. Verhältnis zwischen Auftraggeber und Auftragnehmer

Eine Auslagerung der Datenbearbeitung an einen Dritten stellt eine Auftragsdatenbearbeitung dar und muss vertraglich zwischen dem Auftraggeber und dem Auftragnehmer festgehalten werden. In der vertraglichen Ausgestaltung des Auftragsverhältnisses sind die Parteien grundsätzlich frei, gewisse Punkte sollten allerdings auf jeden Fall adressiert werden.[22]

A. Weisungsrecht

Der Auftragnehmer sollte verpflichtet werden, ausschliesslich im Namen und für die Zwecke des Auftraggebers gemäss dessen ausdrücklichen Weisungen die übertragenen Daten zu bearbeiten, um sicherzustellen, dass der Auftragnehmer die Daten nur in dem Rahmen bearbeitet, den auch der Auftraggeber einzuhalten hätte.[23] Die Pflicht zur Weisungsgebundenheit des Auftragnehmers gegenüber seinem Auftraggeber ist Ausfluss des Grundsatzes der Zweckgebundenheit. Dieser besagt, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.[24] Aus den Umständen ersichtlich sind solche Zwecke, die bei der Beschaffung der Daten zwar nicht erkennbar waren, jedoch vernünftigerweise mit dem Ursprungszweck vereinbar sind.[25] Wenn der Auftragnehmer die übertragenen Daten für eigene Zwecke nutzt, kommt es durch diese Zweitnutzung zu einer unrechtmässigen Zweckentfremdung.[26]

---

18 Art. 8 revDSG, welcher im Wesentlichen den geltenden Art. 10a DSG übernimmt, sieht hier einige terminologische Anpassungen vor, indem neu die Begriffe Verantwortlicher (statt Auftraggeber) und Auftragsbearbeiter (statt Auftragnehmer) eingeführt werden. Für weitere Änderungen im revDSG siehe generell die Botschaft über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, insb. 7031 ff.

19 Art. 11a Abs. 3 lit. b DSG; David Rosenthal, Das neue Datenschutzgesetz, Jusletter vom 16. November 2020, N 38.

20 Art. 14 Abs. 2 lit. a DSG.

21 Vorbehalten bleibt stets das kantonale Recht, welches detailliertere Regelungen beinhalten kann.

22 Siehe dazu beispielhaft EDÖB, Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland vom November 2013, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/unternehmen/anmeldung-einer-datensammlung/mustervertrag-fuer-das-outsourcing-von-datenbearbeitungen-ins-au.html, abgerufen am 21. Juli 2022.

23 Rosenthal (Fn. 17), N 52.

24 Art. 4 Abs. 3 DSG.

25 David Rosenthal, Die rechtlichen und gefühlten Grenzen der Sekundärnutzung von Personendaten, sic! 2021, 168 ff., 172.

26 Rosenthal (Fn. 17), N 35; Florent Thouvenin, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Rolf Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 61 ff., 75.

B. Garantie der Datensicherheit

Weiter sollte eine Pflicht des Auftragnehmers stipuliert werden, vor jeder Datenverarbeitung die angemessenen technischen und organisatorischen Massnahmen vorzunehmen,[27] um die Daten gegen unbefugtes Bearbeiten, versehentliche Beschädigungen und weitere nicht ausdrücklich genehmigte Verarbeitungen zu schützen. In Situationen, wo Daten im Besitz des Auftragnehmers in irgendeiner Weise unrechtmässig bearbeitet wurden, sei es durch den Auftragnehmer selbst oder (un-)befugte Dritte, sollte eine Pflicht zur sofortigen Benachrichtigung des Auftraggebers bestehen. Das Gleiche muss auch in Bezug auf zukünftig drohende Eingriffe in die Datensicherheit gelten, beispielsweise im Fall einer behördlichen Anordnung oder repetitiver Hackerangriffe.

C. Kontrollrecht

Damit der Auftraggeber sicherstellen kann, dass der Auftragnehmer die Datensicherheit gewährleistet, muss ihm das Recht eingeräumt werden, jederzeit in angemessener Weise und mit der vollen Kooperation des Auftragnehmers die Einhaltung der vertraglich festgehaltenen Regelungen selbst zu überprüfen oder durch einen externen Experten kontrollieren zu lassen.[28] Denn sich lediglich vertraglich die Einhaltung der datenschutzrechtlichen Bestimmungen und der technisch notwendigen Sicherheitsvorgaben zusichern zu lassen, genügt zur Kontrolle nicht. Teilweise (besonders im Fall von Cloud-Dienst-Anbietern, siehe dazu V.) hat der Auftragnehmer bereits selbst eine Audit-Firma, welche die Einhaltung der Sicherheitsmassnahmen vor Ort überprüft und zuhanden der Auftraggeber die Datensicherheit garantiert.[29] Fällt es dem Auftraggeber – beispielsweise aufgrund fehlenden Sachverstands – schwer, die Datensicherheit beim Auftragnehmer abzuschätzen, kann er auf eine Zertifizierung abstellen. In diesem Zusammenhang besonders bekannt ist die ISO/IEC 27001, welche als weltweit verbreitete Norm die Zertifizierung des Informationssicherheitsmanagementsystems sicherstellt und einen Mindeststandard an Datensicherheit gewährleistet.[30]

Wie die Datenschutzanforderungen spezifisch umgesetzt werden, sprich welche technischen und organisatorischen Massnahmen konkret ergriffen werden, hängt letztlich vom Auftraggeber, vom Auftragnehmer und von den bearbeiteten Daten ab.[31]

D. Informations- und Bewilligungspflichten

Idealerweise ist auch die Übertragung des Datenbearbeitungsauftrags an einen Subbeauftragten vertraglich geregelt, insbesondere die Erforderlichkeit der Zustimmung des Auftraggebers.[32] Grundsätzlich sollte der Auftragnehmer über sämtliche relevanten Veränderungen bei der Datenbearbeitung wie beispielsweise einen Standortwechsel selbstständig informieren und allenfalls eine Bewilligung des Auftraggebers abwarten müssen.

E. Zusicherung der rechtmässigen Datenerhebung

Der Auftraggeber sollte dem Auftragnehmer im Gegenzug zusichern, dass die übertragenen Daten von ihm rechtmässig erhoben wurden und das Outsourcing rechtlich zulässig ist. Denn eine solche Überprüfung kann vom Auftragnehmer in der Regel – wenn überhaupt – nur mit unverhältnismässig grossem Aufwand selbst vorgenommen werden und kann vernünftigerweise kaum verlangt werden.

IV. Rechte der betroffenen Personen

Jede Person hat das Recht, vom Inhaber einer Datensammlung Auskunft darüber zu verlangen, ob Daten über sie bearbeitet werden.[33] Im Falle eines Outsourcings kann sich die betroffene Person dafür an den Auftraggeber wenden. Diesen trifft die Pflicht, dem Auftragnehmer das Auskunftsbegehren zur Beantwortung weiterzuleiten, sofern er nicht selbst dazu in der Lage ist, eine zufriedenstellende Auskunft zu erteilen.[34] Der Auftragnehmer ist sodann auch selbst auskunftspflichtig, wenn er den Auftraggeber nicht bekannt gibt oder der Auftraggeber keinen (Wohn-)Sitz in der Schweiz hat.[35]

---

27 Art. 7 Abs. 1 DSG.

28 Claudia Keller, Datenschutz, schulthess manager dossier 2019, 15.

29 Keller (Fn. 28), 24.

30 Gerade erschienen ist die neuste Version ISO/IEC 27002:2022, einsehbar unter https://www.iso.org/standard/75652.html, abgerufen am 7. Juni 2022.

31 Keller (Fn. 28), 24.

32 Neu soll das Zustimmungserfordernis analog zu Art. 28 Abs. 2 DSGVO explizit in Art. 9 Abs. 3 revDSG festgehalten werden. Eine leicht abgeschwächte Regelung sieht die FINMA bereits heute vor: FINMA (Fn. 14), N 33. Nach dem revidierten DSG werden Auftragnehmer auf Antrag mit einer Busse von bis zu CHF 250'000 bestraft, wenn sie vorsätzlich die Datenbearbeitung einem Dritten übertragen, ohne die Erlaubnis des Auftraggebers eingeholt zu haben (Art. 61 lit. b rev-DSG).

33 Art. 8 Abs. 1 DSG.

34 Art. 1 Abs. 6 VDSG.

35 Art. 8 Abs. 4 DSG.

Neben der Auskunftspflicht ist der Auftraggeber auch dafür verantwortlich, dass die betroffene Person weitere Rechte, namentlich die Berichtigung, Sperrung oder Löschung ihrer Daten, vollumfänglich wahrnehmen kann.[36] Obwohl nicht ausdrücklich im Gesetz festgehalten, muss dem Auftraggeber konsequenterweise auch in einem solchen Fall die Pflicht auferlegt werden, den Auftragnehmer so rasch wie möglich entsprechend zu informieren und zu instruieren. Denn die Haftung gegenüber der betroffenen Person trägt (ohne anderweitige vertragliche Regelung) in erster Linie der Auftraggeber.[37]

V. Spezialfall Cloud-Dienste

In vielen Fällen werden heutzutage beim Outsourcing Cloud-Dienste genutzt. Diese Dienstleister bieten ihren Kunden einen Speicher, auf welchen Daten übertragen werden können. Diese Daten werden anschliessend verwaltet, gesichert und dem Kunden über ein Netzwerk wie beispielsweise das Internet zur Verfügung gestellt.[38] Die IT-Infrastruktur und infolgedessen auch die gespeicherten Daten sind demnach nicht auf lokalen Rechnern vor Ort verfügbar, sondern befinden sich «in der Cloud».[39] Grundsätzlich gelten für Cloud-Dienste dieselben Vorschriften wie für andere Auftragnehmer, allerdings sind für den Auftraggeber besondere datenschutzrechtliche Risiken mit der Nutzung eines Cloud-Dienstes verbunden.

Der Auftraggeber verliert weitgehend die Kontrolle über den Ort der Datenspeicherung (und wird über diesen teilweise nicht einmal in Kenntnis gesetzt) und – besonders bei einem im Ausland stationierten Cloud-Server – wird Mühe haben, eine vor Ort stattfindende Überprüfung der Datensicherheit gewährleistenden Infrastruktur vorzunehmen. Hinzu kommt, dass die Nutzung von Cloud-Diensten aufgrund der weltweit stationierten Server vermehrt mit einer Datenverarbeitung im Ausland einhergeht und die Datenverarbeitung allenfalls nicht den in der Schweiz geltenden Datenschutzstandards entspricht (siehe dazu auch VI.).[40] Ein zusätzliches Risiko stellen die häufig vorkommenden Unterauftragsverhältnisse der Cloud-Service-Anbieter dar, welche oftmals nicht transparent sind.[41] Ein weiteres in der Praxis bekanntes Problem ist die Rückforderung von Personendaten. Insbesondere im Konkursfall des Cloud-Anbieters können sich hier Schwierigkeiten ergeben, da allenfalls kein Anspruch auf die Herausgabe der Daten besteht.[42] Zusätzlich bleibt dem Auftraggeber regelmässig kein Verhandlungsspielraum für individuelle Anliegen, weshalb für ihn in der Regel kaum bis gar keine Einflussmöglichkeiten auf die Ausgestaltung der Cloud bestehen.[43]

Aufgrund der soeben aufgezeigten Risiken sollte der Ausgangspunkt jeder Nutzung eines Cloud-Dienstes eine umfassende Risikoanalyse sein. Für öffentliche Organe teilweise bereits heute explizit gesetzlich vorgeschrieben,[44] können auch Private davon profitieren, die Nutzung eines Cloud-Dienstes je nach Gefährdungspotenzial in Sicherheitsstufen einzuteilen und anhand dieser Kategorisierung die notwendigen Schutzziele zu definieren.[45] Geplant ist mit Art. 22 revDSG sodann eine zwingende Datenschutz-Folgenabschätzung auch für Private, sobald eine beabsichtigte Auslagerung der Datenbearbeitung ein hohes Risiko für die Grundrechte oder die Persönlichkeit der betroffenen Personen mit sich bringt.[46]

VI. Outsourcing ins Ausland

Lehre und Praxis stimmen darin überein, dass Outsourcing ins Ausland eine grenzüberschreitende Datenbe-

36 Art. 10a Abs. 1 lit. a DSG.

37 Keller (Fn. 28), 15; Privatim, Merkblatt Cloud-spezifische Risiken und Massnahmen vom 17. Dezember 2019, 1; David Vasella, Verantwortliche und Auftragsverarbeiter: Zu den Leitlinien des EDSA (Entwurf) zum «Controller» und «Processor», datenrecht.ch vom 14. September 2020, Ziff. 1.2.1.

38 Sonja Lelii et al., Cloud Storage (Cloud-Speicher) vom Dezember 2021, https://www.computerweekly.com/de/definition/Cloud-Storage, abgerufen am 21. Juli 2022.

39 Dominika Blonski, Cloud Computing – Datenschutzrechtliche Rahmenbedingungen am Beispiel des Kantons Zürich, Forum Europarecht, Bd./Nr. 42, Künstliche Intelligenz und Datenschutz, Zürich 2021, 65 ff., 65.

40 Blonski (Fn. 39), 74.

41 Keller (Fn. 28), 24.

42 Ausführlich dazu David Schwaninger/Michelle Merz, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke 2.0, Jusletter vom 21. Juni 2021.

43 Blonski (Fn. 39), 75.

44 Z.B. § 10 Abs. 1 Kantonales Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG ZH; LS 170.4).

45 Empfohlen wird die Kategorisierung in eine der folgenden drei Sicherheitsstufen: 1. Grundschutz mit kleinen Negativfolgen, 2. Mittlerer Schutz mit mittleren Negativfolgen, 3. Hoher Schutz mit grossen Negativfolgen. Insbesondere die Cloud-spezifischen Risikobereiche Geheimnisschutz, anwendbares Recht und Gerichtsstand sowie der Ort der Datenbearbeitung sollten ausführlich analysiert und entsprechend bewertet werden. Dazu ausführlich Blonski (Fn. 39), 74 ff.

46 EDÖB, Das neue Datenschutzgesetz aus Sicht des EDÖB vom 9. Februar 2021. Ebenfalls vorgesehen ist in Art. 66 lit. a revDSG eine Busse von bis zu CHF 250'000 für Privatpersonen, welche eine Auslagerung von Personaldaten ins Ausland nicht rechtskonform vornehmen.

kanntgabe darstellt.[47] Personendaten dürfen grundsätzlich nur ins Ausland bekannt gegeben werden, wenn durch die ausländische Gesetzgebung ein angemessener Schutz gewährleistet wird.[48] Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) führt eine öffentlich zugängliche Staatenliste, welche die Länder mit vermutungsweise angemessenem Datenschutzniveau aufzeigt.[49] Sämtliche EU-Mitgliedstaaten finden sich auf dieser Liste wieder.[50] Die USA hingegen, um nur ein wichtiges Land in Bezug auf Cloud-Server-Standorte zu nennen, sind aufgrund des US-amerikanischen CLOUD Act[51] nicht Teil dieser Liste. Ein Outsourcing in ein solches Land muss deshalb die in Art. 6 Abs. 2 DSG genannten Voraussetzungen erfüllen.[52] Der Auftraggeber muss sich auch bewusst sein, dass eine vertragliche Garantie des Cloud-Dienstes den Zugriff auf Personendaten durch ausländische Behörden nicht verhindern kann, wenn das ausländische Recht diese Möglichkeit vorsieht.[53] Der Auftraggeber hat in einem solchen Fall allenfalls einzig einen Haftungsanspruch gegenüber dem entsprechenden Cloud-Dienst – eine Datenschutzverletzung wird dadurch jedoch nicht verhindert.[54]

Wie politisch brisant dieses Thema werden kann, zeigt das neuste Outsourcing-Projekt des Bundes: Geplant wird eine Auslagerung von Personendaten von Schweizer Bürgern an Cloud-Dienste, welche in China und den USA ihren Sitz haben. Dies schlug im Juni 2021 hohe Wellen in den Medien und die Sorge um die Sicherheit dieser Daten führt aktuell zu politischen Diskussionen in der ganzen Schweiz.[55]

VII. Fazit

Zusammenfassend kann gesagt werden, dass der Datenschutz bei einem Outsourcing rechtlich genauso gewährleistet werden muss, wie wenn die Daten bei der Person verblieben wären, welche die Daten in erster Linie gesammelt hat. Allerdings ist eine weitere Partei involviert und bei einer unsorgfältigen Vertragsgestaltung kann dies durchaus zu einem tieferen Datenschutzniveau führen, insbesondere bei einer Verlagerung der Datenbearbeitung ins Ausland und/oder an einen Cloud-Dienst. Die Person, von der die Daten stammen, könnte natürlich eine Einwilligung betreffend Outsourcing verweigern – inwiefern dies aber in gewissen Situationen (z.B. als AGB-Klausel einer Bank) durchsetzbar ist, bleibt fraglich.

Outsourcing kann für betroffene Personen allerdings durchaus auch von Vorteil sein. Datenschutzverletzungen, insbesondere gezielte kriminelle Angriffe auf sensitive Daten, nahmen in den letzten Jahren markant zu.[56] Spezialisierte Auftragnehmer können solchen Attacken mit professioneller Infrastruktur entgegenhalten und haben im Fall einer Verletzung auch entsprechende Cybersecurity-Versicherungen abgeschlossen.[57]

---

47 Rosenthal (Fn. 17), N 28; BGE 144 I 126, 149, E. 8.3.6; EDÖB, Auslagerung einer Datenbearbeitung ins Ausland: «Outsourcing», das Zusammenspiel von Art. 10a DSG und Art. 6 Abs. 2 lit. a DSG (Stand: September 2010).

48 Art. 6 Abs. 1 DSG.

49 EDÖB, Stand des Datenschutzes weltweit (Stand: 15. November 2021), https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html, abgerufen am 21. Juli 2022. Art. 16 revDSG sieht neu vor, dass der Bundesrat diese Aufgabe übernimmt. Gleichzeitig soll mit der geplanten Revision auch eingeführt werden, dass bei einem Outsourcing ins Ausland die betreffenden Länder bekannt zu geben sind, genauso wie die zur Anwendung kommenden Datenschutzgarantien bzw. auf welche Ausnahme in Art. 17 revDSG sich die Datenauslagerung stützt. Das revDSG enthält somit strengere Vorgaben in diesem Punkt als die europäische DSGVO.

50 Anselm Filliger, Digitalisierung, Datenbearbeitung durch Dritte und gesetzlicher Auftrag, dargelegt anhand eines Beispielfalles im Bereich der Unfallversicherung, HAVE 2019, 94 ff., 96.

51 Clarifying Lawful Overseas Use of Data Act, in Kraft seit 23. März 2018; Bundesamt für Justiz, Bericht zum US CLOUD Act vom 17. September 2021.

52 EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG vom 8. September 2020.

53 Vertragliche Garantien können bspw. durch die Inkorporation der Standard Contractual Clauses (SCC) der EU oder sogenannter «Binding Corporate Rules» Vertragsbestandteil werden. David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, Jusletter vom 10. August 2020.

54 EDÖB (Fn. 49), 6.

55 Stefan Häberli, Begibt sich die Schweiz in eine gefährliche Abhängigkeit von ausländischen Cloud-Anbietern?, NZZ vom 25. Oktober 2021; Interpellation von Daniel Marti betreffend Auslagerung sensitiver Zuger Daten an ausländische Cloud-Anbieter vom 18. Januar 2022, Kanton Zug, Vorlage Nr. 3362.1, Lauf-Nr. 16847.

56 Keller (Fn. 28), 15; Nationales Zentrum für Cybersicherheit, Aktuelle Zahlen, https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html, abgerufen am 9. Juni 2022.

57 Keller (Fn. 28), 16.