

Universität St. Gallen – Hochschule für
Wirtschafts-, Rechts- und Sozialwissenschaften, Internationale Beziehungen
und Informatik (HSG)



**Die Rolle der datenschutzrechtlichen Einwilligung für eine effiziente Se-
kundärnutzung von Gesundheitsdaten**

Eine Analyse unterschiedlicher Modelle und Regulierungsansätze im Kontext der digitalen
Selbstbestimmung

Pascale Illi (19-614-494)
Oberdorf 1
8548 Ellikon an der Thur
pascale.illi@student.unisg.ch

Universität St.Gallen
Masterarbeit

betreut durch
Prof. Dr. Franziska Sprecher, Rechtsanwältin
Prof. Dr. Alexander Geissler

18. November 2024

Erlassverzeichnis

Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht OR) vom 31. März 1911 (SR 220).

Bundesgesetz über das elektronische Patientendossier (EPDG) vom 19. Juni 2015 (SR 816.1).

Bundesgesetz über den Datenschutz (DSG) vom 25. September 2020 (SR 235.1).

Bundesgesetz über die Forschung am Menschen (HFG) vom 30. September 2011 (SR 810.30).

Bundesverfassung der Schweizerischen Eidgenossenschaft (BV) vom 18. April 1999 (SR 101).

Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) 4. November 1950 (SR 0.101).

Schweizerisches Zivilgesetzbuch (ZGB) vom 10. Dezember 1907 (SR 210).

Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (DSGVO) vom 27. April 2016 (2016/679).

Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten COM/2022/197 (EHDS-VO) vom 3. Mai 2022 (2022/0140(COD)).

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

Verordnung über die Humanforschung mit Ausnahme der klinischen Versuche (HFV) vom 20. September 2013 (SR 810.301).

Literaturverzeichnis

AUGSBERG STEFFEN/V. ULMENSTEIN ULRICH, Modifizierte Einwilligungserfordernisse: Kann das Datenschutzrecht vom Gesundheitsrecht lernen?, GesR 6/2018 S. 341-346 (zit. AUGSBERG/V. ULMENSTEIN, S.).

BAERISWYL BRUNO, Datenschutz und Forschung – Das Paradox der Einwilligung (Branchenwort), LSR 1/2023, S. 3-4 (zit. BAERISWIYL, S.).

BAERISWYL BRUNO, Die Einwilligung hilft (nicht) weiter, digma 2020 S.62-66 (zit. BAERISWYL Einwilligung, S.).

BAERISWYL BRUNO, DSG 6 - Datenschutzgesetz (DSG) Bundesgesetz vom 25. September 2020 über den Datenschutz, in: BAERISWYL BRUNO (Hrsg.)/PÄRLI KURT (Hrsg.)/ BLONSKI DOMINIKA (Hrsg.), Stämpfli's Handkommentar (Zürich/Basel 2023) S. 88-111 (zit. SHK Art. 6 DSG, Rz.).

BLECHTA GABOR P./DAL MOLIN LUCA/WESIAK-SCHMIDT KRISTEN, Art. 5 DSG, in: BLECHTA GABOR P. (Hrsg.)/VASELLA DAVID (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz 2024 (Basel 2024) S. 1-58 (zit. BSK Art. 5 DSG, Rz.).

BREITENMOSER STEPHAN/SCHWEIZER RAINER J./STRIEGEL LEA S., Art. 13 BV – Bundesverfassung, in: EHRENZELLER BERNHARD/EGLI PATRICIA/HETTICH PETER/HONGLER PETER/SCHINDLER BENJAMIN/SCHMID STEFAN G./SCHWEIZER RAINER J., St.Galler Kommentar (St.Gallen 2023) S. 1-8 (zit. SGK Art. 13 BV, Rz.).

BUCHHOLZ GABRIELE/SCHMALHORST LOUISA/BRAUNECK ALISSA, Der Gesetzgeber im Spannungsfeld zwischen Patientensouveränität und Forschungsinteressen – eine Bewertung der neuesten Gesetzgebungsaktivitäten auf EU-Ebene und nationaler Ebene, MedR 42/2024, S. 471-476 (zit. BUCHHOLZ *et al.*, S.).

BÜHLMANN LUKAS/SCHÜEPP MICHAEL, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht - Eine kritische Analyse anhand des Helsana+-Urteils, Jusletter 15. März 2021 S. 1-46 (zit. BÜHLMANN/SCHÜEPP, Rz.).

BÜHLMANN LUKAS /REINLE MICHAEL, Art. 6 DSG, in: BLECHTA GABOR P. (Hrsg.)/VASELLA DAVID (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz 2024 (Basel 2024) S. 1-80 (zit BSK Art. 6 DSG, Rz.).

BRÜNGGER LISA/HERMANN MICHAEL/WENGER VIRGINIA, CSS Gesundheitsstudie 2024 (zit. BRÜNGGER/HERMANN/WENGER, S.).

DE MAN YVONNE/WIELAND-JORNA YVONNE/TORENSMA BART/DE WIT KOOS/FRANCKE ANNEKE L./OOSTERVELD-VLUG MARISKA G./VERHEIJ ROBERT A., Opt-In and Opt-Out Consent Procedures for the Reuse of Routinely Recorded Health Data in Scientific Research and Their Consequences for Consent Rate and Consent Bias: Systematic Review, J Med Internet Res. 02/2023 (zit. DE MAN, *et al.*).

DIRKSEN HANS-HERMANN/HAMEL MIRIAM/SCHERER SOPHIA/SPRECKELSEN CORD/WILKE FELIX/ZIEGER MICHAEL, Datenspende von Gesundheitsdaten –Nutzen, Risiken und Perspektiven, AVATAR Verbundprojekt 15.04.2024 S. 1-11 (zit. DIRKSEN *et al.*, S.).

DRECHSLER CHRISTIAN, Art. 2 DSG, in: BLECHTA GABOR P. (Hrsg.)/VASELLA DAVID (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz 2024 (Basel 2024) S. 1-18 (zit. BSK Art. 2 DSG, Rz.).

EPINEY ASTRID (Hrsg.)/NÜESCH DANIELA (Hrsg.)/ ROVELLI SOPHIA (Hrsg.), Datenschutzrecht in der Schweiz – Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderen Akzent auf den für Bundesorgane relevanten Vorgaben (Bern 2023) (zit. EPINEY/NÜESCH/ROVELLI, S.).

FASNACHT TOBIAS/GAUCH PETER (Hrsg.), Die Einwilligung im Datenschutzrecht – Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht (Zürich 2017) (zit. FASNACHT, Kap. Rz.).

FISCHER MARKUS/HAFEN ERNST/JELITTO JENS/KAIERSWERTH MATTHIAS/KOSSMANN DONALD/MARCHIORI CHIARA/MARTIN MIKE, Big Data im Gesundheitswesen – White Paper, Swiss Academies Communications 10(2)/2015 S.1-39 (zit. FISCHER *et al.*, S.).

FLOREA MARCU, Withdrawal of consent for processing personal data in biomedical research, International Data Privacy Law 06/2023 S.107-123 (zit. FLOREA, S.).

FRICK JEAN-CLAUDE, Comparis-Datenvertrauensstudie 2024 (zit. Comparis, S.).

GASSNER ULRICH M., Forschung und Innovation im europäischen Gesundheitsdatenraum - Zur künftigen Sekundärnutzung elektronischer Gesundheitsdaten, DuD 12/2022, S. 739-746 (zit. GASSNER, S.).

GASSNER ULRICH M., Informed Consent und Digital Health, in: Stiftung Datenschutz, Big Data und E-Health (Berlin 2017) S. 35-58 (zit. GASSNER Informed Consent, S.).

GUIRGUIS KATHARINA/ PLEGER LYN E./ DIETRICH SIMONE/MERTES ALEXANDER/BRÜESCH CAROLINE, Datenschutz in der Schweiz – eine quantitative Analyse der gesellschaftlichen Bedenken und Erwartungen an den Staat, YSAS 12(1)/2021 S. 16-30 (zit. GUIRGUIS *et al.*, S.).

HEIDELBERGER ANJA/MEYER LUZIUS/SCHNEUWLY JOËLLE/SCHUBIGER MAXIMILIAN/TÖNY NIC, Ausgewählte Beiträge zur Schweizer Politik - Dossier: Digitalisierung im Gesundheitswesen 2010-2024, Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern (Bern 2024) (zit. HEIDELBERGER *et. al.*, S.).

HERMANN MICHAEL/BÜHLER GORDON, Monitor „Datengesellschaft und Solidarität“ - Einstellung und Verhalten der Schweizer Bevölkerung 2023 (Mai 2023) (zit. HERMANN/BÜHLER, S.).

HORNSTEIN DANIELLE/NAKAR SHARON/WEINBERGER SARA/GREENBAUM DOV, More nuanced informed consent is not necessarily better informed consent, American Journal of Bioethics 9/2015 S. 51-53 (zit. HORNSTEIN *et. al.*, S.).

HUMMEL PATRIK/BRAUN MATTHIAS/AUGSBERG STEFFEN/V. ULMENSTEIN ULRICH/DABROCK PETER, Dynamic Consent als Umsetzungsmechanismus von Datensouveränität, in: HUMMEL PATRIK/BRAUN MATTHIAS/AUGSBERG STEFFEN/V. ULMENSTEIN ULRICH/DABROCK PETER,

Datensouveränität – Governance-Ansätze für den Gesundheitsbereich (Wiesbaden 2021)
S. 13-20 (zit. HUMMEL *et. al.*, S.).

JARCHOW THOMAS/ESTERMANN BEAT, Big Data: Chancen, Risiken und Handlungsbedarf des Bundes
- Ergebnisse einer Studie im Auftrag des Bundesamts für Kommunikation (Bern 2015)
(zit. JARCHOW/ESTERMANN, S.).

JUNOD VALÉRIE/ELGER BERNICE, Données codées, non-codées ou anonymes - des choix compliqués
dans la recherche médicale rétrospective, Jusletter 10. Dezember 2018 S. 1-26 (zit. JUNOD/
ELGER, Rz.).

LESCH WIEBKE/RICHTER GESINE/ SEMLER SEBASTIAN C., Daten teilen für die Forschung: Einstellungen und Perspektiven zur Datenspende in Deutschland, in: RICHTER GESINE (Hrsg.)/LOH WULF (Hrsg.)/BUYX ALENA (Hrsg.)/GRAF VON KIELMANSEGG SEBASTIAN (Hrsg.), Datenreiche Medizin und das Problem der Einwilligung - Ethische, rechtliche und sozialwissenschaftliche Perspektiven (Berlin 2022) S. 211-224 (zit. LESCH/RICHTER/SEMLER, S.).

KAYE JANE/ WHITLEY EDGAR A./ LUND DAVID/MORRISON MICHAEL/TEARE HARRIET/MEHLHAM KAREN, Dynamic consent - a patient interface for twenty-first century research networks, EJHG 23/2015 S. 141-146 (zit. KAYE *et al.*, S.).

KLAUS SAMUEL/THOMANN KENZO, DSG 6 – Art. 6 Grundsätze, in: BIERI ADRIAN (Hrsg.)/POWELL JULIAN (Hrsg.), OFK DSG Kommentar (Zürich, 2023) S.149-170 (zit. KLAUS/THOMANN, Rz.).

MAUSBACH JULIAN, Dynamische Einwilligung zur Forschung am Menschen, Jusletter 28. Januar 2019 S. 1-27 (zit. MAUSBACH, Rz.).

MÄTZLER SAMUEL, Datenschutz in der (Human-)Forschung: Grundlagen und Probleme bei der Sekundärnutzung von Personendaten, Jusletter 30. Januar 2023 S. 1-22 (zit. MÄTZLER, Rz.).

MOLNÁR-GÁBOR FRUZSINA, Ausgestaltung der Einwilligung in die Datenspende für die Gesundheitsforschung - Der Blick auf Europa, DuD 12/2021 S.799-805 (zit. MOLNÁR-GÁBOR, S.).

PETRI THOMAS, Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten - Zum Vorschlag der EU-Kommission für einen Europäischen Gesundheitsdatenraum, DuD 7/2022, S. 413-418 (zit. PETRI, S.)

PLOUG THOMAS/HOLM SØREN, Meta consent - A flexible solution to the problem of secondary use of health data, Bioethics 30(9)/2016, S. 721-732 (zit. PLOUG/HOLM, S.).

RICHTER GESINE/BUYX ALENA, Breite Einwilligung (broad consent) zur Biobank-Forschung – die ethische Debatte, Ethik Med 28/2016 S. 311-325 (zit. RICHTER/BUYX, S.).

RICHTER GESINE/TRIGUIC NOURANE/CALIEBE AMKE/KRAWCZAK MICHAEL, Attitude towards consent-free research use of personal medicaldata in the general German population, Heлиyon 10/2024 S. 1-9 (zit. RICHTER *et al.*, S.).

ROITINGER STEFANIE/RACHAMIN YAEL/ANTONOV JANINE, Chancen und rechtliche Herausforderungen bei der Nutzung von Real World Data, LSR 2022 S. 3-6 (zit. ROITINGER/RACHAMIN/ANTONOV, S.).

ROSENTHAL DAVID, Die rechtlichen und gefühlten Grenzen der Zweitnutzung von Personendaten, sic! 2021 S. 168-175 (zit. ROSENTHAL, S.).

RUDIN BEAT, HFG 32 – Humanforschungsgesetz (HFG) Bundesgesetz vom 30. September 2011 über die Forschung am Menschen, in: RÜTSCHE BERNHARD (Hrsg.), Stämpfli's Handkommentar (Bern 2015) S. 488-495 (zit SHK Art. 32 HFG, Rz.).

SCHMITT TUGCE/COSGROVE SHONA/PAJIC VANJA/PAPADOPOULOS KIMON/GILLE FELIX, Was ist für die Schaffung eines europäischen Gesundheitsdatenraums nötig? Internationale Ambitionen und nationale Realitäten, ZEFQ 179/2023, S. 1-7 (zit. SCHMITT, S.).

SCHÖNBÄCHLER MATTHIAS R./MAURER-LAMBOU URS/KUNZ SIMON, Art. 1 DSG - Datenschutzgesetz/Öffentlichkeitsgesetz 2024, in: BLECHTA GABOR P. (Hrsg.)/BÜHLER ROBERT (Hrsg.)/BÜHLMANN LUKAS (Hrsg.), Basler Kommentar (Basel 2024) S. 1-14 (zit. BSK Art. 1 DSG, Rz.).

SCHWEIZER RAINER J., Digitalisierung im Gesundheitswesen - Kranke und pflegebedürftige Menschen sind keine blassen Objekte der Digitalisierungen, *digma* 2020 S. 204-213 (zit. SCHWEIZER, S.).

SPRECHER FRANZISKA, Datenschutz im Gesundheitsbereich: Aktuelle Entwicklungen, in: KIESER UELI (Hrsg.)/PÄRLI KURT (Hrsg.)/UTTINGER URSULA (Hrsg.), Datenschutzttagung 2018 – Ein Blick auf aktuelle Rechtsentwicklungen (Zürich/St.Gallen 2019) S. 137-150 (zit. SPRECHER Datenschutz, S.).

SPRECHER FRANZISKA, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, *ZBJV* 154/2018 S. 482-552 (zit. SPRECHER Datenschutz und Big Data, S.).

SPRECHER FRANZISKA, Digitalisierung im Gesundheitswesen – Zum Umgang mit Gesundheitsdaten und zur Schaffung von Gesundheitsdatenräumen, in: EPINEY ASTRID/ HAVALDA STEFANIE/ ZLATESCU PETRU E. (Hrsg.), Datenschutz und Gesundheitsschutz (Zürich 2023) S. 29-44 (zit. SPRECHER Gesundheitsdatenräume, S.).

SPRECHER FRANZISKA, Regulierung von Gesundheitsdaten und Gesundheitsdatenräumen, *MedR* 40/2020, S. 829-838 (zit. SPRECHER, S.).

SPRECHER FRANZISKA, Sozialpflichtigkeit von Gesundheitsdaten - Mehr Daten für die Forschung dank einer Widerspruchslösung für Gesundheitsdaten?, *digma* 2019 S. 184-187 (zit. SPRECHER Sozialpflichtigkeit, S.).

SPRECHER FRANZISKA/HOFER ALINE, Das elektronische Patientendossier, in: EPINEY ASTRID (Hrsg.)/SANGSUE DÉBORAH (Hrsg.), Datenschutz und Gesundheitsschutz (Zürich 2019) S. 43-78 (zit. SPRECHER/HOFER, S.).

STÖCKLI ANDREAS /GRÜNINGER CHRISTOPH, Art. 34 DSG, in: BLECHTA GABOR P. (Hrsg.)/VASELLA DAVID (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz 2024 (Basel 2024) S. 1-9 (zit BSK Art. 34 DSG, Rz.).

PAULI-MAGNUS CHRISTINE, Entwicklung und Umsetzung eines schweizweiten elektronischen Generalkonsents für die Weiterverwendung von Patientendaten und –proben (zit. SPHN E-General Consent).

WALDMEIER STEFANIE-DANIELA, Informationelle Selbstbestimmung - ein Grundrecht im Wandel? (Diss., Basel 2001, Bern 2015) (zit. WALDMEIER, S.).

WIDMER BARBARA, ePatientendossier und Datenschutz, digma 2017 S.160-168 (zit. WIDMER Patientendossier, S.).

WIDMER BARBARA, Ist Einwilligung gleich Einwilligung?, digma 2017 S.188-189 (zit. WIDMER Einwilligung, S.).

WIDMER URSULA/BÜHLMANN LUKAS ET AL., Gutachten Sekundärnutzung Gesundheitsdaten (Zürich 2022) (zit. WIDMER/BÜHLMANN *et al.*, S.).

Materialienverzeichnis

Bericht des Bundesrates in Erfüllung des Postulates 15.4225 Humbel vom 18. Dezember 2015, S. 1-73 (zit. Bericht Po. Humbel, S.).

Bericht des UVEK und des EDA an den Bundesrat „Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung“ vom 30. März 2022, S. 1-65 (zit. Bericht Datenräume, S.).

Botschaft zum Bundesgesetz über das elektronische Patientendossier (EPDG) vom 29. Mai 2013, BBI 2013 S. 5321- 5416 (zit. Botschaft EPDG, S.).

Botschaft zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise vom 22. November 2023 BBI 2023 S. 2842ff. (zit. Botschaft E-ID, S.).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017 BBI 2017 S. 6941- 7192 (zit. Botschaft DSG, S.).

Botschaft zum Verpflichtungskredit für ein Programm zur Förderung der digitalen Transformation im Gesundheitswesen für die Jahre 2025–2034 vom 22. November 2023 BBI 2023 S. 2908- 2986 (zit. Botschaft DigiSanté, S.).

Diskussionspapier „Schweizer Datenökosystem“ vom 31. Januar 2023 (zit. Diskussionspapier Datenökosystem).

Erläuternder Bericht Teilrevision des Ausführungsrechts zum Bundesgesetz über die Forschung am Menschen (HFG) vom 26. April 2023 (zit. Bericht Teilrevision Ausführungsrecht HFG, S.).

Erläuternder Bericht zur Änderung des Bundesgesetzes über das elektronische Patientendossier (EPDG) (Umfassende Revision) vom 21. Juni 2023 (zit. Bericht Revision EPDG, S.).

Faktenblatt „Europäischer Raum für Gesundheitsdaten“ vom 22.05.2024 (zit. Faktenblatt EHDS).

Gesetzgebungsleitfaden Datenschutz „Auswirkungen des neuen Datenschutzgesetzes auf die Erarbeitung von Rechtsgrundlagen“ (zit. Gesetzgebungsleitfaden DSG, S.).

Interpellation RIEDER (20.4173) „Nationale Datenkompetenzkampagne. Datenkompetenz (Data-Literacy) ist gefragt“ (zit Ip. Data-Literacy).

Motion Kommission für soziale Sicherheit und Gesundheit NR (22.3016) „Implementierung einer nachhaltigen Data-Literacy-Strategie in der digitalen Transformation des Gesundheitswesens“ (zit. Mo. Data-Literacy).

Motion Kommission für Wissenschaft, Bildung und Kultur SR (22.3890) „Rahmengesetz für die Sekundärnutzung von Daten“ (zit. Mo. Kom. Wiss.).

Postulat BELLAICHE (20.3700) „Nutzung anonymisierter persönlicher Daten im öffentlichen Interesse. Prüfung der Machbarkeit einer freiwilligen Datenspende“ (zit. Po. BELLAICHE).

Postulat HUMBEL (15.4225) „Bessere Nutzung von Gesundheitsdaten für eine qualitativ hochstehende und effiziente Gesundheitsversorgung“ (zit. Po. HUMBEL).

Strategie eHealth Schweiz 2.0 2018-2024 vom 14. Dezember 2018 (zit. Strategie eHealth, S.).

Hilfsmittelverzeichnis

Perplexity AI (Version 2024) von Perplexity Labs, Inc., die Verwendung erfolgte ausschliesslich für redaktionellen Änderungen im Sinne eines digitalen Lektorats <<https://www.perplexity.ai>>.

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
Aufl.	Auflage
BAG	Bundesamt für Gesundheit
BBI	Bundesblatt
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
BSK	Basler Kommentar
bspw.	beispielsweise
BV	Bundesverfassung
BVGer	Bundesverwaltungsgericht
bzgl.	bezüglich
bzw.	beziehungsweise
d.h.	das heisst
digma	Zeitschrift für Datenrecht und Informationssicherheit
Diss.	Dissertation
DSG	Bundesgesetz über den Datenschutz
DSGVO	Europäische Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit (Fachzeitschrift)
E.	Erwägung
EHDS	European Health Data Space
E-ID	elektronische Identität
EJHG	European Journal of Human Genetics
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten
EPD	Elektronisches Patientendossier
EPDG	Bundesgesetz über das elektronische Patientendossier
EPDV	Verordnung über das elektronische Patientendossier
et al.	et alii (und andere)
etc.	et cetera
Ethik Med	Ethik in der Medizin (Zeitschrift)
EU	Europäische Union
f./ff.	und folgende (Seite / Seiten)
f./ff.	und folgende (Seite / Seiten)
g.M.	gleicher Meinung

GesR	GesundheitsRecht - Zeitschrift für Arztrecht, Kranknehausrecht, Apotheken- und Arzneimittelrecht
grds.	ätzlich
HFG	Humanforschungsgesetz
Hrsg.	Herausgeber
inkl.	inklusive
Ip.	Interpellation
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
J Med Internet Res.	Journal of Medical Internet Research
Kap.	Kapitel
KI	Künstliche Intelligenz
Kom.	Komission
KRG	Krebsregistrierungsgesetz
lit.	litera
LSR	Life Science Recht – Juristische Zeitschrift für Pharma, Biotech und Medtech
MedR	Medizinrecht (Fachzeitschrift)
mind.	mindestens
Mo.	Motion
Nr.	Nummer
OFK	Orell Füssli Kommentar
OR	Obligationenrecht
RWD	Real World Data
Rz.	Randziffer(n)
S.	Seite
SAMW	Schweizerische Akademie der Medizinischen Wissenschaften
SGK	St.Galler Kommentar
SHK	Stämpfli's Handkommentar
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SPHN	Swiss Personalized Health Network
SR	Systematische Sammlung des Bundesrechts
u.a.	unter anderem
v.a.	Vor allem
vgl.	Vergleiche

Wiss.	Wissenschaft
z.B.	zum Beispiel
z.G.	zum Ganzen
YSAS	Yearbook of Swiss Administrative Sciences
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZEFQ	Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen
ZGB	Schweizerisches Zivilgesetzbuch
zit.	zitiert
Ziff.	Ziffer(n)

Inhaltsverzeichnis

Erlassverzeichnis.....	I
Literaturverzeichnis	III
Materialienverzeichnis	X
Hilfsmittelverzeichnis	XII
Abkürzungsverzeichnis	XIII
1 Einleitung.....	1
2 Die Sekundärnutzung von Gesundheitsdaten auf Bundesebene	2
<i>2.1 Kompetenzverteilung im Datenschutz.....</i>	<i>2</i>
<i>2.2 Das Bundesgesetz über den Datenschutz und die Sekundärnutzung von Daten.....</i>	<i>2</i>
<i>2.2.1 Persönlicher Geltungsbereich.....</i>	<i>3</i>
<i>2.2.2 Sachlicher Geltungsbereich.....</i>	<i>3</i>
<i>2.2.3 Räumlicher Geltungsbereich</i>	<i>4</i>
<i>2.2.4 Gesundheitsdaten</i>	<i>4</i>
<i>2.2.5 Primär- vs. Sekundärnutzung</i>	<i>5</i>
<i>2.2.6 Anforderungen an die Sekundärnutzung.....</i>	<i>5</i>
<i>2.3 Spannungsfeld Forschungsfreiheit und digitale Selbstbestimmung.....</i>	<i>8</i>
3 Aktuelle Trends und Regulierungsbemühungen in Bezug auf die Sekundärnutzung von Gesundheitsdaten.....	10
<i>3.1 Ausgangslage</i>	<i>10</i>
<i>3.1.1 Real World Data (RWD) und Big Data</i>	<i>10</i>
<i>3.1.2 Einstellung der Schweizer Bevölkerung zur Gesundheitsdatennutzung.....</i>	<i>11</i>
<i>3.2 Entwicklungen im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten in der Schweiz.....</i>	<i>12</i>
<i>3.2.1 Strategie Digitale Schweiz im Gesundheitsbereich</i>	<i>12</i>
<i>3.2.2 Rahmengesetz für die Sekundärnutzung von Daten</i>	<i>15</i>
<i>3.2.3 DigiSanté</i>	<i>16</i>
<i>3.3 Entwicklungen im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten in der EU</i>	<i>16</i>
<i>3.3.1 European Health Data Space (EHDS).....</i>	<i>16</i>
<i>3.3.2 Zugang zum EHDS durch die Schweiz.....</i>	<i>17</i>
<i>3.3.3 Gesundheitsdatenräume in der Schweiz.....</i>	<i>18</i>
<i>3.4 Schlussfolgerung zu den künftigen Anforderungen an die Regulierung der Sekundärnutzung von Gesundheitsdaten</i>	<i>18</i>

4 Die Einwilligung gemäss DSG	20
<i>4.1 Bedeutung der Einwilligung.....</i>	20
4.1.1 Öffentliches Recht.....	20
4.1.2 Privatrecht	21
<i>4.2 Anforderungen an die Einwilligung.....</i>	21
4.2.1 Angemessene Information.....	21
4.2.2 Freiwilligkeit	24
4.2.3 Weitere Anforderungen an die Einwilligung	24
<i>4.3 Anforderungen an die Einwilligung bei der Bearbeitung von Gesundheitsdaten</i>	26
<i>4.4 Kritik im Zusammenhang mit der datenrechtlichen Einwilligung</i>	27
4.4.1 Limitationen des Opt-in Modells	27
4.4.2 Unsicherer Rechtsrahmen	27
4.4.3 Herausfordernde Umsetzung der Einwilligungsanforderungen.....	28
4.4.4 Schwächung des Datenschutzes	28
4.4.5 Grenzen des Einwilligungskonzepts im digitalen Zeitalter.....	29
4.4.6 Fazit für die künftige Ausgestaltung der Einwilligung	29
5 Zukünftige Modelle und Regulierungsansätze der Einwilligung	30
<i>5.1 Ausgangslage</i>	30
<i>5.2 Einwilligungsmodelle.....</i>	30
5.2.1 <i>broad consent</i>	30
5.2.2 <i>dynamic consent</i>	33
5.2.3 <i>meta consent</i>	35
5.2.4 Datentreuhänder	37
5.2.5 Datenspende	39
<i>5.3 Regulierungsansätze in Bezug auf die Einwilligung.....</i>	40
5.3.1 Wechsel zum Opt-out.....	41
5.3.2 Stärkung der Datenkompetenz	42
5.3.3 Transparenz durch Datenbrief.....	43
5.3.4 Modifikation der Anforderungen an eine gültige Einwilligung.....	43
5.3.5 Steigerung der Wirksamkeit über verlässliche Governance-Strukturen	45
<i>5.4 Einwilligung und Sekundärdatennutzung im EHDS.....</i>	46
<i>5.5 Diskussion</i>	46
5.5.1 Das Kaskadenmodell als Vorbild für die künftige Einwilligungspraxis.....	47
5.5.2 Chancen und Herausforderungen in der Umsetzung der Kaskadeneinwilligung	47
6 Zusammenfassung und Ausblick	49

1 Einleitung

"No data, no health" - verdeutlicht eine zentrale Herausforderung des Gesundheitswesens im Zeitalter der Digitalisierung. Datenbasierte Innovationen in Forschung, Medizin und Pflege entwickeln sich dynamisch und eröffnen signifikante Potenziale für die Optimierung der Lebens- und Versorgungsqualität. Exemplarisch sind Forschungsvorhaben im Rahmen der personalisierten Medizin, KI-gestützte Präzisionsdiagnostik oder Effizienzsteigerungen durch optimierte Behandlungsprozesse zu nennen. Bei aller Diversität dieser Ansätze besteht eine fundamentale Gemeinsamkeit: Sämtliche Vorhaben sind für ihre Realisierung auf grosse Mengen von Gesundheitsdaten angewiesen. Die Verfügbarkeit dieser Daten wird dabei massgeblich durch den geltenden Rechtsrahmen determiniert. "No data, no health" zeichnet sich somit auch als bedeutsame juristische Herausforderung ab.

Die Bearbeitung von Gesundheitsdaten ist durch die komplexe Struktur des schweizerischen Datenschutzrechts und dessen zahlreiche spezialgesetzliche Regelungen auf Bundes- und Kantonsebene stark fragmentiert. Die Sekundärnutzung dieser Daten erfolgt ohne spezifisches Rahmengesetz und führt zu erheblicher Rechtsunsicherheit, weshalb in der Praxis meist auf das Instrument der Einwilligung zurückgegriffen wird, um strafrechtliche Risiken zu minimieren.

Die fortschreitende Digitalisierung stellt das klassische Einwilligungskonzept hinsichtlich seiner Fähigkeit zur Gewährleistung digitaler Selbstbestimmung zunehmend in Frage. Die vorliegende Arbeit analysiert daher Regulierungsmodelle und -ansätze im Bereich der datenschutzrechtlichen Einwilligung, die eine Balance zwischen effizienter Sekundärnutzung von Gesundheitsdaten und der Wahrung digitaler Selbstbestimmung der betroffenen Personen ermöglichen.

Ausgangspunkt dieser Arbeit bildet die aktuelle bundesrechtliche Gesetzgebung zur Sekundärnutzung von Gesundheitsdaten. Als erster Schritt erfolgt eine Konkretisierung des rechtlichen Bezugsrahmens sowie eine Präzisierung der zentralen Begrifflichkeiten. Simultan werden die normativen Anforderungen an die Sekundärnutzung von Gesundheitsdaten systematisch dargelegt und die damit verbundenen rechtlichen Herausforderungen erörtert. Hierauf folgt eine kritische Auseinandersetzung mit Entwicklungstendenzen, gesellschaftlichen Haltungen sowie nationalen und internationalen Regulierungsinitiativen im Kontext der Sekundärdatennutzung. Das gewählte Vorgehen zielt darauf ab, aktuelle Entwicklungen zu identifizieren und zentrale Aspekte in die nachfolgende Analyse der Einwilligungsmodelle zu integrieren. Nachfolgend werden die bestehende Einwilligungspraxis sowie deren rechtlichen Vorgaben einer eingehenden Prüfung unterzogen und kritisch gewürdigt. Auf der Grundlage von gewonnenen Erkenntnissen erfolgt abschliessend eine Gegenüberstellung potenzieller Einwilligungsmodelle und spezifischer Regulierungsansätze unter besonderer Berücksichtigung der digitalen Selbstbestimmung.

Die Ausführungen basiert auf der Auswertung einschlägiger Fachliteratur, amtlicher Materialien, nationaler und internationaler Fachbeiträgen aus Medizin und Recht sowie wissenschaftlichen Studien.

2 Die Sekundärnutzung von Gesundheitsdaten auf Bundesebene

Die vorliegende Arbeit betrachtet die Rolle der Einwilligung im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten. Daher gilt es vordergründig das Begriffsverständnis der Sekundärnutzung sowie jenes der Gesundheitsdaten zu definieren und den dafür betrachteten Rechtsrahmen zu konkretisieren.

2.1 Kompetenzverteilung im Datenschutz

Die Bundesverfassung weisst dem Bund in Bezug auf den Datenschutz keine direkte Regelungskompetenz zu. Soweit keine verfassungsrechtliche Kompetenz des Bundes vorliegt, sind die Kantone ermächtigt, eigene datenschutzrechtliche Bestimmungen zu erlassen. Kommunale Organe unterstehen bei der Datenverarbeitung dem kantonalen Recht, vorbehaltlich bundesrechtlicher Spezialvorschriften. Der Bund hat im Rahmen seiner eigenen gesetzgeberischen Tätigkeit die kantonale Organisationsautonomie zu wahren.¹ Die verfassungsrechtliche Kompetenzverteilung im Datenschutzrecht zwischen Bund und Kantonen führt zu einer fragmentierten Rechtslandschaft, die rechtliche Unsicherheiten bei der Sekundärdatennutzung begünstigt.² Der Umfang dieser Masterarbeit erlaubt keine vollständige Analyse aller relevanten Rechtsgrundlagen. Die nachfolgenden Ausführungen beschränken sich daher auf die bунdesrechtlichen Regelungen zur Sekundärdatennutzung.

2.2 Das Bundesgesetz über den Datenschutz und die Sekundärnutzung von Daten

Das Datenschutzgesetz des Bundes fungiert als eidgenössischer Rahmenerlass im Bereich des Datenschutzes, welcher auch die Sekundärnutzung von Daten miteinschliesst. Es dient als Umsetzung des Grundrechtschutzes auf informelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV und gewährleistet den betroffenen Personen entsprechende Rechtsansprüche. Der Fokus liegt dabei nicht auf dem Schutz der Daten selbst, sondern auf dem Schutz der Persönlichkeit und der Grundrechte natürlicher Personen bei der Datenverarbeitung. Das DSG regelt sektorübergreifend sowohl die öffentlich-rechtlichen als auch die privatrechtlichen Rechtsverhältnisse.³ Auch bei Vorrang spezialgesetzlicher Bestimmungen behält das DSG seine subsidiäre Geltung, insbesondere wenn sektorspezifische Vorschriften eine Rechtsfrage nicht abschliessend regeln.⁴

¹ Botschaft DSG, S. 7186f.; Gesetzgebungsleitfaden DSG, S.4.

² WIDMER/BÜHLMANN *et al.*, S. 1.

³ Art. 1 DSG; Botschaft DSG, S. 7006;7186; BSK Art. 1 DSG, Rz. 3; SGK Art. 13 BV, Rz. 76; WIDMER/BÜHLMANN *et al.*, S. 33.

⁴ WIDMER/BÜHLMANN *et al.*, S. 33.

2.2.1 Persönlicher Geltungsbereich

Das DSG schützt natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten. Juristische Personen fallen nicht in diesen passiven Schutzbereich. Als Normadressaten sind jedoch sowohl natürliche als auch juristische Personen neben den Bundesbehörden zur Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet.⁵ Lediglich die Kantone sind vom Anwendungsbereich des DSG ausgenommen.⁶ Als Bundesorgane gelten Behörden und Dienststellen des Bundes sowie Personen, die mit öffentlichen Aufgaben des Bundes betraut sind. Besondere Bedeutung kommt der Unterscheidung zwischen privatrechtlich handelnden Institutionen und privaten Institutionen mit übertragenen öffentlichen Aufgaben zu. Letztere unterliegen als Bundesorgane strenger datenschutzrechtlichen Anforderungen bei der Datenverarbeitung.⁷

2.2.2 Sachlicher Geltungsbereich

Das DSG erfasst ausschliesslich Sachverhalte, die mit der Bearbeitung von Personendaten im Zusammenhang stehen:

a) „Bearbeiten“

Der datenschutzrechtliche Bearbeitungsbegriff des DSG ist geprägt durch eine weites sowie umfassendes Verständnis. Exemplarisch bezeichnet Art. 5 lit. d DSG jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren. Dies beinhaltet insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.⁸ Es handelt sich dabei nicht um eine abschliessende Aufzählung von Bearbeitungsschritten. Angesichts der rasch voranschreitenden technologischen Entwicklungen sind auch sämtliche künftige Datenbearbeitungsvorgänge auch von dieser Definition implizit erfasst.⁹

b) Personendaten

Personendaten umfassen sämtliche Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.¹⁰ Der Begriff "Angaben" schliesst sowohl Tatsachenfeststellungen als auch

⁵ Als verfassungsrechtliche Grundlage für die Regelung privatrechtlicher Sachverhalte wird die allgemeine Rechtssetzungskompetenz des Bundes nach Art. 122 BV im Zivilrecht herangezogen. Im öffentlichen Recht bildet die organisatorische Zuständigkeit nach Art. 173 Abs. 2 BV die Regelungskompetenz.

⁶ BSK Art. 2 DSG, Rz. 1-16.

⁷ WIDMER/BÜHLMANN *et al.*, S. 31; EPINEY/NÜESCH/ROVELLI, S.70.

⁸ Art. 5 lit. d DSG.

⁹ BSK Art. 5 DSG, Rz. 98.

¹⁰ Art. 5 lit. a DSG.

Werturteile ein, sofern diese in dokumentierter Form vorliegen.¹¹ Der Personenbezug kann dabei direkt oder indirekt bestehen. Eine Person gilt als bestimmbar, wenn ihre Identität aus den vorliegenden Informationen, dem Kontext oder durch Kombination verschiedener Angaben ermittelt werden kann.¹² Daten, die keine Rückschlüsse auf natürliche Personen zulassen, werden nicht als Personendaten klassifiziert. Dies gilt insbesondere für anonymisierte oder pseudonymisierte Datensätze, deren Zuordnung zu einer bestimmten Person entweder ausgeschlossen ist oder einen unverhältnismässigen Aufwand erfordern würde. Das Datenschutzgesetz findet auf anonymisierte oder pseudonymisierte Daten keine Anwendung. Lediglich die Verfahren zur Unkenntlichmachung der Personendaten unterliegen den DSG-Bestimmungen.¹³

Die Anonymisierung muss dem Kriterium der Irreversibilität entsprechen und angesichts des aktuellen Stands der Technik dauerhaft sein. Die fortschreitende technologische Entwicklung erfordert eine regelmässige Überprüfung der Anonymisierungsmassnahmen, um eine persönlichkeitsverletzende Datenbearbeitung auszuschliessen. Diese kontinuierliche Anpassungsnotwendigkeit schafft rechtliche Unsicherheiten bei der Nutzung anonymisierter Daten.¹⁴

2.2.3 Räumlicher Geltungsbereich

Gemäss Art. 3 Abs. 1 DSG fokussiert sich der räumliche Geltungsbereich auf alle datenschutzrechtlichen Sachverhalte, die in der Schweiz Wirkungen entfalten, auch wenn deren Veranlassung im Ausland erfolgt ist.

2.2.4 Gesundheitsdaten

Das Datenschutzgesetz klassifiziert Gesundheitsdaten als besonders schützenswerte Personendaten¹⁵ und unterwirft ihre Verarbeitung strenger Anforderungen als gewöhnliche personenbezogene Informationen. Eine explizite Definition des Begriffs "Gesundheitsdaten" fehlt im Gesetz.

Nach h. L. umfassen Gesundheitsdaten sämtliche Informationen, die Rückschlüsse auf den physischen oder psychischen Gesundheitszustand einer Person ermöglichen. Dies umfasst sodann auch Angaben über das Beziehen von Gesundheitsleistungen, aus welchen Informationen über den Gesundheitszustand ersichtlich sind. Gesundheitsdaten stellen weitestgehend einen medizinischen Befund dar, welcher sich für die Betroffenen negativ auswirken könnte.¹⁶

¹¹ BSK Art. 5 DSG, Rz. 15f.; EPINEY/NÜESCH/ROVELLI, S.75.

¹² BSK Art. 5 DSG, Rz. 25-27.

¹³ Botschaft DSG, S. 7019.

¹⁴ WIDMER/BÜHLMANN *et al.*, S. 10.

¹⁵ Art. 5 lit. c Ziff. 2 DSG.

¹⁶ BSK Art. 5 DSG, Rz. 60; 63; SPRECHER, S. 833; SPRECHER Gesundheitsdatenräume, S. 29.

2.2.5 Primär- vs. Sekundärnutzung

Bevor die Anforderungen an die Sekundärnutzung von Gesundheitsdaten thematisiert werden, ist es für das weitere Verständnis zentral die Primär- von der Sekundärnutzung voneinander abzugrenzen. In der Literatur finden sich verschiedene teils uneinheitliche Definitionsansätze zu den beiden Nutzungsarten. Diese Arbeit folgt dem Begriffsverständnis nach SPRECHER. Demnach handelt es sich bei der Primärnutzung um die ursprüngliche Datenerhebung zu einem vordefinierten oder erkennbaren Bearbeitungszweck. Die Sekundärnutzung hingegen bezeichnet die Weiterverwendung dieser Daten, ungeachtet des originären Erhebungsgrunds.¹⁷ Entgegen der verbreiteten Annahme beschränkt sich die Sekundärnutzung von Gesundheitsdaten nicht ausschliesslich auf Forschungszwecke.¹⁸ Ihr Anwendungsbereich erstreckt sich vielmehr auf verschiedene Sektoren des Gesundheitswesens, insbesondere die Optimierung der Versorgungsqualität und gesundheitsökonomische Analysen.

2.2.6 Anforderungen an die Sekundärnutzung

Im Kontext der Sekundärnutzung von Daten ist eine differenzierte Betrachtung der Bearbeitungsanforderung notwendig. Einerseits sind die allgemeingültigen Prinzipien der Datenbearbeitung zu berücksichtigen, andererseits bedarf es einer spezifischen Analyse der rechtlichen Voraussetzungen für die Weiterverwendung von Gesundheitsdaten. Zudem variieren die gesetzlichen Vorgaben an die Sekundärdatennutzung, abhängig davon, ob die Bearbeitung durch private Akteure oder Bundesorgane vorgenommen wird.

a) *Grundsätze der Datenbearbeitung*

Die Grundsätze an die Datenbearbeitung werden durch Art. 6 DSG vorgegeben. Diese gelten für die Bearbeitung von Personendaten in sämtlichen Gesellschaftsbereichen, insbesondere auch im Gesundheitssektor.

Rechtmässigkeit (Art. 6 Abs. 1 DSG)

Die Beschaffung und Bearbeitung von Personendaten muss rechtmässig erfolgen. Allerdings führt nicht jeder Gesetzesverstoss automatisch zu einer Verletzung des Rechtmässigkeitsgrundsatzes. Nach h. L. und der Rechtsprechung des BGer liegt eine Verletzung nur dann vor, wenn die missachtete

¹⁷ Die Begriffe „Sekundärnutzung“ und „Weiterverwendung“ werden in der vorliegenden Arbeit als Synonyme verwendet; SPRECHER Datenschutz und Big Data, S. 507; g.M. MÄTZLER, Rz. 1.

¹⁸ vgl. BUCHHOLZ *et al.*, S. 472; MOLNÁR-GÁBOR, S. 800; ROITINGER/RACHAMIN/ANTONOV, S. 4.

Rechtsnorm explizit dem Persönlichkeitsschutz dient, wie dies bspw. bei den Bestimmungen des Datenschutzgesetzes der Fall ist.¹⁹

Eine rechtmässige Sekundärnutzung von Daten setzt eine gesetzeskonforme ursprüngliche Datenerhebung (Primärnutzung) voraus. Diese lässt sich durch schriftliche Dokumentationen zum Erhebungszeitpunkt nachweisen. Die Praxis zeigt jedoch, dass solche Dokumentationen häufig unzureichend sind und damit die Rechtmässigkeit der Datenweiterverwendung gefährden.²⁰

Treu und Glauben (Art. 6 Abs. 2 DSG)

Die Datenverarbeitung nach Treu und Glauben stellt eine Generalklausel dar, die greift, wenn andere Bearbeitungsgrundsätze nicht anwendbar sind. Im Kontext der Sekundärnutzung beschränkt sich ihre Bedeutung auf die grundsätzlichen Anforderungen an Loyalität und Vertrauenswürdigkeit im Geschäftsverkehr.²¹

Verhältnismässigkeit (Art. 6 Abs. 2 und 4 DSG)

Der Grundsatz der Verhältnismässigkeit verpflichtet private Akteure bei der Datenverarbeitung zur Einhaltung der Kriterien der Geeignetheit, Erforderlichkeit und Zumutbarkeit. Für Bundesorgane ergibt sich diese Verpflichtung bereits aus Art. 5 Abs. 2 BV. Eine verhältnismässige Datenverarbeitung muss drei Voraussetzungen erfüllen:

- Sie ist zur Erreichung des beabsichtigten Zwecks geeignet
- Sie stellt das mildeste verfügbare Mittel dar
- Sie ist für die betroffene Person zumutbar

Die Prüfung der Verhältnismässigkeit erfolgt einzelfallbezogen anhand objektiver Kriterien.²²

Im Kontext der Sekundärnutzung erweist sich die Wahrung der Verhältnismässigkeit als komplexe Aufgabe. Dies gilt besonders für Big Data-Anwendungen²³, bei denen eine fundierte einzelfallbezogene Verhältnismässigkeitsprüfung aufgrund der Datenmenge kaum durchführbar ist.²⁴

Zweckbindung (Art. 6 Abs. 3 DSG)

Die Zweckbindung erfordert, dass sowohl die Datenbeschaffung als auch der Bearbeitungszweck für die betroffene Person erkennbar sind. Diese Voraussetzung ist erfüllt, wenn die betroffene Person

¹⁹ BSK Art. 6 DSG, Rz. 19ff.; BÜHLMANN/SCHÜEPP, Rz. 135; BVGer in A-3548/2018; EPINEY/NÜESCH/ROVELLI, S. 84ff.; WIDMER/BÜHLMANN *et al.*, S. 37.

²⁰ WIDMER/BÜHLMANN *et al.*, S. 37-38.

²¹ BSK Art. 6 DSG, Rz. 49; EPINEY/NÜESCH/ROVELLI, S. 88.

²² BSK Art. 6 DSG, Rz. 51ff.; EPINEY/NÜESCH/ROVELLI, S. 91.

²³ siehe Kap. 3.1.1.

²⁴ WIDMER/BÜHLMANN *et al.*, S. 54.

informiert wurde, eine gesetzliche Grundlage besteht oder der Zweck aus den Umständen eindeutig hervorgeht. Eine Datenbearbeitung verstößt gegen den Grundsatz der Zweckbindung, wenn sie für:²⁵

- vage oder undefinierte Zwecke erfolgt
- unpräzise Ziele durchgeführt wird
- eine Vorratsdatenhaltung vorgesehen ist

Eine nachträgliche Änderung des ursprünglichen Bearbeitungszwecks ist ausschliesslich zulässig, wenn eine neue gesetzliche Bestimmung dies zwingend erfordert.²⁶

Der Grundsatz der Zweckbindung gilt auch für die Sekundärnutzung von Gesundheitsdaten. Eine Weiterverwendung ist demnach unzulässig, wenn die betroffene Person diese berechtigterweise als unerwartet, unangemessen oder anfechtbar erachten kann.²⁷

Ein häufiges Problem besteht darin, dass die Informationen über mögliche Sekundärnutzungsvorhaben zum Zeitpunkt der ursprünglichen Datenerhebung (Primärnutzung) oft zu unspezifisch sind. Diese Vagheit in den vorhandenen Angaben führt dazu, dass eine Verletzung des Zweckbindungsgrundsatzes bei der Weiterverwendung von Daten häufig nicht ausgeschlossen werden kann.²⁸

Erkennbarkeit (Art. 6 Abs. 3 DSG)

Die Grundsätze der Erkennbarkeit und Zweckbindung stehen in einem engen sachlichen Zusammenhang und sind in einem gemeinsamen Artikel geregelt.²⁹ Der Erkennbarkeitsgrundsatz zielt darauf ab, Transparenz bei der Beschaffung und Verarbeitung von Personendaten zu gewährleisten. Die Beurteilung erfolgt stets einzelfallbezogen, wobei nach dem Prinzip von Treu und Glauben zu prüfen ist, welche Verarbeitungszwecke für die betroffene Person in der konkreten Situation erkennbar waren. Der Umfang der erforderlichen Transparenz richtet sich dabei nach dem Verhältnismässigkeitsprinzip.³⁰

Datenrichtigkeit (Art. 6 Abs. 5 DSG)

Die Datenrichtigkeit basiert auf zwei Kernprinzipien: Die Verantwortlichen müssen die sachliche Richtigkeit der Personendaten im Hinblick auf den Verarbeitungszweck sicherstellen und gem. Art. 6 Abs. 5 DSG unrichtige oder unvollständige Daten korrigieren, löschen oder vernichten. Diese Verpflichtung erstreckt sich auch auf nicht mehr benötigte Daten, auch wenn dies nicht explizit im Gesetz verankert ist.³¹

²⁵ Botschaft DSG, S.7025.

²⁶ EPINEY/NÜESCH/ROVELLI, S.98 f.

²⁷ Botschaft DSG, S.7025.

²⁸ WIDMER/BÜHLMANN *et al.*, S. 38-39.

²⁹ WIDMER/BÜHLMANN *et al.*, S. 38.

³⁰ BSK Art. 6 DSG, Rz. 151 ff.; EPINEY/NÜESCH/ROVELLI, S. 101 ff.

³¹ EPINEY/NÜESCH/ROVELLI, S.105 f.

b) Beachtung des Legalitätsprinzips für Bundesorgane

Bundesorgane müssen im Unterschied zu privaten Datenverarbeitern das Legalitätsprinzip als zusätzliche Kernanforderung beachten. Behörden und Dienststellen des Bundes sowie Private mit öffentlichen Aufgaben dürfen Personendaten nur auf Basis einer gesetzlichen Grundlage oder eines gesetzlichen Ausnahmetatbestands³² bearbeiten. Für Gesundheitsdaten gelten aufgrund ihres besonderen Schutzcharakters erhöhte Anforderungen an die gesetzliche Grundlage:

- Es wird ein formelles Gesetz verlangt, das vom Parlament im ordentlichen Gesetzgebungsverfahren erlassen wurde
- Die Rechtsgrundlage muss eine hinreichend bestimmte Ermächtigung zur Datenverarbeitung enthalten

Das DSG kann von Bundesorganen nur in Ausnahmefällen als Rechtsgrundlage herangezogen werden. Stattdessen ist eine bereichsspezifische Regelung in Form einer Spezialgesetzgebung erforderlich.³³

2.3 Spannungsfeld Forschungsfreiheit und digitale Selbstbestimmung

Die fortschreitende Digitalisierung mit ihren exponentiell wachsenden Datenmengen und Verknüpfungsmöglichkeiten verstärkt das Interesse an der Sekundärnutzung von Gesundheitsdaten. Die Forschung nimmt dabei eine zentrale Position ein, da die wissenschaftliche Datenbearbeitung mit erheblichen gesellschaftlichen und politischen Erwartungen verbunden ist. In diesem Zusammenhang wird das Recht auf informationelle Selbstbestimmung³⁴ häufig dem Grundrecht der Wissenschaftsfreiheit³⁵ und dem öffentlichen Interesse an Fortschritt und Innovation gegenübergestellt. Die Bedeutung dieser Abwägung zeigt sich in diversen gesetzlichen Erleichterungen, die durch Spezialerlasse für Forschungszwecke eingeführt wurden.³⁶

Die ausschliessliche Fokussierung auf die Wissenschaft wird dem Potenzial der Sekundärnutzung jedoch nicht gerecht.³⁷ Gesundheitsdaten können in vielen Bereichen des Gesundheitswesens wesentliche Beiträge leisten, etwa in der Gesundheitsüberwachung, der Versorgungsplanung und der Qualitätssicherung.

³² z.B. das Forschungsprivileg z.G. WIDMER/BÜHLMANN *et al.*, S. 49.

³³ BSK Art. 34 DSG, Rz. 6-11; EPINEY/NÜESCH/ROVELLI, S. 131-140.; WIDMER/BÜHLMANN *et al.*, S. 48 ff.

³⁴ Art. 13 Abs. 2 BV.

³⁵ Art. 20 BV.

³⁶ z.B. die Escape Clause gem. Art. 34 HFG, das Forschungsprivileg gem. Art. 39 DSG oder Nudging Instrumente im KRG und EPDG z.G. MÄTZLER, Rz. 19ff. ; 47ff.; SPRECHER Sozialpflichtigkeit, S.185.

³⁷ vgl. Mo. Kom. Wiss.

Die enge Verknüpfung mit der Forschung verzerrt die Wahrnehmung der Sekundärnutzung und überschattet die Bedeutung anderer Anwendungsfelder. Eine differenzierte Betrachtung muss neben der Forschung auch die vielfältigen Interessen und Bedürfnisse weiterer Akteure im Gesundheitssektor einbeziehen.

Diese Arbeit konzentriert sich daher auf die Weiterverwendung von Gesundheitsdaten im Kontext der Regulierungsbemühungen auf Bundesebene. Ziel ist die Identifikation von Datennutzungskonzepten, die sowohl die staatliche Digitalisierung fördern als auch die selbstbestimmte Kontrolle der Betroffenen über ihre persönlichen Daten sicherstellen (digitale Selbstbestimmung³⁸).

³⁸ Die digitale Selbstbestimmung bildet ein spezifischer Ansatz im Rahmen der staatlichen Datenpolitik, welcher das Grundrecht der informationellen Selbstbestimmung miteinschliesst, z.G. siehe Bericht Datenräume, S. 13ff.

3 Aktuelle Trends und Regulierungsbemühungen in Bezug auf die Sekundärnutzung von Gesundheitsdaten

Dieses Kapitel analysiert die politischen Initiativen zur Sekundärnutzung von Gesundheitsdaten in der Schweiz und der EU. Untersucht werden aktuelle Entwicklungen sowie nationale und internationale Vorhaben. Die Betrachtung dient als Grundlage für künftige Regulierungsmassnahmen, indem sie zentrale Herausforderungen identifiziert und erfolgversprechende Ansätze zur Sekundärnutzung von Gesundheitsdaten aufzeigt.

3.1 Ausgangslage

Technologische Entwicklungen als auch gesellschaftliche Einstellungen spielen für die Regulierungsbemühungen im Zusammenhang mit der Sekundärnutzung eine grundlegende Rolle.

3.1.1 Real World Data (RWD) und Big Data

Zwei zentrale Vorgänge, die die derzeitige Handhabung der Nutzung von Gesundheitsdaten in Frage stellen werden unter den Begriffen RWD und Big Data zusammengefasst.

a) RWD

Kennzeichnend für RWD ist, dass diese Art von Gesundheitsdaten nicht im Rahmen klinischer Studien erhoben wird. Es handelt sich um Alltagsdaten, welche vermehrt über die Nutzung von Wearables und Apps direkt bei der betroffenen Person selbst ermittelt werden. Daten lassen sich über ein solches Vorgehen kostengünstiger erheben und stehen in einer grösseren Quantität zur Verfügung, als es bei herkömmlichen Studien der Fall wäre. Das Potential von RWD ist vielseitig, bspw. lassen sich darüber Sicherheit und Effektivität von Therapien besser abschätzen. Ebenfalls denkbar ist, dass RWD künftig den Prozess von Neuzulassungen bei Arzneimittel erleichtern.³⁹

b) Big Data

Während Phänomene wie RWD die Menge an verfügbaren Daten vervielfachen, beschreibt Big Data den Prozess der Verarbeitung und Verknüpfung dieser Daten. Das Ziel ist es, mithilfe geeigneter Technologien relevante Informationen aus einer grossen Zahl an Datensätzen zu gewinnen und so den Erkenntnisfortschritt zu fördern. Besonders die personalisierte Medizin kann von solchen Verfahren profitieren. Die Weiterverwendung von Daten spielt bei Big Data eine zentrale Rolle, wird jedoch

³⁹ Interpharma, Real World Data <<https://www.interpharma.ch/themen/fuhrend-in-forschung-entwicklung/mithochwertigen-gesundheitsdaten-medizinischen-fortschritt-sichern/real-world-data/>> (besucht am 27.10.2024); SPRECHER, S. 829.

gleichzeitig durch datenrechtliche Grundsätze wie die Verhältnismässigkeit oder die Zweckbestimmung behindert.⁴⁰ Auch die Verwendung anonymisierter Daten, bietet aufgrund des technologischen Fortschritts keine ausreichende Sicherheit. Obwohl das DSG hier keine Anwendung findet, besteht aufgrund der Re-Identifikationsgefahr jederzeit das Risiko einer persönlichkeitsverletzenden Datenbearbeitung⁴¹. In dieser Hinsicht ist die Kritik von SPRECHER gerechtfertigt, dass Aspekte wie Big Data in der jüngsten Revision des DSG unzureichend berücksichtigt wurden.⁴²

3.1.2 Einstellung der Schweizer Bevölkerung zur Gesundheitsdatennutzung

Laut einer Umfrage von Comparis bewerten etwa 63,8 % der Schweizer Bevölkerung die aktuelle Datenschutzregelung als "eher gut" bis "gut".⁴³ Trotz eines Anstiegs im Vergleich zum Vorjahr bestehen jedoch grundlegende Bedenken gegenüber der Digitalisierung des Gesundheitswesens, wobei der mögliche Missbrauch von Gesundheitsdaten die grösste Sorge darstellt. Weitere oft genannte Risiken umfassen Nachteile durch fehlenden Zugang, Abhängigkeiten und den Verlust der Privatsphäre.⁴⁴

Gleichzeitig zeigt sich die Bevölkerung zunehmend aufgeschlossen gegenüber der digitalen Speicherung und zentralisierten Verwaltung von Gesundheitsdaten. Die Bereitschaft zur Datenweitergabe an medizinisches Fachpersonal und die Forschung steigt ebenfalls kontinuierlich. Personen teilen ihre Daten bevorzugt mit ärztlichen Fachkräften und zeigen weniger Bereitschaft zur Datenfreigabe für wissenschaftliche Zwecke. Grundlegend für die Entscheidung, Daten freiwillig zu teilen, ist das Vertrauen in ein robustes Datenschutzsystem, das insbesondere Datenkontrolle, Zweckbindung und Transparenz in der Nutzung gewährleistet.⁴⁵

Aus Sicht der Bevölkerung liegt die Verantwortung zur Sicherstellung dieser Aspekte sowie zur Schaffung eines rechtlichen Rahmens, der diese Grundsätze schützt, beim Staat.⁴⁶ Auf parlamentarischer Ebene werden verstärkt Forderungen nach transparenter Information über datenschutzrelevante Gesetzesänderungen sowie nach gezielten Bildungsmassnahmen im Umgang mit Daten erhoben. Diese Initiativen zielen darauf ab, die Data Literacy in der Gesellschaft zu stärken und damit das Verständnis datenschutzrechtlicher Grundlagen zu fördern, um fundierte Entscheidungen zu ermöglichen.⁴⁷

⁴⁰ FISCHER *et al.*, S. 15; 21; JARCHOW/ESTERMANN, S. 3.

⁴¹ BSK Art. 6 DSG, Rz 400ff.; vgl. Kap. 2.2.2 lit. b).

⁴² SPRECHER Datenschutz, S. 157.

⁴³ Comparis, S. 6.

⁴⁴ BRÜNGGER/HERMANN/WENGER, S. 9;62; GUIRGUIS *et al.*, S. 16.

⁴⁵ HERMANN/BÜHLER, S. 5-7; 29-35.

⁴⁶ GUIRGUIS *et al.*, S. 16; HERMANN/BÜHLER, S. 5-6.

⁴⁷ Ip. Data-Literacy; Mo. Data Literacy; vgl. GUIRGUIS *et al.*, S. 16.

3.2 Entwicklungen im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten in der Schweiz

Die Bestrebungen zur Digitalisierung im Schweizer Gesundheitswesen gestalten sich bislang eher zögerlich und stagnieren im internationalen Vergleich.⁴⁸ Während Länder wie Estland oder Kanada erhebliche Investitionen in die digitale Transformation ihres Gesundheitswesens tätigen, rangiert die Schweiz im Digital-Health-Index der Bertelsmann Stiftung nur auf Platz 14 von 17.⁴⁹

Nachfolgend werden die bisherigen staatlichen Initiativen zur Förderung der Digitalisierung im Gesundheitswesen vorgestellt und ausführlich auf ihr Potenzial sowie ihre Auswirkungen auf die Sekundärnutzung von Gesundheitsdaten untersucht.

3.2.1 Strategie Digitale Schweiz im Gesundheitsbereich

In der Rahmenstrategie des Bundes „Digitale Schweiz“ sind verschiedene Teilspekte vorgesehen, die gezielt die Digitalisierung des Gesundheitswesens vorantreiben und begünstigen sollen.

a) *Strategie eHealth Schweiz 2.0*

Die Strategie eHealth Schweiz 2.0 (2018-2024) beabsichtigt die Verbreitung des elektronischen Patientendossiers (EPD) sowie die Koordination der Digitalisierung in diesem Zusammenhang. Diese von Bund und Kantonen gemeinsam entwickelte Strategie verfolgt dabei jedoch bewusst keine umfassende Steuerung der digitalen Transformation im Gesundheitswesen.⁵⁰

Die Vision der von eHealth setzt sich u.a. zum Ziel, die Mehrfachnutzung von einmal erfassten Daten zu gewährleisten. Nicht gemeint ist damit die Förderung der Sekundärnutzung von digitalen Gesundheitsdaten, wie die Strategie klarstellt.⁵¹ Entsprechend fragt sich, was die Mehrfachverwendung von Daten im Rahmen von eHealth konkret umfasst. Ausgehend von den verfügbaren Informationen, will die Mehrfachnutzung sicherstellen, dass „...Daten in allen Bereichen des Gesundheitssystems so erfasst werden, dass sie für verschiedene Zwecke genutzt werden können“.⁵² Es ist daher anzunehmen, dass hier von einer für die Mehrfachverwendung günstigen Datenerfassung die Sprache ist, nicht aber von der

⁴⁸ Botschaft DigiSanté, S. 2926.

⁴⁹ Bertelsmann Stiftung, Digital-Health-Index <<https://www.bertelsmann-stiftung.de/de/unsere-projekte/der-digitale-patient/projektthemen/smarthealthsystems>> (besucht am 28.10.2024).

⁵⁰ BAG, Strategie eHealth Schweiz 2.0 <<https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz.html>> (besucht am 28.10.2024).

⁵¹ Strategie eHealth, S. 3; 11.

⁵² Strategie eHealth, S. 33.

eigentlichen Weiterverwendung dieser Daten. Folglich klammert die eHealth-Strategie die Sekundärnutzung von Gesundheitsdaten bislang aus.⁵³

b) EPD

Das EPD konstituiert ein virtuelles Dossier zur strukturierten Erfassung behandlungsrelevanter Patientendaten. Die Zugriffssteuerung auf die im EPD gespeicherten Informationen obliegt ausschliesslich der betroffenen Person. Die Einrichtung und Nutzung eines EPD durch Patientinnen und Patienten erfolgt auf freiwilliger Basis, macht jedoch eine informierte Einwilligung unter hinreichender Aufklärung zur Datenbearbeitung und deren Folgen erforderlich. Für stationäre Gesundheitseinrichtungen⁵⁴ und deren Gesundheitsfachpersonen besteht hingegen eine gesetzliche Verpflichtung zur EPD-Teilnahme.⁵⁵ Die gesetzlichen Grundlagen des EPD sind seit dem 15. April 2017 in Kraft.⁵⁶ Die rechtliche Ausgestaltung erforderte besondere Sorgfalt, da im Rahmen des EPD die Verarbeitung einer grossen Menge an besonders schützenswerter Personendaten durch eine Vielzahl von Akteuren vorgesehen ist. Der gewählte Regelungsansatz fand in Fachkreisen hinsichtlich seiner datenschutzrechtlichen Konformität überwiegend positive Resonanz. Die Kritik richtete sich primär gegen den Einsatz von Nudging-Instrumenten⁵⁷ im Einwilligungsverfahren, da diese die digitale Selbstbestimmung potenziell gefährden könnten. Für die Personalisierung der Einwilligung wählte die Gesetzgebung eine Widerspruchslösung (Opt-out-Modell). Dies bedeutet, dass die betroffene Person im Einwilligungsprozess mit Standardeinstellungen zur Datenbearbeitung konfrontiert wird, die ohne ihre explizite Ablehnung automatisch aktiviert werden. Anders als beim Opt-in-Verfahren, das eine ausdrückliche Zustimmung erfordert, führt das Opt-out-Prinzip durch den Verzicht auf eine explizite Einwilligung erfahrungsgemäss zu einer erhöhten Datenbereitstellung durch die betroffenen Personen. Die gewählte Opt-out-Lösung ist datenschutzrechtlich zulässig, sofern die Bearbeitungsgrundsätze nach Art. 6 DSG gewahrt bleiben. Als weiteres Nudging-Element sieht das EPD standardmässig ein zeitlich unbefristetes Zugriffsrecht für

⁵³ vgl. Strategie eHealth, S. 18.

⁵⁴ Akutspitäler, psychiatrische Kliniken, Rehabilitationskliniken, Pflegeheime, Geburtshäuser und ab 2022 neu zugelassene Arztpraxen.

⁵⁵ Botschaft EPDG, S.5322-5323; eHealth Suisse, Das EPD, <<https://www.e-health-suisse.ch/koordination/elektronisches-patientendossier/das-epd>> (besucht am 30.10.2024).

⁵⁶ BAG, Gesetzgebung Elektronisches Patientendossier (EPDG) <<https://www.bag.admin.ch/bag/de/home/ge-setze-und-bewilligungen/gesetzgebung/gesetzgebung-mensch-gesundheit/gesetzgebung-elektronisches-patientendossier.html>> (besucht am 30.10.2024).

⁵⁷Nudging-Instrumente dienen der subtilen Verhaltensbeeinflussung. Ziel ist es, menschliche Aktivitäten zu steuern, ohne dabei die Wahlfreiheit von Personen tatsächlich einzuschränken. Es fragt sich daher, ob unter Nudging weiterhin in einer selbstbestimmten Weise über die Weitergabe persönlicher Daten entschieden werden kann.

Gesundheitsfachpersonen vor. Auch diese Regelung entspricht den gesetzlichen Anforderungen, da die betroffenen Personen berechtigt sind, die Zugriffszeit jederzeit individuell zu beschränken.⁵⁸

c) Revision des EPDG

Für die gesetzliche Grundlage des EPD ist künftig eine umfassende Revision geplant. Ziel ist die Weiterentwicklung und Verbesserung des EPDG. Angestrebt wird eine Ausweitung der Anschlusspflicht neben bisher stationären Leistungserbringer auf ambulante Gesundheitseinrichtungen, eine klare Kompetenzaufteilung zwischen Bund und Kantonen, die Umstellung von der freiwilligen Eröffnung des EPD zu einem Opt-out-Modell sowie die Einführung einer zentralen durch den Bund betriebene Datenbank anstelle der bisher dezentralen Datenspeicherung. In Bezug auf die Sekundärnutzung von Gesundheitsdaten sollen Forschende künftig mittels Zustimmung der betroffenen Person Zugriff auf nicht anonymisierte Daten des EPD erhalten. Bearbeitungsvorgaben für die Sekundärnutzung sind nicht vorgesehen, stattdessen gelten die Bestimmungen des DSG und des HFG.⁵⁹

Die Vernehmlassung zur Revision des EPDG ist abgeschlossen. Die entsprechende Botschaft des Bundesrates wird dem Parlament voraussichtlich im kommenden Jahr vorgelegt.⁶⁰

d) E-ID

E-ID bezeichnet die Bemühungen zur Implementierung eines staatlich anerkannten elektronischen Identifikationsnachweises. Der Zugang zur E-ID soll allen Inhaberinnen und Inhabern eines Schweizer Passes, einer Schweizer Identitätskarte oder eines schweizerischen Ausländerausweises ermöglicht werden. Der Bund ist für die Bereitstellung und Verwaltung der technischen Infrastruktur (Vertrauensinfrastruktur) der E-ID verantwortlich. Dies soll höchste Sicherheitsstandards gewährleisten und den Betroffenen maximale Kontrolle über ihre persönlichen Daten zu ermöglichen. Die E-ID soll mittels einer staatlichen App schweizweit sowohl für die digitale als auch analoge Identifikation eingesetzt werden können.⁶¹ Darüber hinaus ist die E-ID als Identifikationsfaktor bzw. Zugangsvoraussetzung für

⁵⁸ WIDMER Patientendossier, S.160 ff. siehe auch SPRECHER Sozialpflichtigkeit, S.185-187; dennoch bedienen sich bspw. auch das KRG einem Opt-Out-Einwilligungsmodell.

⁵⁹ Bericht Revision EPDG, S. 2-3; 29.

⁶⁰ BAG, Weiterentwicklung des elektronischen Patientendossiers <<https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/umsetzung-vollzug/weiterentwicklung-epd.html#749790968>> (besucht am 02.11.2024).

⁶¹ Botschaft E-ID, S. 2843f.

das EPD vorgesehen. Ohne E-ID wird die Eröffnung eines EPD nicht möglich sein.⁶² Das Gesetzgebungsverfahren zur Einführung der E-ID ist gegenwärtig noch nicht abgeschlossen.⁶³

3.2.2 Rahmengesetz für die Sekundärnutzung von Daten

Die Motion „Rahmengesetz für die Sekundärnutzung von Daten“ zielt darauf ab, einen klaren Rechtsrahmen für die Weiterverwendung von Daten zu etablieren. Diese geplante Erweiterung des Datenschutzrechts erstreckt sich auf alle gesellschaftlich relevanten Bereiche. Das Rahmengesetz soll durch die Definition grundlegender Begriffe und Prinzipien den Aufbau und Betrieb von Datennutzungsinfrastrukturen regulieren. Weiter sind Bestimmungen zur Steuerung und Finanzierung der Infrastrukturen, zur Zugänglichkeit und Verknüpfung von Daten sowie zur Gewährleistung von Datenschutz und Datensicherheit vorgesehen. Zudem werden Standards für die bereichsübergreifende Zusammenarbeit von Dateninfrastrukturen festgelegt.⁶⁴ Die Etablierung verbindlicher Vorgaben durch ein Rahmengesetz würde die Sekundärnutzung von Daten vereinheitlichen und die Rechtssicherheit stärken. Diese Entwicklung käme nicht nur der Forschung und Digitalisierung im Gesundheitsbereich zugute, sondern hätte einen gesamtgesellschaftlichen Nutzen.⁶⁵

Der Bundesrat hat die Bedeutung der Sekundärnutzung von Daten, insbesondere im Kontext von Gesundheitsdaten⁶⁶, erkannt und am 23. November 2022 die Annahme der Motion „Rahmengesetz für die Sekundärnutzung von Daten“ beantragt. Zwischenzeitlich haben beide Räte dem Vorhaben zugestimmt, was den Weg für die Ausarbeitung des Gesetzes ebnet und dessen Bedeutung für die zukünftige Entwicklung des Schweizer Datenschutzrechts unterstreicht.⁶⁷

⁶² Art. 7 EPDG; SPRECHER/HOFER, S. 63.

⁶³ Der Gesetzesentwurf befindet sich aktuell im parlamentarischen Differenzbereinigungsverfahren siehe: Das Schweizer Parlament, Parlament ist sich über Ausgestaltung der E-ID im Grundsatz einig <https://www.parlament.ch/de/services/news/Seiten/2024/20240910100146714194158159026_bsd059.aspx> (besucht am 30.10.2024).

⁶⁴ Mo. Kom. Wiss.

⁶⁵ vgl. Positionierung Interpharma in: Interpharma, Medienmitteilung - Expertenkreis präsentiert Anforderungen an Rahmengesetz für Sekundärnutzung von Daten inkl. zugehörige Dokumente <<https://www.interpharma.ch/blog/medienmitteilung-expertenkreis-praesentiert-anforderungen-an-rahmengesetz-fuer-sekundaernutzung-von-daten/>> (besucht am 31.10.2024).

⁶⁶ Der Bundesrat schlägt bereits im Rahmen der Erfüllung des Po. HUMBEL ein nationales System zur Weiterverwendung und Verknüpfung von Gesundheitsdaten vor, dass durch ein rechtliches Rahmenwerk gesteuert werden soll: vgl. z.G. Bericht Po. Humbel, S. 6f.

⁶⁷ Das Schweizer Parlament, Rahmengesetz für Sekundärnutzung von Daten <<https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223890>> (besucht am 31.10.2024).

3.2.3 DigiSanté

Das Programm DigiSanté treibt die digitale Transformation im Gesundheitswesen voran. Es zielt auf die Verbesserung der Versorgungsqualität, die Steigerung der Effizienz und Transparenz sowie die Erhöhung der Patientensicherheit ab. Die Umsetzung ist für den Zeitraum 2025 bis 2034 geplant und wird durch einen Verpflichtungskredit von 391.7 Millionen Franken unterstützt. DigiSanté entwickelt die Vision eines digitalen Gesundheitswesens im Rahmen der Strategie „Gesundheit 2030“⁶⁸ weiter.⁶⁹

Im Zusammenhang mit der Sekundärdatennutzung setzt sich DigiSanté zum Ziel den Zugang zu Gesundheitsdaten für Forschende zu gewährleisten. Auch die Datennutzung für Planung und Steuerung des Gesundheitswesens durch Behörden und beteiligte Akteure soll künftig verbessert werden. Die Sekundärnutzung im engeren Sinn ist jedoch ausschliesslich für die akademische sowie für die privatwirtschaftliche Forschung vorgesehen.⁷⁰ Zusätzlich zur Datenweiterverwendung ist die Etablierung eines spezialisierten Datenraums für gesundheitswissenschaftliche Untersuchungen geplant. Alle diese Vorhaben werden mit dem Rahmengesetz für Sekundärnutzung und der E-ID-Entwicklung koordiniert. Zudem soll das EPD ausgebaut werden, dessen spezialisierte Infrastruktur für Gesundheitsdaten eine wichtige Basis für DigiSanté bildet.⁷¹ Neben technischen Standards ist Schaffung von angemessenen rechtlichen Rahmenbedingungen im Kontext von DigiSanté grundlegend, um die Sekundärnutzung von Gesundheitsdaten zu ermöglichen.

3.3 Entwicklungen im Zusammenhang mit der Sekundärnutzung von Gesundheitsdaten in der EU

Im Bereich der Sekundärnutzung von Gesundheitsdaten sind auch die europäischen Regulierungsvorhaben für die Schweiz von grösstem Interesse. Die enge politische und wirtschaftliche Zusammenarbeit zwischen der Schweiz und der EU sowie deren Mitgliedstaaten macht eine Abstimmung der nationalen Datenschutzpolitik mit europäischen Initiativen unumgänglich.⁷²

3.3.1 European Health Data Space (EHDS)

Die EU hat erkannt, dass im Rahmen der Digitalisierung weitere Massnahmen erforderlich sind, und hat die Initiative des EHDS lanciert. Geplant ist ein Datenraum für Gesundheitsdaten, der als europäischer digitaler Binnenmarkt konzipiert ist. Das Projekt fördert den grenzüberschreitenden Austausch elektronischer Gesundheitsdaten und erleichtert gleichzeitig deren Datenzugang.

⁶⁸ Gesundheitspolitische Strategie des Bundesrates.

⁶⁹ Botschaft DigiSanté, S. 2909.

⁷⁰Botschaft DigiSanté, S. 2955.

⁷¹Botschaft DigiSanté, S. 2920.

⁷² vgl. Botschaft DigiSanté, S. 2928.

Neben der Primärnutzung, die im Datenaustausch für die Erbringung von Gesundheitsdienstleistungen besteht, wird auch die Sekundärnutzung aktiv berücksichtigt. Die Weiterverwendung von Gesundheitsdaten soll künftig für Forschung, Innovation, Politikgestaltung, Regulierung sowie personalisierte Medizin ermöglicht werden. Die Datenverarbeitung ist ausschliesslich für festgelegte Zwecke zulässig und muss die Anonymität der betroffenen Personen gewährleisten. Der Zugriff auf Gesundheitsdaten erfolgt in einer geschlossenen sicheren digitalen Umgebung. Neben der Erleichterung der Sekundärnutzung zielt der EHDS darauf ab, Bürgerinnen und Bürger in die Lage zu versetzen, die Kontrolle über ihre Gesundheitsdaten zu übernehmen. Der Betrieb dieses gesundheitsspezifischen Ökosystems wird durch einen soliden Rechtsrahmen, gemeinsame Standards und Verfahren, geeignete Infrastrukturen sowie klare Governance-Vorgaben unterstützt.⁷³ Mit der Annahme des Verordnungsvorschlags zum EHDS durch das Europäische Parlament am 24. April 2024 wurde ein weiterer entscheidender Schritt im Umsetzungsprozess vollzogen.⁷⁴

3.3.2 Zugang zum EHDS durch die Schweiz

Der aktuelle Entwicklungsstand erlaubt noch keine abschliessende Aussage über eine mögliche Beteiligung der Schweiz am EHDS. Technisch erfüllt das EPD bereits die wesentlichen Standards, sodass eine Integration in den EHDS mit überschaubarem Aufwand realisierbar wäre. Problematisch sind jedoch die unkoordinierten Ansätze zur Ermöglichung der Sekundärnutzung von Gesundheitsdaten in der Schweiz sowie die regulatorischen Unterschiede zur Sekundärnutzung im EHDS. Während der EHDS die Sekundärnutzung auch für nicht-wissenschaftliche Zwecke vorsieht, ist in der Schweiz die Nutzung ausschliesslich zugunsten der Forschung vorgesehen – sowohl aktuell als auch in Zukunft. Zudem wird der Aspekt der Sekundärnutzung in der geltenden Gesetzgebung zum EPD vollständig vernachlässigt. Das Programm DigiSanté, das die Weiterentwicklung des EPD vorantreibt, definiert zwar die Weiterverwendung von Gesundheitsdaten als strategisches Ziel, jedoch nicht spezifisch für das EPD. DigiSanté konzentriert sich beim EPD auf die Optimierung der Mehrfachnutzung durch die Harmonisierung von Prozessen und die Entwicklung von Schnittstellen. Die Sekundärnutzung von Gesundheitsdaten soll dagegen unabhängig vom EPD durch einen separaten Gesundheitsdatenraum für die Forschung ermöglicht werden.⁷⁵ Obwohl Gesundheitsdatenraum und EPD getrennt entwickelt werden sollen, verwischt die EPDG-Revision diese Grenze, indem sie Forschenden künftig einen bedingten Zugriff auf EPD-Gesundheitsdaten gewährt.

⁷³ Faktenblatt EHDS; EHDS-VO.

⁷⁴ Europäische Kommission, Kommission begrüßt Annahme des europäischen Raums für Gesundheitsdaten und der Verordnung über Substanzen menschlichen Ursprungs durch das Europäische Parlament <https://ec.europa.eu/commission/presscorner/detail/de/ip_24_2250> (besucht am 01.11.2024).

⁷⁵ Botschaft DigiSanté, S. 2; 18; 24; 52; vgl. Kap. 3.2.1. und 3.2.3.

3.3.3 Gesundheitsdatenräume in der Schweiz

Im Bericht zur Erfüllung des Postulats Humbel erkennt der Bundesrat die Notwendigkeit, ein nationales System für die Weiterverwendung und Verknüpfung von Gesundheitsdaten zu etablieren.⁷⁶ Diese Aufgabe soll durch das Programm DigiSanté mit dem Vorhaben „Gesundheitsdatenraum für die Forschung“ umgesetzt werden.⁷⁷

Im Unterschied zum EHDS beschränkt sich der Nutzen des Gesundheitsdatenraums ausschliesslich auf die Sekundärnutzung von Daten. Der Zugang wird dabei exklusiv der Forschung gewährt, während weder die Bevölkerung noch andere Akteure Zugriff erhalten. Eine weitere Besonderheit besteht darin, dass die zur Verfügung gestellten Daten in identifizierender Form vorliegen. Die Bearbeitung ist somit ohne das Erfordernis der vorgängigen Anonymisierung möglich.⁷⁸

3.4 Schlussfolgerung zu den künftigen Anforderungen an die Regulierung der Sekundärnutzung von Gesundheitsdaten

Ein angemessener rechtlicher Rahmen für RWD und Big Data ist essentiell, um deren Potenzial für Gesellschaft und Wirtschaft zu nutzen und dabei die digitale Selbstbestimmung der Einzelnen zu schützen.

Datenschutz basiert wesentlich auf Vertrauen und bedarf staatlicher Regulierung. Die Schweizer Bevölkerung steht der digitalen Speicherung und Weitergabe von Daten grundsätzlich aufgeschlossen gegenüber, wünscht jedoch Transparenz über deren Verwendung, eine klare Kommunikation und Schutz vor Datenmissbrauch.

Die Strategie Digitale Schweiz enthält zentrale Vorhaben zur Förderung der Sekundärnutzung von Gesundheitsdaten. Das EPD könnte künftig als Datenquelle für die Sekundärnutzung dienen und bildet gemeinsam mit der E-ID ein fundamentales Infrastrukturelement. Allerdings wird bei der Ausgestaltung des EPD eine mögliche Sekundärnutzung von Gesundheitsdaten bisher unzureichend berücksichtigt. Die Weiterentwicklung des EPD durch die anstehende Revision des EPDG und das Programm DigiSanté sehen lediglich einen erleichterten Zugang für die Forschung vor.

Diese einseitige Fokussierung auf die Forschung und die zögerlichen Regulierungsbemühungen erscheinen angesichts des Digitalisierungsdrucks und des Ziels, die digitale Selbstbestimmung zu stärken, nicht zeitgemäss. Zudem erschweren sie die Harmonisierung mit europäischen Gesetzgebungsvorhaben und einen potenziellen Anschluss an den EHDS.

⁷⁶ Bericht Po. Humbel, S. 7.

⁷⁷ Botschaft DigiSanté, S. 50.

⁷⁸ SPRECHER Gesundheitsdatenräume, S. 41-42.

Die Schweiz plant mit dem Gesundheitsdatenraum für Forschung ein eigenes Datenraumprojekt. Dieses unterscheidet sich jedoch vom EHDS durch seine ausschliessliche Ausrichtung auf wissenschaftliche Zwecke und verzichtet bspw. auf zentrale Aspekte wie die selbstbestimmte Kontrolle über Gesundheitsdaten durch Betroffene.

Mit dem geplanten Rahmengesetz zur Sekundärnutzung von Daten entsteht dagegen ein umfassender, bereichsübergreifender Regulierungsrahmen. Die Tragweite dieses Vorhabens kann während der aktuellen Gesetzgebungsphase allerdings noch nicht vollständig eingeschätzt werden.

Die Analyse zeigt eine zentrale Herausforderung im Bereich der Sekundärnutzung von Gesundheitsdaten: Trotz zahlreicher staatlicher Initiativen fehlt ein koordinierter, gesamtheitlicher Ansatz zur Sekundärnutzung von Daten. Die bestehenden Projekte entwickeln sich weitgehend isoliert und fokussieren sich primär auf den Forschungsbereich. Eine zukunftsfähige Sekundärnutzung erfordert jedoch ein umfassendes Regulierungskonzept, das sämtliche gesellschaftliche Bereiche einbezieht und sich an internationalen Entwicklungen angemessen orientiert. Zentral dabei sind die Stärkung der digitalen Selbstbestimmung z.B. mittels Digital-Literacy Massnahmen sowie der Aufbau von Vertrauen in die staatliche Datenschutzpolitik.

4 Die Einwilligung gemäss DSG

Die Einwilligung stellt sowohl für die Primär- als auch für die Sekundärnutzung einen wichtigen Rechtfertigungsgrund dar, der die gesetzeskonforme Bearbeitung von Personendaten sicherstellt. Das folgende Kapitel analysiert die rechtlichen Rahmenbedingungen der datenschutzrechtlichen Einwilligung unter besonderer Berücksichtigung der gesetzlichen Anforderungen an die Sekundärnutzung von Gesundheitsdaten. Abschliessend erfolgt eine kritische Evaluation der gegenwärtigen Einwilligungspraxis hinsichtlich ihrer Eignung für Vorhaben der digitalen Transformation.

4.1 Bedeutung der Einwilligung

Der Rechtfertigungsgrund der Einwilligung innerhalb des DSG findet sowohl im öffentlichen als auch im privaten Recht Anwendung. Die spezifische Bedeutung variiert jedoch abhängig vom betrachteten Rechtsgebiet.

4.1.1 Öffentliches Recht

Die Verarbeitung von Daten durch Bundesorgane oder private Träger staatlicher Aufgaben erfordert primär eine gesetzliche Ermächtigungsgrundlage gemäss Art. 34 ff. DSG. Von diesem Erfordernis des Legalitätsprinzips kann im Einzelfall durch die Einwilligung der betroffenen Person abgewichen werden. Gleichwohl sind die Grundsätze nach Art. 6 DSG bei der staatlichen Datenverarbeitung durch Bundesorgane zwingend einzuhalten.⁷⁹

Ein zentraler Unterschied zur Wirkung der Einwilligung unter Privaten besteht darin, dass in eine Verletzung der Bearbeitungsgrundsätze nicht eingewilligt⁸⁰ werden kann. Die Einwilligung kann ausschliesslich in Ermangelung einer spezifischen Rechtsnorm als subsidiäre Rechtsgrundlage die Datenverarbeitung rechtfertigen. Die asymmetrische Machtkonstellation zwischen Staat und Privatperson bedingt zudem erhöhte Anforderungen an die Bestimmtheit und Freiwilligkeit der Einwilligung⁸¹. Folglich bleibt die praktische Bedeutung der Einwilligung im Kontext der staatlichen Datenverarbeitung begrenzt.⁸²

⁷⁹ FASNACHT, Kap. 2 Rz. 214ff.; WIDMER/BÜHLMANN *et al.*, S. 48; 52.

⁸⁰ Eine Ausnahme hiervon bildet das Forschungsprivileg, dass unter gegebenen Voraussetzungen eine Missachtung des Zweckbindungsgebots rechtfertigen, kann z.G. WIDMER/BÜHLMANN *et al.*, S.48ff.

⁸¹ vgl. Kap. 4.2.

⁸² WIDMER/BÜHLMANN *et al.*, S. 48; 52.

4.1.2 Privatrecht

Im privatrechtlichen Rechtsverkehr ist die Datenverarbeitung grundsätzlich zulässig, sofern sie keine Persönlichkeitsverletzung nach Art. 30 Abs. 2 DSG darstellt. Eine Persönlichkeitsverletzung liegt u.a. vor, wenn Personendaten entgegen den Grundsätzen in Art. 6 und 8 DSG bearbeitet werden, eine Bearbeitung gegen die ausdrückliche Willenserklärung der betroffenen Person verstößt sowie bei Bekanntgabe besonders schützenswerter Personendaten an Dritte. Eine rechtsgültige Einwilligung vermag eine solche Persönlichkeitsverletzung zu legitimieren und hebt die Widerrechtlichkeit der Datenverarbeitung auf. Im Gegensatz zum öffentlichen Recht dient die Einwilligung im Privatrecht als Rechtfertigungsgrund bei Abweichungen von den Bearbeitungsgrundsätzen nach Art. 6 DSG. Dies erklärt ihre regelmässige Einholung in der Praxis als Absicherung gegen potenzielle Persönlichkeitsklagen.⁸³

4.2 Anforderungen an die Einwilligung

Die rechtfertigende Wirkung einer Einwilligung setzt deren Rechtsgültigkeit voraus. Das im schweizerischen Recht verankerte Modell des *informed consent* definiert die Wirksamkeit der Einwilligung durch folgende kumulative Voraussetzungen:

4.2.1 Angemessene Information

Eine zentrale Voraussetzung der Einwilligung ist das Erfordernis der angemessenen Information. Dieses orientiert sich weitgehend am Modell der aufgeklärten Patientin bzw. des aufgeklärten Patienten (*informed consent*) und erfährt durch die Rechtsprechung eine fortlaufende Präzisierung.⁸⁴ Eine Einwilligung erlangt Rechtswirksamkeit, wenn die betroffene Person in Kenntnis aller relevanten Umstände ihre Zustimmung zur Datenverarbeitung freiwillig erteilt. Der erforderliche Informationsumfang bemisst sich dabei an der Rechtfertigung der Persönlichkeitsverletzung.⁸⁵ Das Prinzip der angemessenen Information basiert auf den Vorgaben des Transparenz- und Zweckbindungsgrundsatzes nach Art. 6 Abs. 3 DSG⁸⁶ sowie der Informationspflicht gemäss Art. 19ff. DSG.⁸⁷ Im Folgenden werden die wesentlichen Voraussetzungen der angemessenen Information systematisch dargestellt:

⁸³ FASNACHT, Kap. 2 Rz. 214ff.; WIDMER/BÜHLMANN *et al.*, S. 46.

⁸⁴ FASNACHT, Kap. 2 Rz. 243ff.; vgl. BVGer in A-3548/2018.

⁸⁵ FASNACHT, Kap. 2 Rz. 241ff.

⁸⁶ vgl. Kap. 2.2.6.

⁸⁷ Botschaft DSG, S. 7053; BÜHLMANN/SCHÜEPP, Rz. 51; KLAUS/THOMANN, Rz. 18.

a) Zeitpunkt

Die Aufklärung über die Datenverarbeitung muss vor oder spätestens mit der Erteilung der Einwilligung erfolgen.⁸⁸ Der betroffenen Person ist zwischen der Information und ihrer Willenserklärung eine angemessene Bedenkzeit zu gewähren.⁸⁹ Eine nachträgliche Information und die damit verbundene rückwirkende Einwilligung stellen nach FASNACHT primär einen Rechtsverzicht auf Ansprüche aus Persönlichkeitsverletzung dar.⁹⁰

b) Form

Das Gesetz schreibt für die angemessene Information keine spezifische Form vor. Die Aufklärung über die Datenverarbeitung kann daher sowohl mündlich als auch schriftlich erfolgen, wobei aus Beweisgründen die schriftliche Form vorteilhaft sein kann. Für die Informationsvermittlung sind verschiedene, auch mehrstufige Konzepte möglich. Entscheidend ist, dass die Informationen für die betroffene Person zugänglich sind. Je nach gewähltem Informationsverfahren muss auf die Verfügbarkeit und Auffindbarkeit der Informationen hingewiesen werden, beispielsweise durch Webadresse oder QR-Code.⁹¹

c) Kenntnisnahme

Der betroffenen Person muss die Möglichkeit zur Kenntnisnahme der relevanten Informationen eingeräumt werden. Eine tatsächliche Einsichtnahme in die Details der Datenverarbeitung ist hingegen nicht erforderlich.⁹²

d) Inhalt

Die angemessene Information soll ein Verständnis über Umfang und Folgen der Einwilligung ermöglichen. Der erforderliche Mindestinhalt orientiert sich an der Informationspflicht zur Datenbeschaffung gemäss Art. 19ff. DSG, wobei der Detaillierungsgrad von der Sensibilität der verarbeiteten Daten abhängt. Während im Regelfall allgemeine Umschreibungen ausreichen, sind bei sensiblen Daten umfassendere Erläuterungen erforderlich.⁹³

Nach FASNACHT umfasst der Mindestinhalt der angemessenen Information folgende zentrale Kategorien:⁹⁴

⁸⁸ FASNACHT, Kap. 2 Rz. 252.

⁸⁹ z.G. siehe FASNACHT, Kap. 2 Rz. 254.

⁹⁰ FASNACHT, Kap. 2 Rz. 253.

⁹¹ BÜHLMANN/SCHÜEPP, Rz. 49ff.; FASNACHT, Kap. 2 Rz. 251.

⁹² BSK Art. 6 DSG, Rz. 295, KLAUS/THOMANN, Rz. 26.

⁹³ FASNACHT, Kap. 2 Rz. 261; BSK Art. 6 DSG, Rz. 289; BÜHLMANN/SCHÜEPP, Rz. 54; KLAUS/THOMANN, Rz. 21.

⁹⁴ FASNACHT, Kap. 2 Rz. 256ff.

- Identität der Datenempfänger
- Zweck und Art der Datenbearbeitung
- Umfang der Datenbearbeitung (angewandte Bearbeitungsmethoden)
- Transparenz in Bezug auf die bearbeiteten Datentypen (z.B. Daten zur Kreditwürdigkeit) und Präzisierung der verwendeten Personendaten (z.B. Adresse) sowie eine spezifische Anzeige bei besonders schützenswerten Daten

Situationsabhängig können folgende zusätzliche Informationen relevant sein:

- Zeitlicher Umfang der Datenbearbeitung
- Spezifische Gefahren und Risiken⁹⁵
- Konsequenzen bei Verweigerung der Einwilligung
- Informationen in Verbindung mit der grenzüberschreitenden Datenbekanntgabe

Die konkrete Ausgestaltung der Information richtet sich nach den spezifischen Bedürfnissen der Adressaten. Obgleich grundsätzlich von einer verständigen Person ausgegangen werden kann, muss das Verständnis im Einzelfall sichergestellt werden. Die Information hat dabei den Anforderungen der Sachlichkeit und Korrektheit zu entsprechen.⁹⁶ Zudem sollte sie in einer für die betroffene Person verständlichen Sprache erfolgen. KLAUS/THOMANN empfehlen diesbezüglich, dass die Sprache der Information mit der Sprache der zugrundeliegenden Leistung übereinstimmen, für die die Datenverarbeitung notwendig ist.⁹⁷ Gemäss der Ungewöhnlichkeitsregel⁹⁸ sind überraschende oder ungewöhnliche Aspekte der Datenverarbeitung im Rahmen der angemessenen Information ausdrücklich hervorzuheben. Ein unterlassener Hinweis kann zur Unwirksamkeit der Einwilligung hinsichtlich Bearbeitungsvorgänge führen, mit welcher die betroffene Person nicht rechnen musste.⁹⁹

e) Beurteilungsmassstab

Die Angemessenheit einer Information bestimmt sich nach einem objektiven Massstab. Die Beurteilung erfolgt anhand der Grundsätze der Verhältnismässigkeit, des Prinzips von Treu und Glauben gemäss Art. 2 Abs. 1 ZGB sowie der Voraussetzungen der Ungewöhnlichkeitsregel.¹⁰⁰

⁹⁵ Allgemein bekannte Risiken und Gefahren können im Rahmen der angemessenen Information vernachlässigt werden.

⁹⁶ FASNACHT, Kap. 2 Rz. 263ff. ; BÜHLMANN/SCHÜEPP, Rz. 57; BSK Art. 6 DSG, Rz. 290f.

⁹⁷ KLAUS/THOMANN, Rz. 22.

⁹⁸ Die Ungewöhnlichkeitsregel findet vorrangig im AGB-Recht Anwendung, wobei die h.L. ihre Relevanz auch im Datenschutzrecht anerkennt. Im Kontext der Allgemeinen Geschäftsbedingungen führt sie zur Unwirksamkeit der Zustimmung bezüglich ungewöhnlicher Vertragsklauseln, sofern auf diese nicht gesondert hingewiesen wurde vgl. z.G. BÜHLMANN/SCHÜEPP, Rz. 62ff.

⁹⁹ BÜHLMANN/SCHÜEPP, Rz. 62ff.

¹⁰⁰ BSK Art. 6 DSG, Rz. 294, BÜHLMANN/SCHÜEPP, Rz. 69ff.

f) Entfall der angemessenen Information

Eine Unterlassung der angemessenen Information ist gesetzlich unzulässig. FASNACHT definiert spezifische Ausnahmefälle, in denen eine Information aufgrund aussergewöhnlicher Umstände entfallen kann. Die praktische Anwendung dieser Ausnahmen wird durch hohe Anforderungen an die Begründungspflicht des Datenverarbeiters erheblich eingeschränkt.¹⁰¹

4.2.2 Freiwilligkeit

Eine gültige Einwilligung muss freiwillig erfolgen. Die Anforderungen an die Freiwilligkeit sind nicht vollständig geklärt, jedoch ist von einem grosszügigen Begriffsverständnis auszugehen¹⁰². Eine Einwilligung, die unter Täuschung, Drohung oder Zwang erfolgt, ist unwirksam. Im Kontext der Freiwilligkeit bedeuten Zwang oder Druck das Fehlen einer Handlungsalternative, die frei von unzumutbaren Nachteilen ist. Das heisst, dass die betroffene Person bei Ablehnung der Einwilligung Nachteile erfährt, die nicht mit der Datenverarbeitung und der damit verbundenen Persönlichkeitsverletzung in Verbindung stehen. Zwang liegt auch dann vor, wenn die Verweigerung der Einwilligung zu unverhältnismässigen¹⁰³ Nachteilen führt.¹⁰⁴

Ob eine Einwilligung freiwillig erteilt wurde, ist anhand des konkreten Einzelfalls und der Begleitumstände zu beurteilen. Ein Abhängigkeitsverhältnis oder ein Machtgefälle zwischen den beteiligten Parteien kann auf Zwang hindeuten. In solchen Fällen sind die verfügbaren Handlungsoptionen bei Verweigerung der Einwilligung im Hinblick auf ihre Verhältnismässigkeit zu prüfen.¹⁰⁵ Das Fehlen von Freiwilligkeit im Kontext der Verarbeitung von Gesundheitsdaten kann bspw. angenommen werden, wenn bei einer lebensbedrohlichen Krankheit kein Handlungsspielraum bezüglich einer Einwilligung zur Datenverarbeitung besteht und diese Situation gezielt ausgenutzt wird.¹⁰⁶

4.2.3 Weitere Anforderungen an die Einwilligung

Neben den Kernkriterien der Freiwilligkeit und der angemessenen Information werden folgende weitere zivil- und obligationenrechtliche Ansprüche an die Einwilligung gestellt:

¹⁰¹ z.G. FASNACHT, Kap. 2 Rz. 270ff.

¹⁰² Dieser Text folgt der Auffassung der h.L. und verneint ein strenges Kopplungsverbot in Bezug auf die Einwilligung. Für eine tiefergehende Auseinandersetzung mit den Lehrmeinungen zum Kopplungsverbot wird auf BSK Art. 6 DSG, Rz. 310ff. sowie BÜHLMANN/SCHÜEPP, Rz. 29ff. verwiesen.

¹⁰³ Nicht gemeint ist damit die Betrachtung unter dem Grundsatz der Verhältnismässigkeit nach Art. 6 Abs. 2 DSG. Vielmehr handelt es sich um eine vergleichbare Interesseabwägung.

¹⁰⁴ BSK Art. 6 DSG, Rz. 311; FASNACHT, Kap. 2 Rz. 273-275.

¹⁰⁵ FASNACHT, Kap. 2 Rz. 273-278.

¹⁰⁶ WIDMER/BÜHLMANN *et al.*, S. 45.

a) Form

Für die Form der Einwilligung existieren, analog zur angemessenen Information, keine gesetzlichen Vorgaben. Ebenso wenig muss die Einwilligung explizit als solche gekennzeichnet sein.¹⁰⁷ Obwohl die Einwilligung mündlich als auch schriftlich erfolgen kann, empfehlen KLAUS/THOMANN den Zustimmungsakt und dessen Wortlaut aus Beweisgründen schriftlich zu dokumentieren.¹⁰⁸

b) Willensäußerung

Die beabsichtigte Persönlichkeitsverletzung erfordert eine vorherige Willensäußerung der betroffenen Person. Diese Willensäußerung ist zwar nicht empfangsbedürftig, unterliegt jedoch bestimmten Voraussetzungen.¹⁰⁹ Soweit das Datenschutzgesetz keine ausdrückliche Einwilligung vorschreibt¹¹⁰, kann die Zustimmung der betroffenen Person konkludent erfolgen. Die ausdrückliche Einwilligung erfordert ein aktives Einverständnis, während bei konkludentem Handeln die Genehmigung zur Datenbearbeitung indirekt eingeschlossen ist.¹¹¹ Stillschweigen gilt nur dann als Einwilligung, wenn diese Form der Zustimmung vorab zwischen den Parteien vereinbart wurde.¹¹²

c) Inhaltliche Grenzen

Im öffentlichen Recht wird die Einwilligung durch den Grundrechtsschutz begrenzt. Eine Grundrechtsbeschränkung durch Einwilligung muss den Vorgaben von Art. 36 BV entsprechen und darf den Kerngehalt nicht verletzen.¹¹³

Im Privatrecht bestimmen sich die Grenzen nach Art. 20 Abs. 1 OR. Der Gegenstand, der Zweck und die Art der Einwilligung dürfen weder unmöglich oder widerrechtlich sein noch gegen die guten Sitten verstossen. Im Rahmen der Sittlichkeit ist zudem das Verbot der übermässigen Selbstbindung gemäss Art. 27 Abs. 2 ZGB zu beachten. Unzulässig sind demnach Einwilligungen ohne die Möglichkeit auf Widerruf sowie Zustimmungen in Bezug auf weitreichende, undefinierte sowie in der Zukunft liegende Datenverarbeitungen.¹¹⁴

¹⁰⁷ Botschaft DSG, S. 7027.

¹⁰⁸ KLAUS/THOMANN, Rz. 39.

¹⁰⁹ FASNACHT, Kap. 2 Rz. 314.

¹¹⁰ z.B. in Art. 6 Abs. 7 DSG.

¹¹¹ KLAUS/THOMANN, Rz. 39.

¹¹² Botschaft DSG, S. 7027f.

¹¹³ FASNACHT, Kap. 2 Rz. 320.

¹¹⁴ FASNACHT, Kap. 2 Rz. 321ff.

d) Urteilsfähigkeit

Die Einwilligung als einseitiges Rechtsgeschäft erfordert keine Handlungsfähigkeit der zustimmenden Person, da keine Rechte und Pflichten begründet werden müssen. Aufgrund des höchstpersönlichen Charakters der Einwilligung wird jedoch Urteilsfähigkeit vorausgesetzt. Die betroffene Person muss gem. Art. 16 ZGB in der Lage sein, die Tragweite ihrer Entscheidung zu erkennen und nach dieser Erkenntnis vernunftgemäß zu handeln.¹¹⁵

e) Widerruf

Mit der Erteilung einer Einwilligung ist stets ein Widerrufsrecht verbunden, das formlos und ohne Begründung jederzeit ausgeübt werden kann. Dieses Recht ist unverzichtbar und kann weder vertraglich noch durch andere Rechtsgeschäfte aufgehoben werden¹¹⁶. Die Widerrufserklärung entfaltet ihre Wirkung ausschliesslich für die Zukunft und verhindert weitere Datenbearbeitungen. Dies gilt jedoch nicht für künftige Bearbeitungsvorgänge, die sich auf alternative Rechtfertigungsgründe¹¹⁷ stützen, bspw. ein öffentliches Interesse oder eine gesetzliche Grundlage. Eine vergangenheitsorientierte Wirkung auf bereits vollzogene Datenbearbeitungen ist ausgeschlossen. Somit bleiben Persönlichkeitsverletzungen, die vor der Widerrufserklärung erfolgten, durch die ursprüngliche Zustimmung legitimiert. Darüber hinaus kann der Widerruf auch zu Unzeit erfolgen und Schadensersatzpflichten mit sich ziehen.¹¹⁸

4.3 Anforderungen an die Einwilligung bei der Bearbeitung von Gesundheitsdaten

Gesundheitsdaten als besonders schützenswerte Personendaten erfordern gemäss Art. 6 Abs. 7 DSG eine ausdrückliche Einwilligung zur Datenverarbeitung. Die Bearbeitung von Gesundheitsdaten unterliegt damit im Vergleich zu regulären Personendaten einer zusätzlichen Beschränkung, da eine konkordante Willensäußerung ausgeschlossen ist. Das qualifizierte Erfordernis der ausdrücklichen Einwilligung gilt jedoch nur in Fällen, in denen das Gesetz eine Zustimmung der betroffenen Person grundsätzlich voraussetzt¹¹⁹. Vorbehaltlich anderslautender Gesetzesbestimmungen kann die Bearbeitung von Gesundheitsdaten i.d.R. ohne (ausdrückliche) Einwilligung erfolgen.¹²⁰

¹¹⁵ FASNACHT, Kap. 2 Rz. 306ff; KLAUS/THOMANN, Rz. 28.

¹¹⁶ Art. 27 Abs. 2 ZGB.

¹¹⁷ vgl. Art. 13 Abs. 1 DSG.

¹¹⁸ BSK Art. 6 DSG, Rz. 316ff.; FASNACHT, Kap. 2 Rz. 325f.

¹¹⁹ vgl. Art. 6 Abs. 6 DSG.

¹²⁰ BÜHLMANN/SCHÜEPP, Rz. 31-37; KLAUS/THOMANN, Rz. 43; SHK Art. 6 DSG, Rz. 100ff.

Nach der h.L. bezieht sich die „Ausdrücklichkeit“ sowohl auf den Inhalt als auch auf die Form der Einwilligung.¹²¹ Die Willensäußerung muss in ihrer Ausdrucksweise und ihrem Inhalt unmissverständlich sein und kann mündlich, schriftlich oder durch eindeutige Gesten wie Kopfnicken erfolgen.¹²²

4.4 Kritik im Zusammenhang mit der datenrechtlichen Einwilligung

Angesichts bestehender Rechtsunsicherheiten bei der Sekundärnutzung von Gesundheitsdaten¹²³ hat sich die Einwilligung als zentrales Instrument zur Gewährleistung einer rechtskonformen Datenverarbeitung etabliert. Die gegenwärtigen rechtlichen Vorgaben begrenzen jedoch ihr Potenzial erheblich und schränken damit die Möglichkeiten einer effizienten Sekundärnutzung im Rahmen der digitalen Selbstbestimmung ein. Die nachfolgende Analyse legt diesbezüglich die wichtigsten Kritikpunkte dar.

4.4.1 Limitationen des Opt-in Modells

Das gesetzliche Einwilligungsverfahren basiert auf dem Opt-in-Prinzip. Dies erfordert von der betroffenen Person eine aktive und ausdrückliche Zustimmung zur Bearbeitung personenbezogener Daten, die in deren Persönlichkeitsrechte eingreift. Die Datenempfangenden müssen dabei umfassende gesetzliche Vorgaben für eine gültige Einwilligung erfüllen. Folglich erweist sich die rechtskonforme Erhebung und Bearbeitung von Daten, insbesondere bei grossen Datenmengen, als anspruchsvoll und komplex.¹²⁴ Darüber hinaus belegen empirische Studien eine objektive Realitätsabweichung (Bias) bei Daten, die mittels Opt-in-Verfahren erhoben werden. Bspw. zeigte die Forschungsarbeit von DE MAN, *et al.*, dass vorwiegend männliche Personen mit höherem Bildungsabschluss, grösserem Einkommen sowie höherem sozioökonomischem Status ihre Einwilligung erteilen. Diese selektive Partizipation stellt die Repräsentativität und Validität der erhobenen Datensätze, insbesondere hinsichtlich ihrer Sekundärnutzung, in Frage.¹²⁵

4.4.2 Unsicherer Rechtsrahmen

Die gegenwärtige Regulierungssystematik im Datenschutzrecht erweist sich aufgrund der Vielzahl von Spezialerlassen und deren Ausnahmeregelungen als komplex. Zudem sind im DSG diverse

¹²¹ In Bezug auf die Anforderungen an die „Ausdrücklichkeit“ fehlt es an einer gesetzlichen Definition und die bisherige Rechtslage gestaltet sich als umstritten z.G. siehe BÜHLMANN/SCHÜEPP, Rz. 113; FASNACHT, Kap. 2 Rz. 302ff; Botschaft DSG, S. 7028.

¹²² KLAUS/THOMANN, Rz. 39.

¹²³ vgl. Kap. 2.2.6.

¹²⁴ vgl. Kap. 4.2 und 4.3.

¹²⁵ z.G. DE MAN, *et al.*

Anforderungen an die Datenverarbeitung, einschliesslich jener der Einwilligung, weder umfassend noch abschliessend definiert, was in der Praxis zu erheblicher Rechtsunsicherheit führt. Zur Vermeidung potenzieller Rechtsverletzungen werden häufig extensive Einwilligungserklärungen eingeholt, die über den tatsächlichen Verarbeitungszweck hinausgehen. Dieses Vorgehen erschwert betroffenen Personen die effektive Kontrolle über ihre personenbezogenen Daten. Besonders problematisch erweist sich dies bei unzureichender Informationsbereitstellung oder dem Verweis auf vage formulierte Datenschutzerklärungen.¹²⁶

4.4.3 Herausfordernde Umsetzung der Einwilligungsanforderungen

Die Voraussetzungen für eine rechtswirksame Einwilligung genügen nicht, um die digitale Selbstbestimmung umfassend zu gewährleisten. Dies zeigt sich insbesondere in der praktischen Umsetzung der angemessenen Information und der Freiwilligkeit. Obwohl die angemessene Information die betroffene Person in die Lage versetzen soll, eine informierte Entscheidung zu treffen, kann nicht davon ausgegangen werden, dass alle Detailhinweise zur Datenverarbeitung vollständig zur Kenntnis genommen werden. Ein umfassendes Verständnis sämtlicher Verarbeitungsprozesse ist aufgrund der Informationsfülle für Laien kaum realistisch. Das Konzept der angemessenen Information erweist sich daher in der Praxis als Fiktion.¹²⁷ Hinsichtlich der Freiwilligkeit besteht zudem die Gefahr, dass Personen unter Druck gesetzt werden, ihre Einwilligung zur Datenverarbeitung zu erteilen, um eine notwendige und nicht substituierbare Gegenleistung zu erhalten (Kopplungsgeschäft). Dieses Potenzial zur Fremdbestimmung schwächt das Prinzip der Entscheidungsfreiheit erheblich.¹²⁸

Demgegenüber bedeutet das Recht auf jederzeitigen Widerruf für die datenempfangenden Stellen eine Einschränkung der Datenverarbeitung. Die Notwendigkeit, einen unvorhersehbaren Verarbeitungsabbruch organisatorisch zu bewältigen, stellt nicht nur eine administrative Herausforderung¹²⁹ dar, sondern beeinträchtigt auch die praktische Verlässlichkeit des Einwilligungskonzepts¹³⁰.

4.4.4 Schwächung des Datenschutzes

Die Einwilligung fungiert als Instrument zur Stärkung der informierten Selbstbestimmung, indem sie den betroffenen Personen die Kontrolle über ihre personenbezogenen Daten ermöglicht. Demgegenüber legitimiert die Einwilligung im privatrechtlichen Kontext jedoch auch die Durchbrechung

¹²⁶ BÜHLMANN/SCHÜEPP, Rz. 122; FASNACHT, Kap. Rz. 219.

¹²⁷ BÜHLMANN/SCHÜEPP, Rz. 53; GASSNER Informed Consent, S.48ff.

¹²⁸ ähnlich GASSNER Informed Consent, S. 50f.; vgl. Kap. 4.2.2.

¹²⁹ vgl. zur Herausforderung des datenschutzrechtlichen Widerrufsrechts im internationalen Rechtskontexts z.G. FLOREA, S. 107-123.

¹³⁰ WIDMER/BÜHLMANN *et al.*, S. 46.

fundamentaler Bearbeitungsprinzipien des Datenschutzgesetzes.¹³¹ Hieraus resultiert ein zentraler Widerspruch zwischen dem Schutzgedanken der digitalen Selbstbestimmung und der tatsächlichen Reichweite der Einwilligung, welche die materiellen Schranken des Datenschutzes überwindet.¹³²

4.4.5 Grenzen des Einwilligungskonzepts im digitalen Zeitalter

Die Entwicklungen im Bereich RWD und Big Data sowie der Einsatz von KI stellen neue Anforderungen an das geltende Einwilligungskonzept. Die Wirksamkeitsvoraussetzungen, insbesondere das Erfordernis der angemessenen Information, sind angesichts der zunehmenden Datenverknüpfung mit den Realitäten der Digitalisierung kaum vereinbar.¹³³ Darüber hinaus eröffnet der Aufbau spezifischer digitaler Infrastrukturen, wie bspw. des EPD, gleichzeitig neue technische Möglichkeiten und vielfältige Integrationspotenziale für die kontrollierte Datennutzung und Zugriffssteuerung. Angesichts dieser Entwicklungen ist der derzeitige Einwilligungsprozess nicht mehr zeitgemäß und bedarf einer umfassenden Überarbeitung, die auf die Stärkung der digitalen Selbstbestimmung abzielt.¹³⁴

4.4.6 Fazit für die künftige Ausgestaltung der Einwilligung

Die Betrachtung zeigt deutlich, dass im bestehenden Einwilligungsmodell die digitale Selbstbestimmung und damit die Interessen der Bürgerinnen und Bürger unzureichend berücksichtigt werden. Darüber hinaus bestehen erhebliche Rechtsunsicherheiten hinsichtlich der Frage, wann eine rechtswirksame Einwilligung tatsächlich vorliegt. Angesichts der neuen Entwicklungen im Zuge der Digitalisierung und den damit verbundenen Nutzungsszenarien ist eine grundlegende Modernisierung des klassischen Einwilligungskonzepts geboten.

¹³¹ vgl. Kap. 4.1.

¹³² BAERISWIYL, S. 3-4; BAERISWYL Einwilligung, S. 65.

¹³³ AUGSBERG/V. ULMENSTEIN, S. 343 ff.; Bericht Po. H umbel, S. 34; vgl. Kap. 3.1.1.

¹³⁴ vgl. Kap. 3.2.

5 Zukünftige Modelle und Regulierungsansätze der Einwilligung

Basierend auf den bisherigen Erkenntnissen zur zukünftigen Gestaltung der Einwilligung analysiert dieses Kapitel alternative Regulierungsmodelle und -ansätze. Als ergänzender Bezugsrahmen dient die Zugangsregelung für die Sekundärnutzung im EHDS. Abschliessend erfolgt eine systematische Gegenüberstellung der vorgestellten Konzepte hinsichtlich ihrer spezifischen Eignung für die künftige Gesetzgebung, wobei die Feststellungen der vorangegangenen Kapitel als Bewertungsgrundlage dienen.

5.1 Ausgangslage

Die effizientere Sekundärnutzung von Gesundheitsdaten erfordert die Erfüllung vielfältiger Anforderungen. Zentral ist die Etablierung eines übergreifenden Rechtsrahmens mit verbindlichen, aber flexiblen Bestimmungen, der die Weiterverwendung von Daten fördert und gleichzeitig Rechtssicherheit gewährleistet. Die rechtliche Ausgestaltung muss dabei die nachhaltige Koordination zwischen internationalen und nationalen politischen sowie legislativen Initiativen und dem technologischen Fortschritt gewährleisten. Diese mehrdimensionale Abstimmung ist essentiell für die grenzüberschreitende Harmonisierung der Sekundärnutzung von Gesundheitsdaten. Gleichzeitig gilt es, das Vertrauen der Bevölkerung durch transparente und sichere Datenverwendung zu wahren sowie die digitale Selbstbestimmung zu stärken. Das Konzept der Einwilligung nimmt hierbei eine zentrale Rolle ein: Es garantiert einerseits die Verfügungsmacht über persönliche Daten und bietet andererseits den Datenempfängern Rechtssicherheit bei der Datenverarbeitung. Das derzeit geltende Einwilligungsmodell, basierend auf dem *informed consent* mit Opt-in-Prinzip, steht jedoch angesichts der Anforderungen an ein zukunfts-fähiges Modell zunehmend in der Kritik¹³⁵.

5.2 Einwilligungsmodelle

Basierend auf den eingangs definierten Anforderungen an ein zukunfts-fähiges Einwilligungsmodell erfolgt eine systematische Eignungsprüfung verschiedener Ansätze.

5.2.1 *broad consent*

Das geltende Konzept der informierten Einwilligung wird insbesondere im Forschungskontext als zu restriktiv erachtet. Die wissenschaftliche Forschung ist für ihre Untersuchungen auf ein umfangreiches Volumen an Gesundheitsdaten angewiesen. Im Widerspruch zum *informed consent* lassen sich die konkreten Forschungsziele und potenziellen späteren Verwendungszwecke zum Zeitpunkt der

¹³⁵ vgl. Kap. 4.4.

Einwilligungserteilung oft nicht genau festlegen, was die Information der Betroffenen erschwert. Bevorzugt wird daher das *broad consent*-Modell¹³⁶. Dieses Konzept sieht eine erweiterte Form der Einwilligung vor: Anstelle einer spezifischen, zweckgebundenen Zustimmung ermöglicht es eine allgemeine Einwilligung für ein breites Spektrum zukünftiger Datenverwendungen. Diese pauschale Zustimmung umfasst sowohl die künftige Nutzung als auch die Weitergabe der Daten. Der Datenbearbeitung kann in diesem Zusammenhang jederzeit widersprochen werden. Der *broad consent* erweist sich insbesondere für die wissenschaftliche Forschung als vorteilhaft, da er den administrativen und finanziellen Aufwand für die wiederholte Einholung von Einwilligungen erheblich reduziert.¹³⁷

a) *broad consent im HFG*

Das Schweizer Datenschutzrecht ermöglicht die Anwendung eines *broad consent* im Rahmen der spezialgesetzlichen Regelungen gemäss in Art. 32 Abs. 2 sowie Art. 33 Abs. 1 HFG. Demnach ist die Weiterverwendung von genetischen Daten und biologischem Material in verschlüsselter Form sowie nichtgenetischen gesundheitsbezogenen Personendaten in unverschlüsselter Form für Forschungszwecke zulässig, sofern die betroffenen Personen vorab über die Datenverarbeitung informiert wurden und dieser nicht widersprochen haben. Aufgrund der erhöhten Gefährdung der Persönlichkeitsrechte muss die Aufklärung in diesem Kontext mündlich erfolgen. Zudem besteht für die Einwilligung ausnahmsweise ein Schriftformerfordernis.¹³⁸ Die Generaleinwilligung des HFG wird durch die Generalkonsent-Vorlage der Schweizerischen Akademie der Medizinischen Wissenschaften (SAMW) und swissethics konkretisiert. Diese nicht bindende Vorlage zielt auf eine schweizweite Harmonisierung des Generalkonsents ab und soll die Zusammenarbeit zwischen Forschungsinstitutionen erleichtern. Bislang haben sich lediglich fünf Universitätsspitäler zur Übernahme entschlossen.¹³⁹

Die nationale Initiative des Swiss Personalized Health Network (SPHN) entwickelt das Konzept des Generalkonsents durch die Implementierung eines elektronischen Generalkonsents (E-General Consent) weiter. Diese digitale Transformation des Einwilligungsprozesses verfolgt zwei zentrale Bestrebungen: Einerseits soll durch einen effizienteren Zustimmungsprozess die Anzahl der Einwilligungen erhöht werden, andererseits die informierte Aufklärung für die betroffenen Personen verständlicher gestaltet werden.¹⁴⁰

¹³⁶ Das *broad consent* Modell ist auch unter folgenden Begriffen bekannt: General Consent/ Generaleinwilligung, oder Blanket consent/Blankovollmacht.

¹³⁷ AUGSBERG/V. ULMENSTEIN, S. 344; RICHTER/BUYX, S. 315ff.

¹³⁸ SPRECHER Datenschutz und Big Data, S.526ff. Art. 29 Abs. 1 und 2 HFV.

¹³⁹ SPRECHER Datenschutz und Big Data, S. 526ff.; Universitäre Medizin Schweiz, Generalkonsent für die Forschung <<https://www.unimedssuisse.ch/de/projekte/generalkonsent>> (besucht am 13.11.2024).

¹⁴⁰ SPHN E-General Consent.

b) *broad consent im Kontext der Sekundärnutzung*

Die Sekundärnutzung von Gesundheitsdaten gestaltet sich durch eine Generaleinwilligung im Vergleich zum *informed consent* effizienter.¹⁴¹ Der praktische Nutzen steht jedoch im Spannungsverhältnis zum Recht auf digitale Selbstbestimmung der betroffenen Personen. Die einmalige allgemeine Zustimmung für diverse, noch nicht definierte Bearbeitungszwecke verschiebt die Kontrolle über personenbezogene Daten von den Betroffenen zu den Datenverwendern.¹⁴² Darüber hinaus widerspricht die Generaleinwilligung auch dem privatrechtlichen Persönlichkeitsschutz sowie dem Zweckbindungsgebot in Art. 6 Abs. 3 DSG.¹⁴³

In Anlehnung an das HFG müssen insbesondere mit der Einschränkung der Selbstbestimmung erhöhte Anforderungen an die Einwilligung einhergehen. Potenzielle Massnahmen, wie die zwingende schriftliche Dokumentation der Zustimmung, hätten jedoch erneut einen gesteigerten administrativen Aufwand zur Folge.¹⁴⁴

c) *Kritische Würdigung des broad consent im HFG*

Die bisherige Implementierung des *broad consent* im HFG reflektiert primär die Forschungsinteressen. Demgegenüber sehen sich die betroffenen Personen durch die Umsetzung des Generalkonsents aus datenschutzrechtlicher Perspektive mit einer ungünstigeren Ausgangslage konfrontiert.¹⁴⁵ Die unzureichend detaillierte Regelung des *broad consent* sowie deren Ergänzung durch Soft Law bieten keine hinreichende Absicherung gegen Datenmissbrauch. Zudem mangelt es dem Generalkonsent an ausreichender demokratischer Legitimation.¹⁴⁶ Diese grundlegende Problematik wird auch durch die Entwicklung eines E-General-Consent und die damit verbundene verbesserte Information der Betroffenen nicht gelöst. Die künftige Relevanz des E-General-Consent wird durch die geringe Anzahl von nur fünf teilnehmenden Universitätsspitalern aktuell erheblich eingeschränkt.¹⁴⁷

d) *Fazit*

Die Generaleinwilligung erleichtert die Sekundärnutzung von Gesundheitsdaten, und digitale Initiativen wie der E-General-Consent entsprechen dem Trend zur Digitalisierung im Gesundheitswesen. Der

¹⁴¹ RICHTER/BUYX, S. 315ff.

¹⁴² AUGSBERG/V. ULMENSTEIN, S. 344; MAUSBACH, Rz. 32ff.

¹⁴³ MAUSBACH, Rz 32ff.

¹⁴⁴ vgl. siehe oben.

¹⁴⁵ Auch der Bundesrat ist sich der datenschutzrechtliche und zivilrechtliche Kritik hinsichtlich der relativen Unbestimmtheit des Verwendungszwecks und der auf unbestimmte Zeit angelegten Einwilligung bewusst, vgl. Teilrevision Ausführungsrecht HFG, S.S. 41.

¹⁴⁶ SPRECHER Datenschutz und Big Data, S. 526ff.; SPRECHER Gesundheitsdatenräume, S. 43.

¹⁴⁷ vgl. siehe oben.

broad consent privilegiert jedoch primär die Forschungsinteressen, während die digitale Selbstbestimmung der betroffenen Personen substantiell eingeschränkt wird. Diese signifikante Beeinträchtigung der individuellen Kontrolle über personenbezogene Daten limitiert eine standardmässige Implementierung des Generalkonsents als zukunftsfähiges Einwilligungsmodell.

5.2.2 *dynamic consent*

Die dynamische Einwilligung (*dynamic consent*) nimmt eine Position zwischen den Extremen des *broad consent* und des *informed consent* ein.¹⁴⁸ Diese vermittelnde Lösung basiert auf einer elektronischen Kommunikationsplattform, die den Austausch zwischen Datengebenden und Datenverarbeitenden ermöglicht. Die Einwilligung erfolgt dabei gezielt für ausgewählte Datenbearbeitungsprojekte, wobei die betroffenen Personen ihre Einwilligungserklärungen jederzeit ändern, widerrufen oder für neue Vorhaben erteilen können. Die dynamische Charakteristik dieses Modells manifestiert sich in der kontinuierlichen Anpassungsmöglichkeit der Einwilligungen. Die digitale Plattform stellt die erforderlichen Informationen zu den Verarbeitungszwecken bereit und unterstützt durch medienübergreifende Aufbereitung das Verständnis komplexer Sachverhalte. Zugleich ermöglicht sie den betroffenen Personen eine transparente Dokumentation und Verwaltung ihrer Einwilligungserklärungen. Diese digitale Infrastruktur vereinfacht im Vergleich zu analogen Prozessen die Kontrolle und insbesondere die Ausübung des Widerrufsrechts erheblich.¹⁴⁹

a) *dynamic consent im Schweizer Datenschutzrecht*

Die dynamische Einwilligung ist bislang nicht in der Schweizer Gesetzgebung verankert. Im Rahmen der langfristigen Erfassung und nachhaltigen Optimierung der Gesundheits- und Versorgungssituation wird dieses Modell jedoch als bevorzugte Alternative zum bisherigen *informed consent* betrachtet. Vorgesehen ist, dass betroffene Personen im Rahmen der Primärnutzung, nach angemessener Information, ihre Einwilligung elektronisch für spezifische Projekte erteilen (Opt-in). Für die Sekundärnutzung der Daten wird ein fallspezifisches Widerspruchsrecht in Erwägung gezogen. Ab der ersten Einwilligung werden die betroffenen Personen fortlaufend über die Weiterverwendung ihrer Daten informiert und können einzelnen Vorhaben jederzeit widersprechen (Opt-out).¹⁵⁰

¹⁴⁸ RICHTER/BUYX, S. 318.

¹⁴⁹ KAYE *et al.*, S. 141-143; MAUSBACH, Rz. 4ff.

¹⁵⁰ Bericht Po. Humbel, S.40.

b) *dynamic consent im Kontext der Sekundärnutzung*

Für die Sekundärnutzung von Gesundheitsdaten sind insbesondere die Modifikationsmöglichkeiten der dynamischen Einwilligung bedeutsam. Die Einwilligung könnte dabei nicht nur für spezifische Forschungsvorhaben, sondern für übergeordnete Kategorien oder Verarbeitungszwecke erteilt werden. Eine alternative Option wäre die Ableitung von Präferenzen aus dem bisherigen Einwilligungsverhalten. Beide Ansätze vereinfachen den Zustimmungsprozess und ermöglichen potenziell ein höheres Datenaufkommen als der *informed consent*.¹⁵¹ Die digitale Selbstbestimmung erfährt durch dieses Modell eine aktive Stärkung. Der hohe Stellenwert der Selbstbestimmung manifestiert sich in der anwendungsorientierten Umsetzung der Einwilligungskriterien - insbesondere der angemessenen Information und Freiwilligkeit - über die digitale Plattform.¹⁵² Das Modell fördert zudem die Transparenz und Kommunikation zwischen den beteiligten Parteien sowie die Festigung des öffentlichen Vertrauens.¹⁵³ Aus Forschungsperspektive erleichtert die dynamische Einwilligung die Identifikation und Kontaktaufnahme mit geeigneten Studienteilnehmenden.¹⁵⁴

Die erfolgreiche Implementierung der dynamischen Einwilligung ist massgeblich von der zugrundeliegenden Infrastruktur abhängig. Die Gewährleistung der Selbstbestimmung sowie der Schutz der Gesundheitsdaten erfordern eine hochwertige technische Ausgestaltung der digitalen Plattform. Zudem setzt das Konzept eine verstärkte Zusammenarbeit zwischen den beteiligten Akteuren voraus.¹⁵⁵

Die Verlagerung zu einem elektronischen Einwilligungsverfahren entspricht zwar dem Digitalisierungstrend, birgt jedoch spezifische Risiken. Ein Teil der Bevölkerung könnte die Nutzung einer elektronischen Plattform grundsätzlich ablehnen. Diese selektive Partizipation bestimmter Personengruppe führt möglicherweise zu systematischen Verzerrungen (Bias) in den verfügbaren Daten.¹⁵⁶ Zudem zeigen Befragungen im Kontext des EPD, dass ein Teil der Nutzenden sich durch die elektronische Handhabung von Entscheidungsprozessen überfordert fühlen und Unterstützung benötigen.¹⁵⁷ Ein zentraler Kritikpunkt betrifft die potenzielle Informationsüberlastung der betroffenen Personen. Besonders relevant ist die Gefahr einer Routinisierung des Einwilligungsprozesses durch excessive Einwilligungsanfragen. Dies könnte zu einer oberflächlichen, mechanischen Bestätigung statt einer fundierten Prüfung

¹⁵¹ MAUSBACH, Rz. 6ff.

¹⁵² MOLNÁR-GÁBOR, S. 803; vgl. KAYE *et al.*, S. 145.

¹⁵³ KAYE *et al.*, S. 141; MAUSBACH, Rz. 4ff.

¹⁵⁴ KAYE *et al.*, S. 145.

¹⁵⁵ AUGSBERG/V. ULMENSTEIN, S. 344.

¹⁵⁶ MAUSBACH, Rz. 14.

¹⁵⁷ gfs.bern, Künstliche Intelligenz als grosse Unbekannte mit viel Potenzial – Bevölkerung zeigt sich offen für nächste Digitalisierungsschritt im Gesundheitswesen <<https://cockpit.gfsbern.ch/de/cockpit/ehealth-bevoelkerung-2024/>> (besucht am 14.11.2024).

der Anfragen führen. Als Alternative sollte den betroffenen Personen daher auch die Option eines *broad consent* als Präferenz zur Verfügung stehen.¹⁵⁸

c) *Kritische Würdigung des dynamic consent im Schweizer Datenschutzrecht*

Die Integration einer dynamischen Einwilligung in das schweizerische Datenschutzrecht stellt primär infrastrukturelle Anforderungen. Integrationspotenziale könnten durch eine Verknüpfung der Einwilligung mit dem EPD genutzt werden. Die EPD-Strukturen sind gegenwärtig jedoch nicht auf die Sekundärnutzung von Gesundheitsdaten ausgerichtet, und künftige Entwicklungen konzentrieren sich ausschliesslich auf den Forschungszugang. Alternativ könnte die technische Basis des geplanten Gesundheitsdatenraums genutzt werden, insbesondere da dieser die Sekundärnutzung gezielt fördern soll. Dagegen spricht jedoch, dass betroffene Personen keinen Zugang zum Gesundheitsdatenraum erhalten sollen. Nicht die Selbstbestimmung über die Verwendung persönlicher Gesundheitsdaten, sondern deren Verfügbarkeit für die Forschung steht bei diesem Projekt im Vordergrund. Die Etablierung einer eigenständigen technischen Basis für die dynamische Einwilligung ist zwar möglich, würde jedoch das vorhandene Synergiepotenzial - auch im Hinblick auf einen EHDS-Anschluss - ungenutzt lassen und zur Komplexität der Gesamtsituation beitragen.¹⁵⁹

Sodann ist die vorgeschlagene Ausgestaltung der dynamischen Einwilligung für die Sekundärnutzung von Gesundheitsdaten kritisch zu bewerten. Der implementierte Nudging-Mechanismus sieht eine standardmässige Generaleinwilligung für alternative Verwendungszwecke vor, sofern kein aktiver Widerspruch erfolgt. Diese Konzeption schränkt das Selbstbestimmungspotenzial des *dynamic consent* beachtlich ein.

d) *Fazit*

Der *dynamic consent* überzeugt durch die flexible Kontrolle und individuelle Gestaltung des Einwilligungsprozesses. Die transparente Informationsvermittlung wahrt die rechtlichen Anforderungen an die Einwilligung und stärkt das Vertrauen in den Datenschutz. Die Digitalisierung und Automatisierung bisher analoger Prozesse ermöglicht zudem eine effiziente und sichere Sekundärnutzung von Gesundheitsdaten. Die Umsetzung in das schweizerische Datenschutzrecht steht jedoch vor einer zentralen Herausforderung: Es fehlt an einer kompatiblen technischen Infrastruktur.

5.2.3 *meta consent*

Die Kaskadeneinwilligung (*meta consent*) stellt als Weiterentwicklung des *dynamic consent* ein alternatives Modell zur Harmonisierung einer effizienten Datennutzung und digitaler Selbstbestimmung

¹⁵⁸ MOLNÁR-GÁBOR, S. 803; PLOUG/HOLM, S. 723.

¹⁵⁹ vgl. Kap. 3.2 und 3.4.

dar.¹⁶⁰ Der *meta consent*¹⁶¹ basiert auf der Abgabe von Präferenzen. Die Einwilligung erfolgt nicht direkt, sondern auf einer Metaebene. Die betroffene Person definiert vorab anhand festgelegter Kategorien ihre Einwilligungspräferenzen. Diese umfassen bspw.

- das präferierte Einwilligungsmodell,
(*informed consent, broad consent, consent to govern etc.*)
- die Art der bereitzustellenden Daten
(genetische Daten, nicht-genetische Daten, Behandlungsdaten, Lifestyle Daten etc.)
- sowie die bevorzugten Verwendungszwecke.
(private oder öffentliche Forschung, klinische Studien, öffentliche Verwaltung etc.)

Die digitale Plattform interagiert auf Basis dieser Präferenzen mit den betroffenen Personen und informiert über die Auswirkungen der festgelegten Entscheidungen, die aktuelle Nutzungssituation der persönlichen Daten sowie die Anzahl der Zustimmungsanfragen. Basierend auf diesen Rückmeldungen können die individuellen Präferenzen jederzeit angepasst werden. Wenn keine Einwilligungsprioritäten festgelegt werden, kommen vordefinierte Standardeinstellungen zur Anwendung. Im Optimalfall widerspiegelt diese Default-Option neben dem Forschungsinteresse auch die Anforderungen an den Persönlichkeitsschutz. Um Präferenzen konsistent an den jeweiligen Lebenslagen zu orientieren, erinnert die Plattform regelmässig an die getroffenen Einwilligungsprioritäten und hinterfragt diese damit aktiv.¹⁶²

a) *meta consent im Kontext der Sekundärnutzung*

Der *meta consent* stellt eine präferenzbasierte Variante des *dynamic consent* dar. Beide Modelle beeinflussen die Sekundärnutzung von Gesundheitsdaten in ähnlicher Weise. Ein wesentlicher Unterschied manifestiert sich jedoch in den Auswirkungen der Kaskadeneinwilligung auf die angemessene Information als zentrale Gültigkeitsvoraussetzung der Einwilligung. Diese erfolgt nicht wie beim *dynamic consent* detailliert und projektspezifisch, sondern im breiteren Kontext und bildet primär die Präferenzen ab. Die betroffene Person wird anschliessend im Rahmen des Einwilligungsprozesses mit einer komprimierten, aber zielgerichteten Informationsmenge konfrontiert, die auf ihre individuellen Bedürfnisse und Interessen abgestimmt ist.¹⁶³ In der Fachliteratur wird argumentiert, dass dieser Kompromiss zu konsistenteren Entscheidungen führt, die gleichermaßen informiert und überlegt sind.¹⁶⁴ Kritische

¹⁶⁰ AUGSBERG/V. ULMENSTEIN, S. 344.

¹⁶¹ Im Folgenden wird der von PLOUG/HOLM beschriebene *meta consent* als repräsentativer Ansatz diskutiert. Obwohl dieser primär auf die Forschung ausgerichtet ist, lässt sich das Konzept auch allgemein auf die Sekundärnutzung anwenden.

¹⁶² z.G. PLOUG/HOLM, S. 721ff.

¹⁶³ PLOUG/HOLM, S. 724ff.

¹⁶⁴ PLOUG/HOLM, S. 728; 731.

Stimmen hinterfragen jedoch, inwiefern eine vollständige Information und Schutz der Betroffenen unter diesen Umständen gewährleistet werden kann.¹⁶⁵

Der *meta consent* basiert auf einem anspruchsvollen Konzept, das ein komplexes Einwilligungssystem erfordert. Diese Komplexität beeinflusst die praktische Handhabung der digitalen Verwaltungsplattform. Die Fachliteratur empfiehlt daher, die Umsetzung durch Informationskampagnen und Bildungsmaßnahmen zu begleiten, um der Bevölkerung die Tragweite der Präferenzabgabe zu vermitteln.¹⁶⁶ Diese Massnahmen ergänzen bestehende Initiativen zur Förderung der digitalen Kompetenz¹⁶⁷ und stellen im Hinblick auf eine potenzielle Einführung der Kaskadeneinwilligung einen zukunftsweisenden Ansatz dar.

b) Fazit

Die Kaskadeneinwilligung kompensiert Schwachstellen des *dynamic consent* durch die Weiterentwicklung des dynamischen Modells mittels Präferenzabbildung und gezielter Reduktion der Informationsflut. Die Bestrebungen nach einer effizienteren Sekundärnutzung von Gesundheitsdaten führen zu einem vereinfachten Einwilligungsprozess. Dies resultiert wiederum in einer eingeschränkteren Information der betroffenen Personen. Die inhärente Komplexität - sowohl des Konzepts als auch der technischen Verwaltungsplattform - könnte zu Akzeptanzproblemen auf Seiten der Nutzenden führen. Mangelndes Verständnis der zugrundeliegenden Prozesse kann darüber hinaus das Vertrauen der Bevölkerung in den Datenschutz beeinträchtigen.

5.2.4 Datentreuhänder

Das Modell des Datentreuhänders stellt eine Variante des *dynamic consent* dar. In der Fachliteratur wird das zugrundeliegende Prinzip unter verschiedenen Bezeichnungen diskutiert: *attorney model*, *consent to govern* oder Einwilligungsassistent. Das Konzept zielt auf die Stärkung der Autonomie und Kontrolle betroffener Personen im digitalen Umfeld ab. Parallel dazu erfolgt die Übertragung des Rechts auf angemessene Information sowie der darauf basierenden Einwilligungsfähigkeit an eine Drittpartei. Diese Lösung adressiert simultan zwei Herausforderungen des Ursprungsmodeells der dynamischen Einwilligung: die Reduktion der Informationsfülle und die Überbrückung laienbedingter Informationsdefizite. Die Delegation der Einwilligung richtet sich primär an Fachgremien, Ethikkommissionen, Governance Boards oder speziell entwickelte KI-Systeme. Die Zustimmung zur Datenverarbeitung erfolgt vorrangig nach den von der betroffenen Person definierten Instruktionen und Präferenzen. Bei fehlenden Vorgaben fließen die durch den jeweiligen Treuhänder vertretenen Interessen in den

¹⁶⁵ RICHTER/BUYX, S. 318

¹⁶⁶ PLOUG/HOLM, S. 727.

¹⁶⁷ vgl. Kap. 3.1.2.

Entscheidungsprozess ein. Der Einwilligungsassistent hingegen trifft Entscheidungen auf Basis bisheriger Verarbeitungspräferenzen.¹⁶⁸

a) Datentreuhänder-Modell im Kontext der Sekundärnutzung

Das geltende schweizerische Datenschutzrecht ist mit dem Konzept des Datentreuhänders nicht vereinbar. Die Einwilligung stellt ein höchstpersönliches Recht der betroffenen Person dar, was eine Delegation grundsätzlich ausschliesst. Ein Lösungsansatz dieser Inkompatibilität manifestiert sich auf technischer Ebene: Anstelle einer Übertragung von Persönlichkeitsrechten soll die betroffene Person durch technische Hilfsmittel bei der Rechtsausübung unterstützt werden. Hierzu bieten sich standardisierte Vertragsbestandteile in Form von "Design your Privacy"-Lizenzen¹⁶⁹ an. Alternativ wäre der Einsatz einer KI-gestützten Anwendung als Einwilligungsassistent denkbar, die ausschliesslich auf Basis individueller Präferenzen agiert. Die einzige weitere rechtskonforme Alternative bestünde in der Einführung eines gesetzlichen Erlaubnistatbestands für Vertretungen im Kontext der Einwilligung, wobei die grundsätzliche Zulässigkeit der Delegation weiterhin kontrovers diskutiert werden würde.¹⁷⁰

b) Fazit

Das Konzept des Datentreuhänders weist erhebliche Defizite bei der Unterstützung einer effizienten Sekundärnutzung unter Wahrung der digitalen Selbstbestimmung auf. Kritisch erscheint insbesondere die vollständige Delegation des Rechts auf angemessene Information an eine externe Stelle. Diese Übertragung umfasst zudem die Einwilligungskompetenz, wodurch die Drittpartei umfassende Entscheidungsgewalt über die Freigabe persönlicher Daten von Betroffenen erhält. Mit der Skalierung des Konzepts des Datentreuhänder steigt das Potenzial für eine missbräuchliche Datenverarbeitung aufgrund der gebündelten Entscheidungskompetenzen auf Seiten der Treuhänder. Ohne eine effektive Kontrolle und Aufsicht besteht das substantielle Risiko, dass wirtschaftliche oder forschungsbezogene Drittinteressen bei der Datenverwaltung Vorrang vor den individuellen Präferenzen der betroffenen Personen erhalten. Auch der Einsatz KI-basierter Einwilligungsassistenten birgt aufgrund potenzieller algorithmischer Verzerrungen die Gefahr einer missbräuchlichen Datenverwendung. Ein sinnvoller Einsatz des Datentreuhänder Modell bietet dagegen die Integration als optionale Einwilligungsform im Rahmen eines *meta consent*. Hierfür müsste jedoch eine gesetzliche Grundlage geschaffen werden.

¹⁶⁸ FASNACHT, Kap. 3 Rz. 448ff.; HORNSTEIN *et. al.*, S. 52; HUMMEL *et. al.*, S. 17; RICHTER/BUYX, S. 17.

¹⁶⁹ z.G. FASNACHT, Kap. 3 Rz. 451.

¹⁷⁰ FASNACHT, Kap. 3 Rz. 448; RICHTER/BUYX, S. 317.

5.2.5 Datenspende

Die Datenspende bezeichnet die freiwillige Bereitstellung persönlicher Daten durch die betroffene Person ohne spezifische Gegenleistung. Im Gegensatz zur regulären Einwilligung basiert die Datenspende primär auf altruistischen Motiven und dem Wunsch, gemeinnützige Vorhaben zu unterstützen. Die Erlangung persönlicher Vorteile durch die Datenfreigabe tritt dabei in den Hintergrund. Ein weiterer fundamentaler Unterschied zur Einwilligung manifestiert sich in der flexibleren Handhabung des Zweckbindungsgebots. Datenspenden erfolgen typischerweise mit der Intention, die Daten einem breiten Nutzungsspektrum zugänglich zu machen. Die betroffene Person behält dabei das Recht, die Datenverarbeitung jederzeit durch Widerruf zu unterbinden.¹⁷¹

a) *Datenspende im Schweizer Datenschutzrecht*

Der Bericht zum Po. Humbel evaluiert die Datenspende neben dem *dynamic consent* als potenzielle künftige Einwilligungsform für die Sekundärdatennutzung. Die Prüfung dieses Ansatzes geht auf das Postulat „Nutzung anonymisierter persönlicher Daten im öffentlichen Interesse. Prüfung der Machbarkeit einer freiwilligen Datenspende“ zurück, wonach der Bundesrat dem Parlament Lösungsvorschläge zur Förderung der Datenspende in anonymisierter Form unterbreiten sollte.¹⁷² Das resultierende Konzept sieht eine freiwillige Datenspende vor, die an eine nicht weiter spezifizierungsbedürftige Sekundärnutzung gekoppelt ist. Die Datennutzung unterliegt voraussichtlich einer zeitlichen Beschränkung, während der das Widerrufsrecht temporär suspendiert ist. Nach Ablauf dieser Frist lebt das Widerrufsrecht wieder auf. Für die Spende kommen sowohl neu erhobene, bestehende als auch künftige Daten in Betracht. Eine kommerzielle Nutzung ist hingegen ausgeschlossen.¹⁷³

b) *Datenspende im Kontext der Sekundärnutzung*

Die rechtliche Legitimation der Datenspende stützt sich auf die ausgeprägte informationelle Selbstbestimmung der betroffenen Personen.¹⁷⁴ Die Eignung dieses Ansatzes als Instrument für eine effiziente Weiterverwendung von Gesundheitsdaten hängt dagegen massgeblich von der Spendebereitschaft der Bevölkerung ab. Erhebungen in der Schweiz und in Deutschland zeigen, dass Individuen dem Konzept grundsätzlich positiv gegenüberstehen, ihre Partizipation jedoch primär vom Verwendungszweck der

¹⁷¹ DIRKSEN *et al.*, S. 1; Stiftung Risiko-Dialog, Vorstudie Datenkooperation CH / COVID-19 Schlussbericht, Oktober 2020, <https://www.risiko-dialog.ch/wp-content/uploads/2020/10/Schlussbericht_Vorstudie_Datenkooperation_261020.pdf> (besucht am 14.10.2024); vgl. Bericht Po. Humbel, S. 41.

¹⁷² Po. BELLAICHE.

¹⁷³ Bericht Po. Humbel, S. 41.

¹⁷⁴ vgl. Stiftung Risiko-Dialog, Vorstudie Datenkooperation CH / COVID-19 Schlussbericht, Oktober 2020, <https://www.risiko-dialog.ch/wp-content/uploads/2020/10/Schlussbericht_Vorstudie_Datenkooperation_261020.pdf> (besucht am 14.10.2024).

Daten abhängig machen. Insbesondere für Forschungszwecke besteht ein hohes Engagement zur Bereitstellung persönlicher Daten. Das Spendenverhalten basiert daneben auf einem hinreichenden Vertrauen in die datenverarbeitenden Organisationen, Prozesse und Personen. Vorbehalte existieren gegenüber einer Kommerzialisierung gespendeter Daten. Eine breite gesellschaftliche Akzeptanz der Datenspende erfordert daher gezielte Informationskampagnen zur Ausräumung dieser Bedenken.¹⁷⁵

c) Kritische Würdigung der Datenspende im Schweizer Datenschutzrecht

Der schweizerische Ansatz der Datenspende zeichnet sich positiv durch den Ausschluss der kommerziellen Nutzung aus. Die temporäre Suspendierung des Widerrufsrechts stellt hingegen eine erhebliche Einschränkung der Verfügungsgewalt betroffener Personen über ihre persönlichen Daten dar. Ein solcher Kontrollverlust, insbesondere angesichts der Möglichkeit einer unspezifizierten Weiterverwendung bestehender und zukünftiger Daten, könnte nicht nur Misstrauen in der Bevölkerung wecken, sondern auch die Spendenbereitschaft massgeblich reduzieren. Darüber hinaus existieren keine Vorschläge wie die konkrete Einwilligung in die Datenspende erfolgen soll bzw. inwiefern auf ein bestehendes Einwilligungsmodell zurückgegriffen wird.¹⁷⁶

d) Fazit

Das geplante Konzept der Datenspende im schweizerischen Datenschutzrecht zeigt in seiner aktuellen Form wesentliche Ungereimtheiten. Diese betreffen insbesondere die Handhabung des Widerrufsrechts und die Ausgestaltung der Einwilligung. Der Grundgedanke des Ansatzes verdient unter einer Bedingung eine positive Bewertung: Die Gewährleistung eines jederzeitigen Widerrufsrechts. Dies würde den spendenden Personen eine ausgeprägte Selbstbestimmung und Entscheidungsgewalt sichern. Die Implementation der Datenspende als eigenständige Einwilligungsform erscheint, wie beim Konzept des Datentreuhänders, nicht zielführend. Eine Integration als optionale Einwilligungsform im Rahmen eines *meta consent* bietet sich stattdessen eher an.

5.3 Regulierungsansätze in Bezug auf die Einwilligung

Die im Folgenden analysierten Regulierungsansätze entwickeln das bestehende Modell der informierten Einwilligung gezielt weiter. Sie passen die geltende Rechtslage an, bewahren jedoch die grundlegende Systematik der informierten Einwilligung, ohne ein neues Modell einzuführen.

¹⁷⁵ LESCH/RICHTER/SEMLER, S. 215ff.; Stiftung Risiko-Dialog, Datenspende für Gemeinnützigkeit, <https://www.risiko-dialog.ch/wp-content/uploads/2024/02/Whitepaper_Datenspende-fuer-Gemeinnuetzigkeit_Risiko-Dialog_Final.pdf> (besucht am 14.10.2024).

¹⁷⁶ Das Po. BELLAICHE nennt diesbezüglich die Kaskadeneinwilligung als Möglichkeit.

5.3.1 Wechsel zum Opt-out

Der Opt-out-Ansatz wurde in dieser Arbeit bereits im Kontext des EPD¹⁷⁷ erörtert. Bei diesem Konzept handelt es sich um eine Widerspruchslösung, die ein aktives Verweigern der datenschutzrechtlichen Einwilligung voraussetzt, wobei jede andere Reaktion automatisch als Zustimmung gewertet wird.

a) *Opt-out im Kontext der Sekundärnutzung*

Der primäre Vorteil des Opt-out-Prinzips liegt in seiner kostengünstigen und unkomplizierten Umsetzung, die auf Basis des Forschungsinteresses den Zugang zu Gesundheitsdaten erleichtert. Hinsichtlich der digitalen Selbstbestimmung wird dagegen an die Eigenverantwortung der betroffenen Personen appelliert.¹⁷⁸

Kritisch zu bewerten ist der Entwicklungstrend, dass die gesetzgeberischen Erleichterungen im Zusammenhang mit der Sekundärnutzung und die Digitalisierungsbemühungen in sämtliche Fällen einseitig die Forschung begünstigen. Dabei wird eine Einschränkung der digitalen Selbstbestimmung als selbstverständlich in Kauf genommen.¹⁷⁹ Diese Tendenz steht nicht nur im Konflikt mit nationalen verfassungsrechtlichen Prinzipien wie dem Grundsatz der Verhältnismässigkeit, sondern widerspricht auch internationalen Rechtsgrundsätzen.¹⁸⁰ Die systematische Verwendung von Opt-out-Mechanismen als Nudging-Instrument ist besonders bedenklich. Zwar bleibt die Selbstbestimmung formal gewahrt, doch die implizite Verhaltenssteuerung dient primär der Durchsetzung externer Interessen. Die automatische Deutung einer passiven Haltung als Einwilligung zur Datenfreigabe unterläuft dabei die Prinzipien einer echten informierten Selbstbestimmung.¹⁸¹ Diese Problematik verschärft sich durch das Fehlen ausreichender Datenkompetenz der Bevölkerung und dem Mangel an amtlichen Informations- und Aufklärungskampagnen zur Förderung der Data-Literacy.¹⁸² Angesichts dieser Umstände erscheint es zweifelhaft, ob die Betroffenen die ihnen übertragene Verantwortung für den Umgang mit ihren Gesundheitsdaten in angemessener Weise ausüben können.

b) *Fazit*

Die Implementierung des Opt-out-Prinzips in der Schweizer Datenschutzgesetzgebung dient derzeit nicht vorrangig den Interessen der Bevölkerung. Die wiederkehrende Berufung auf das öffentliche Forschungsinteresse als Legitimationsgrund erscheint überstrapaziert und führt zu einer schlechenden

¹⁷⁷ vgl. Kap. 3.2.1.

¹⁷⁸ BUCHHOLZ *et al.*, S. 474; JUNOD/ELGER, Rz. 21ff.

¹⁷⁹ vgl. Kap. 2.3 und 3.4.

¹⁸⁰ SPRECHER Sozialpflichtigkeit, S. 186ff.

¹⁸¹ SPRECHER Datenschutz und Big Data, S. 529ff.

¹⁸² vgl. Kap. 3.4.

Aushöhlung des Rechts auf Selbstbestimmung. Diese Entwicklung birgt die erhebliche Gefahr, das Vertrauen der Bevölkerung in die staatliche Datenpolitik nachhaltig zu erschüttern.

5.3.2 Stärkung der Datenkompetenz

Ein oft vernachlässigter Kernaspekt bei der Sekundärnutzung von Gesundheitsdaten ist die Datenkompetenz. Nach der Data-Literacy-Charta Schweiz umfasst diese die Fähigkeit, „...Daten auf kritisch-reflexive Weise in ihrem jeweiligen Kontext zu sammeln, zu verwalten und zu bewerten“¹⁸³. Gegenwärtig ist einem Grossteil der Bevölkerung der Wert ihrer persönlichen Daten und die damit verbundenen Rechte nur unzureichend bewusst.¹⁸⁴

a) *Stärkung der Datenkompetenz in der Sekundärnutzung*

Staatliche Data-Literacy-Initiativen sollten diesem Defizit durch eine geeignete und transparente Kommunikationsstrategie begegnen. Zentral ist dabei die Sensibilisierung der Bevölkerung im Umgang mit Daten durch gezielte Bildungsmassnahmen. Parallel dazu müssen datenverarbeitende Stellen angemessen geschult werden, um eine rechtskonforme Datenverwendung sicherzustellen.¹⁸⁵ Der Bund weisst in dieser Hinsicht die Verantwortung grösstenteils den Kantonen zu.¹⁸⁶

Im privatrechtlichen Bereich und im alltäglichen Geschäftsverkehr gilt es ebenfalls, die Transparenz der Datenverarbeitung zu erhöhen. Zur wirksamen Reduzierung der Komplexität bieten sich „Privacy Policies“ an, die Kunden in allgemeinverständlicher Sprache über die Verwendung ihrer personenbezogenen Daten informieren. Ein innovativer Ansatz sind „Privacy Nutrition Labels“, die - analog zu Nährwertangaben auf Lebensmitteln - relevante Verarbeitungsdetails kompakt und verständlich darstellen.¹⁸⁷

b) *Fazit*

Eine fundierte Datenkompetenz ist elementare Voraussetzung für die Wahrnehmung digitaler Selbstbestimmung. Obwohl das Parlament bereits Vorstösse zur Förderung der Data-Literacy unternommen

¹⁸³ akademien der wissenschaften schweiz, Data-Literacy-Charta Schweiz <https://api.swiss-academies.ch/site/assets/files/127302/data_literacy_charta_web_de.pdf> (besucht am 17.11.2024).

¹⁸⁴ SPRECHER Datenschutz und Big Data, S. 549ff.

¹⁸⁵ SPRECHER Datenschutz und Big Data, S. 549ff.

¹⁸⁶ Ip. Data-Literacy; Inwiefern die Kantone die Verantwortung im Zusammenhang mit der Datenkompetenz wahrnehmen, ist unterschiedlich und derzeit schwierig abzuschätzen. Als Beispiel sind die Bemühungen des Kanton Zürichs anzuführen vgl. Statistisches Amt Kanton Zürich, Datenkompetenz <<https://www.zh.ch/de/politik-staat/statistik-daten/datenkompetenz.html>> (besucht am 17.11.2024).

¹⁸⁷ FASNACHT, Kap. 2 Rz. 375ff.

hat¹⁸⁸, berücksichtigen aktuelle Initiativen zur Sekundärnutzung diese zentrale Komponente nur unzureichend. Der Bund sollte daher künftig der Durchführung gezielter Aufklärungskampagnen eine deutlich höhere Priorität einräumen.

5.3.3 Transparenz durch Datenbrief

Als regulatorisches Instrument zur Verbesserung der Transparenz dient der Datenbrief der periodischen Information über die aktuelle Bearbeitung persönlicher Daten. Diese Massnahme adressiert das Problem, dass Betroffene im bestehenden Einwilligungssystem häufig den Überblick über ihre erteilten Zustimmungserklärungen verlieren. Dies kann zu unbeabsichtigten, wenn auch formal legitimen Datenverarbeitungen führen kann. Durch regelmässige Erinnerungen in Form von Statusmitteilungen ermöglicht der Datenbrief eine kontinuierliche Kontrolle über die Verwendung persönlicher Daten.¹⁸⁹

a) *Der Datenbrief im Kontext der Sekundärnutzung*

Das Konzept des Datenbriefs hat sich im Kontext der Sekundärnutzung von Gesundheitsdaten bislang nicht etabliert. Stattdessen erscheint die Integration einer digitalen Einwilligungsübersicht im Rahmen der bestehenden Infrastrukturprojekte als effizientere und praktikablere Lösung. Diese könnte im Zuge der ohnehin laufenden Digitalisierungsbemühungen mit geringerem Implementierungsaufwand realisiert werden.

b) *Fazit*

Eine transparente Einwilligungspraxis bei der Sekundärnutzung von Gesundheitsdaten bleibt ein zentrales Anliegen, auch wenn der Datenbrief in der gegenwärtigen Situation keinen unmittelbaren Mehrwert bietet.

5.3.4 Modifikation der Anforderungen an eine gültige Einwilligung

Um die Reichweite der Einwilligung zu Gunsten der digitalen Selbstbestimmung wirkungsvoll einzuschränken werden verschiedene Anpassung der Einwilligungsvoraussetzungen diskutiert.

¹⁸⁸ vgl. Ip. Data-Literacy; Mo. Data-Literacy.

¹⁸⁹ FASNACHT, Kap. 2 Rz. 379ff.

a) Die zeitliche Beschränkung der Einwilligung

Eine erteilte Einwilligung behält ihre Gültigkeit unbefristet, solange kein Widerruf erfolgt¹⁹⁰ oder der ursprüngliche Verarbeitungszweck nicht wesentlich modifiziert wird¹⁹¹. Die Einführung einer zeitlichen Befristung würde die betroffenen Personen zu einer regelmässigen Überprüfung ihrer Einwilligungsentscheidung veranlassen und damit die aktive Ausübung der digitalen Selbstbestimmung fördern. Für datenverarbeitende Stellen böte dieses Vorgehen zugleich eine rechtliche Absicherung sowie die Möglichkeit, Verarbeitungszwecke bei Bedarf anzupassen. Allerdings ist zu berücksichtigen, dass die regelmässige Einholung von Rückbestätigungen einen erheblichen administrativen Aufwand verursacht und zu zusätzlichen Kosten führt, was die praktische Umsetzbarkeit dieser Massnahme einschränken könnte.¹⁹²

b) Einwilligungsverbote

Einwilligungsverbote stellen als regulatorische Massnahme einen erheblichen Eingriff in die Selbstbestimmung dar und werden daher kontrovers diskutiert. Solche Verbote sollten ausschliesslich dort zur Anwendung kommen, wo keine anderen Instrumente zum Schutz verfassungsmässiger Rechte wie der Privatsphäre oder dem Diskriminierungsverbot ausreichen. Die massive Beschränkung der Privatautonomie durch solche Verbote führt jedoch zu erheblichen Umsetzungsschwierigkeiten und Akzeptanzproblemen.¹⁹³

c) Stärkung des Widerrufsrechts

Die Stärkung des Widerrufsrechts zielt darauf ab, dessen Ausübung möglichst anwendungsfreundlich zu gestalten. Dies bedeutet in formeller Hinsicht, dass die künftige Gesetzgebung von zusätzlichen Hürden, wie beispielsweise einem Schriftformerfordernis, absehen sollte. Auf technischer und infrastruktureller Ebene muss die Widerrufserklärung unkompliziert und unverzüglich durchführbar sein. Eine weitere Stärkung des Widerrufsrechts manifestiert sich in der Möglichkeit eines differenzierten (Teil-)Widerrufs, wie er im Konzept des *dynamic consent* vorgesehen ist.¹⁹⁴

d) Fazit

Die Einführung einer befristeten Einwilligung fördert die Legitimität der Datenverarbeitung und stärkt die digitale Selbstbestimmung. Die Umsetzung innerhalb des *informed consent* erfordert jedoch sowohl von den betroffenen Personen als auch von den datenverarbeitenden Stellen einen erheblichen Aufwand

¹⁹⁰ vgl. Kap. 4.2.3.

¹⁹¹ vgl. Kap. 2.2.6 und Art. 6 Abs. 3 DSG

¹⁹² vgl. FASNACHT, Kap. 2 Rz. 412ff.

¹⁹³ FASNACHT, Kap. 2 Rz. 420ff.

¹⁹⁴ vgl. FASNACHT, Kap. 2 Rz. 417ff.; FLOREA, S. 107.

durch die notwendige Erneuerung der Zustimmung. Zukünftige technologische Entwicklungen könnten die Befristung allerdings als personalisierbares Element in das *dynamic consent*-Konzept integrieren. Der vorgeschlagene Teilwiderruf liesse sich ebenfalls in diesen Ansatz und das System des *dynamic consent* einbetten. Von Einwilligungsverboten sollte hingegen aufgrund ihrer bevormundenden Wirkung künftig Abstand genommen werden.

5.3.5 Steigerung der Wirksamkeit über verlässliche Governance-Strukturen

Effektive Governance-Strukturen sind im Kontext von Big Data eine zentrale Voraussetzung zur Prävention von Machtmissbrauch und zur Sicherstellung eines fairen Datenzugangs. Durch Governance werden einheitliche Standards für den Umgang mit Daten etabliert, wobei regulatorische und technische Massnahmen systematisch verknüpft werden. Das primäre Ziel besteht darin, durch die Gewährleistung einer verantwortungsvollen, kompetenten und regelkonformen Datenverarbeitung die digitale Selbstbestimmung zu stärken und das Vertrauen der betroffenen Personen zu fördern.¹⁹⁵

Besondere Relevanz erfährt das Governance-Konzept bei der Ausgestaltung von Datenräumen.¹⁹⁶ Ein massgebliches Beispiel hierfür bietet der EHDS, der Governance-Standards gezielt einsetzt, um technische, rechtliche und organisatorische Barrieren zwischen den Mitgliedstaaten zu überwinden.¹⁹⁷

a) *Governance-Strukturen im Kontext der Sekundärnutzung*

Im Kontext der informierten Einwilligung würde deren Bedeutung und Wirksamkeit als Instrument zur selbstbestimmten Datennutzung durch ein stabiles Governance-System zusätzlich verstärkt. Die Integration in etablierte Governance-Strukturen erhöht somit die Rechtssicherheit und Verlässlichkeit von Sekundärnutzungen von Gesundheitsdaten, die auf Basis einer Einwilligung erfolgen.

b) *Fazit*

Die Etablierung robuster und zuverlässiger Governance-Strukturen optimiert nicht nur die praktische Umsetzung des Einwilligungskonzepts, sondern stärkt auch den verantwortungsvollen Umgang mit sensiblen Daten. Diese regulatorische Herangehensweise verdient insbesondere vor dem Hintergrund der Governance-Entwicklung im EHDS weitere Beachtung und konsequente Weiterentwicklung.

¹⁹⁵ SPRECHER Datenschutz und Big Data, S. 537ff.

¹⁹⁶ z.G. siehe Bericht Datenräume, S. 1-65.

¹⁹⁷ SCHMITT, S. 5.

5.4 Einwilligung und Sekundärdatennutzung im EHDS

Der EHDS verfolgt bei der Sekundärnutzung von Gesundheitsdaten einen regelbasierten Ansatz anstelle der bisher diskutierten Einwilligungspraxis. Grundvoraussetzung für die Datenverarbeitung ist eine Zulassungsprüfung durch die nationale Koordinationsstelle des jeweiligen Mitgliedstaates, wobei diese Stellen auf der allgemeinverbindlichen Grundlage der Daten-Governance-Rahmengesetzgebung etabliert werden. Der Datenzugriff bleibt dabei einem klar definierten Kreis vorbehalten: Akteure aus Forschung und Innovation, politische Entscheidungsträger sowie Regulierungsbehörden. Die erlaubten Datenbearbeitungszwecke sind in Art. 34 Abs. 1 der EHDS-VO abschliessend festgelegt. Anders als in der schweizerischen Einwilligungspraxis sieht der EHDS kein Widerrufsrecht für betroffene Personen vor, die ihre persönlichen Daten nicht zur Verfügung stellen wollen. Stattdessen gewährleistet das System den Datenschutz durch zwei zentrale Mechanismen: Zum einen erfolgt die Datenverarbeitung ausschliesslich in anonymisierter oder pseudonymisierter Form, zum anderen ist die Verarbeitung nur innerhalb der vom EHDS bereitgestellten sicheren Arbeitsumgebung zulässig.¹⁹⁸

Der Verzicht auf das Einwilligungserfordernis bei der Sekundärnutzung von Gesundheitsdaten signalisiert nicht nur einen Paradigmenwechsel¹⁹⁹ in der etablierten Einwilligungspraxis, sondern eröffnet auch Wege für effizientere Verfahren. Die Integration des europäischen Ansatzes in die schweizerische Rechtsordnung stösst jedoch auf strukturelle Hindernisse: Die bestehenden datenschutzrechtlichen Rahmenbedingungen und die aktuelle Ausgestaltung der Sekundärnutzungsinitiativen lassen eine direkte Übernahme aktuell nicht zu.²⁰⁰ Die fundamentale Diskrepanz zwischen dem schweizerischen und dem europäischen Ansatz liegt derzeit in der unterschiedlichen Handhabung identifizierbarer Gesundheitsdaten: Während die Schweiz deren Sekundärnutzung sowohl auf Basis einer Einwilligung²⁰¹ als auch künftig im Rahmen des Gesundheitsdatenraums ausdrücklich ermöglicht²⁰², schliesst der EHDS die Verarbeitung nicht anonymisierter oder pseudonymisierter Daten kategorisch aus.

5.5 Diskussion

Die Modernisierung der Einwilligungspraxis erfordert eine sorgfältige Abwägung zwischen der Stärkung digitaler Selbstbestimmung einerseits und der Gewährleistung einer effizienten Sekundärdatennutzung andererseits. Die Herausforderung besteht darin, einen durchdachten Ansatz zu entwickeln, der drei zentrale Aspekte harmonisch vereint: die Kompatibilität mit dem schweizerischen Rechtssystem,

¹⁹⁸ EHDS-VO, Folgenabschätzung; GASSNER, S. 739-746.

¹⁹⁹ vgl. GASSNER, S. 739.

²⁰⁰ vgl. Kap. 3.4.

²⁰¹ vgl. Kap. 2.2.2.

²⁰² vgl. Kap. 3.3.3.

die Anforderungen der digitalen Transformation sowie die angemessene Berücksichtigung der Interessen aller beteiligten Akteure.

5.5.1 Das Kaskadenmodell als Vorbild für die künftige Einwilligungspraxis

Die vergleichende Analyse der Einwilligungsmodelle zeigt deutliche Unterschiede in ihrer Wirkungsweise: Während der *broad consent* die effizienteste Form der Sekundärnutzung gewährleistet, ermöglicht das *dynamic consent*-Modell die optimale Ausübung der digitalen Selbstbestimmung. Der *meta consent* vereint diese komplementären Ansätze in einem innovativen Konzept: Er ermöglicht den betroffenen Personen, zwischen *broad* und *dynamic consent* als präferiertes Einwilligungsformat zu wählen. Diese Flexibilität lässt sich durch die Integration weiterer Einwilligungsoptionen wie Datenspende und Datentreuhänderschaft noch erweitern, wodurch die Steuerungsmöglichkeiten der betroffenen Personen zusätzlich gestärkt werden.

Die Analyse der Regulierungsansätze bestätigt die Vorteile des *meta consent*-Modells. Dieses berücksichtigt bereits in seiner Konzeption und geplanten Umsetzung zentrale Elemente moderner Datengovernance: die Förderung der Datenkompetenz, die transparente Einwilligungsübersicht durch Datenbriefe, die technologisch optimierte Widerrufsgestaltung sowie flexible Optionen zur zeitlichen Befristung der Einwilligung. Selbst das Opt-Out-Prinzip liesse sich als Präferenzwahl implementieren, ohne die Selbstbestimmung der betroffenen Personen wesentlich einzuschränken. Im Gegensatz dazu würde die Integration dieser Konzepte in das klassische Modell der informierten Einwilligung einen erheblichen administrativen, infrastrukturellen und koordinativen Mehraufwand verursachen.

Die vollständige Abkehr von der Einwilligungspraxis, wie sie der EHDS vorsieht, ist im aktuellen schweizerischen Rechtsrahmen nicht umsetzbar. Gleichwohl verdienen die europäischen Entwicklungen in diesem Bereich besondere Aufmerksamkeit, insbesondere die Governance-Strukturen des entstehenden EU-weiten Gesundheitsdatenraums, da sie wichtige Impulse für die Weiterentwicklung des schweizerischen Systems liefern können.

5.5.2 Chancen und Herausforderungen in der Umsetzung der Kaskadeneinwilligung

Die strategische Kombination verschiedener Einwilligungsmodelle und Regulierungsansätze bietet einen ausgewogenen Weg zur Gestaltung eines zukunftsfähigen Einwilligungspraxis. Diese flexible Herangehensweise ermöglicht die Anpassung an die dynamische technologische Entwicklung und verschafft Akteuren gleichzeitig die notwendige Rechtssicherheit. Die Implementierung des Kaskadeneinwilligungsmodells erfordert eine systematische Konsolidierung und Weiterentwicklung der Sekundärnutzungsvorhaben auf Bundesebene. Ein effizienter Ansatz bedeutet dabei die Abkehr von Opt-out-Kompromissen und forschungsorientiertem Nudging zugunsten einer einheitlichen Praxis, die die digitale Selbstbestimmung stärker in den Fokus rückt. Die erfolgreiche Umsetzung des Kaskadenmodells basiert auf einer robusten und sicheren Infrastruktur, die Synergien mit dem EPD und der E-ID optimal

nutzt. Begleitet werden muss dieser Transformationsprozess durch koordinierte Digital Literacy-Maßnahmen auf gesamtstaatlicher Ebene, die gezielt das Vertrauen der Bevölkerung stärken und ihre digitale Entscheidungskompetenz fördern.

6 Zusammenfassung und Ausblick

Die Betrachtung der Sekundärnutzung von Gesundheitsdaten verdeutlicht ein zentrales Spannungsfeld der Digitalisierung im Gesundheitswesen: Sie offenbart die divergierenden Interessen zwischen dem Forschungsbedarf nach umfassender Datennutzung, den gesetzlichen Grundlagen des DSG und dem individuellen Recht auf digitale Selbstbestimmung.

Die rechtlichen Grundvoraussetzungen für die Sekundärnutzung von Gesundheitsdaten auf Bundes-ebene stellen eine komplexe Ausgangslage dar. Zwar existiert mit dem DSG ein grundlegendes Rahmengesetz, doch führt die Vielzahl von Spezialregelungen und kantonalen Erlassen zu einer stark fragmentierten Rechtslandschaft. Darüber hinaus bestehen bei diversen Bearbeitungsgrundsätzen des DSG erhebliche Rechtsunsicherheiten, insbesondere hinsichtlich der Datenanonymisierung, der Verhältnismäßigkeitsprüfung und der Handhabung des Zweckbindungsgebots.

Die Sekundärnutzung von Gesundheitsdaten gewinnt im Zuge der digitalen Transformation des Gesundheitswesens zunehmend an Bedeutung, nachdem dieser Bereich in der Gesetzgebung lange vernachlässigt wurde. Von einem gesamtheitlichen Ansatz kann jedoch nicht gesprochen werden: Die staatlichen Initiativen sind unzureichend koordiniert, und die aktuellen Bemühungen fokussieren einseitig auf den Forschungszugang zu Daten, während die digitale Selbstbestimmung vernachlässigt wird. Zudem wird die Sekundärnutzung zu wenig auf europäische Vorhaben wie dem EHDS abgestimmt, womit die Gefahr droht Anschluss an diese wichtige Entwicklung zu verlieren.

Das klassische Modell der informierten Einwilligung wird derzeit primär als Absicherung gegen widerrechtliche Datenverarbeitung genutzt, um bestehende Rechtsunsicherheiten bei der Sekundärnutzung zu überbrücken. Das traditionelle Einwilligungskonzept selbst gerät jedoch angesichts der Digitalisierung und des wachsenden Interesses an der Sekundärdatennutzung zunehmend unter Druck. Die wesentlichen Schwachstellen zeigen sich in der mangelnden Berücksichtigung der digitalen Selbstbestimmung, der unzureichenden Anpassung an technologische Entwicklungen sowie den Unklarheiten bei der rechtskonformen Umsetzung der Einwilligungskriterien.

Das *meta consent*-Modell bietet einen vielversprechenden Ansatz, um die effiziente Sekundärnutzung von Gesundheitsdaten mit der Wahrung digitaler Selbstbestimmung in Einklang zu bringen. Es zeichnet sich durch vielfältige Steuerungsoptionen aus und integriert sowohl die Kaskadeneinwilligung als auch verschiedene unterstützende Regulierungsansätze. Eine flexible elektronische Verwaltungsplattform vereinfacht die Nutzung, gestaltet sie effizienter und wird den Anforderungen der Digitalisierung gerecht. Die grösste Herausforderung bei der Einführung der Kaskadeneinwilligung liegt im Fehlen einer kompatiblen Infrastruktur.

Die effiziente Sekundärnutzung von Gesundheitsdaten wird nicht primär durch Anforderungen der digitalen Selbstbestimmung eingeschränkt. Vielmehr erschweren die komplexe Struktur des schweizerischen Datenschutzrechts und die Vielzahl unkoordinierter staatlicher Digitalisierungsinitiativen eine wirksame Umsetzung. Der Ausblick auf künftige Entwicklungen sollte sich daher auf die systematische

Konsolidierung bestehender Projekte und die verstärkte Zusammenarbeit der Akteure konzentrieren. Erforderlich ist eine ganzheitliche Perspektive, die nationale Anliegen und internationale Entwicklungen gleichermassen miteinbezieht.

Eigenständigkeitserklärung

„Ich erkläre hiermit,

- dass ich die vorliegende Arbeit eigenständig verfasst habe,
- dass ich die Arbeit nur unter Verwendung der im Verzeichnis angegebenen Hilfsmittel verfasst habe;
- dass alle mit Hilfsmitteln erbrachten Teile der Arbeit präzise deklariert wurden;
- dass ich sämtliche verwendeten Quellen erwähnt und gemäss gängigen wissenschaftlichen Zitierregeln korrekt zitiert habe;
- dass ich sämtliche immateriellen Rechte an von mir allfällig verwendeten Materialien wie Bilder oder Grafiken erworben habe oder dass diese Materialien von mir selbst erstellt wurden;
- dass das Thema, die Arbeit oder Teile davon nicht bereits Gegenstand eines Leistungs nachweises einer anderen Veranstaltung oder Kurses waren, sofern dies nicht ausdrücklich mit der Referentin oder dem Referenten im Voraus vereinbart wurde und in der Arbeit ausgewiesen wird;
- dass ich mir über die rechtlichen Bestimmungen zur Publikation und Weitergabe von Teilen oder der ganzen Arbeit bewusst bin und ich diese entsprechend einhalte;
- dass ich mir bewusst bin, dass meine Arbeit elektronisch auf Plagiate und auf Drittautorschaft menschlichen oder technischen Ursprungs überprüft werden kann und ich hiermit der Universität St.Gallen laut Prüfungsordnung das Urheberrecht soweit einräume, wie es für die Verwaltungshandlungen notwendig ist;
- dass ich mir bewusst bin, dass die Universität einen Verstoss gegen diese Eigenständigkeitserklärung verfolgt und dass daraus disziplinarische wie auch strafrechtliche Folgen resultieren können, welche zum Ausschluss von der Universität resp. zur Titelaberkennung führen können.“

Mit Einreichung der schriftlichen Arbeit stimme ich mit konkludentem Handeln zu, die Eigenständigkeitserklärung abzugeben, diese gelesen sowie verstanden zu haben und, dass sie der Wahrheit entspricht.

(50 Seiten)

Pascale Illi



St.Gallen, 18.11.2024

Ort, Datum

Unterschrift