David Rosenthal

Die rechtlichen und gefühlten Grenzen der Zweitnutzung von Personendaten

Immer mehr Unternehmen sitzen auf Bergen von Daten und fragen sich, ob sie diese auch noch für andere Zwecke nutzen dürfen, sei es für die Wissenschaft, sei es für handfeste kommerzielle Anwendungen. Der Datenschutz steht dem selbst bei Personendaten weniger stark entgegen, als gemeinhin angenommen wird. Der Beitrag erläutert, worauf zu achten ist, wie die rechtlichen Grenzen ermittelt werden und auch die gefühlten Schranken nicht vergessen gehen.

De plus en plus d'entreprises sont assises sur des montagnes de données et se demandent si elles sont autorisées à les utiliser à d'autres fins, que ce soit pour des recherches scientifiques ou pour des applications commerciales concrètes. La protection des données, même dans le cas de données personnelles, est un obstacle moins important qu'on ne le pense généralement. Cet article explique à quoi il y a lieu de faire attention, comment déterminer les limites légales et comment prendre en considération les obstacles perçus dans ce contexte.

I. Einleitung

Es ist eines der Zauberworte der datengetriebenen Wirtschaft geworden: *Secondary Use*, die Zweitnutzung von Daten, die es Unternehmen ermöglichen soll, die ihnen in ihrem Geschäft ohnehin anfallende Daten für einen guten (kommerziellen) Zweck zweitverwerten zu können. Vor allem Unternehmen, die im Rahmen ihres angestammten Geschäfts an grosse Mengen an Daten gelangen oder über besonders werthaltige und zugleich maschinell leicht verwertbare Daten verfügen, zerbrechen sich die Köpfe darüber, wofür sie diese auch noch benutzen können. Anwendungsbeispiele gibt es so manche:

– Eine Bank wertet die Zahlungsempfänger ihrer Kunden inhaltlich aus, um gestützt darauf Marketingmassnahmen für sich und Dritte zu steuern – etwa wem Sie welche Rabatte anbieten will aufgrund seines Zahlungsverhaltens. Immerhin weiss sie genau, in welchen Fachgeschäften der Kunde sein Geld ausgibt.
– Eine Krankenkasse analysiert die Leistungsabrechnungen ihrer Versicherten, um Patienten auf gefährliche Kombinationen von Arzneimitteln hinzuweisen, weil nur sie den Überblick über die Bezüge von rezeptpflichtigen und über die Kasse abgerechneten Medikamenten ihrer Versicherten hat. So kann sie nebst gesundheitlichen Komplikationen auch Folgekosten für sich selbst vermeiden. Sie kann mit den Daten aber auch Forschung betreiben, um beispielweise Kostensenkungspotenziale beim Arzneimitteleinsatz zu ermitteln – auch das mit positiven Folgen für sich und ihre Versicherten.
– Fast schon banal erscheint da der Detailhändler, der das Einkaufsverhalten seiner Kunden analysiert, um daraus Erkenntnisse für den Einkauf seiner Ware und die Gestaltung seines Sortiments zu gewinnen
– Ein Unternehmen erwirbt Patientendaten einer Epilepsie-Klinik mit deren Hirnwellen-Aufzeichnungen, um diese anonymisiert der Forschung an Hirnerkrankungen und Anbietern von Selbstdiagnose-Apps zu verkaufen, weil der Markt solche Daten kaum zu bieten hat – die Gewinne werden mit dem Spital geteilt.

Oft geht es um wirtschaftliche Vorteile, die mit einer solchen Zweitnutzung geschaffen werden sollen, jedoch nicht nur. Auch im Zusammenhang mit der COVID-19-Pandemie erlebte das Thema der Sekundärnutzung zeitweise Höhenflüge. Im Fokus war in diesen Fällen die Zweitnutzung von Daten für einen «guten Zweck». Begonnen hatte es in Asien mit der Nutzung von Handy-Positionsdaten für ein Tracking (nicht Tracing!) von Corona-Infizierten. So weit gingen die Regierungen in Europa nicht. Doch auch hier wurde darüber diskutiert, mit Hilfe von Smartphone-Daten zu ermitteln, wo sich Personen angesteckt haben könnten.[1] Die Diskussion war kontrovers, auch wenn schlussendlich selbst in der

David Rosenthal, Partner einer Wirtschaftskanzlei in Zürich, Lehrbeauftragter Universität Basel und ETH Zürich.

Dieser Beitrag geht auf einen Vortrag des Autors vom 15. September 2020 in Zürich anlässlich der Tagung «Data@work: Rechte und Ansprüche rund um das Wirtschaftsgut der Zukunft» in der Reihe ICT-RECHT und PRAXIS des Europa-Instituts der Universität Zürich zurück.

1 ‹www.zeit.de/digital/datenschutz/2020-03/handytracking-coronavirus-mobilfunkdaten-standorte-virus-eindaemmung› (19. Februar 2021).

Schweiz mittels Handy-Daten – selbstverständlich anonym – überprüft wurde, ob und inwieweit die Bevölkerung in der ersten Ansteckungswelle wie aufgefordert zu Hause blieb (sie tat es).[2] In anderen Ländern zeigt sich inzwischen, dass Daten aus Corona Contact Tracing so wertvoll sind, dass sie die Polizei auch zur Aufklärung von Delikten verwenden darf – entgegen ursprünglicher Zusagen, dass es keine Zweitnutzung geben werde.[3]

Doch bei Auswertungen von Bewegungs- und Kontaktdaten blieb es nicht, denn benötigt wurden auch Daten über die Gesundheit der Bevölkerung – die Wissenschaft wusste noch zu wenig über das Virus, musste aber in kurzer Zeit an Daten für Forschung gelangen. Das deutsche Robert Koch-Institut (RKI) lancierte in Deutschland beispielsweise eine Corona-Datenspenden-App: Auch sie war ein klassisches Secondary Use: Freiwillige konnten die von ihrem Fitnessarmband oder ihrer Smartwatch sowieso schon gespeicherten und gesammelten Daten über die App den Forschern des RKI für deren Arbeit zur Verfügung stellen und ihnen so pseudonymisierte Hinweise auf eine Infektion mit COVID-19 liefern. Innert kürzester Zeit meldete die Einrichtung über 500'000 Personen, die dem Aufruf gefolgt waren.[4] Es blieb nicht die einzige solche Initiative. In ganz Europa versuchten Behörden und Forscher auf die eine oder andere Weise an Daten zu gelangen, etwa um damit die Datenlage als Grundlage für Entscheide über Corona-Massnahmen zu verbessern.[5]

II. Zulässigkeit der Sekundärnutzung

1. Grundsatz

Während Krisen wie COVID-19 auch in punkto Datenschutz manche Dinge möglich machen, die in «normalen Zeiten» kaum denkbar sind, stellt sich davon unabhängig die Frage, ob und unter welchen Bedingungen Sekundärnutzungen von Daten im Schweizer Recht erlaubt sind. Handelt es sich nicht um Personendaten im Sinne des Datenschutzgesetzes (DSG)[6], so steht einer solchen Verwendung, abgesehen von etwaigen Geheimhaltungspflichten, den Schranken des Lauterkeits-, Urheber- und Patentrechts und etwaigen spezialgesetzlichen Einschränkungen, meist nichts entgegen.

Handelt es sich um Personendaten, so muss differenziert werden: Steht eine Sekundärnutzung zu nicht personenbezogenen Zwecken zur Diskussion, so fällt die kurze Antwort auf die Frage der datenschutzrechtlichen Zulässigkeit meist positiv aus. Eine Sekundärnutzung zu einem personenbezogenen Zweck wird hingegen regelmässig nur mit rechtzeitiger Ankündigung oder ansonsten einer Einwilligung der betroffenen Person datenschutzrechtlich zulässig sein. Ein «personenbezogener» Zweck liegt dann vor, wenn das Ziel der Bearbeitung eine Aussage oder Wirkung bezüglich einem einzelnen, konkreten Datensubjekt ist. Wenn ein Detailhändler seine Kundschaft oder Kundengruppen *in globo* besser verstehen will[7] und hierzu Daten bearbeitet, liegt kein personenbezogener Zweck vor. Dient die Datenbearbeitung hingegen dazu, einzelne Kunden besser anzusprechen[8], so bearbeitet er seine Daten zu einem personenbezogenen Zweck. Die Bearbeitung richtet sich in diesem Fall «gegen» ein Individuum, nicht mehr die Gruppe.

Ob eine Sekundärnutzung von Personendaten erlaubt ist, ist im Rahmen einer mehrstufigen, in der Folge erläuterten Verfahren zu prüfen.

2. Erster Prüfschritt: Spezialgesetzliche Regelung?

In einem ersten Schritt muss geklärt werden, welche Rechtsquellen bezüglich der gewünschten Sekundärnutzung der Personen zu beachten sind. Dies ist nicht unbedingt das DSG oder nur das DSG. Abgesehen davon, dass die Bearbeitung von Personendaten durch kantonale Organe in erster Linie dem kantonalen Datenschutzrecht untersteht (das hier nicht behandelt wird), ist vor allem an spezialgesetzliche Regelungen zu denken. Hierbei gibt es zwei verschiedene Fälle:

– Der erste Fall betrifft die *abschliessend* spezialgesetzlich geregelte Sekundärnutzung von Personendaten. In diesen Fällen verdrängen die betreffenden gesetzlichen Regelungen die entsprechenden Regelungen des DSG (oder der kantonalen Datenschutzgesetze) – es sei denn, das DSG kommt qua Verweis analog zur Anwendung.[9] Wo eine gesetzliche Regelung als *lex specialis* das DSG verdrängt ergibt sich oft nicht aus dem Wortlaut der Bestimmungen, sondern nur durch deren Auslegung. Von einer Verdrängung des DSG ist allerdings nicht leichthin auszugehen, sondern in der Regel erst dann, wenn die spezialgesetzliche Regelung entweder den Datenschutz selbst regeln will[10] oder mindestens einen gleichwertigen Schutz bietet.[11] Ein in der Praxis wichtiges Beispiel sind die Regelungen zur Sekundärnutzung von gesundheitsbezogenen Personen für die Zwecke der Humanforschung, der sog. *Secondary Research*, im Heilmittelgesetz (HFG) (dazu sogleich). Ein weiteres Beispiel sind die Regelungen

2 ‹www.aargauerzeitung.ch/schweiz/wegen-verbreitung-des-coronavirus-swisscom-wertet-fuer-den-bund-bewegungsdaten-von-handys-aus-137365938›.
3 ‹www.zdnet.com/google-amp/article/singapore-police-can-access-covid-19-contact-tracing-data-for-criminal-investigations/›.
4 ‹www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende-allgemein.html›.
5 Vgl. etwa die Übersicht auf ‹www.bertelsmann-stiftung.de/fileadmin/files/user_upload/ADM-systems-in-the-Covid-19-pandemic__Report_by_AW___BSt__Sept_2020_.pdf›.
6 Also Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, d.h. Angaben, die Rückschlüsse auf eine Person erlauben (Art. 3 Bst. a DSG). Mit dem revidierten DSG wird sich dieser Schutz nur noch auf natürliche Personen beschränkten.
7 Welche Produkte besonders beliebt sind, wie gut Verkaufsaktionen sich auszahlen, wie die Kunden durch den Laden strömen.
8 Anzeige von Werbung derjenigen Produkte, die der betreffende Kunde aufgrund seines Profils mit höherer Wahrscheinlichkeit interessant findet.
9 Indem ein Erlass für bestimmte Fragen auf das DSG, z.B. seine Bestimmungen zum Export von Personendaten verweist (Beispiel: Art. 42 Abs. 2 HFG).
10 D.h. den Schutz der Persönlichkeit betroffener Personen.
11 BGE 126 II 126, E. 5.

bezüglich der Nutzung von Stromnutzungs-Informationen aus Smart Metern im Rahmen der Strommarktregulierung.[12]

– Der zweite Fall sind spezialgesetzliche Regelungen zur Sekundärnutzung von Personendaten, welche *zusätzlich* zum DSG gelten, d.h. dieses nicht verdrängen. Sie können Datenbearbeitungen erlauben bzw. rechtfertigen[13], dazu verpflichten oder sie auch verbieten. So schreibt Art. 6 des Geldwäschereigesetzes (GWG) einem Finanzintermediär vor, die von ihm zum Zwecke der Abwicklung einer Transaktion erhaltenen Personendaten auch dazu zu nutzen, um ungewöhnliche Transaktionen oder Anhaltspunkte für Geldwäscherei festzustellen. Art. 77i des Urheberrechtsgesetzes (URG) erlaubt es dem Inhaber eines urheberrechtlich geschützten Werks von ihm erfasste Personendaten auch für die Durchsetzung seiner Rechte gegen Raubkopierer zu verwenden. Art. 50e des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG) verbietet wiederum privaten Stellen (z.B. einem Arbeitgeber) die systematische Zweitverwertung der Sozialversicherungsnummer (AHV-Nummer) seiner Arbeitnehmer.

Regelt ein Spezialgesetz die Bearbeitung von Personendaten ausnahmsweise selbständig, kann diese bezüglich der Vorgaben für Sekundärnutzung durchaus von jener des DSG abweichen. Im Bereich der *Secondary Research* in der Humanforschung ist das der Fall. Dieser Bereich ist praxisrelevant, weil ein grosser Bedarf an Forschung auf Basis bereits bestehender Gesundheitsdaten besteht, wie sie zum Beispiel im Gesundheitswesen aber auch in für andere Zwecke durchgeführten Studien anfallen. Das HFG und die dazugehörige Humanforschungsverordnung (HFV) sieht hierfür ab Art. 32 HFG ein eigenes System vor: Es unterscheidet zwischen genetischen und nicht genetischen Daten; erstere werden strenger behandelt. Während das klassische Datenschutzrecht beispielsweise nicht zwischen verschiedenen Arten von Einwilligungen unterscheidet, tut dies das HFG hingegen schon: Für nicht genetische Daten kennt es z.B. die «Generaleinwilligung», wie sie heute in vielen Krankenhäusern von eintretenden Patienten in Form einer pauschalen Einwilligungserklärung in die Verwendung ihrer Daten für Forschungszwecke eingeholt werden. Im Bereich der Hochschulmedizin ist dieser «Generalkonsent» in seinem Wortlaut heute einigermassen harmonisiert.[14] Für genetische Daten genügt ein solcher hingegen nur für die pseudonymisierte Verwendung, also wenn den Sekundärnutzern nur codierte (wenngleich singularisierte) Gesundheitsdaten zur Verfügung gestellt werden. Bei nicht pseudonymisierten genetischen Daten braucht es eine Einwilligung im Einzelfall. Für die Verwendung nicht-genetischer pseudonymisierter Gesundheitsdaten sieht es wiederum eine Widerspruchslösung vor, die das DSG so nicht kennt.

Das HFG weicht auch in anderer Weise vom DSG ab: Unter dem DSG würde nämlich die Bekanntgabe von codierten Personendaten an einen Forscher, die dieser selbst nicht einer bestimmten Person zuordnen kann, gar nicht erst als Bekanntgabe von Personendaten gelten. Das HFG regelt diese Sekundärnutzung hingegen. Dasselbe gilt für die Anonymisierung von genetischen Daten zum Zwecke der Zweitverwertung, weil es die Möglichkeit der Re-Identifikation sicherstellen will, falls betroffene Personen über die Ergebnisse der Erforschung ihrer Gene informiert werden wollen. Immerhin sieht es auch Ausnahmen für jene Fälle vor, in denen die Patienten nicht vernünftig informiert oder um eine Einwilligung gebeten werden können.[15] Abweichend zum DSG regelt es auch die Verwendung von Daten verstorbener Personen:[16] Das DSG erfasst sie hingegen nicht mehr – mit dem Tod endet auch die Persönlichkeit.[17] Die spezialgesetzliche Regelung kann sich für die Sekundärnutzung positiv wie auch negativ auswirken: Einerseits bietet sie weniger Spielraum für solche Sekundärnutzungen wie das DSG, andererseits ermöglicht sie solche aber auch, wo diese sonst nicht erlaubt wären – so etwa im Falle des *Secondary Research* von Krankenversicherern in der gesetzlichen Grundversicherung.[18]

	Genetische Daten	Nichtgenetische Daten
Unverschlüsselt (identifizierend)	Spezifische Einwilligung (Art. 32 Abs. 1 HFG, Art. 28 HFV)	Generaleinwilligung (Art. 33 Abs. 1 HFG, Art. 31 HFV)
Verschlüsselt (pseudonymisiert)	Generaleinwilligung (Art. 32 Abs. 2 HFG, Art. 29 HFV)	Kein Widerspruch nach Information (Art. 33 Abs. 2 HFG, Art. 32 HFV)
Anonymisiert	Kein Widerspruch nach Information (Art. 32 Abs. 3 HFG, Art. 30 HFG)	Nicht im Anwendungsbereich des HFG (Art. 2 Abs. 2 lit. c HFG)

Abbildung 1: Regelung der Weiterverwendung von Gesundheitsdaten im Humanforschungsgesetz

3. Zweiter Prüfschritt: Bearbeitungsgrundsätze des DSG eingehalten?

Greift keine abschliessende spezialgesetzliche Regelung, so muss die Sekundärnutzung nach den Grundregeln des DSG beurteilt werden – sowie allfällige Spezialgesetze und vertragliche Regelungen, die parallel dazu gelten. Letztere können sich aus Zusagen und Vereinbarungen ergeben, welche den betroffenen Personen abgegeben worden sind, so etwas dem Versprechen an Kunden eines Unternehmens, dass es ihre Personendaten nur für die Abwicklung ihrer Verträge nutzen wird. Hält es sich nicht an diese Zusage, stellt die Sekundärnutzung von Personendaten auch dann eine Vertragsverletzung dar, wenn sie datenschutzrechtlich an sich

12 Vgl. die gestützt auf Art. 17c Abs. 2 Stromversorgungsgesetz (StromVG) erlassenen Spezialregelungen in Art. 8d der Stromversorgungsverordnung (StromVV); vgl. zum Ganzen: S. Rechsteiner/T. Steiner, Datenschutz bei intelligenten Mess- und Steuersystemen, Jusletter 11. Juni 2018.

13 Art. 13 Abs. 1 DSG.

14 ‹www.unimedsuisse.ch/de/projekte/generalkonsent›.

15 Art. 34 HFG.

16 Art. 36 HFG.

17 Art. 31 Abs. 1 ZGB.

18 In Rahmen der Grundversicherung dürfen die Krankenversicherer nach Art. 17 DSG Personendaten nur mit gesetzlicher Grundlage bearbeiten. Art. 84 Krankenversicherungsgesetz (KVG) sieht letztlich nur Datenbearbeitungen zum Vollzug des KVG vor. Sekundärforschung im Rahmen des HFG bleibt aufgrund der spezialgesetzlichen Regelung aber erlaubt.

erlaubt gewesen wäre. Auf solche Zusagen ist daher mit Vorteil zu verzichten. Diese sind in aller Regel auch zur Vertrauensbildung völlig unnötig, weil die relevante Mehrheit der Kunden sie ohnehin nicht zur Kenntnis nimmt. Besser ist es, sich die möglichen Sekundärnutzungen in der eigenen Datenschutzerklärung als möglicher Verwendungszweck vorzubehalten und im Vertrag bzw. den AGB dazu nichts zu sagen.

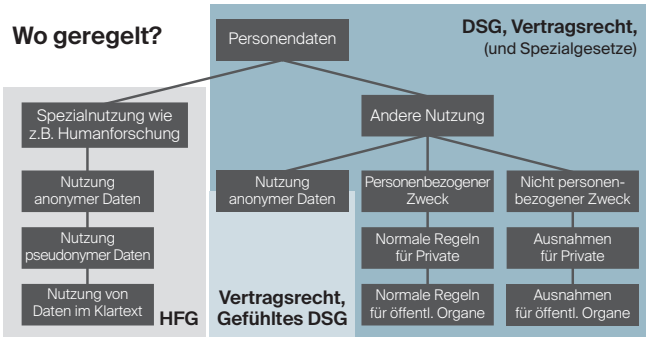

Abbildung 2: Die Sekundärnutzung von Personendaten im Schweizer Recht

Gelten «nur» die Vorgaben des DSG, so sind im Wesentlichen fünf Voraussetzungen zu erfüllen, damit bereits vorhandene Personendaten für einen Sekundärzweck genutzt werden können:

- Die Daten müssen zunächst zulässigerweise vorliegen, d.h. insbesondere im Rahmen der Bearbeitungsgrundsätze nach Art. 4 DSG erhoben worden sein. Es gilt der Grundsatz der «verbotenen Frucht»: Wurden Personendaten in datenschutzwidriger Weise beschafft, stellt auch jede weitere Verwendung dieser Daten zu einem anderen Zweck eine Persönlichkeitsverletzung dar (was nicht bedeutet, dass sie nicht unter Umständen gerechtfertigt werden kann[19]).
- Die Beschaffung und der Zweck der Zeitnutzung muss für die betroffene Person erkennbar gewesen sein, falls die Bearbeitung nicht bereits im Gesetz geregelt ist.[20] Dies muss streng genommen zum Zeitpunkt der Beschaffung der betreffenden Daten der Fall gewesen sein. Das ist etwa der Fall, wenn die Zweitnutzung als möglicher Zweck in der Datenschutzerklärung erwähnt worden ist oder sich aus den Umständen ergibt, weil gemeinhin damit gerechnet werden muss (z.B. dass ein Händler verstehen will, welche seiner Produkte und Dienstleistungen bei seiner Kundschaft wie ankommt). Dieses Transparenzerfordernis ergibt sich aus Art. 4 Abs. 3 und 4 DSG und soll es der betroffenen Person erlauben, der Zweitnutzung zu widersprechen wenn sie ihre Daten bekanntgibt oder sie genutzt werden sollen. Ausnahmsweise greift auch die Pflicht zur aktiven Information nach Art. 14 DSG, wenn für die Zweitnutzung besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft werden. Diese Informationspflicht gilt regelungstechnisch *neben* dem Transparenzgebot. Sie ist öffentlichrechtlicher Natur, während das Transparenzgebot privatrechtlicher Natur ist. Die Verletzung der Informationspflicht führt zur Strafbarkeit[21], die Verletzung des Transparenzgebots zur Persönlichkeitsverletzung[22].
- Die Zweitnutzung muss verhältnismässig sein, d.h. auf das beschränkt, was für den erkennbaren Zweitnutzungszweck nötig, zu dessen Erreichung geeignet ist und was der betroffenen Person zugemutet werden kann (Verhältnismässigkeit im engeren Sinn). Dies ergibt sich aus Art. 4 Abs. 2 DSG, und wird einer Zweitnutzung selten im Wege stehen, da sich die Notwendigkeit und Eignung direkt aus dem verfolgten Zweck ergibt, den wiederum die für die Zweitnutzung verantwortliche Stelle festlegt. Das gilt jedenfalls dort, wo die Zweitnutzung keine wesentlichen negativen Folgen für die betroffene Person hat.
- Schliesslich darf die Zweitnutzung nicht zu einer Weitergabe von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen an eine Person führen, welche diese für ihre eigene Zwecke bearbeiten will.[23]
- Es darf auch kein Widerspruch der betroffenen Person vorliegen.[24] Ein solcher Widerspruch läge z.B. vor, wenn sie vom Unternehmen verlangt, dass all ihre Daten gelöscht oder nicht weiter benutzt werden.

Diese fünf Voraussetzungen stellen normalerweise kein Problem dar – sofern die Möglichkeit der Umnutzung der bereits für andere Zwecke erhobenen Daten den betroffenen Personen im Rahmen deren Beschaffung kommuniziert worden war. Ist dies nicht der Fall, so galt dies bisher als Verletzung des Grundsatzes der Erkennbarkeit und damit als Persönlichkeitsverletzung.[25] Liegt eine Persönlichkeitsverletzung vor, ist die Bearbeitung der betreffenden Personendaten jedenfalls als private Stelle nur mit einem entsprechenden Rechtfertigungsgrund erlaubt.[26] Dies wird im dritten Schritt zu prüfen sein.

Mit dem revidierten Datenschutzgesetz (revDSG[27]) verändert sich dies in zwei Punkten.

- *Erstens* ist der Grundsatz der Zweckbindung neu und etwas anders als bisher formuliert. Damit geht auch eine leichte inhaltliche Neuausrichtung einher. Personendaten dürfen demnach nur «zu einem bestimmten und für die betroffenen Person erkennbaren Zweck beschafft werden» und «nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist» (Art 6 Abs. 3 revDSG). Dies bedeutet, dass der Zweck der Zweitnutzung entweder bei der Beschaffung bereits erkennbar gewesen sein muss oder – und das

19 Auch eine gegen die Bearbeitungsgrundsätze verstossende Datenbearbeitung kann jedenfalls im Bereich der privaten Datenbearbeitung nach Art. 13 Abs. 1 DSG gerechtfertigt werden. Vgl. dazu die Ausführungen zur 3. Stufe.
20 In diesem Falle gilt sie als erkennbar, weil die Kenntnisnahme des Gesetzes vorausgesetzt wird.
21 Art. 34 Abs. 1 Bst. a DSG.
22 Art. 12 Abs. 2 Bst. a DSG.
23 Art. 12 Abs. 2 Bst. c DSG.
24 Art. 12 Abs. 2 Bst. b DSG.
25 Art. 12 Abs. 2 Bst. a DSG.
26 Art. 13 Abs. 1 DSG.
27 Der Text des revidierten DSG ist in verschiedenen Fassungen via ‹www.datenrecht.ch› abrufbar.

ist neu – er muss mit dem bei der Beschaffung erkennbaren Zweck «vereinbar» sein, d.h. er muss diesem nicht genau entsprechen. Dieses Konzept der «Vereinbarkeit» eines Zwecks wurde aus der DSGVO übernommen.[28] Dort werden auch Kriterien definiert, die bei der Prüfung der Vereinbarkeit eines Sekundärzwecks mit dem Primärzweck zu berücksichtigen sind, wie etwa eine Anonymisierung von Personendaten.[29] Gemäss Botschaft ist mit dem Primärzweck das unvereinbar, was als «unerwartet, unangebracht oder beandstandbar» gelten muss.[30] Dies unterscheidet sich vom bisherigen Zweck, wonach der Zweckbindungsgrundsatz jeden Zweck erlaubte, der mindestens «aus den Umständen erkennbar» war. Neu ist auch jeder Sekundärzweck erlaubt, der zwar nicht aus den Umständen erkennbar war, aber trotzdem noch einigermassen im Rahmen dessen liegt, was vernünftigerweise ohne besonderen Hinweis zulässig sein muss. Das ist eine Erweiterung gegenüber der bisherigen Rechtslage zugunsten von Sekundärnutzungen: Eine nachträgliche Umnutzung von Personendaten ist neu in gewissem Umfang zulässig, ohne dass nach den Bearbeitungsgrundsätzen zusätzliche Transparenz geschaffen werden muss (davon unberührt bleibt freilich die öffentlich-rechtliche Informationspflicht nach Art. 19 revDSG, dazu nachfolgend).

Ein klassisches Beispiel für «vereinbare» Zwecke sind solche, die lediglich mit anonymisierten oder pseudonymisierten Daten, für den Empfänger aber nicht re-identifizierbaren Daten verfolgt werden: Bereits der Vorgang der Anonymisierung oder Pseudonymisierung ist genau genommen ein Bearbeiten von Personendaten, welcher dem Zweckbindungsgrundsatz unterliegt. Wer also Daten für den Zweck A beschafft und dann für den Zweck B anonymisiert, bearbeitet sie auch für Zweck B. Unter bisherigen Recht wäre der Zweckbindungsgrundsatz verletzt gewesen, wenn Zweck B nicht aus den Umständen erkennbar war.[31] Nach dem revDSG ist dies nicht mehr der Fall, auch wenn die Unterscheidung selten praxisrelevant sein wird.[32]

In dogmatischer Hinsicht ist zur Abgrenzung zur DSGVO zu beachten, dass unter dem DSG und revDSG die Zweckbindung als Konzept weniger weit geht. Sie ist im Kern «nur» ein Transparenzerfordernis, d.h. um einen bestimmten Zweck verfolgen zu dürfen[33] muss er gegenüber der betroffenen Person transparent gemacht werden (oder neu mit dem transparent gemachten Zweck vereinbar sein). Unter der DSGVO muss zusätzlich eine hinreichende Rechtsgrundlage[34] bestehen, die ebenfalls an den Zweck knüpft. Im DSG und revDSG dient das Vorliegen einer Rechtsgrundlage im Sinne der DSGVO hingegen der Rechtfertigung der Bearbeitungsgrundsätze, welche die DSGVO so nicht kennt.

– *Zweitens* wurde unter dem revDSG die allgemeine Informationspflicht ausgebaut, was dazu führt, dass künftig jeder Bearbeitungszweck und somit auch jede Sekundärnutzung in der Datenschutzerklärung der für die Bearbeitung verantwortlichen Stelle aufgeführt sein muss.[35] Auch die Weitergabe zu solchen Zwecken muss erwähnt werden, jedenfalls unter Angabe der Kategorien der Empfänger.[36] Immerhin genügen vergleichsweise generische Angaben. Über einen bestimmten Zweck muss im Rahmen der neuen Informationspflicht aber erst zum Zeitpunkt der «Beschaffung» der Personendaten für diesen Zweck informiert werden, d.h. zu dem Zeitpunkt, an welchem die Personendaten planmässig dafür erhoben werden.[37] Im Falle einer Sekundärnutzung ist dies nicht notwendigerweise der Zeitpunkt der ursprünglichen Beschaffung. Fällt der Entscheid zur Sekundärnutzung erst später, war sie also nicht Teil des ursprünglichen Plans der Datenbeschaffung, und kann auch erst dann informiert werden, wenn die Daten für die Sekundärnutzung umgenutzt werden. Technisch gesehen liegt in diesem Fall eine Beschaffung in den eigenen, internen Datenbeständen vor. Auch eine solche «indirekte» Beschaffung löst die Informationspflicht aus, doch sieht das revDSG hierfür zusätzliche Ausnahmen vor, etwa für den Fall, dass eine Information nicht möglich oder mit unverhältnismässigem Aufwand verbunden wäre.[38]

Diese beiden Neuerungen bedeuten für die Sekundärnutzung, dass der Verantwortliche bezüglich Zweckbindungs- und Transparenzgebot und Informationspflicht drei Möglichkeiten hat:

– Er kann dann informieren, wenn er die Daten zum ersten Mal beschafft.
– Er kann aber auch erst dann informieren, wenn er sich entscheidet, die bereits für einen anderen unter Einhaltung des Transparenzgebots und der Informationspflicht genannten Zweck beschafft für den Sekundärnutzungszweck umzunutzen, da dies als neue Beschaffung in seinen eigenen Datenbeständen gilt. Sie gibt der betroffenen Person erneut die Möglichkeit zum Widerspruch.
– Er verzichtet auf die Information und nutzt die Daten einfach. Diese dritte Variante wird nur dann zulässig sein, wenn (i) der Sekundärzweck mit einem der erkennbaren Zwecke vereinbar ist (damit Art. 6 Abs. 3 revDSG eingehalten ist), (ii) auch keine anderen neuen Aspekte hinzutreten, über welche Transparenz geschaffen werden müsste, weil sie für eine betroffene Person bei generalisierter, objektiver Betrachtung von datenschutzrechtlicher Relevanz ist (damit das Gebot von Treu und Glauben nach Art. 6

28 Art. 5 Abs. 1 Bst. b DSGVO, welche Bestimmung eine Bearbeitung von Personen in einer mit dem Primärzweck «nicht zu vereinbarenden Weise» untersagt, wobei Forschungszwecke unter Umständen als vereinbar gelten.
29 Art. 6 Abs. 4 DSGVO.
30 BBl 2017 7025.
31 Jedenfalls, wenn derjenige, der sie anonymisiert, sie nach wie vor in personenbezogener Form hat. Hat er dies nicht mehr, kommt die Anonymisierung einer Löschung gleich.
32 Denn auch unter dem bisherigen DSG konnten solche Fälle regelmässig gerechtfertigt werden.
33 Vorbehalten bleibt selbstredend, dass die eigentliche Datenbearbeitung auch den anderen Bearbeitungsgrundsätzen folgt.
34 Art. 6, 9 und 10 DSGVO.
35 Art. 19 Abs. 2 Bst. b revDSG.
36 Art. 19 Abs. 2 Bst. c revDSG.
37 D. Rosenthal, Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 93.
38 Art. 20 Abs. 2 DSG.

Abs. 2 revDSG eingehalten ist) und (iii) die Informationspflicht nach Art. 19 revDSG trotz neuerlicher Beschaffung in den eigenen Datenbeständen (sie gilt als «indirekte» Beschaffung) aufgrund einer der Ausnahmen nach Art. 20 revDSG nicht erforderlich ist (z.B. weil der Aufwand im Verhältnis zum Informationsinteresse der betroffenen Personen unverhältnismässig wäre)[39]. Können (i) oder (ii) nicht eingehalten werden, kann dies freilich auch nach Art. 31 revDSG gerechtfertigt werden (dazu sogleich).

4. Dritter Prüfschritt: Rechtfertigungsgrund nach DSG gegeben?

Können die Bearbeitungsgrundsätze für die Zwecke einer Sekundärnutzung trotz der Erleichterungen unter dem revDSG nicht eingehalten werden, liegt wie im bisherigen DSG[40] eine Persönlichkeitsverletzung vor[41]. Sie kann im privaten Bereich weiterhin durch eine Einwilligung, ein überwiegendes privates oder öffentliches Interesse oder durch das Gesetz gerechtfertigt sein[42] (Pro memoria: Die Rechtfertigung einer Verletzung der Informationspflicht richtet sich hingegen nach anderen Regeln[43]).

An dieser Stelle muss in der Praxis zwischen einer Nutzung zu einem personenbezogenen und zu einem nicht personenbezogenen Zweck unterschieden werden. Denn für letztere Fälle sehen das bisherige und das revidierte DSG einen Rechtfertigungsgrund des überwiegenden privaten Interesses vor: Dieses besteht dann, wenn Personendaten für einen nicht personenbezogenen Zweck wie Forschung, Planung oder Statistik bearbeitet werden – sofern gewisse Voraussetzungen eingehalten werden[44] (eine ähnliche Regelung gibt es im Ergebnis auch für Bundesorgane[45]; kantonale Datenschutzgesetze kennen in der Regel ebenfalls eine solche «Statistikausnahme»). Der private Datenbearbeiter muss drei Voraussetzungen erfüllen[46]: Er muss *erstens* die Daten anonymisieren, sobald es der Bearbeitungszweck erlaubt; ist das mit einem unverhältnismässigen Aufwand verbunden, muss er die Bestimmbarkeit der betroffenen Personen anders verhindern, etwa durch eine Pseudonymisierung. Er darf zweitens besonders schützenswerte Personendaten als solche nicht Dritten weitergeben oder, wenn dies nicht möglich ist, so muss er die nicht-personenbezogene Bearbeitung anderweitig sicherstellen. *Drittens* dürfen die Daten nicht veröffentlicht werden, solange noch Rückschlüsse auf die Identität der betroffenen Personen möglich sind. Dieser letzte Punkt galt schon bisher.

Diese drei Anforderungen an eine nicht personenbezogene Sekundärnutzung lassen sich auf den ersten Blick erfahrungsgemäss in vielen Fällen gut erfüllen, womit der Datenschutz der Sekundärnutzung für nicht personenbezogene Zwecke nicht mehr im Wege steht. Allerdings ist bezüglich dem dritten Erfordernis zu beachten, dass eine Publikation von Personendaten stets ein irreversibler Vorgang ist: Die Anonymität muss dabei nicht nur im Moment der Publikation gewahrt sein, sondern solange, als dass vernünftigerweise von einem Interesse einer Re-Identifikation der betroffenen Personen durch etwaige Dritte auszugehen ist und diese auch die Mittel dazu haben oder erlangen werden.[47] Die Möglichkeiten der Re-Identifikation werden dabei immer wieder unterschätzt, wie entsprechende Pannen und Vorkommnisse immer wieder demonstrieren.[48]

Sollen die Daten für personenbezogene Zwecke genutzt werden, obwohl die Bearbeitungsgrundsätze nicht eingehalten werden können, wird in der Praxis meist mit einer Einwilligung gearbeitet werden müssen – soweit die Sekundärnutzung nicht ausnahmsweise für die Abwicklung eines Vertrags nötig ist oder sonst ein überwiegendes Interesse des Bearbeiters vorliegt. Die Anforderungen an eine Einwilligung sind dabei in der Schweiz weniger hoch als unter der DSGVO. Soweit eine Einwilligung primär aus wirtschaftlichen Interessen erfolgt ist (z.B. im Rahmen eines Studienteilnahmevertrags), wird auch ihr Widerruf der damit ermöglichten Sekundärnutzung nicht unbedingt schaden.[49] Unter der DSGVO gilt hier ein sehr viel strengeres Regime.

5. Vierter Prüfschritt: Sind andere Schranken verletzt?

Ist die Sekundärnutzung nach DSG und etwaigen Spezialgesetzen geklärt, müssen noch zwei weitere Hürden genommen werden. Die erste sind – wie bereits erwähnt – etwaige vertraglichen Regelungen. Zu denken ist dabei nicht nur an die Zusagen gegenüber betroffenen Personen, sondern auch an Vertraulichkeitsvereinbarungen im Kontext klassischer B2B-Geschäftsbeziehungen. Sie enthalten sehr häufig nebst dem Verbot der Preisgabe vertraulicher Informationen der anderen Vertragspartei auch ein Verbot der Nutzung solcher Informationen für eigene Zwecke. Eine solche Bestimmung ist zwar im Einzelfall auszulegen, aber sie kann ohne Weiteres eine Sekundärnutzung untersagen soweit die Daten als Geschäftsgeheimnisse der anderen Vertragspartei einzustufen sind – selbst wenn die Sekundärnutzung nur intern stattfindet. Ein Vorbehalt der eigenen Sekundärnutzung in einer Vertraulichkeitsvereinbarung (z.B. für Know-how-Zwecke oder statistische Auswertungen) beugt dem vor.

Zu prüfen ist weiter die Einhaltung des gefühlten Datenschutzes. Selbst eine rechtlich klar zulässige Bearbeitung von Personendaten kann sozial nicht akzeptiert sein und damit den Datenschutz «gefühlt» verletzen, auch wenn die Datenbearbeitung alle Vorgaben des DSG einhält. Insbeson-

---

39 D. Rosenthal (Fn. 53), Rz. 104.
40 Art. 12 Abs. 2 Bst. a DSG.
41 Art. 30 Abs. 2 Bst. a revDSG.
42 Art. 31 Abs. 1 revDSG, analog zum bisherigen Art. 13 Abs. 1 DSG.
43 Art. 14 DSG, Art. 20 revDSG.
44 Art. 13 Abs. 2 Bst. e DSG, Art. 31 Abs. 2 Bst. e revDSG.
45 Art. 39 revDSG.
46 Vgl. dazu D. Rosenthal (Fn. 53), Rz. 42.
47 Denn in diesem Falle müssen die Daten als Personendaten und damit als nicht anonymisiert gelten (BGE 136 II 508).
48 Vgl. etwa ‹www.arxivblog.com/?p=142%20%20(2007› zu einem Fall betreffend Netflix und dem Fall des US-Filmstars Bradley Cooper, dessen Taxi-Trinkgeld anhand angeblich anonymer Taxidaten im Internet ermittelt werden konnte (‹www.fastcompany.com/3036573/nyc-taxi-data-blunder-reveals-which-celebs-dont-tip-and-who-frequents-strip-clubs›).
49 Vgl. dazu BGE 136 III 401.

dere Sekundärnutzungen, mit welchen Unternehmen bestehende sensible oder wertvolle Daten für sich allein versilbern, sind einem Risiko negativer öffentlicher Reaktionen und Ängsten der Bevölkerung vor einer Verletzung ihrer Privatsphäre ausgesetzt. Dasselbe gilt für neuartige Nutzungen. In der COVID-19-Pandemie haben dies die Diskussionen um die Corona-Tracing-App des Bundes deutlich gezeigt. Datenschutzrechtlich konnte sie von Anfang an als bedenkenlos eingestuft werden, da vom Benutzer keine Personendaten erhoben werden – selbst der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) gab rasch grünes Licht. Doch die zahlreichen negativen Schlagzeilen in den Medien verfehlten ihre Wirkung nicht, auch wenn sie fachlich häufig nicht fundiert waren, sondern lediglich das mulmige Gefühl gewisser Meinungsmacher reflektierten: Der mangelnde Datenschutz war laut einer Erhebung der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) selbst im September 2020 mit 32 Prozent noch der Hauptgrund, warum Schweizer die App nicht installieren wollten.[50]

In anderen Fällen werden Unternehmen, welche gefühlt den Datenschutz verletzen, durch Boykotte, Shitstorms, negativer Publicity, Vertragsfolgen und immer wieder auch durch behördliche Interventionen, sanktioniert. Ein Musterfall dieser Art aus dem Bereich der Sekundärnutzung war das Vorhaben der Postfinance im Jahr 2014, Zahlungsverkehrsdaten ihrer Kunden für personalisierte, aber anonyme Rabattangebote von Werbepartnern einzusetzen. Obwohl das Vorhaben bei Lichte betrachtet damals wie heute als in jeder Hinsicht datenschutzkonform gelten kann und die Persönlichkeitsrechte der betroffenen Personen sehr viel besser schützt als bei manchen anderen Marketingformen, intervenierte der EDÖB nachdem der «Tagesanzeiger» über das Vorhaben negativ zu berichten begann.[51] Der EDÖB bewog die Postfinance schliesslich zum Rückzug[52] – ohne Ausschöpfung des Rechtswegs. Die in Fachkreisen stark kritisierten Ausführungen des EDÖB in seinem Schlussbericht[53] blieben damit gerichtlich ungeprüft und unwidersprochen. Faszinierend an diesem Fall ist, dass die Postfinance mit ihrem Vorhaben vermutlich keine Probleme gehabt hätte, hätte sie nicht versucht, von ihren Kunden über ihre AGB eine Einwilligung einzuholen und zudem nicht so transparent kommuniziert hätte, wie sie es tat.

III. Fazit

Zweitnutzungen von Personendaten sind, wie die vorstehenden Ausführungen zeigen, unter dem bestehenden wie auch dem revidierten Datenschutzrecht vergleichsweise gut möglich. Das gilt vor allem für Vorhaben mit denen nicht personenbezogene Zwecke verfolgt werden sollen. Wichtig ist jedoch, dass eine Zweitnutzung richtig «verpackt» und «verkauft» wird, damit sie weder rechtlich noch gefühlt auf Widerstand stösst. Dies beginnt bei der entsprechenden Ausgestaltung der Datenschutzerklärung und endet damit, wie und wann eine Zweitnutzung dem Publikum gegenüber kommuniziert und begründet wird. Denn auch der gefühlte Datenschutz unterliegt gewissen Gesetzmässigkeiten, wie der Autor dieser Zeilen bereits vor Jahren analysierte.[54] Eine der dabei herausgearbeiteten Regeln lautete: Abwarten, bis sich die Wogen glätten. Der Mensch ist ein Gewohnheitstier – und mit Bekanntem findet er sich über Zeit grundsätzlich ab. Das gilt auch für die Zweitnutzung von Personendaten. Was heute innovativ ist und kritisch beurteilt wird, ist morgen normal und sozial akzeptiert. Ist ein Projekt zum gegenwärtigen Zeitpunkt nicht möglich, ist die Situation in einem oder zwei Jahren womöglich völlig anders.

50 ‹www.netzwoche.ch/news/2020-11-23/covid-apps-angst-vor-fehlendem-datenschutz-und-ueberwachung›.
51 ‹www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/postfinance-droht-onlinekunden-mit-dem-rauswurf/story/19453761›.
52 ‹www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/finanzwesen/e-banking-bei-postfinance–datenanalyse-wird-freiwillig-sein.html›.
53 Schlussbericht betr. E-Finance von PostFinance vom 28. Juli 2015.
54 D. Rosenthal, Das Bauchgefühl im Datenschutz, in: Datenschutz-Forum Schweiz (Hg.), Von der Lochkarte zum Mobile Computing, Zürich 2012.

Zusammenfassung

Auch die Zweitnutzung von Personendaten unterliegt dem Datenschutz. Während die «Umnutzung» von Personendaten datenschutzrechtlich auf den ersten Blick grundsätzlich verpönt erscheint, eröffnen sich bei genauerer Betrachtung einige Spielräume. Dabei muss vor allem zwischen einer personenbezogenen und nicht personenbezogenen Nutzung unterschieden werden. Geht es um Letzteres und damit nicht um die einzelne betroffene Person, lässt sich eine Zweitnutzung oft gut rechtfertigen, wenn die nötigen Vorsichtsmassnahmen getroffen werden, um eine personenbezogene Nutzung zu verhindern. Eine personenbezogene Zweitnutzung erfordert hingegen eine frühzeitige Information der betroffenen Personen oder deren Einwilligung. Das revidierte DSG eröffnet dabei mit der Erweiterung des Zweckbindungsgrundsatzes um das Prinzip der «Vereinbarkeit» noch etwas mehr Spielraum als es das bisherige Datenschutzrecht tat. Allerdings ist in jedem Einzelfall zu prüfen, ob die geplante Datennutzung nicht auch spezialgesetzlich geregelt ist. Im Bereich der Humanforschung, wo Sekundärnutzungen besonders wichtig und häufig sind, gelten zum Beispiel ganz eigene, andere Regeln. Und dann sind auch noch andere Schranken zu beachten, so zum Beispiel vertragliche Umnutzungsverbote, denen sich Unternehmen insbesondere im Rahmen von Geheimhaltungsklauseln oft unterwerfen, ohne sich darüber wirklich Gedanken zu machen. Zu beachten ist allerdings auch der gefühlte Datenschutz, der speziell bei Sekundärnutzungen, die dem Publikum noch nicht vertraut sind, einen dicken Strich durch die Rechnung machen kann, selbst wenn alle rechtlichen Regeln beachtet werden.

Résumé

La réutilisation de données personnelles est également soumise à la protection des données. Si la «réaffectation» de données personnelles semble à première vue généralement désapprouvée par la législation sur la protection des données, un examen plus approfondi révèle une certaine marge de manœuvre. À cet égard, il convient surtout de distinguer l'utilisation visant une personne de celle qui ne vise pas une personne en particulier. Dans ce dernier cas, une réutilisation peut souvent être justifiée si les précautions nécessaires sont prises pour empêcher une utilisation visant des personnes particulières. La réutilisation de données personnelles visant des personnes particulières, en revanche, exige que les personnes concernées en soient informées à un stade précoce ou qu'elles y donnent leur consentement. À cet égard, la LPD révisée, en élargissant le principe de la finalité pour y inclure le principe de «compatibilité», ouvre une marge de manœuvre un peu plus grande que ne le faisait la précédente loi sur la protection des données. Toutefois, il convient de vérifier au cas par cas si l'utilisation prévue des données n'est pas également régie par une législation spéciale. Dans le domaine de la recherche sur l'être humain, par exemple, où les réutilisations de données sont particulièrement importantes et fréquentes, des règles complètement différentes s'appliquent. D'autres obstacles doivent également être pris en compte, comme les interdictions contractuelles de réutilisation des données, auxquelles se soumettent souvent les entreprises, notamment dans le cadre de clauses de confidentialité, sans vraiment y réfléchir. Il y a toutefois également lieu de tenir compte de la perception de la protection des données, surtout dans le cas de réutilisations qui ne sont pas encore connues du public, cette perception pouvant entraîner bien des désagréments même si toutes les règles juridiques sont respectées.