Zwischen Schutz und Scheinanonymität

Pseudonymisierte Daten im Spannungsfeld von Technik, Recht und Cloud-Outsourcing

Sandra Husi-Stämpfli* Roman Gubser**

Der vorliegende Beitrag untersucht, wann pseudonymisierte Daten nach Schweizer Datenschutzrecht als Personendaten gelten. Ausgangspunkt ist die relative Bestimmbarkeit gemäss Art. 5 lit. a DSG: Ob eine Person identifizierbar ist, hängt von den verfügbaren Mitteln und der Perspektive des jeweiligen Akteurs ab. Am Beispiel des Cloud-Outsourcings wird gezeigt, dass dieselben Daten für den Verantwortlichen mit Schlüsselzugang weiterhin Personendaten, für den Cloud-Anbieter ohne Schlüssel jedoch faktisch anonym sein können. Der technologische Fortschritt – insbesondere generative KI, Machine Learning und Datenverknüpfung – senkt die Hürden der Re-Identifizierbarkeit stetig. Daraus folgt eine Pflicht zur fortlaufenden Re-Evaluation: Pseudonymisierung bleibt ein zentrales, aber kein hinreichendes Schutzinstrument. Datenschutz wird im digitalen Zeitalter zur Daueraufgabe, die juristische und technologische Entwicklungen kontinuierlich integrieren muss.

Le présent article examine les circonstances dans lesquelles le droit suisse de la protection des données considérera des données pseudonymisées comme des données personnelles. Tout se base sur la déterminabilité relative définie à l'art. 5 let. a LPD. Savoir si une personne est identifiable dépend toutefois des moyens à disposition et du point de vue de l'acteur concerné. En effet, il arrive que des mêmes données constituent à la fois des données personnelles, par exemple pour le responsable du traitement qui dispose d'une clé d'accès à des données stockées dans un cloud externalisé, et des données anonymes, pour le fournisseur cloud ne disposant pas de la clé d'accès. Les progrès technologiques – en particulier l'IA générative, l'apprentissage automatique et l'appariement de données – réduisent progressivement les obstacles à la réidentification. Il en résulte une obligation de réévaluation continue, à mesure que la pseudonymisation reste un instrument de protection essentiel, mais pas suffisant. À l'ère du numérique, la protection des données devient une mission à assurer de manière continue, qui doit intégrer en permanence les évolutions juridiques et technologiques.

Inhaltsübersicht

I. Einleitung

Mit Entscheid vom 4. September 2025[1] hat der Europäische Gerichtshof (EuGH) klargestellt, dass pseudonymisierte Personendaten nicht mehr als Personendaten zu behandeln seien, sofern *für den Empfänger der Daten keine Möglichkeit* bestehe, die erfolgte Pseudonymisierung aufzuheben. Auch das Handelsgericht Zürich kam in einem früheren Fall zum gleichen Schluss, wonach pseudonymisierte Daten für einen Betrachter ohne Zugang zur Referenzliste keine Personendaten darstellten und damit wie anonymisierte Personendaten oder Sachdaten zu behandeln seien.[2]

Für Unternehmen in der datengetriebenen Wirtschaft wie auch für öffentliche Organe sämtlicher föderalen Stufen ist die Abgrenzung zwischen Personen- und Sachdaten im schweizerischen Datenschutzgesetz (DSG) von grosser strategischer Bedeutung, denn die Unterschei-

* Sandra Husi-Stämpfli, Dr. iur., LL.M., Executive MPA Unibe, Leiterin Stab GS-EJPD, Leiterin Digital Compliance und Governance EJPD.
** Roman Gubser, lic. iur., Rechtsanwalt, Executive MBA HSG, Leiter Rechtsdienst Berner Kantonalbank AG. Die Autoren geben in diesem Beitrag ihre persönliche Einschätzung wieder.

1 EuGH, C-413/23 P (EDSB/SRB), 4.9.2025.
2 HGer ZH, HG190107-O, 4.5.2021, E. 3.2.3a; Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff. (zit. Botschaft DSG-Revision), 7019; Beat Rudin, Art. 5 N 14, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Stämpflis Handkommentar zum DSG, 2. A., Zürich 2023 (zit. SHK DSG-Verfasser).

dung entscheidet darüber, ob in der Datenbearbeitung die umfassenden Schutzmechanismen und Pflichten der einschlägigen[3] Datenschutzgesetze anwendbar und zu beachten sind.[4]

Eine fälschliche Qualifikation von Daten als «pseudonymisiert» oder «anonymisiert» kann in zweierlei Hinsicht weitreichende Auswirkungen mit sich bringen. Einerseits kann die Datenbearbeitung als non-compliant[5] beurteilt werden (und damit zu erheblichen Rechtsrisiken führen), andererseits kann eine konservative Beurteilung der Frage, ob die jeweiligen Informationen tatsächlich noch als «Personendaten» zu qualifizieren sind oder nicht, Innovation und insbesondere in der Privatwirtschaft Wettbewerbsvorteile hemmen.

In diesem Spannungsfeld stellt sich die entscheidende und längst nicht mehr nur juristisch zu beleuchtende Frage: Unter welchen Umständen sind pseudonymisierte Daten als Personendaten gemäss Art. 5 lit. a DSG zu qualifizieren und wann nicht? Mit anderen Worten: Wann ist eine Person noch «bestimmbar»?

Der in Art. 5 lit. a DSG sowie im europäischen Datenschutzrecht in Erwägungsgrund 26 DSGVO[6] verankerte Massstab der «Bestimmbarkeit» verweist auf die jeweils verfügbaren Mittel, den Stand der Technik und die künftige technologische Entwicklung.[7] Diese Offenheit gegenüber dem technischen Wandel hat zur Folge, dass der Aufwand zur Re-Identifizierung nicht statisch bestimmt werden kann, sondern fortlaufend zu re-evaluieren ist.

Zur empirischen und praxisnahen Konkretisierung dieser Fragestellung untersucht der vorliegende Beitrag den Anwendungsfall der Auslagerung pseudonymisierter Daten an Cloud-Dienstleister. Die Untersuchung gliedert sich in drei Hauptteile: Zunächst werden die rechtlichen Grundlagen der Datenqualifikation und das Konzept der relativen Bestimmbarkeit nach Schweizer Datenschutzrecht[8] systematisch dargelegt. Im Anschluss wird die praktische Anwendung auf das Cloud-Outsourcing-Szenario vorgenommen, einschliesslich der Rollenverteilung zwischen Verantwortlichem und Auftragsbearbeiter sowie der Implikationen für die Qualifikation pseudonymisierter Daten. Abschliessend werden die technologischen Entwicklungen im Bereich künstlicher Intelligenz und deren Einfluss auf die zukünftige Re-Identifizierbarkeit analysiert.

II. Rechtliche Grundlagen der Datenqualifikation

A. Der Begriff der Personendaten nach Schweizer Recht

Das Datenschutzgesetz definiert Personendaten als *alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.*[9] Der Begriff der Personendaten wird dabei von der Rechtsprechung bewusst sehr weit gefasst.[10] Er umfasst jede Art von Information, unabhängig davon, ob es sich um objektive Tatsachenfeststellungen oder subjektive Werturteile wie Meinungen und Beurteilungen handelt.[11] Auch die Form der Information ist unerheblich; sie kann als Text, Bild, Ton oder in jeder anderen analogen oder digitalen Form vorliegen.[12]

---

3 Für Unternehmen und Organe des Bundes: Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1), dort Art. 2 Abs. 1; für kantonale öffentliche Organe sind aufgrund der föderalen Kompetenzordnung die jeweiligen kantonalen Datenschutzgesetze relevant (dazu Sandra Husi-Stämpfli/Anne-Sophie Morand, Datenschutzrecht litera B, 2. A., Zürich 2024, N 65 ff.).

4 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt, Art. 5 N 6, in: David Vasella/Gabor P. Blechta (Hrsg.), Datenschutzgesetz, Basler Kommentar, 4. A., Basel 2024 (zit. BSK DSG-Verfasser).

5 Während Compliance in der Privatwirtschaft häufig auf die Einhaltung von Gesetzen und internen Richtlinien zur Vermeidung von Haftungsrisiken ausgerichtet ist, hat sie in der öffentlichen Verwaltung eine erweiterte, normative und vertrauensbezogene Dimension. Im Kontext der öffentlichen Verwaltung dient die Compliance mit anderen Worten nicht nur der Vermeidung von Rechtsverstössen, sondern auch der Sicherung von Rechtsstaatlichkeit und Gemeinwohlorientierung und trägt zur institutionellen Vertrauensbildung bei, indem sie regelkonformes, transparentes und ethisch verantwortungsvolles Verwaltungshandeln gewährleistet. Im Rahmen dieses Aufsatzes wird der Begriff der Compliance sowohl für die Privatwirtschaft wie auch für die öffentliche Verwaltung synonym verwendet.

6 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), ABl. L 119 vom 4. Mai 2016, 1 ff.

7 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 35.

8 Wo nicht anders vermerkt, wird in diesem Beitrag primär auf das Datenschutzgesetz des Bundes eingegangen. Die Überlegungen lassen sich aufgrund des Charakters des allgemeinen Datenschutzrechts als «Grundsatzgesetzgebung» (dazu Husi-Stämpfli/Morand [FN 3], N 68) jedoch ohne Weiteres auch auf kantonale Sachverhalte adaptieren.

9 Art. 5 lit. a DSG.

10 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 14.

11 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 15; BGE 136 II 508 E. 3.2; SHK DSG-Rudin (FN 2), Art. 5 N 5.

12 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 15; BGE 136 II 508 E. 3.2.

B. Das Kriterium der «Bestimmbarkeit»: Die relative Methode

Die bewusst weit gefasste Kontur des Begriffs der Personendaten findet ihren Niederschlag auch im Umstand, dass nicht nur Angaben, die zu einer direkten, unmittelbaren Identifikation einer Person führen, als Personendaten zu qualifizieren sind, sondern auch Angaben, die die fragliche Person *bestimmbar* machen. Eine Person gilt als bestimmbar, wenn ihre Identität nicht direkt aus der Information selbst, sondern erst durch die Verknüpfung mit weiteren, zusätzlichen Informationen hergestellt werden kann.[13] Ob diese Identifikation mittels weiterer Angaben zur Person, eines Schlüssels, eines Aktenzeichens oder einer Kundennummer erfolgt, ist grundsätzlich nicht von Relevanz.[14]

Nach etablierter Rechtsprechung[15] und Lehre[16] genügt für die Bestimmbarkeit jedoch nicht, dass eine Identifizierung *theoretisch* möglich ist. Vielmehr ist einerseits zu beurteilen, ob die konkrete Person, die Zugang zu den Informationen hat, in der Lage ist, herauszufinden, auf welche natürliche Person sich die Angaben beziehen (sog. objektive Bestimmbarkeit), und ob sie andererseits auch willens ist, den entsprechenden Aufwand auf sich zu nehmen (sog. subjektive Bestimmbarkeit).[17] Die Bestimmbarkeit ist somit relativ: Massgebend ist die Sicht jener Personen, denen die fraglichen Angaben aktuell zugänglich sind, planmässig zugänglich gemacht werden sollen oder die mit einer praktisch relevanten Wahrscheinlichkeit auf die Angaben zugreifen werden.[18] Ist ihr Aufwand derart gross, dass nach allgemeiner Lebenserfahrung nicht damit gerechnet werden muss, dass dieser in Kauf genommen wird, liegt keine Bestimmbarkeit vor.[19]

Die Frage, ob Daten als Personendaten zu qualifizieren sind, kann daher für unterschiedliche Parteien zu unterschiedlichen Antworten führen. Massgeblich sind die konkreten Umstände des Einzelfalles.[20]

C. Abgrenzung: Anonymisierung vs. Pseudonymisierung

Für die Beurteilung, ob Informationen eine konkrete Person bestimmbar machen, ist in der Praxis die Unterscheidung von Anonymisierung und Pseudonymisierung relevant.

Unter dem Begriff der *Anonymisierung* versteht man das irreversible Entfernen des Personenbezugs, sodass eine Re-Identifizierung der betroffenen Person nicht mehr oder nur mit einem unverhältnismässigen (dazu später II.C.) Aufwand möglich ist.[21] Es existiert kein «Schlüssel» zur einfachen Wiederherstellung des Personenbezugs. Anonymisierte Daten sind keine Personendaten mehr[22] und fallen damit nicht (mehr) in den Anwendungsbereich des DSG.

Demgegenüber definiert der Begriff der *Pseudonymisierung* das reversible Ersetzen von direkten Identifikatoren (wie Name oder Adresse) durch ein Pseudonym (z.B. einen Code oder eine Nummer).[23] Die Information zur Wiederherstellung des Personenbezugs (der «Schlüssel» oder die «Referenzliste») wird getrennt von den pseudonymisierten Daten aufbewahrt. Pseudonymisierte Daten bleiben für denjenigen, der über den Schlüssel zur Re-Identifizierung verfügt, Personendaten.[24] Für andere Parteien ohne Schlüsselzugang stellen die pseudonymisierten Daten quasi-anonymisierte Daten dar[25]: Sie haben keine Möglichkeit, die fragliche Person zu bestimmen.

III. Relativität der Pseudonymisierung

Die relative Natur der Bestimmbarkeit nach Art. 5 lit. a DSG führt auch bei pseudonymisierten Daten zu differenzierten Ergebnissen, je nachdem, welche Partei die Daten bearbeitet, ob sie Zugriff auf den Schlüssel hat oder ob sie die Mittel und den Willen hat, eine Re-Identifikation durchzuführen. Das Bundesgericht hat diese Relativität der Pseudonymisierung in mehreren Leitentscheiden bestätigt. Im Urteil *Logistep*[26] und im Entscheid *Zürcher*

---

13 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 27; Botschaft DSG-Revision (FN 2), 7019; BGE 138 II 346 E. 6.1; 136 II 508 E. 3.2; SHK DSG-Rudin (FN 2), Art. 5 N 10. Früher wurde in diesem Kontext auch von sog. «indirekten Personendaten» gesprochen.

14 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 27.

15 Unter vielen: BGE 138 II 346 E. 6.1; 136 II 508 E. 3.2.

16 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 28; SHK DSG-Rudin (FN 2), Art. 5 N 10.

17 Husi-Stämpfli/Morand (FN 3), N 104.

18 BGE 136 II 508 E. 3.4; BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 33.

19 Botschaft DSG-Revision (FN 2), 7019.

20 BGE 136 II 508 E. 3.5.

21 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 35.

22 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 35.

23 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 36; SHK DSG-Rudin (FN 2), Art. 5 N 14; vgl. auch die Legaldefinition der «Pseudonymisierung» in Art. 4 Nr. 5 DSGVO.

24 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 36; HGer ZH, HG190107-O, 4.5.2021, E. 3.2.3a; Luca Dal Molin, § 1 N 86, in: Luca Dal Molin/Kirsten Wesiak-Schmidt (Hrsg.), Datenschutz im Unternehmen, Zürich/St. Gallen 2023; noch zum alten DSG David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, 2. A., Zürich 2021, Art. 3 N 36.

25 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 36.

26 BGE 136 II 508 E. 3.2 ff.

Steuerdatenbank[27] hielt es fest, dass es auf den «nach der allgemeinen Lebenserfahrung zu erwartenden Aufwand» ankomme und dass eine rein hypothetische Re-Identifizierungsmöglichkeit nicht genüge, um einen Personenbezug zu begründen. Massgebend sei vielmehr auch im Kontext der Pseudonymisierung, ob die Re-Identifikation für die konkret zugriffsberechtigte Personengruppe innerhalb realistischer Grenzen liege.[28]

A. Relativität der Pseudonymisierung im technologischen Wandel

Die Grenzen der Re-Identifikationsmöglichkeiten verringern sich mit dem technologischen Fortschritt jedoch zunehmend und immer schneller: Moderne Datenanalyseplattformen, Machine-Learning-Modelle und generative künstliche Intelligenz können Muster in grossen Datensätzen erkennen, die für Menschen unsichtbar sind.

Die Relativität der Pseudonymisierung angesichts des technologischen Wandels wurde schon vor zwanzig Jahren eindrücklich illustriert: Im Jahr 2006 konnte nachgewiesen werden, dass die Kombination weniger und scheinbar harmloser Merkmale wie Geschlecht, Geburtsdatum und Postleitzahl ausreicht, um 63 % der US-Bevölkerung eindeutig zu identifizieren;[29] werden 15 demografische Attribute genutzt, lassen sich 99,98 % der Amerikanerinnen und Amerikaner re-identifizieren.[30] Forscherinnen und Forscher konnten im gleichen Jahr zudem gestützt auf die «AOL-Suchdaten»[31] aufzeigen, wie leicht pseudonymisierte Daten durch den Abgleich mit öffentlich zugänglichen Informationen einzelnen Nutzerinnen und Nutzern zugeordnet werden können[32] – der Beweis wurde kurz darauf anhand des «Netflix-Filmratings»[33] im Jahr 2007 wiederholt. Neueren Datums – aber immer noch vor dem grossen Boom der KI-Möglichkeiten der letzten fünf Jahre[34] – und etwas pikanter ist schliesslich der Re-Identifizierungsfall des Dating-Dienstes Grindr aus dem Jahr 2018: Hier wurden öffentlich verfügbare App-Nutzungsdaten mit Standortdaten verknüpft, um Personen und ihre Besuche an sensiblen Orten zu identifizieren.[35]

Es ist entsprechend nicht verwunderlich, dass Experten davon ausgehen, dass die Aufrechterhaltung der Datenanonymität in einer Welt aus Datenhändlern, generativer KI und maschinellem Lernen immer schwieriger wird:[36] Fortgeschrittene Algorithmen finden selbst in stark aggregierten oder verwaschenen Datensätzen subtile Korrelationen und können so die Identität einzelner Personen offenbaren.[37] Die Datenschutzexperten von GDPR Local weisen darauf hin, dass die hohe Messlatte des Erwägungsgrunds 26 der DSGVO[38] eine laufende Bewertung der verfügbaren Technologie, der Hilfsdatensätze und der künftigen Entwicklungen verlangt.[39] Sie warnen, dass die zunehmende Verfügbarkeit von Zusatzdatensätzen und fortschrittlichen Analytikverfahren dazu führt, dass eine echte Anonymisierung bei datenreichen Datensätzen in der Praxis möglicherweise gar nicht erreichbar ist.[40] Zusammen mit der wachsenden Menge an öffentlich zugänglichen Informationen – von sozialen Medien über öffentliche Verzeichnisse bis hin zu Datenhändlern und akademischen Publikationen – wird es immer leichter, pseudonymisierte Datensätze zu verknüpfen.

Auch Regulierungsbehörden warnen mittlerweile vor neuen Bedrohungen durch KI-gesteuerte Angriffe

---

27 BGE 138 II 346 E. 6.1 ff.

28 BGE 138 II 346 E. 6.1; 136 II 508 E. 3.2.

29 Philippe Golle, Revisiting the Uniqueness of Simple Demographics in the US Population, 5 ACM WORKSHOP ON PRIVACY IN THE ELEC. SOC'Y 77, 78 (2006) (using 2000 census data).

30 Boris Lubarsky, Re-Identification of «Anonymized» Data, 1 GEO. L. TECH. REV. 202 (2017), Internet: https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/ (Abruf 27.10.2025), sowie die weitere Berichterstattung von Isla Sibanda, Reidentifying the Anonymized: Ethical Hacking Challenges in AI Data Training, Internet: https://www.isaca.org/resources/news-and-trends/industry-news/2024/reidentifying-the-anonymized-ethical-hacking-challenges-in-ai-data-training (Abruf 27.10.2025).

31 Alexander von Streit, Suchanfragen verraten Surfer, Focus vom 9.8.2006, Internet: https://www.focus.de/digital/internet/suchanfragen-verraten-surfer-aol-datenpanne_id_1747432.html (Abruf 27.10.2025).

32 Narayana Pappu, How Easy Is It To Re-Identify Data and What Are The Implications?, Internet: https://www.zendata.dev/post/how-easy-is-it-to-re-identify-data-and-what-are-the-implications (Abruf 27.10.2025).

33 Konrad Lischka, Informatiker knacken anonymisierte Datenbank per Web-Suche, Spiegel vom 13.12.2007, Internet: https://www.spiegel.de/netzwelt/web/datenschutz-debakel-informatiker-knacken-anonymisierte-datenbank-per-web-suche-a-523216.html (Abruf 27.10.2025).

34 Aktuelles AI, Die letzten 5 Jahre rasanter KI Entwicklung, Internet: https://aktuelles.ai/ki-grundlagen/ein-rueckblick-auf-die-letzten-5-jahre-ki-entwicklung/ (Abruf 27.10.2025).

35 Pappu (FN 32).

36 Pappu (FN 32).

37 Pappu (FN 32).

38 «Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.»

39 Ana Mishova, Data Pseudonymisation vs Anonymisation: Key Differences, 28.7.2025, Internet: https://gdprlocal.com/data-pseudonymisation-vs-anonymisation (Abruf 27.10.2025).

40 Mishova (FN 39).

auf Modelle. Die britische Datenschutzaufsichtsbehörde (ICO) erklärt, dass bei «Model-Inversion-Angriffen»[41] Angreifer anhand der Eingaben und Ausgaben eines maschinellen Lernmodells zusätzliche personenbezogene Informationen über die im Trainingsdatensatz enthaltenen Personen ableiten können.[42] Ein bekanntes Beispiel betraf ein medizinisches Modell zur Dosierung eines Medikaments zur Hemmung der Blutgerinnung. Angreifer waren in der Lage, genetische Biomarker zu rekonstruieren, obwohl ihnen nur demografische Daten vorlagen.[43] Bei Gesichtserkennungssystemen konnte ein ähnlicher Angriff mittels Zufallsbildern und Auswertung der Ausgabewahrscheinlichkeiten Gesichter rekonstruieren, die menschliche Betrachter zu 95 % den Trainingsteilnehmern zuordnen konnten.[44]

Derartige Angriffe sind längst nicht mehr Utopie, sondern werden zunehmend praktikabel. Veale/Binns/Edwards zeigen beispielsweise, dass sowohl White- als auch Black-Box-Angriffe[45] Modelle rückwärts entwickeln und so einzelne Personen aus ursprünglich anonymisierten Befragungsdaten oder Gesichtserkennungssystemen mit hoher Treffsicherheit identifizieren können.[46] Sie weisen darauf hin, dass bestimmte Modelltypen (z.B. Support-Vector-Maschinen[47] oder k-Nearest-Neighbour[48]) Teile der Trainingsdaten von vornherein enthalten.[49] Die Autoren ziehen eine Parallele zur Pseudonymisierung, denn wenn ein Verantwortlicher sowohl das Modell als auch zusätzliche Informationen besitzt und eine Re-Identifizierung technisch möglich ist, müsse das Modell selbst als personenbezogenes Datum qualifiziert werden.[50]

Diese Entwicklungen deuten darauf hin, dass der «vertretbare Aufwand» zur Re-Identifizierung in Zukunft deutlich sinken und sich die Relativität der Bestimmbarkeit noch weiter akzentuieren wird. Was bislang nur spezialisierten Angreifern mit erheblichem Ressourceneinsatz möglich war, könnte mit zunehmendem technischem Fortschritt und dem Einsatz leicht verfügbarer KI-Werkzeuge bald für weitaus breitere Akteursgruppen realisierbar sein.

B. Perspektive des Dateninhabers mit Schlüsselzugang

Für die Partei, die sowohl über die pseudonymisierten Daten als auch über die Referenzliste (den Schlüssel) zur Re-Identifizierung verfügt, bleiben die Daten uneingeschränkt Personendaten. Der Personenbezug ist für diese Partei nicht aufgehoben, sondern lediglich temporär verschleiert. Sie kann durch eine einfache Zusammenführung der beiden Datensätze die Identität der betroffenen Personen wiederherstellen. Die Pseudonymisierung dient hier primär als interne Sicherheitsmassnahme, ändert aber nichts an der datenschutzrechtlichen Qualifikation der Daten und den damit zusammenhängenden Pflichten bei der Datenbearbeitung. Der Datenbearbeiter bleibt Verantwortlicher im Sinne von Art. 5 lit. j DSG und unterliegt sämtlichen gesetzlichen Pflichten, namentlich den Grundsätzen der Rechtmässigkeit, Transparenz, Zweckbindung, Verhältnismässigkeit und Datensicherheit.[51] Zudem werden ihm auch allfällige Bearbeitungsvorgänge des Dritten als Verantwortlichen zugerechnet, auch wenn die

---

41 Bei einer «Model Inversion Attack» handelt es sich um ein Verfahren, mit dem Angreifer aus einem bereits trainierten maschinellen Lernmodell Rückschlüsse auf die in den Trainingsdaten enthaltenen personenbezogenen Informationen ziehen können. Dabei wird das Modell so lange abgefragt oder analysiert, bis sich bestimmte Eingabemuster rekonstruieren lassen, die Rückschlüsse auf einzelne Trainingsdatensätze – etwa Gesichter, medizinische Merkmale oder Textinhalte – ermöglichen. Der Angriff kehrt damit den Lernprozess teilweise um («Inversion»), indem aus den Parametern des Modells Informationen über die ursprünglichen Trainingsdaten extrahiert werden. Siehe dazu bspw. Lior Romano, Model Inversion Attacks: A Growing Threat to AI Security, 14.3.2025, Internet: https://www.tillion.ai/blog/model-inversion-attacks-a-growing-threat-to-ai-security (Abruf 27.10.2025).

42 Information Commissioner UK, How should we assess security and data minimisation in AI?, Internet: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai (Abruf 27.10.2025).

43 Information Commissioner UK (FN 42).

44 Information Commissioner UK (FN 42).

45 White-Box-Angriffe setzen voraus, dass der Angreifer vollständige Kenntnisse über das angegriffene System besitzt (z.B. Quellcode, Modellarchitektur, Parameter), während Black-Box-Angriffe ohne solches Wissen erfolgen und nur auf Eingaben und Ausgaben basieren. Erstere prüfen die Sicherheit bei voller Transparenz, Letztere spiegeln realistische Angriffsszenarien wider.

46 Michael Veale/Reuben Binns/Lilian Edwards, Algorithms that remember: model inversion attacks and data protection law. Philosophical transactions, Mathematical, physical, and engineering sciences, Series A, 376(2133), 20180083, Internet: https://doi.org/10.1098/rsta.2018.0083 (Abruf 27.10.2025).

47 Eine Support Vector Machine (SVM) ist ein überwacht lernender Algorithmus, der Datenpunkte mittels einer optimalen Trennlinie (Hyperplane) klassifiziert und dadurch Muster oder Kategorien in Datensätzen erkennt, siehe dazu bspw. Internet: https://www.geeksforgeeks.org/machine-learning/support-vector-machine-algorithm (Abruf 27.10.2025).

48 Der k-Nearest-Neighbour-Algorithmus (k-NN) ordnet neue Datenpunkte anhand der Klassenzugehörigkeit ihrer *k* nächstgelegenen Nachbarn im Merkmalsraum zu und beruht damit auf einem Ähnlichkeitsprinzip, siehe dazu Internet: https://www.geeksforgeeks.org/machine-learning/k-nearest-neighbours/ (Abruf 27.10.2025).

49 Veale/Binns/Edwards (FN 46).

50 Veale/Binns/Edwards (FN 46).

51 Art. 6 ff. DSG.

Daten aus der Perspektive des Dritten keine Personendaten sind.[52]

C. Perspektive eines Dritten ohne Schlüsselzugang

Wird ein Datensatz ausschliesslich in pseudonymisierter Form und ohne den zugehörigen Schlüssel an einen Dritten weitergegeben, so ist a priori[53] davon auszugehen, dass dieser die Daten keiner bestimmten oder bestimmbaren Person zuordnen kann. Die Pseudonymisierung wirkt damit «[…] wie eine Anonymisierung […]»,[54] es liegen aus Perspektive des Dritten keine Personendaten (mehr) vor. Dieses Konzept wird als «faktische Anonymisierung» bezeichnet.[55] Die Daten sind für den Empfänger zwar singularisiert (d.h., Datensätze können einem bestimmten Pseudonym zugeordnet werden), aber grundsätzlich[56] nicht identifizierbar.[57]

D. Führt die Relativität der Pseudonymisierung zu einem rechtlichen gordischen Knoten?

Angesichts der illustrierten Relativität der Pseudonymisierung stellt sich die Frage, ob damit nicht ein rechtlicher gordischer Knoten geschaffen wird. Wie können ein und dieselben Daten aus Perspektive des Verantwortlichen schützenswert im Sinne des DSG sein, gleichzeitig aber aus Perspektive des Empfängers gar nicht mehr unter das DSG fallen – wie soll dieses Problem in einem Rechtsverhältnis geklärt werden?

Die Lösung liegt in der rechtlichen Beurteilung des *Vorgangs der Bekanntgabe* von Daten, wie das Bundesgericht im bereits erwähnten Logistep-Entscheid verdeutlicht hat.[58] Art. 5 lit. e DSG definiert die Bekanntgabe als «das Übermitteln oder Zugänglichmachen von Personendaten» – und Personendaten sind, wie bereits dargelegt, «alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen».[59] Das DSG gelangt damit zur Anwendung, sobald zwischen zwei Parteien Informationen ausgetauscht werden, die potentiell zur Identifikation einer natürlichen Person herangezogen werden können, unabhängig davon, ob die Daten für eine Partei de facto anonymisiert sind oder nicht. Mit anderen Worten ist für die Anwendbarkeit des DSG nicht der faktische Zustand der Daten beim Verantwortlichen oder Empfänger relevant, sondern die rechtliche Qualifikation des Übermittlungsvorgangs. In der Konsequenz bedeutet dies, dass die Pflichten qua DSG, insbesondere die Verantwortlichkeit nach Art. 5 lit. j bzw. die Vorgaben nach Art. 9 DSG, auch dann bestehen bleiben, wenn pseudonymisierte Personendaten übermittelt werden. Wie sich das in der Praxis auswirkt, wird sogleich anhand des Anwendungsfalls der Auslagerung von pseudonymisierten Daten an einen Cloud-Anbieter illustriert.

IV. Anwendungsfall: Auslagerung pseudonymisierter Daten an einen Cloud-Anbieter

Cloud-Outsourcing ist für Unternehmen, aber auch für die öffentliche Verwaltung von strategischer Wichtigkeit, um Skaleneffekte zu nutzen und sich auf Kernkompetenzen zu konzentrieren. Die Auslagerung der Datenbearbeitung wirft jedoch zentrale datenschutzrechtliche Fragen auf, in deren Zentrum die korrekte Einordnung der beteiligten Akteure und der betroffenen Daten steht.

A. Rollenverteilung: Verantwortlicher und Auftragsbearbeiter

Im typischen Cloud-Szenario lassen sich die datenschutzrechtlichen Rollen klar zuordnen. Das auslagernde Unternehmen bzw. Organ ist als «Verantwortlicher» (Controller) gemäss Art. 5 lit. j DSG zu qualifizieren. Es entscheidet allein über den Zweck (z.B. Datenanalyse, Speicherung) und die wesentlichen Mittel der Datenbearbeitung. Der Cloud-Anbieter agiert als «Auftragsbearbeiter» (Processor) gemäss Art. 5 lit. k DSG. Er fungiert als «verlängerter Arm» des Verantwortlichen und bearbeitet die Daten ausschliesslich auf dessen Weisung und für dessen – aber nicht für eigene – Zwecke.[60]

Die Bekanntgabe von Daten an einen Auftragsbearbeiter ist datenschutzrechtlich privilegiert.[61] Sie wird als Teil der Datenbearbeitung des Verantwortlichen gesehen und

---

52 David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 17.6.2019, 40.
53 Zur Möglichkeit der Re-Identifikation oben III.
54 HGer ZH, HG190107-O, 4.5.2021, E. 3.2.3a; BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 36.
55 Botschaft DSG-Revision (FN 2), 7076.
56 Zur Möglichkeit der Re-Identifikation oben III.
57 BSK DSG-Blechta/Dal Molin/Wesiak-Schmidt (FN 4), Art. 5 N 33.
58 BGE 136 II 508 E. 3.4 und E. 3.5.
59 Art. 5 lit. a DSG.
60 SHK DSG-Baeriswyl (FN 2), Art. 9 N 15 ff.; BSK DSG-Bühler/Rampini (FN 4), Art. 9 N 8 ff.; Husi-Stämpfli/Morand (FN 3), N 147 ff. sowie N 407 ff.
61 BSK DSG-Bühler/Rampini (FN 4), Art. 9 N 15; Husi-Stämpfli/Morand (FN 3), N 409.

bedarf keiner gesonderten Rechtfertigung. Voraussetzung ist jedoch der Abschluss eines Auftragsdatenbearbeitungsvertrags (ADV) nach Art. 9 DSG, der die weisungsgebundene Bearbeitung, die Datensicherheit und weitere Pflichten regelt (siehe dazu sogleich IV.C.).

B. Datenqualifikation im Cloud-Szenario

Ob im Cloud-Szenario «scharfe», d.h. direkt lesbare, pseudonymisierte oder verschlüsselte Personendaten ausgelagert werden sollen, ist vom verantwortlichen Unternehmen bzw. öffentlichen Organ vor Abschluss des Vertrages mit dem Cloud-Dienstleister zu evaluieren (siehe dazu unten IV.C.1.). Ausschlaggebend wird die Wahl des jeweiligen Cloud-Service-Models sein:

Bei *Infrastructure as a Service (IaaS),* wo der Anbieter lediglich Rechen- oder Speicherkapazität bereitstellt, dürften in der Regel entweder verschlüsselte oder pseudonymisierte Personendaten übermittelt werden. Im Cloud-Kontext ist der Unterschied zwischen Verschlüsselung und Pseudonymisierung nicht nur terminologisch, sondern grundlegend technischer und rechtlicher Natur. Beide Verfahren dienen zwar dem Schutz personenbezogener Daten, verfolgen jedoch unterschiedliche Zielrichtungen und haben unterschiedliche Auswirkungen auf die Verarbeitung und Kontrolle der Daten.

– Die *Verschlüsselung* schützt in erster Linie die Vertraulichkeit der Informationen. Sie sorgt dafür, dass Daten ohne den passenden Schlüssel nicht lesbar sind und somit auch ein Cloud-Provider, der lediglich die Infrastruktur bereitstellt, keinen Zugriff auf die Inhalte hat. Technisch bedeutet dies, dass die Daten in der Cloud zwar gespeichert, aber nicht verarbeitet oder analysiert werden können, solange sie verschlüsselt bleiben. Entscheidend ist das Schlüsselmanagement – hier zeigt sich eine Parallele zur Pseudonymisierung: Nur wenn der Schlüssel beim Dateninhaber verbleibt (etwa bei Ende-zu-Ende-Verschlüsselung), ist gewährleistet, dass Dritte – einschliesslich des Cloud-Anbieters – keinen Zugriff haben.[62] In diesem Fall verliert der Cloud-Provider faktisch jede Möglichkeit der Re-Identifikation, sodass die Daten für ihn nicht mehr als personenbezogen (bzw. faktisch anonymisiert) gelten – in der Konsequenz bedeutet dies, dass das DSG nicht zur Anwendung gelangt.
– Die *Pseudonymisierung* verfolgt im Cloud-Kontext hingegen das Ziel, den Personenbezug zu reduzieren, ohne die Nutzbarkeit der Daten aufzugeben. Der Vorteil liegt darin, dass pseudonymisierte Daten weiterhin analysiert, kombiniert und verarbeitet werden können – beispielsweise für statistische oder KI-basierte Zwecke –, ohne dass unmittelbar Rückschlüsse auf Einzelpersonen gezogen werden. Aus rechtlicher Sicht bleibt der Personenbezug jedoch wie bereits ausgeführt bestehen, da eine Rückführung grundsätzlich möglich bleibt. Folglich unterliegt der gesamte Vorgang der Auslagerung (die «Bekanntgabe») an den Cloud-Anbieter den Bestimmungen des DSG.

Wird vom Cloud-Dienstleister jedoch *Software as a Service (SaaS)* angeboten, verarbeitet die Applikation des Anbieters die Daten direkt – womit aus Sicht des Verantwortlichen der Transfer von entweder direkt lesbaren oder pseudonymisierten Personendaten in Frage kommt.[63] Der Anbieter hat damit potenziell Zugriff auf Daten, die die Bestimmung einzelner Personen zulassen – entweder direkt oder aber mit einem vertretbaren Re-Identifizierungs-Aufwand.[64] In diesen Fällen ist die Anwendbarkeit des DSG ebenfalls zu bejahen, da grundsätzlich von einer Identifizierbarkeit auszugehen ist.[65]

C. Rechtliche Implikationen

Aus dieser differenzierten Betrachtung ergeben sich konkrete rechtliche Konsequenzen, wobei nachfolgend der Fokus[66] auf die Risikovorprüfung und Datenschutz-Folgenabschätzung (DSFA) im Sinne von Art. 22 DSG, die Klärung der Rahmenbedingungen für eine Übermittlung der Daten an einen im Ausland domizilierten Cloud-Anbieter (Art. 16 DSG) sowie den Abschluss eines ADV gelegt werden soll.

1. Risikovorprüfung und DSFA im Cloud-Outsourcing-Kontext

Nach Art. 22 DSG ist eine DSFA vorzunehmen, wenn eine geplante Bearbeitung voraussichtlich ein hohes Ri-

[62] Christian Schwarzenegger, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Anwaltsrevue 2019, 25 ff., 26.

[63] Schwarzenegger (FN 62), 26.

[64] Dazu oben III.A.

[65] David Roth, Cloud-basierte Dienstleistungen im Licht der DSGVO, AJP 2020, 68 ff., 75 m.w.H.

[66] Die Anwendbarkeit des DSG bringt auch weitere Governance-Pflichten mit sich wie bspw. die Informationspflicht nach Art. 19 DSG, Protokollierungspflichten oder aber auch die Pflicht zur Führung eines Bearbeitungsverzeichnisses, dazu Husi-Stämpfli/Morand (FN 3), N 418 ff.

siko für die Persönlichkeit oder Grundrechte der betroffenen Personen begründet.[67]

Je nach gewähltem Cloud-Modell und den bearbeiteten Daten wird die Frage, ob von einem potenziell hohen Risiko für die betroffenen Personen auszugehen ist, unterschiedlich zu beantworten sein.

Bei *SaaS-Lösungen* kontrolliert der Anbieter Applikation, Updates und Speicherung, während der Verantwortliche kaum Einfluss auf technische Massnahmen hat. Das Risiko eines Kontrollverlusts ist entsprechend hoch; eine Risikovorprüfung ist regelmässig erforderlich.

Platform-as-a-Service-Lösungen (PaaS) erlauben dagegen grössere Kontrolle über Sicherheitsarchitektur und Verschlüsselung. Das Risiko kann hier reduziert werden, etwa durch eigene Schlüsselverwaltung oder Zugriffskontrollen. Gleichwohl ist nach Auffassung der Autorin bzw. des Autors auch bei PaaS eine Risikovorprüfung angezeigt, wenn besonders schützenswerte oder grenzüberschreitend bearbeitete Daten (dazu sogleich IV.C.2.) betroffen sind.

Identifizierende Daten begründen stets ein hohes Risiko, da Cloud-Anbieter potenziell Zugriff auf personenbezogene Informationen haben.

Pseudonymisierte Daten mindern das Risiko nur graduell. Eine Re-Identifikation ist angesichts technischer Fortschritte und Datenverknüpfung häufig möglich. Entscheidend ist, ob der Anbieter über Zusatzinformationen verfügt. In SaaS-Umgebungen ist die Pseudonymisierung meist wenig wirksam, während PaaS-Architekturen eine stärkere Trennung zwischen Daten- und Anwendungsebene erlauben.[68]

Verschlüsselte Daten können das Risiko erheblich senken, sofern die Schlüssel clientseitig beim Verantwortlichen verbleiben. Bei serverseitiger Verschlüsselung, bei der der Anbieter Zugriff auf die Schlüssel hat, muss von einem unzureichenden Schutz bzw. davon ausgegangen werden, dass die Daten für den Anbieter lesbar und damit als Personendaten zu qualifizieren sind.[69] SaaS-Lösungen bieten typischerweise nur diese Form; bei PaaS kann eine eigenständige Schlüsselverwaltung implementiert werden.

Kommt die Risikovorprüfung zum Schluss, dass die Umstände des Cloud-Outsourcings eine DSFA erforderlich machen (dass mit anderen Worten ein hohes Risiko für die betroffenen Personen angenommen werden muss), ist in einem zweiten Schritt die geplante Bearbeitung zu umschreiben sowie die Bewertung der Gefahren und die Beurteilung der Wirksamkeit bestehender Schutzmassnahmen vorzunehmen.[70] Im Cloud-Kontext sind dabei insbesondere Datenflüsse, Speicherorte, Subprozessoren, Schnittstellen und Verschlüsselungsmechanismen systematisch zu erfassen. Zu prüfen sind insbesondere Risiken wie unautorisierte Zugriffe, Drittstaatenübermittlungen (sogleich IV.C.2.), Fehlkonfigurationen und mangelnde Schlüsselverwaltung.

Die Bewertung erfolgt anhand von Eintrittswahrscheinlichkeit und Schadensschwere. Damit wird deutlich, dass ein allgemeiner «Blueprint» für eine Risikovorprüfung bzw. eine DSFA im Cloud-Kontext nicht erstellt werden kann. Die Verantwortlichen im Unternehmen oder des öffentlichen Organs sind gezwungen, einzelfallbezogene Beurteilungen vorzunehmen.

Das Ergebnis der Risikovorprüfung bzw. der DSFA ist gemäss Art. 14 DSV schriftlich und während mindestens zwei Jahren aufzubewahren – auch wenn die Verantwortlichen zum Schluss kommen, dass das Cloud-Outsourcing keine (hohen) Risiken für die betroffenen Personen mit sich bringt. Änderungen in Architektur, Subprozessoren oder Datenklassifikation erfordern eine Aktualisierung.

2. Datenübermittlung ins Ausland

Aufgrund der Anwendbarkeit des DSG auch auf die Übermittlung von pseudonymisierten Personendaten an Cloud-Anbieter sind auch die Vorgaben zur Bekanntgabe von Personendaten ins Ausland einzuhalten. Da es sich bei dieser Thematik zwar um ein Risiko handelt, welches im Rahmen der DSFA adressiert werden muss, gleichzeitig aber auch rechtliche Konsequenzen mit einem Transfer von Daten ins Ausland verbunden sind, empfiehlt es sich, diesen Punkt separat und nicht nur in der DSFA aufzunehmen.

Gemäss Art. 16 DSG sind Datenübermittlungen ins Ausland zulässig, wenn der Empfängerstaat (mit anderen Worten der Staat, in welchem das Partner-Unternehmen, der Cloud-Anbieter, niedergelassen ist) über ein angemessenes Datenschutzniveau verfügt. Die Angemessenheit des Datenschutzniveaus ergibt sich dabei aus der Gesamtheit der rechtlichen Vorgaben und organisatorischen Massnahmen, die ein Staat zur Wahrung der informatio-

---

67 Husi-Stämpfli/Morand (FN 3), N 469, zu den Risikoüberlegungen im Cloud-Kontext insb. N 621 ff.; BSK DSG-Glatthaar/Schröder (FN 4), Art. 22 N 11 ff.; SHK DSG-Blonski (FN 2), Art. 22 N 10 ff.

68 Roth (FN 65), AJP 2020, 75.

69 Vgl. Roth (FN 65), AJP 2020, 81.

70 EDSA, Guidelines 4/2019 on Data Protection Impact Assessment, N 20 ff., Internet: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (Abruf 27.10.2025).

nellen Selbstbestimmung definiert hat.[71] Der Bundesrat entscheidet gestützt auf Art. 16 Abs. 1 DSG i.V.m. Art. 8 DSV über die Angemessenheit des Datenschutzniveaus in Drittstaaten – die entsprechende Liste findet sich im Anhang 1 der DSV. Der Bundesrat orientiert sich bei seinen Entscheiden auch an jenen der Europäischen Kommission, die gestützt auf Art. 45 DSGVO ihrerseits die Angemessenheit des Datenschutzniveaus von Drittstaaten aus Sicht der EU beurteilt. Dies führte beispielsweise auch dazu, dass die Schweiz[72] das Schrems-II-Urteil des EuGH[73] autonom «nachvollzog» und das Datenschutzniveau der USA als nicht angemessen beurteilte,[74] nun aber auch dem Urteil Latombe v. Kommission[75] folgt, im Rahmen dessen der Europäische Gerichtshof EuG die Angemessenheit des EU-U.S. Privacy Shields bestätigte.

Verfügt ein Staat über kein angemessenes Datenschutzniveau, ist der Schutz der Grund- bzw. Persönlichkeitsrechte der betroffenen Personen auf anderem Wege zu gewährleisten.[76] Dazu gehört typischerweise der Einsatz von Standardvertragsklauseln, ergänzt durch weitere Schutzmassnahmen – wie sie im ADV festzuhalten sind.

3. Der ADV

Nach Art. 9 DSG darf der Verantwortliche Personendaten – und entsprechend den vorangehenden Ausführungen damit auch pseudonymisierte Personendaten – nur dann durch Dritte bearbeiten lassen, wenn diese hinreichende Gewähr für eine datenschutzkonforme Bearbeitung bieten und ein entsprechender Vertrag abgeschlossen wird. Der ADV ist damit zentrales Steuerungsinstrument, um die Verlagerung der Pflichten bei Cloud-Outsourcing rechtlich abzusichern.

Art. 9 DSG und Art. 7 DSV verlangen insbesondere die Festlegung folgender Punkte: Gegenstand und Zweck der Bearbeitung (inkl. Beschreibung der Datenkategorien), die Art der bearbeiteten Daten und die Kategorien der betroffenen Personen, die technischen und organisatorischen Massnahmen (TOM) zur Gewährleistung von Datenschutz und Informationssicherheit, Regelung von Subprozessoren (Zulässigkeit, Genehmigungsverfahren, Informationspflichten), Ort der Datenbearbeitung inkl. allfälliger Drittstaatenübermittlungen und Schutzgarantien, Kontroll- und Auditrechte des Verantwortlichen, Pflichten bei Verletzungen der Datensicherheit[77] sowie Regelungen zur Löschung, Rückgabe und Beendigung der Bearbeitung.

Die Vertragsgestaltung muss dabei das konkrete Cloud-Servicemodell sowie die Schutzstufe der übermittelten Daten berücksichtigen.

Bei SaaS-Anwendungen kontrolliert der Anbieter die gesamte Applikationsebene, weshalb der ADV besonders detaillierte Bestimmungen zu Transparenz und Kontrolle enthalten muss. Dazu gehören insbesondere die Verpflichtung des Anbieters zur Offenlegung sämtlicher Subprozessoren und Datenstandorte, ein vertragliches Audit- oder Prüfungsrecht, mindestens in Form von standardisierten Auditreports,[78] klare Vorgaben zu Backup, Löschung und Zugriff auf Logfiles sowie die Pflicht zu Security-by-Design und Datenschutzfolgeabschätzungen bei Systemänderungen. Da der Verantwortliche nur begrenzt Einfluss auf technische Massnahmen nehmen kann, ist die vertragliche Absicherung hier entscheidend.

Bei PaaS besteht eine geteilte Verantwortung. Der Anbieter sichert die Plattform, der Verantwortliche konfiguriert Anwendungen und Zugriffe selbst. Der ADV muss diese Rollen präzise abgrenzen.[79] Erforderlich sind mindestens Vorgaben zur Zugriffstrennung (Multi-Tenancy), Regelungen zum Schlüsselmanagement, sofern Verschlüsselung kundenseitig erfolgt, klare Prozesse zur Incident-Meldung und Eskalation sowie die Dokumentation der Sicherheitszertifizierungen.[80]

Zusätzlich hat auch die Art der übermittelten Daten einen wesentlichen Einfluss auf den Vertragsinhalt. Werden klare bzw. identifizierende Daten übermittelt, gelten die vollen Anforderungen des DSG. Der Vertrag muss umfassende Garantien zur Datensicherheit, Vertraulichkeit und Kontrolle enthalten. Eine Beschränkung der Haftung des Auftragsbearbeiters ist nur zulässig, wenn sie den Schutzzweck des DSG nicht unterläuft. Pseudonymisierte Daten wiederum bleiben Personendaten, solange der Anbieter oder ein Dritter eine Re-Identifikation nicht ausschliessen

---

71 SHK DSG-Husi-Stämpfli (FN 2), Art. 16 N 5 ff.

72 Damals noch der EDÖB, welcher unter dem alten DSG bis am 31. August 2023 für die Beurteilung der Angemessenheit zuständig war.

73 EuGH (Grosse Kammer), C-311/18 (Facebook Ireland/Schrems), 16.7.2020.

74 EDÖB, Stellungnahme zur Übermittlung von Personendaten in die USA und weitere Staaten ohne angemessenes Datenschutzniveau i.S.v. Art. 6 Abs. 1 DSG, 8. September 2020, Internet: https://www.newsd.admin.ch/newsd/message/attachments/64258.pdf (Abruf 27.10.2025), und dazu bspw. Swisslegal, Schrems II Urteil: Auswirkungen auf schweizerische Unternehmen, Internet: https://www.swisslegal.ch/documents/news/fuw_swisslegal-_schrems-ii-28-08-2021.pdf (Abruf 27.10.2025).

75 EuG, T-553/23 (Latombe/Kommission), 3.9.2025.

76 Art. 16 Abs. 2 DSG.

77 Art. 24 DSG.

78 Z.B. ISAE 3000 oder SOC 2.

79 Z.B. in einer Shared-Responsibility-Matrix.

80 Z.B. ISO 27001, ISO 27017.

kann.[81] Der ADV sollte daher ergänzende Pflichten vorsehen, etwa die strikte Trennung von Identifikatoren und Nutzdaten, das Verbot der Zusammenführung mit anderen Datensätzen oder die Pflicht zur dokumentierten Bewertung des Re-Identifikationsrisikos bei jeder Systemänderung.

Wird die Verschlüsselung der Daten gewählt, hängt der Vertragsinhalt stark von der Schlüsselverwaltung ab. Bei einer clientseitigen Verschlüsselung erhält der Anbieter keinen Zugriff auf Klartextdaten. Der ADV kann hier auf reduzierte Kontrollrechte und Auditpflichten abgestuft werden, sollte aber Schlüsselmanagement, Incident-Meldungen und Rückgabeprozesse regeln. Bei einer serverseitigen Verschlüsselung verwaltet hingegen der Anbieter die Schlüssel. Der ADV muss dann sicherstellen, dass kein unautorisierter Zugriff auf Schlüsselmaterial erfolgt, und sollte Zugriffsprotokollierung sowie Transparenzpflichten vorsehen.

Der ADV fungiert im Cloud-Kontext damit als rechtliches Gegengewicht zum Kontrollverlust des Verantwortlichen. Während SaaS-Verträge hohe Anforderungen an Transparenz, Unterauftragsregelung und Sicherheitsnachweise stellen, kommt es bei PaaS-Modellen auf eine präzise Abgrenzung der Verantwortlichkeiten an. Der Umgang mit pseudonymisierten und verschlüsselten Daten erlaubt eine risikobasierte Differenzierung, hebt aber die vertragliche Pflicht zur Nachvollziehbarkeit nicht auf. Auch bei hohem technischem Schutzniveau bleibt der ADV ein unverzichtbares Element der datenschutzrechtlichen Governance.[82]

V. Technologischer Wandel und die Pflicht zur steten Re-Evaluation

Die insbesondere (aber nicht nur!) im Cloud-Kontext relevanten Instrumente des Datenschutzrechts – Risikovorprüfung und DSFA, Auftragsbearbeitungsvertrag und Regelungen zur Auslandsbekanntgabe – beruhen konzeptionell auf einer klaren Grenzziehung zwischen personenbezogenen und nicht personenbezogenen Daten. Diese Dichotomie wird durch den technischen Fortschritt zunehmend in Frage gestellt. Verfahren der Datenanalyse, Mustererkennung und KI-gestützten Korrelation führen dazu, dass ehemals pseudonymisierte oder scheinbar anonymisierte Datensätze wieder einer Person zugeordnet werden können. Die Re-Identifizierbarkeit ist damit kein hypothetisches Risiko mehr, sondern wird zum dynamischen Faktor, der die Tragfähigkeit bestehender Schutzmechanismen kontinuierlich untergräbt.

Nach geltendem Recht erfolgen Risikovorprüfung bzw. DSFA[83], ADV[84] und die Beurteilung der Angemessenheit von Datenübermittlungen ins Ausland[85] jeweils auf Grundlage einer Ex-ante-Bewertung. Diese berücksichtigt den Stand der Technik und die zum Zeitpunkt der Entscheidung erkennbaren Gefährdungen. Der rasche technologische Fortschritt im Bereich der Datenanalyse und Cloud-Verarbeitung führt jedoch dazu, dass solche Bewertungen rasch veralten. Was heute als hinreichend pseudonymisiert oder sicher verschlüsselt gilt, kann morgen bereits wieder de-anonymisierbar oder kompromittierbar sein.

Daraus folgt, dass Verantwortliche ihre Einschätzungen nicht als statisch verstehen dürfen. Sowohl im Rahmen der Risikovorprüfung wie auch bei der Auftragsbearbeitung ist eine periodische Überprüfung der getroffenen Massnahmen unumgänglich. Einmalige Prüfungen genügen nicht mehr – vielmehr ist ein kontinuierliches Datenschutz-Risikomanagement erforderlich, das technische Entwicklungen, neue Re-Identifikationsmethoden und Veränderungen der Cloud-Infrastruktur berücksichtigt.

Besonders herausgefordert ist auch das System der Auslandsdatenbekanntgabe nach Art. 16 ff. DSG. Dessen Ausgangspunkt ist die Annahme, dass ein ausreichendes Schutzniveau durch Angemessenheitsentscheide oder Standardvertragsklauseln gewährleistet werden kann. Doch selbst bei formal gleichwertigen rechtlichen Garantien bleibt die technische Realität fluid: Cloud-Anbieter

---

81 Vgl. dazu oben IV.B.

82 Obschon für die öffentliche Verwaltung formuliert, lassen sich die nachfolgenden Quellen auch auf die Notwendigkeit der ADV im privatwirtschaftlichen Kontext heranziehen: EDPS, Guidelines on the use of cloud computing Services by the European institutions and bodies, 16.3.2018, Internet: https://www.edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_en.pdf (Abruf 27.10.2025), oder aber Bundeskanzlei, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, 11.6.2025, Internet: https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/cloud/Rechtlicher%20Rahmen%20f%C3%BCr%20die%20Nutzung%20von%20Public-Cloud-Diensten%20in%20der%20Bundesverwaltung_V2.0_DE.pdf.download.pdf/Rechtlicher%20Rahmen%20f%C3%BCr%20die%20Nutzung%20von%20Public-Cloud-Diensten%20in%20der%20Bundesverwaltung_V2.0_DE.pdf (Abruf 27.10.2025).

83 Art. 22 DSG.

84 Art. 9 DSG.

85 Art. 16 ff. DSG.

mit multinationaler Infrastruktur können Datenströme innerhalb weniger Millisekunden zwischen Regionen verlagern, während Überwachungs- und Zugriffsmöglichkeiten Dritter stetig zunehmen. Damit droht die Annahme einer sicheren Drittstaatenbearbeitung zur Fiktion zu werden, wenn sie nicht laufend mit der tatsächlichen technologischen Entwicklung abgeglichen wird. Auch hier ist eine regelmässige Re-Evaluation geboten – nicht nur juristisch, sondern auch technisch-organisatorisch. Der Verantwortliche muss plausibel darlegen können, dass das ursprünglich als angemessen beurteilte Schutzniveau weiterhin gewährleistet ist.

Die wachsende Re-Identifizierbarkeit pseudonymisierter Daten macht deutlich, dass Datenschutz im Cloud- und KI-Zeitalter nicht mehr als fixer Zustand, sondern als fortlaufender Prozess der Anpassung und Überprüfung verstanden werden muss. Rechtliche Pflichten wie Risikovorprüfung, ADV und Drittstaatenbewertung sind daher nicht einmalige Formalakte, sondern Elemente eines zirkulären Governance-Prozesses.

Die Herausforderung liegt darin, die normative Stabilität des Datenschutzrechts mit der technischen Volatilität zu verbinden. Dies erfordert von Verantwortlichen eine Kultur der präventiven Beobachtung – eine Art «technologisches Frühwarnsystem», das neue Risiken früh erkennt und in die bestehenden Verfahren integriert.

VI. Fazit

Der technologische Fortschritt verschiebt die Grenzen des Personenbezugs fortlaufend. Wo das Recht bislang auf stabile Kategorien abstellt, entsteht ein gleitendes Kontinuum zwischen anonym, pseudonym und identifizierbar. Die Pflichten zur Risikovorprüfung und DSFA, Auslandsbekanntgabe und Auftragsbearbeitung behalten ihre Geltung, müssen jedoch dynamisch interpretiert werden. Datenschutz wird damit zur Daueraufgabe: Nur durch stetige Re-Evaluation der gewählten Lösungen kann die materielle Wirksamkeit der Schutzmechanismen erhalten bleiben.

Die Analyse zeigt zugleich, dass die Frage, ob pseudonymisierte Daten als Personendaten zu behandeln sind, nicht absolut, sondern nur relativ beantwortet werden kann. Die Qualifikation hängt entscheidend von der Perspektive des jeweiligen Akteurs und dessen praktischer Möglichkeit ab, mit vertretbarem Aufwand einen Personenbezug herzustellen. Für auslagernde Unternehmen oder öffentliche Organe, die den Schlüssel zur Re-Identifizierung behalten, bleiben pseudonymisierte Daten Personendaten; für den Cloud-Anbieter ohne Schlüsselzugriff sind dieselben Daten faktisch anonym – zumindest in der Theorie, denn der technologische Kontext zwingt auch hier zu einer dynamischeren Betrachtung.

Die bisherige Annahme, dass eine Re-Identifizierung nur mit unverhältnismässigem Aufwand möglich sei, verliert fortlaufend an Stabilität. Fortschritte in generativer künstlicher Intelligenz, maschinellem Lernen und Datenverknüpfung senken die Hürden der Bestimmbarkeit kontinuierlich. Verfahren wie Model Inversion oder Membership Inference Attacks zeigen, dass selbst stark pseudonymisierte oder aggregierte Datensätze unter Einsatz moderner KI-Werkzeuge wieder einzelnen Personen zugeordnet werden können. Damit wird der bisher als «vertretbar» geltende Aufwand zur Re-Identifizierung sukzessive geringer.

Aus rechtlicher Sicht bedeutet dies, dass die Einordnung von Daten als «faktisch anonym» stets nur eine Momentaufnahme bleibt. Der in Art. 5 lit. a DSG und in Erwägungsgrund 26 DSGVO verankerte Massstab des «Standes der Technik» verlangt eine fortlaufende Neubewertung der technischen Möglichkeiten. Unternehmen oder öffentliche Organe, die sich gerade im Cloud-Kontext auf Pseudonymisierung als Schutzmassnahme stützen, müssen regelmässig prüfen, ob die eingesetzten Verfahren noch dem aktuellen technologischen Stand entsprechen und ob ergänzende Schutzmassnahmen – etwa Differential Privacy, sichere Mehrparteien-Berechnungen oder verteiltes Lernen (Federated Learning) – erforderlich sind, um die Re-Identifizierbarkeit dauerhaft zu minimieren.

Für Unternehmen und öffentliche Organe bedeutet dies in letzter Konsequenz, dass Pseudonymisierung zwar ein zentrales, aber kein hinreichendes Instrument bleibt. Sie muss regelmässig überprüft, dokumentiert und durch zusätzliche Sicherheits- und Governance-Massnahmen ergänzt werden. Langfristig werden stärker mathematisch begründete Verfahren wie Differential Privacy oder verteilte Datenverarbeitung wohl unverzichtbar sein, um den steigenden Re-Identifizierungsrisiken zu begegnen.

Im Ergebnis kann Pseudonymisierung weiterhin als Brücke zwischen Datenschutz und Innovation dienen – jedoch nur, wenn sie als fortlaufender Prozess verstanden wird. Datenschutzrechtliche Compliance ist kein statischer Zustand, sondern ein zyklischer Vorgang der technischen Nachjustierung und rechtlichen Neubewertung. Nur so lassen sich die (wirtschaftlichen) Chancen der Datenbearbeitung mit einem nachhaltigen Schutz der Persönlichkeit in Einklang bringen.