Michael Widmer (Hrsg.)

Datenschutz
Rechtliche Schnittstellen

Mit Beiträgen von:
Tobias Fasnacht
Philip Glass
Thomas Steiner

DIKE

Michael Widmer (Hrsg.)

Datenschutz
Rechtliche Schnittstellen

Michael Widmer (Hrsg.)

Datenschutz
Rechtliche Schnittstellen

Mit Beiträgen von:
Tobias Fasnacht
Philip Glass
Thomas Steiner

DIKE

Open-Access-Gold

Publiziert von:
Dike Verlag
Weinbergstrasse 41
CH-8006 Zürich
www.dike.ch

ISBN (Paperback): 978-3-03891-513-3
ISBN (PDF): 978-3-03929-027-7

DOI: https://doi.org/10.3256/978-3-03929-027-7

Vorwort

Das Zentrum für Sozialrecht (ZSR) an der School of Management and Law der ZHAW befasst sich mit sozialrechtlichen Fragen im nationalen und internationalen Kontext. Das Datenschutzrecht ist einer der Themenschwerpunkte des ZSR.

Von diversen Autoren wurden am und für das ZSR verschiedene Beiträge zu datenschutzrechtlichen Themen verfasst, die im vorliegenden Sammelband publiziert werden.

Ich bedanke mich herzlich bei den Autoren für ihre Arbeit und das Engagement, welches sie im Bereich des Datenschutzes an den Tag legen. Zudem danke ich BLaw Kevin Neeranal für seine wertvolle Mithilfe bei der Fertigstellung dieses Buches.

Michael Widmer

Inhaltsübersicht

Abkürzungsverzeichnis

A.	Auflage
a.a.O.	am angeführten Ort
AB	Aktiebolag (schwedisch für Aktiengesellschaft)
ABl.	Amtsblatt
abl.	ablehnend
Abs.	Absatz
AEPD	*Agencia Española de Protección de Datos*
AEUV	Vertrag über die Arbeitsweise der europäischen Union
AG	Aktiengesellschaft
AGAV	Bundesgesetz über die Allgemeinverbindlicherklärung von Gesamtarbeitsverträgen vom 28. September 1956
AGI	Artificial General Intelligence
AHVG	Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (SR 831.10)
AJB	Amt für Jugend und Berufsberatung des Kantons Zürichs
AJP	Aktuelle Juristische Praxis
akt.	aktuelle
AI	Artificial Intelligence
ANAG	Bundesgesetz vom 26 März 1931 über Aufenthalt und Niederlassung der Ausländer (SR 142.20)
Anm.	Anmerkung
AR	Aargau
Art.	Artikel
AsylG	Asylgesetz vom 26. Juni 1998 (SR 142.31)
ATSG	Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG; SR 830.1)
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BDSG	Deutsches Bundesdatenschutzgesetz vom 30. Juni 2017

BetmG	Bundesgesetz vom 3. Oktober 1951 über die Betäubungsmittel und die psychotropen Stoffe (Betäubungsmittelgesetz; SR 812.121)
BGE	amtlich publizierte Entscheidungen des schweizerischen Bundesgerichts
BGer	Bundesgericht
BGFA	Bundesgesetz vom 23. Juni 2000 über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz; SR 935.61)
BJ	Bundesamt für Justiz
BK	Berner Kommentar
BL	Basel-Land
BR	Bundesrat
BS	Basel-Stadt
BSK	Basler Kommentar
bspw.	beispielsweise
Bst.	Buchstabe
BÜPF	Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1)
BV	Bundesverfassung vom 18. April 1999 der Schweizerischen Eidgenossenschaft (SR 101)
BVG	Bundesgesetz vom 25. Juni 1982 über die berufliche Altern-, Hinterlassenen- und Invalidenvorsorge (SR 831.40)
BVGer	Bundesverwaltungsgericht
BVerfG	Bundesverfassungsgericht
BVerGE	Sammlung Entscheidung des Bundesverfassungsgerichts (Deutschland)
bzw.	beziehungsweise
CH	Confoederatio Helvetica
CNIL	*Commission Nationale de l'Informatique et des Libertés*
d.	des
d.h.	das heisst

DBG	Bundesgesetz vom 14. Dezember 1990 über die direkte Bundessteuer
DGRI	Deutsche Gesellschaft für Recht und Informatik
digma	Zeitschrift für Datenrecht und Informationssicherheit, Zürich
Diss.	Dissertation
Dr.	Doktor
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 17, April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
DSB	Datenschutzbeauftragte
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz; SR 235.1)
E./Erw.	Erwägung
E-DSG	Entwurf Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz
EDK	Schweizerische Konferenz der kantonalen Erziehungsdirektoren
Ed.	Edition
Eds.	Edition
EDSA	European Data Protection Law Review
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDPL	European Data Protection Law Review
EG	Europäische Gemeinschaft
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ELG	Bundesgesetz vom 6. Oktober 2006 über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung (SR 831.30)
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten, abgeschlossen in Rom am 4. November 1950 (SR 0.101)

erw.	erweiterte
et al.	und andere
ETH	Eidgenössische Technische Hochschule
EU	Europäische Union
EuGH	Europäischer Gerichthof
EuZ	Zeitschrift für Europarecht
EWR	Europäischer Wirtschaftsraum
f./ff.	und folgende
FIDLEG	Bundesgesetz vom 15. Juni 2018 über die Finanzdienstleistungen (Finanzdienstleistungsgesetz; SR 950.1)
FinfraG	Bundesgesetz vom 19. Juni 2015 über die Finanzmarkinfrastrukturen des Marktverhalten im Effekten- und Derivathandel (Finanzmarkinfrastrukturgesetz; SR 958.1)
FINIG	Bundesgesetz vom 15. Juni 2018 über die Finanzinstitute (Finanzinstitutsgesetz, SR 954.1
FLG	Bundesgesetz vom 20. Juni 1952 über die Familienzulagen in der Landwirtschaft (SR 836.1)
FMG	Fernmeldegesetz vom 30. April 1997 (SR 784.10)
FN	Fussnote
FR	Freiburg
FusG	Bundesgesetz vom 3. Oktober 2003 über Fusion, Spaltung, Umwandlung und Vermögensübertragung (Fusionsgesetz; SR 221.301)
FZG	Bundesgesetz vom 17. Dezember 1993 über die Freizügigkeit in der beruflichen Alters-, Hinterlassenen- und Invalidenvorsorge (Freizügigkeitsgesetz; SR 831.42)
GE	Genf
GesG ZH	Gesundheitsgesetz vom 2. April 2007 des Kantons Zürich (GesG ZH; ON 810.1)
GIG	Bundesgesetz vom 24. März 1995 über die Gleichstellung von Frau und Mann (Gleichstellungsgesetz; SR 151.1)

GL	Glarus
Gl.M.	gleicher Meinung
GmbH	Gesellschaft mit beschränkter Haftung
GOFAI	good old fashioned AI
GTG	Bundesgesetz vom 21. März 2003 über die Gentechnik im Ausserhumanbereich (Gentechnikgesetz; SR 814.91)
GUMG	Bundesgesetz vom 8. Oktober 2004 über genetische Untersuchungen beim Menschen (SR 810.12)
HMG	Bundesgesetz vom 15. Dezember 2000 über Arzneimittel und Medizinprodukte (Heilmittelgesetz; SR 812.21)
Hrsg.	Herausgeber
i.S.	im Sinne
i.S.v.	im Sinne von
i.V.m.	In Verbindung mit
IDG BS	Gesetz vom 9. Juni 2010 über die Information und den Datenschutz des Kantons Basel-Stadt (Informations- und Datenschutzgesetz; ON 153.260)
IDG ZH	Gesetz vom 12. Februar 2007 über die Information und den Datenschutz des Kanton Zürich (Informations- und Datenschutzgesetz; ON 170.4).
IDV ZH	Verordnung vom 28. Mai 2008) über die Information und den Datenschutz des Kantons Zürich (ON 170.41)
IJACSA	International Journal of Advanced Computer Science and Applications
IKV	Interkantonale Vereinbarung vom 25. Oktober 2007 über die Zusammenarbeit im Bereich der Sonderpädagogik
Insb.	insbesondere
IPRG	Bundesgesetz vom 18. Dezember 1987 über das internationale Privatrecht (SR 291)
IRIS	Internationales Rechtsinformatik Symposion
IPTZ	Zurich Center for Information Technology and Privacy
iur.	iuris

IVG	Bundesgesetz vom 19. Juni 1959 über die Invalidenversicherung (SR 831.20)
JU	Jura
KAG	Bundesgesetz vom 23. Juni 2006 über die kollektiven Kapitalanlagen (Kollektivanlagengesetz; SR 951.31)
Kap.	Kapitel
KESB	Kindes- und Erwachsenenschutzbehörde
KG	Bundesgesetz vom 6. Oktober 1995 über Kartelle und andere Wettbewerbsbeschränkungen (Kartellgesetz; SR 251)
KI	Künstliche Intelligenz
KJG	Kinder- und Jugendheimgesetz vom 27. November 2017 des Kantons Zürich (ON 852.2)
KJGH ZH	Kinder- und Jugendhilfegesetz (KJHG) vom 14. März 2011, ZH-Lex ON 852.1.
KKG	Bundesgesetz vom 23. März 2001 über den Konsumkredit (SR 221.214)
KRK	Übereinkommen vom 20. November 1989 über die Rechte des Kindes (Kinderrechtskonvention; SR 0.107)
KuKo	Kurzkommentar
KVG	Bundesgesetz vom 18. März 1994 über die Krankenversicherung (SR 832.10)
LFG	Bundesgesetz vom 21. Dezember 1948 über die Luftfahrt (Luftfahrtgesetz; SR 748.0)
lit.	litera
LLC	Limited Liability Company
LMG	Bundesgesetz über Lebensmittel und Gebrauchsgegenstände (SR 817.0)
LU	Luzern
LWG	Bundesgesetz vom 29. April 1998 über die Landwirtschaft (Landwirtschaftsgesetz; SR 910.1)
m.a.W.	mit anderen Worten
m.w.H.	mit weiteren Hinweisen

MERG	Gesetz vom 11. Mai 2015 über das Meldewesen und die Einwohnerregister des Kantons Zürich (ON 142.1)
MWSTG	Bundesgesetz vom 12. Juni 2009 über die Mehrwertsteuer (Mehrwertsteuergesetz; SR 641.20)
N	Randnote
NBG	Bundesgesetz vom 3. Oktober 2003 über die Schweizerische Nationalbank (Nationalbankgesetz; SR 951.11)
nDSG	Bundesgesetz über den Datenschutz vom 25. September 2020 (Datenschutzgesetz; AS 2022 491; Inkrafttreten: 1. September 2023)
NE	Neuenburg
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFK	Orell Fuessli Kommentar
ON	Ordnungsnummer
OR	Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht; SR 220)
OW	Obwalden
PatG	Bundesgesetz vom 25. Juni 1954 über die Erfindungspatenente (Patentgesetz; SR 232.14)
ParlG	Bundesgesetz vom 13. Dezember 2002 über die Bundesversammlung (Parlamentsgesetz; SR 171.10)
PBG	Bundesgesetz vom 20. März 2009 über die Personenbeförderung (Personenbeförderungsgesetz, SR 745.1)
PrHG	Bundesgesetz vom 18 Juni 1993 über die Produktehaftpflicht (Produktehaftpflichtgesetz; SR 221.112.944)
PrSG	Bundesgesetz vom 12. Juni 2009 über die Produktesicherheit (SR 930.11)
Prof.	Professor
RTVG	Bundesgesetz vom 24. März 2006 über Radio und Fernsehen (SR 784.40)
Rz.	Randziffer

S.	Seite
s.a.	siehe auch
S.A/SA	Société Anonyme
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
Sc.	Science
SDSG	Bundesgesetz vom 28. September 2018 über den Datenschutz im Rahmen der Anwendung des Schengen-Besitzstands in Strafsachen (Schengen-Datenschutzgesetz; SR 235.3)
SEV	Übereinkommen vom 28 Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SR 0.235.1).
SH	Schaffhausen
SHK	Schweizerische Hochschulkonferenz
SJZ	Schweizerische Juristen-Zeitung
SP	Sozialdemokratische Partei
SPK-N	Staatspolitische Kommissionen des Nationalrats
SPK-S	Staatspolitische Kommissionen des Ständerats
SR	Systematische Rechtssammlung
St.	Sankt
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR. 331.0)
StHG	Bundesgesetz vom 14. Dezember 1990 über die Harmonisierung der direkten Steuern der Kantone und Gemeinden, Steuerharmonisierungsgesetz (Steuerharmonisierungsgesetz; SR.642.14)
sog.	sogenannt
SVG	Strassenverkehrsgesetz vom 19. Dezember 1958 (SR 741.01)
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht
THG	Bundesgesetz vom 6. Oktober 1995 über die technischen Handelshemmnisse (SR 946.51)
TI	Tessin

u.	und
u.a.	unter andere, unter anderem
u.U	unter Umständen
Univ.	Universität
UR	Uri
URG	Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz; SR 231.1)
UVG	Bundesgesetz vom 20 März 1981, über die Unfallversicherung (SR 832,20)
UWG	Bundesgesetz vom 10. Dezember 1986 gegen den unlauteren Wettbewerb (SR 241)
VD	Waadt
VE-DSG	Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz
vgl.	vergleich
VS	Wallis
VSG ZH	Volksschulgesetz vom 7. Februar 2005 des Kantons Zürich (ON 412.100)
VSM ZH	Verordnung vom 11. Juli 2007 über die sonderpädagogischen Massnahmen des Kantons Zürich (ON 412.103)
VO	Verordnung
WEKO	Wettbewerbskommission
www	world wide web
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210)
ZH	Zürich
ZHAW	Zürcher Hochschule für angewandte Wissenschaften
Ziff.	Ziffer
zugl.	zugleich

Autorenverzeichnis

Fasnacht, Tobias Dr. iur., Rechtsanwalt, selbständiger Rechtsanwalt in Dornach SO, nebenamtlicher Richter am Sozialversicherungsgericht des Kantons Basel-Stadt.

Glass, Philip Dr. iur., Rechtsanwalt, wissenschaftlicher Mitarbeiter Zentrum für Sozialrecht (ZSR) der ZHAW School of Management and Law, Post Doc am Lehrstuhl für Staats- und Verwaltungsrecht bei Prof. Markus Schefer und Lehrbeauftragter an der Universität Basel.

Steiner, Thomas Dr. iur., LL.M. (Berkeley), Rechtsanwalt und Senior Advisor/Partner bei LAUX LAWYERS AG in Zürich.

Einleitung

Michael Widmer*

Die datenschutzrechtlichen Normen sind in unterschiedlichsten Kontexten und Fachbereichen zu beachten.[1] Dementsprechend ist das Datenschutzgesetz ein Rahmengesetz. Daneben finden sich in unzähligen (Spezial-)Gesetzen ebenfalls datenschutzrechtliche Normen, weshalb Datenschutz oft als Querschnittsmaterie bezeichnet wird.[2]

Datenschutz spielt in unterschiedliche Kontexte und Fachbereiche hinein, so dass diverse Schnittstellen entstehen – innerhalb des Datenschutzes selbst sowie zwischen dem Datenschutz und anderen Themen. Er kann demnach auch als Schnittstellenmaterie bezeichnet werden.

Die vier Beiträge im vorliegenden Sammelband befassen sich mit solchen Schnittstellen.

Zunächst untersucht Dr. Philip Glass die Abgrenzung zwischen kantonalem Datenschutzrecht und bundesrechtlichen Regelungen zum Kindesrecht sowie das Zusammenspiel zwischen Datenschutzrecht und Informationstechnologie. In seinem Beitrag «Datenschutzrechtliche Optimierung der Dokumentation in Wohnheimen für Kinder und Jugendliche im Kanton Zürich» entwickelt er Ansätze für «Best Practices» und Vorschläge für softwarebasierte Unterstützung zur Umsetzung von Datenschutz.

Dr. Thomas Steiner untersucht in «Zwischen Autonomie und Angleichung» die Schnittstelle zwischen dem neuen Schweizer DSG und dem europäischen Recht, der Datenschutz-Grundverordnung (DSGVO). Er befasst sich ins-

* Dr. iur. Michael Widmer LL.M., Rechtsanwalt, Dozent und Leiter der Fachstelle für Datenschutz und IT-Recht an der ZHAW.

1 Bpsw. Regina Meier, Revision des Datenschutzgesetzes: kollektive Rechtsdurchsetzung im Datenschutzrecht?, in: sui-generis 2018, 139 ff., 145; https://review.datenschutz.ch/datenschutz/index.php?jss=1 (Abruf 23.09.2022).

2 Regina Meier (FN 2), 145; M. Sonntag, Datenschutz – Eine Querschnittmaterie. Softwaretechnik-Trends, 2006/26.

besondere mit der Frage, welche Anpassung an die DSGVO der Schweizer Gesetzgeber gewollt hat und welche Folgerungen daraus für die Anwendung des neuen Schweizer DSG gezogen werden können.

Sodann widmet sich Dr. Tobias Fasnacht unter dem Titel «Zusammenspiel informationsrechtlicher Bestimmungen in der schulinternen Logopädie und Sozialarbeit» der Frage, was für die an der Schule involvierten Fachpersonen in diesen Bereichen hinsichtlich der Bearbeitung und Weitergabe von Informationen über Schülerinnen und Schüler erlaubt ist. Dabei werden vor allem die Schnittstellen zwischen allgemeinen Datenschutzgesetzen (als Rahmengesetzen) und den Berufsgeheimnissen, zwischen Datenschutzgesetzen und kantonalen Spezialgesetzen sowie zwischen Datenschutz und Meldepflichten untersucht.

Schliesslich werden in einem weiteren Beitrag von Dr. Philip Glass Themen an der Schnittstelle zwischen neuen Technologien und Datenschutz aufgegriffen. Er befasst sich in «Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung» mit spezifisch datenschutzrechtlichen Fragen, welche die KI-Technologie mit sich bringt, und erläutert diese an konkreten Use-Cases.

Datenschutzrechtliche Optimierung der Dokumentation in Wohnheimen für Kinder und Jugendliche im Kanton Zürich

Philip Glass

Inhaltsübersicht

I. Ausgangslage

In der Schweiz leben Schätzungen zufolge rund 13'000 Kinder und Jugendliche in Wohnheimen.[1] Mit der Obhut, in die sie gegeben werden, entsteht eine gesetzliche Pflicht des Staates, den Tagesablauf sowie diverse Ereignisse im Leben der Jugendlichen festzuhalten. Dies ist die Aktenführungspflicht. Die Führung der Akten hat im gesetzlichen Rahmen zu erfolgen und muss daher insbesondere auch die Vorgaben des einschlägigen Datenschutzrechts erfüllen.

Hier vermischt sich nun das kantonale, öffentlich-rechtliche Datenschutzrecht mit dem Datenschutzgesetz sowie dem zivilrechtlichen Familienrecht des Bundes. Letzteres regelt die rechtlichen Beziehungen zwischen den Beteiligten, insbesondere den Kindern, Eltern, Wohnheimen, Beiständen und weiteren Behörden, die Aufgaben des ZGB erfüllen, beispielsweise im Bereich des Kindesschutzes.

Das ZGB bildet damit zugleich die bedeutendste rechtliche Grundlage für die Betreuung und damit für die Datenbearbeitung durch die Mitarbeitenden eines Wohnheims, wie auch die Rechtsgrundlage für die Einsichtsrechte der Eltern und weiterer interessierten Parteien.

Das zentrale Instrument der Dokumentation in Wohnheimen ist das Journal. Darin halten die Betreuerinnen und Betreuer für jedes Kind die wichtigen Ereignisse fest, wie etwa externe Termine, schulische und ärztliche Zeugnisse, Elterngespräche. Ergänzt wird das Journal durch Administrationssoftware, welche den organisatorischen Ablauf des Wohnheims widerspiegelt.

Die in diesen Informationssystemen enthaltenen Personendaten der Kinder können grundsätzlich im Rahmen der Dateneinsichts- und Informationsrechte nach § 20 ff. IDG ZH[2] von den Kindern, den Eltern sowie berechtigten Drittparteien eingesehen werden. In Fällen, da ein Kind bereits mehrere Jahre in einem Heim untergebracht ist, kann dies einen hohen Sortierungsaufwand verursachen. Sodann können kollidierende Rechte dazu führen, dass nicht immer klar ist, wer einsichtsberechtigt ist, welche Daten hierbei bekanntgegeben werden dürfen und inwieweit die betroffenen Kinder dies verhindern können.

---

[1] Nicolette Seiterle, Ergebnisbericht Bestandesaufnahme Pflegekinder Schweiz 2015, PACH Pflege- und Adoptivkinder Schweiz, Zürich 2017.

[2] Gesetz vom 12. Februar 2007 über die Information und den Datenschutz des Kanton Zürich (Informations- und Datenschutzgesetz, IDG ZH; ON 170.4).

Den Wohnheimen, die ihre Dienstleistungen im Rahmen einer Leistungsvereinbarung mit einem Gemeinwesen anbieten, kommt in dieser Konstellation der Datenbearbeitung eine nicht alltägliche Doppelrolle zu. Aus Sicht des ZGB werden sie als Pflegeeltern qualifiziert, aus Sicht des kantonalen Datenschutzrechts als öffentliche Organe im Sinn von § 3 IDG ZH. Ziel dieser Studie ist es, die sich daraus ergebenden rechtlichen Fragen zu beleuchten und einzuordnen.

II. Studienaufbau

Im Rahmen der vorliegenden Studie werden die folgenden Fragekomplexe untersucht. Dabei liegt der Fokus auf den Journaldaten, also jenen Daten, die im Rahmen der Dokumentation des Aufenthalts der Klientinnen und Klienten erhoben und bearbeitet werden. Andere Kategorien von Daten, wie insbesondere Daten zur administrativen Führung eines Heims, werden nur zu Zwecken der Abgrenzung zu den Journaldaten berücksichtigt.

– Erstens werden die rechtlichen Grundlagen für die Journalführung, insbesondere die Aktenführungspflicht, beleuchtet.
– Zweitens werden die rechtlichen Grundlagen für Rechte an den in den Journalen enthaltenen Personendaten überblicksartig dargestellt.
– Drittens wird untersucht, welche Funktionen die hierbei eingesetzte Software bereitstellt und inwiefern diese datenschutzrechtlich optimiert werden kann.
– Schliesslich werden die Ergebnisse rechtlich gewürdigt und Vorschläge erarbeitet.

III. Journalführung

A. Funktionen des Journals

Wohnheime führen Tagesjournale über die bei ihnen untergebrachten Kinder und Jugendlichen. In den Interviews kam zum Ausdruck, dass diese Journale verschiedene Funktionen erfüllen, namentlich als Arbeitsinstrument, insbe-

sondere als Grundlage des internen Wissensmanagements, der Evaluationen und Entwicklungsberichte sowie als institutionelles Gedächtnis.

1. Arbeitsinstrument

Das Journal dient zunächst dazu, die tägliche Arbeit mit den Klienten zu protokollieren und dokumentieren. Zum einen wird damit die Aktenführungspflicht erfüllt,[3] zum anderen bilden die Einträge in das Journal die Grundlage für die fortlaufende Begleitung und Betreuung. Die Funktion als Arbeitsinstrument umfasst insbesondere die nachfolgenden Funktionen, kann indes für die einzelnen Mitarbeiterinnen und Mitarbeiter auch die Anfertigung von persönlichen Arbeitsnotizen im Sinne von § 3 Abs. 2 IDG ZH bedeuten.

2. Wissensmanagement

Eine weitere wichtige Funktion des Journals ist jene des Wissensmanagements innerhalb des Betreuungsteams des Wohnheims.

3. Rohdaten für Evaluationen und Entwicklungsberichte

Schliesslich bilden die Journaldaten regelmässig Rohdaten für die Ausfertigung von Berichten. In diesen Berichten werden periodisch die Entwicklungen der Klientinnen und Klienten in verschiedenen Lebensbereichen dokumentiert und besprochen.

4. Institutionelles Gedächtnis

Diese Funktion umfasst die vorangehenden und deren Fortdauer über Zeit. Sie bezweckt primär, den Klientinnen und Klienten zu ermöglichen, zu einem späteren Zeitpunkt Informationen über ihre Kindheit zu erhalten. Sekundär entspricht sie zudem dem Archivierungsinteresse, wie es im Archivierungsgesetz festgelegt ist. Entsprechend ist hier eine ähnliche Zäsur vorzunehmen, wie dies im Rahmen der Archivierung vorgesehen ist.

Gemäss § 9 IDG ZH dürfen die erhobenen Personendaten so lange für das Tagesgeschäft zur Verfügung gehalten werden, wie dies für die Erledigung der

[3] Siehe zur Aktenführungspflicht III.B.

entsprechenden Aufgaben notwendig ist. Ist diese Voraussetzung nicht mehr erfüllt, erlaubt § 5 Abs. 2 IDG ZH eine weitere Aufbewahrung für maximal 10 Jahre. Danach sind die Personendaten gemäss § 5 Abs. 3 IDG ZH dem Archiv anzubieten bzw. zu vernichten.[4] Dies wird regelmässig dann der Fall sein, wenn die betreffenden Klientinnen und Klienten das Wohnheim wieder verlassen.

5. Sicherstellen des Lebenszyklus der Daten

Das Datenschutzrecht gilt für die ihm unterstellten Personendaten über den gesamten Lebenszyklus dieser Daten bzw. den entsprechenden Informationsprozess hinweg und schreibt für gewisse Phasen dieses Prozesses Fristen und Bearbeitungsgrundsätze vor. Als Grundlage gelten zunächst die allgemeinen Aktenführungspflichten, die sich aus der Pflicht zur korrekten Informationsverwaltung ergeben.[5]

Das Datenschutzrecht unterteilt den Lebenszyklus von Daten in zwei Hauptphasen, namentlich die Phase der aktiven Bearbeitung und jene der Löschung bzw. Zweckänderung für die Archivierung.

Die aktive Phase umfasst die in § 3 Abs. 5 IDG ZH aufgezählten Bearbeitungsformen des Beschaffens (Erheben), Aufbewahrens (Speichern), Verwendens, Umarbeitens und Bekanntgebens von Personendaten. Die Aufzählung im Gesetz ist illustrativ und nicht abschliessend, da der Begriff des Bearbeitens jede Art des Umgangs mit Personendaten umfasst.[6]

Die Archivierungsphase beginnt mit Ablauf der Aufbewahrungsfrist. Solche Fristen ergeben sich teilweise aus den gesetzlichen und vertraglichen Grundlagen der Datenbearbeitung. Das IDG ZH sieht lediglich eine relative maximale Aufbewahrungsdauer beim bearbeitenden Organ vor. Gemäss § 5

---

4 Siehe dazu sogleich III.A.5.

5 Siehe dazu III.B.3.b.

6 Beat Rudin, in: Bruno Baeriswyl/Beat Rudin, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zürich 2012 (zit. VerfasserIn, PraKom IDG ZH), § 3, N 33; DSB Kanton Zürich, Merkblatt Informationsverwaltung, Version 1.2, Dezember 2019, https://www.zh.ch/de/politik-staat/wie-behoerden-informationen-verwalten.html (hier in 3 Phasen: laufende Ablage, ruhende Ablage, Archiv; Abruf 01.07.2022).

Abs. 2IDG darf das öffentliche Organ Informationen und Findmittel, bzw. die entsprechenden Dokumente und Daten, noch höchstens zehn Jahre nach jenem Zeitpunkt aufbewahren, da es sie nicht mehr zur Erfüllung der durch den Bearbeitungszweck definierten Aufgabe benötigt. Danach müssen sie gemäss § 5 Abs. 3 IDG ZH dem Archiv angeboten bzw. vernichtet werden. Über die Vernichtung befindet indirekt das Archiv, indem es angebotene Daten ablehnt oder nur teilweise übernimmt.

Die unterschiedliche Einteilung der Phasen im Vergleich zum Lebenszyklus der Information im Rahmen der Informationsverwaltung ist wohl darauf zurückzuführen, dass die datenschutzrechtliche Aufteilung sich am jeweils verantwortlichen Organ orientiert: während der aktiven Phase ist das Organ, bei dem die Daten angefallen sind, für diese verantwortlich. Mit der Archivierung geht die datenschutzrechtliche Verantwortung auf das Archiv über.

Im Ergebnis muss die Journalsoftware demnach darauf angelegt sein, erstens Personendaten über einen Zeitraum von mehreren Jahren bzw. Jahrzehnten zur Verfügung zu halten, zweitens eine möglichst reibungslose Kommunikation mit dem zuständigen Archiv zu ermöglichen und drittens eine sichere Löschung der nicht mehr benötigten und nicht archivierten Personendaten zu gewährleisten.[7]

B. Aktenführungspflicht der Wohnheime

1. Allgemeines zur Aktenführungspflicht

Gemäss der Legaldefinition des Archivgesetzes sind Akten «schriftliche, elektronische und andere Aufzeichnungen der öffentlichen Organe sowie ergänzende Unterlagen, insbesondere dazugehörige Verzeichnisse». Sie umfassen entsprechend sowohl Papierdossiers als auch die Führung von elektronischen Akten.[8]

---

[7] Einzelheiten zur Archivierung auf der Informationsseite des Staatsarchivs des Kantons Zürich unter https://www.zh.ch/de/politik-staat/wie-behoerden-informationen-verwalten/unterlagen-anbieten-und-abliefern.html (Abruf 01.07.2022).

[8] DSB Kanton Zürich (FN 6), Ziff. 3.3.

Auf gesetzlicher Ebene existieren einige wenige ausdrückliche Aktenführungspflichten. Illustrativ ist Art. 46 ATSG[9] als eine der wenigen Normen, welche die Aktenführungspflicht gesetzlich umschreibt. Gemäss dieser Bestimmung sind «für jedes Sozialversicherungsverfahren […] alle Unterlagen, die massgeblich sein können, vom Versicherungsträger systematisch zu erfassen». Stichwort ist hier die Massgeblichkeit, welche den Umfang der Aktenführungspflicht definiert. Dies entspricht sodann auch dem datenschutzrechtlichen Gebot der Gesetzmässigkeit von Datenbearbeitungen, das in § 8 IDG ZH enthalten ist und festlegt, dass öffentliche Organe Personendaten bearbeiten dürfen, soweit dies zur Erfüllung ihrer gesetzlich umschriebenen Aufgaben geeignet und erforderlich ist.

Insgesamt betrachtet dienen Aktenführungspflichten der Beweissicherung sowie der Nachvollziehbarkeit staatlichen Handelns.[10] Der Umfang und die Modalitäten der Aktenführung ergeben sich jeweils aus den Rechten an den betreffenden Akten, sei dies aus Verwaltungsverfahrens- oder Datenschutzrecht. Letzteres enthält zudem spezifische Anforderung an die Aktenführung, soweit in den Akten Personendaten enthalten sind. Im Folgenden werden die wichtigsten rechtlichen Grundlagen kurz dargestellt.

2. Verfassungsrechtliche Grundlage

Die allgemeine Aktenführungspflicht der Verwaltung stützt sich gemäss bundesgerichtlicher Rechtsprechung auf Art. 29 Abs. 2 BV. Diese *verfassungsrechtliche Aktenführungspflicht* ist nicht ausdrücklich festgelegt, sondern wird mittels Umkehrschlusses aus den Akteneinsichts- und Beweisführungsrechten der Adressaten staatlichen Handelns abgeleitet.[11] Aus diesem Zusammenhang heraus werden sodann die einzelnen Pflichten sowie deren Umfang bestimmt. Nach bundesgerichtlicher Rechtsprechung verpflichtet die Aktenführungspflicht Behörden dazu, «alles in den Akten festzuhalten, was zur Sache gehört und ent-

[9] Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG; SR 830.1).

[10] Roger Peter, Die Aktenführungspflicht im Sozialversicherungsrecht, in: Jusletter vom 14.10.2019, N 10.

[11] Giovanni Biaggini, BV Kommentar, 2. A., Zürich 2017 (zit. OFK BV-Biaggini), Art. 29 N 21.

scheidwesentlich sein *kann*».[12] Entsprechend können sich Aktenführungspflichten auch aus der Wahrnehmung von rechtlichen Pflichten ergeben, um zu einem späteren Zeitpunkt die sorgfältige Erfüllung einer solchen Pflicht nachweisen und damit Rechenschaft über den Umgang mit Daten ablegen zu können.[13]

3. Archivarisches Interesse an der Aktenführung

Neben den verfassungsrechtlichen Rechtsschutzinteressen besteht ein Aktenführungsinteresse aus archivarischen Zwecken. Archive dienen gemäss der Legaldefinition in § 4 des Archivgesetzes[14] der «dauernden authentischen Überlieferung der Tätigkeit der öffentlichen Organe zu rechtlichen, administrativen, kulturellen und wissenschaftlichen Zwecken». Die Aktenführung aus archivarischem Interesse ist deckungsgleich mit der allgemeinen Aktenführung, doch steht hier die Sicherstellung einer authentischen Überlieferung des laufenden Verwaltungsbetriebs im Vordergrund und nicht individuelle Rechtsinteressen.

4. Informations- und datenschutzrechtliche Aspekte der Aktenführungspflicht

Bestimmte Aspekte der Aktenführungspflicht ergeben sich direkt aus dem Datenschutzrecht bzw. werden durch dieses weiter konkretisiert. Es handelt sich hierbei einerseits um die Pflichten der Informationsverwaltung, insb. die doppelte Zielsetzung der Nachvollziehbarkeit und Rechenschaftsfähigkeit in § 5 IDG ZH sowie um weitere Bestimmungen, die im Sinne der Datensicherheit den Schutz der geführten Akten und deren Inhalt bezwecken. Andererseits enthält das IDG ZH zur Sicherung der informationellen Selbstbestimmung aus Art. 13 Abs. 2 BV, der Meinungs- und Informationsfreiheit in Art. 16 BV und damit verbunden der demokratischen Rechte[15] gewisse Einsichts- und Informationsrechte, die analog zu den allgemeinen Verfahrensrechten in Art. 29 Abs. 2 BV eine spezifische Aktenführungspflicht auslösen. Diese lassen sich

---

[12] BGE 130 II 473 E. 4.1 (Hervorhebung durch den Autor).

[13] Baeriswyl, PraKom IDG ZH (FN 6), § 5 N 6.

[14] Archivgesetz des Kantons Zürich vom 24. September 1995 (Archivgesetz; ON 170.6).

[15] Vgl. § 1 Abs. 2 lit. a IDG ZH; Antrag des Regierungsrates vom 9. November 2005, A. 2005 1283, Erläuterungen zu § 1, 20.

in der Regel jeweils auf die allgemein anerkannten Teilpflichten der Aktenführungspflicht abbilden.

a. Akten, Dokumente, Notizen und Personendaten

Für die Geltung des Datenschutzrechts spielt es keine Rolle, in welcher Form Personendaten bei einem öffentlichen Organ gespeichert sind. Gemäss der Legaldefinition in § 3 IDG ZH fallen sämtliche Informationen darunter, die sich auf eine bestimmte oder bestimmbare Person beziehen. Dies umfasst grundsätzlich sämtliche Akten, Dokumente und Notizen, die in irgendeiner Form eine Personenbezug aufweisen.[16] Allerdings gilt es zu beachten, dass Form und Kontext eines Personendatums durchaus für die Bestimmung des Persönlichkeitsrisikos für die betroffene Person heranzuziehen sind.

b. Informationsverwaltung (§ 5 IDG ZH)

Der Kern der informationsrechtlichen Aktenführungspflichten findet sich in § 5 IDG ZH. Gemäss § 5 Abs. 1 IDG ZH sind öffentliche Organe verpflichtet, ihre Informationen so zu verwalten, dass das Verwaltungshandeln nachvollziehbar und die Rechenschaftsfähigkeit gewährleistet ist. Dies entspricht dem bundesgerichtlichen Konzept, wie es aus Art. 29 Abs. 2 BV abgeleitet wird.

Die Erfüllung der Aktenführungspflicht des IDG ZH erfordert einen organisierten Umgang mit Information über den gesamten Lebenszyklus diesbezüglicher Daten hinweg, also von der Erstellung eines Dokuments über die Aufbewahrung bis hin zur Archivierung bzw. Vernichtung.[17] Für den Kanton Zürich hat die Datenschutzbeauftragte die wichtigsten Punkte zur Informationsverwaltung in einem Merkblatt zuhanden der öffentlichen Organe des Kantons und der Gemeinden zusammengefasst.[18]

Von Bedeutung ist in diesem Zusammenhang die Unterscheidung zwischen der laufenden Ablage, der ruhenden Ablage und dem Archiv.[19] Jede dieser

---

[16] Rudin, PraKom IDG ZH (FN 6), § 3 N 16.

[17] Baeriswyl, PraKom IDG ZH (FN 6), § 5 N 2.

[18] DSB Kanton Zürich (FN 6), *passim*.

[19] Vgl. Dazu die Kurzdarstellung «Lebenszyklus von Verwaltungsunterlagen» auf https://www.zh.ch/de/politik-staat/wie-behoerden-informationen-verwalten.html (Abruf 01.07.2022).

Phasen im Lebenszyklus von Akten entspricht auch einer je eigenen Zwecksetzung in Bezug auf die darin befindlichen Personendaten.

Die laufende Ablage umfasst sämtliche Bearbeitungen von der Eröffnung bis zum Abschluss eines Geschäfts. In diesen Akten dürfen sich nur (besondere) Personendaten befinden, welche das öffentliche Organ zur Erfüllung seiner gesetzlichen Aufgaben als geeignet und erforderlich i.S.v. § 8 Abs. 1 IDG ZH erachtet bzw. deren Bearbeitung i.S.v. § 8 Abs. 2 IDG ZH gesetzlich vorgesehen ist.

c. Richtige und vollständige Information (§ 7 Abs. 2 Bst. b & § 8 IDG ZH)

Eine erste bedeutende Konkretisierung erfährt die verfassungsrechtliche Aktenführungspflicht in § 7 IDG ZH, wonach Personendaten, die aufgrund der allgemeinen Aktenführungspflicht gespeichert sind, richtig und vollständig sein müssen. Diese Anforderung stellt einen Aspekt des Rechtsstaatsprinzip in Art. 5 BV dar,[20] der durch das IDG ZH im Hinblick auf die Bearbeitung von Personendaten konkretisiert wird: Gemäss § 8 IDG ZH dürfen staatliche Organe nur jene Personendaten bearbeiten, die sie für die Erfüllung ihrer gesetzlichen Aufgabe benötigen.

Die Anforderung der Richtigkeit bedeutet zunächst, dass Einträge «tatsachengemäss bzw. wahrheitsgemäss» zu erfolgen haben,[21] dass sich Behörden vergewissern müssen, dass die von ihnen erhobenen und geführten Personendaten den in diesen Daten beschriebenen Tatsachen entsprechen.

Die Anforderung der Vollständigkeit bekräftigt die Grundregel der allgemeinen Aktenführungspflicht, wonach sämtliche entscheidwesentlichen Tatsachen bzw. Informationen aktenkundig sein müssen. Dies beinhaltet auch die zugehörigen Metainformationen, anhand derer Echtheit und Richtigkeit der Daten verifiziert werden können. In der Lehre wird die Vollständigkeit der Daten zudem als Ausprägung der Gesetzmässigkeit für den Bereich der verwaltungsrechtlichen Informationsverarbeitung aufgefasst.[22]

---

[20] Peter (FN 10), N 13 ff.

[21] Peter (FN 10), N 15; «Prinzip der Aktenwahrheit».

[22] Baeriswyl, PraKom IDG ZH (FN 6), § 7 N 24.

Als entscheidwesentlich sind sämtliche Informationen zu qualifizieren, die für die Begründung einer Entscheidung notwendig sind. Dies umfasst Informationen mit deren Hilfe Argumente sowohl für als auch gegen einzelne Teilelemente einer Entscheidung gebildet werden und dadurch eine rechtsgenügliche Begründung ermöglichen sowie jene Informationen, welche in die Gewichtung zwischen diesen Argumenten einfliessen. Der Umfang der vollständigen Daten ergibt sich mit anderen Worten aus der allgemeinen rechtsstaatlichen *Begründungspflicht*: Entscheide sind durch Argumente zu begründen und diese durch Informationen aus den Akten zu belegen. Der Umfang der Begründungspflicht ergibt sich wiederum aus dem Umfang des Anspruchs auf rechtliches Gehör.[23]

d. Erkennbarkeit und Nachvollziehbarkeit von Veränderungen von Information (§ 7 Abs. 2 Bst. e IDG ZH)

Weitere bedeutende Aspekte der Aktenführungspflicht sind die Grundsätze der Erkennbarkeit und der damit eng verbundenen Nachvollziehbarkeit der Veränderung von Information. Sie auferlegen den Behörden eine Pflicht, sogenannte Metadaten der behördeninternen Informationsnutzung zu speichern. Hierbei handelt es sich um Daten über Daten, hier: Daten, welche Auskunft darüber geben, wer innerhalb einer Organisation Daten bearbeitet hat.

Die Erkennbarkeit ist zudem aufs engste mit der Informationspflicht der Behörden verbunden.

e. Vermeidung des Personenbezugs (§ 11 IDG ZH)

Der wohl bedeutendste Aspekt der datenschutzrechtlichen Konkretisierungen der allgemeinen Aktenführungspflicht ergibt sich aus dem sog. Prinzip der Datensparsamkeit.

Das Zürcher Gesetz bekräftigt dieses Prinzip in § 11 Abs. 1 IDG ZH, indem es den Behörden vorschreibt, Datenbearbeitungssysteme und -programme so zu gestalten, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht (mehr) notwendig sind.

Der Regelungszweck dieser Bestimmung zielt primär auf Metadaten, also auf Daten über Daten, mittels derer eine Verbindung zwischen anonymen Daten

[23] BGE 126 I 97 E. 2b.

und Personendaten hergestellt werden kann. Von besonderer Bedeutung sind hier sog. Randdaten, d.h. Daten, die für den Betrieb eines Informationssystems notwendig sind und die unter Umständen einer bestimmbaren Person zugerechnet werden können.[24] Allerdings fallen vom Wortlaut her alle Personendaten darunter, die in einem Informationssystem bearbeitet werden.[25] Insofern bildet § 11 Abs. 1 IDG ZH das Gegenstück zu Art. 8 IDG ZH.

Entsprechend muss der Grundsatz der Datenvermeidung auch für Fälle gelten, da Personendaten, die von einem Organ rechtmässig bearbeitet werden, für ein anderes Organ indes als Randdaten gelten. Typischerweise trifft dies beispielsweise auf das Verhältnis zwischen einer Verwaltungsstelle und der zuständigen IT-Abteilung zu.

Für die Aktenführung bedeutet dies zunächst in Ergänzung zum Grundsatz der Zweckbindung, dass Metadaten, welche einen Personenbezug für Daten herstellen, nur dann bearbeitet werden dürfen, wenn dies für den Betrieb des Informationssystems unerlässlich ist. Weiter ergibt sich aus § 11 Abs. 2 IDG ZH, dass Personendaten, soweit sie zur Aufgabenerfüllung notwendig sind, möglichst frühzeitig anonymisiert oder pseudonymisiert werden müssen und dass solche Personendaten, die nicht ano- oder pseudonymisiert werden können, möglichst zeitnah zu löschen sind, sobald sie nicht mehr für die Erledigung einer Aufgabe benötigt werden. Hieraus ergeben sich gemäss § 11 IDG ZH gewisse gesetzliche Designvorgaben an Datenbearbeitungssysteme und -programme.[26]

f. Meldepflicht beim Verlust von Personendaten (§ 12a IDG ZH)

Seit dem 1. Juli 2020 sieht das Gesetz eine Meldepflicht beim Verlust von Personendaten vor. Gemäss § 12a IDG ZH sind Behörden verpflichtet, die unbefugte Bearbeitung oder den Verlust von Personendaten der oder dem zuständigen Datenschutzbeauftragten unverzüglich zu melden, «wenn die Grundrechte der betroffenen Person gefährdet sind». Weiter sieht das Gesetz in gewissen Fällen eine Informationspflicht gegenüber den Betroffenen vor, die bei einem entgegenstehenden und überwiegenden öffentlichen oder privaten

---

[24] Baeriswyl, PraKom IDG ZH (FN 6), § 11 N 1.

[25] Baeriswyl, PraKom IDG ZH (FN 6), § 11 N 9.

[26] Siehe dazu VIII.B.

Interesse eingeschränkt werden kann. Eine Informationspflicht ist beispielsweise dann zu bejahen, wenn die Betroffenen Personen Schutzmassnahmen treffen müssen.[27] Denkbar wäre hier beispielsweise ein Datensicherheitsvorfall bei einem mit Passwort geschützten Informationssystem mit der Folge, dass die Betroffenen ihr Passwort ändern müssen.

Um die Meldepflicht wahrnehmen zu können, müssen Behörden nicht nur Akten führen, sondern sie müssen darüber hinaus in der Lage sein, die missbräuchliche Bearbeitung von Personendaten in ihren Akten zu erkennen. Die Meldepflicht stellt damit einen Massstab für die Massnahmen der Datensicherheit zur Verfügung, an dem diese auszurichten sind. Sie ergänzt und stärkt damit auch den Grundsatz der Datenintegrität.

5. Einsichtsrechte und Informationspflichten (§ 20 und § 12 IDG ZH)

Schliesslich konkretisieren die Datenschutzrechte sowie die korrespondierenden Transparenz- und Informationspflichten eine spezifische, auf Personendaten gerichtete Aktenführungspflicht, wie sie im Allgemeinen aus Art. 29 Abs. 2 BV abgeleitet wird. Es handelt sich um einen ausserprozessualen Unterfall des in Art. 29 Abs. 2 BV garantierten rechtlichen Gehörs. Auf diese wird in Kapitel V eingegangen.

IV. Datenschutzrechtliche Vorüberlegungen

A. Anwendbares Recht

Grundsätzlich gelten Wohnheime, die von einer privaten Betreibergesellschaft oder Stiftung betrieben werden, als private Datenbearbeiter und unterstehen gemäss Art. 2 Abs. 1 lit. a DSG (Art. 2 nDSG)[28] dem Datenschutzgesetz des

---

[27] DSB Kanton Zürich, Merkblatt Meldepflicht bei Datenschutzvorfällen, V. 1.1., September 2020, 2.

[28] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1); zum neuen Datenschutzgesetz des Bundes (nDSG) siehe Botschaft vom 25. September 2020 zum Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), BBl 2020 7639.

Bundes. Unter gewissen Bedingungen werden sie indes durch das kantonale Recht als «öffentliche Organe» qualifiziert und dem kantonalen Datenschutzgesetz unterstellt.

Für den Kanton Zürich bestimmt § 3 Bst. c IDG ZH, dass Datenbearbeitungen durch privatrechtliche Organisationen und Personen dem kantonalen Datenschutzrecht unterstehen, soweit diese mit der Erfüllung öffentlicher Aufgaben betraut sind. Im Umkehrschluss macht der Wortlaut deutlich, dass solche Privaten nur in Bezug auf Datenbearbeitungen dem jeweiligen öffentlichen Datenschutzrecht unterstellt sind, als diese der Erfüllung einer öffentlichen Aufgabe dienen, mit der sie betraut wurden.

Die Voraussetzung der Betrauung mit einer öffentlichen Aufgabe bringt zwei Abgrenzungsprobleme mit sich. Erstens ist nicht immer klar, ob die Bearbeitung von Personendaten durch eine private Person der Erfüllung einer öffentlichen Aufgabe dient bzw. ob die Wahrnehmung einer öffentlichen Aufgabe übertragen wurde. Zweitens kann bei der Bejahung einer Wahrnehmung von übertragenen öffentlichen Aufgaben unklar sein, ob und gegebenenfalls welche Datenbearbeitungen der privaten Person weiterhin als privat gelten und sich weiterhin im Geltungsbereich des Datenschutzgesetzes des Bundes befinden. Der Einbezug von gewissen privaten Datenbearbeitungen in den Geltungsbereich eines kantonalen Gesetzes kann denn auch dazu führen, dass eine private (natürliche oder juristische) Person insgesamt zwei Datenschutzgesetzen unterstellt ist (und damit auch zwei Aufsichtsbehörden).[29]

Die Voraussetzung der Wahrnehmung einer übertragenen öffentlichen Aufgabe ist zumindest dann erfüllt, wenn eine Leistungsvereinbarung oder eine andere Form der Übertragung entsprechender Aufgaben zwischen der Betreiberin des Wohnheims und einem Gemeinwesen vorliegt.[30] Sofern dies nicht der Fall ist, müsste wohl nach dem Rechtsgrund des Aufenthalts unterschieden werden: freiwillige Platzierungen basieren auf einem Dienstleistungsvertrag zwischen Privaten und unterstehen damit zunächst dem DSG des Bundes, während Platzierungen durch die KESB bzw. kantonale Behörden dem Da-

[29] Dazu Astrid Epiney, Zur Abgrenzung des Anwendungsbereichs des Datenschutzgesetzes des Bundes und der kantonalen Datenschutzgesetze, in: Jusletter vom 02.03.2015, N 14.

[30] Epiney (FN 29), N 13.

tenschutzgesetz des jeweiligen Kantons unterstehen. Da in solchen Fällen die Situation entstehen könnte, dass die Daten der Klientinnen und Klienten je nach Aufenthaltsgrund in einem anderen Datenschutzgesetz geregelt wären, müsste wohl aus Praktikabilitätsgründen nach bewährter Praxis der höhere Standard des kantonalen Rechts für sämtliche Datenbearbeitungen gelten.[31]

Für den Kanton Zürich ist auf den 1. Januar 2022 das neue Kinder- und Jugendheimgesetz in Kraft getreten.[32] Dieses sieht in § 5 Bst. b KJG eine Gesamtplanung des Angebots vor, für welche künftig langfristig angelegte Leistungsvereinbarungen mit den betreffenden Institutionen abgeschlossen werden sollen.[33] Diese sind an eine bestehende Bewilligung geknüpft. Es ist davon auszugehen, dass im Bereich des stationären Wohnens die Erbringung der Leistungen aufgrund einer Vereinbarung zum Standard wird.[34]

B. Befugnis zur Bearbeitung von Personendaten durch Wohnheime

Die von Wohnheimen im Rahmen der Betreuung ihrer Klientinnen und Klienten bearbeiteten Daten betreffen je nach Art und Umfang der Dienstleistungen verschiedene Lebensbereiche. Darunter sind regelmässig auch Daten, welche entweder den in § 3 IDG ZH aufgelisteten Lebensbereich der besonderen Personendaten betreffen oder deren Bearbeitung das Risiko einer Persönlichkeitsverletzung begründet.

Das Gesetz enthält keine ausdrücklichen Bearbeitungsgrundlagen für diese besonderen Datenkategorien. Indes werden Wohnheime vom Zivilrecht als Pflegeeltern qualifiziert. Als solche üben sie gemäss Art. 300 Abs. 1 ZGB stellvertretend die elterliche Sorge aus. Entsprechend stützt sich die Bearbeitungsbefugnis eines Wohnheims analog zu jener der Eltern, auf Befugnisse

---

31 Epiney (FN 29), N 14 m.w.H.

32 Kinder- und Jugendheimgesetz vom 27. November 2017 (KJG; ON 852.2).

33 Vgl. KJG Abschnitt C.

34 Weitere Informationen auf der Informationsseite des AJB unter https://www.zh.ch/de/familie/ergaenzende-hilfen-zur-erziehung/kinder-und-jugendheime.html (Abruf 01.07.2022).

aus der Wahrnehmung der elterlichen Sorge.[35] Aufgrund der ausführlichen Bestimmungen des Zivilrechts zur elterlichen Sorge und der damit verbundenen gesetzlichen Legitimierung ist daher davon auszugehen, dass implizit auch die zur Wahrnehmung der entsprechenden Rechte und Pflichten erforderliche Bearbeitung von besonderen Personendaten ermöglicht werden soll.[36]

C. Kategorisierung der Personendaten

1. Gesetzlich als sensitiv vermutete Personendaten

Als besondere Personendaten gelten gemäss § 3 Abs. 4 Bst. a Ziff. 1–4 IDG ZH zunächst einmal Daten über Klientinnen und Klienten, die den Bereichen der religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, der Gesundheit, der Intimsphäre oder der ethnischen Herkunft zuzurechnen sind sowie genetische und biometrische Daten. Ebenso Daten über Massnahmen der sozialen Hilfe sowie betreffend administrative oder strafrechtliche Verfolgungen oder Sanktionen. Solche Daten, die aus sich heraus als persönlichkeitsgefährdend qualifiziert werden, nennt die Lehre «sensitive Personendaten».[37] Es besteht eine gesetzliche Vermutung, dass ihre Bearbeitung eine *besondere Gefahr einer Persönlichkeitsverletzung* birgt. Entsprechend können sie im Einzelfall wie «gewöhnliche» Personendaten behandelt werden, wenn diese Vermutung widerlegt wird.[38]

In Erweiterung der Regelung des Bundes (dessen Kategorien von sensitiven Daten im Zürcher Gesetz als Beispiele aufgelistet sind) knüpft § 3 IDG ZH für die Qualifikation eines Datums als besonderes Personendatum nicht primär an die sensitiven Datenkriterien des Bundesrechts an, sondern an eine durch die jeweilige Bearbeitung der Daten begründete, besondere Gefahr einer Persönlichkeitsverletzung für die aus den Daten bestimmbaren Personen. Weder

---

[35] Zur Bearbeitungsbefugnis der Eltern in Bezug auf die Personendaten ihrer Kinder siehe V.C.

[36] Vgl. Philip Glass, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz – Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Zürich/St. Gallen 2017, 225 f.

[37] Rudin, PraKom IDG ZH (FN 6), § 3 N 20.

[38] Rudin, PraKom IDG ZH (FN 6), § 3 N 25.

das Gesetz noch die Anträge des Regierungsrates führen aus, wie der Begriff der Persönlichkeitsverletzung zu verstehen ist, auf den hier abgestellt wird.[39] Es muss daher an den Begriff der Persönlichkeitsverletzung in Art. 28 Abs. 1 ZGB sowie auf den Gehalt der grundrechtlichen Persönlichkeitsrechte als Schutzziele des bundesrechtlichen Datenschutzrechts[40] angeknüpft werden.

Gemäss Lehre ist die Voraussetzung der besonderen Gefahr für die Persönlichkeit in § 3 IDG ZH erfüllt, wenn eine Bearbeitung von Daten geeignet ist, das Ansehen und die soziale Geltung von bestimmten oder bestimmbaren Personen wesentlich zu beeinflussen bzw. wenn das Risiko einer stigmatisierenden Wirkung der Bearbeitung auf die Betroffenen besteht.[41] Darüber hinaus kann Art. 12 Abs. 1 Bst. b DSG analog und konkretisierend zur Anwendung gelangen, soweit dabei beachtet wird, dass dieser Persönlichkeitsverletzungen unter Privaten regelt und daher einen weniger umfassenden Schutz bietet. Diese Bestimmung vermutet[42], dass eine Verletzung der Persönlichkeit dann vorliegt, wenn Daten einer Person ohne Rechtfertigungsgrund gegen deren ausdrücklichen Willen bearbeitet werden. Keine Persönlichkeitsverletzung soll gemäss Art, 12 Abs. 2 DSG dann vorliegen, wenn jemand eigene Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Dazwischen liegt ein relativ weiter Interpretationsspielraum.

In Bezug auf die Situation von Wohnheimen erscheint schliesslich von Bedeutung, dass es sich bei ihren Klientinnen und Klienten um Kinder und/oder Jugendliche handelt. Ihre rechtliche Stellung legt nahe, dass die Bearbeitung ihrer Daten stets mit einer besonderen Gefahr für die Persönlichkeit verbunden ist, da sie in der Regel kaum in der Lage sein dürften, sich rechtlich gegen eine missbräuchliche Bearbeitung ihrer Personendaten zu wehren. Hinzu kommt, dass ihre diesbezüglichen Rechte aufgrund von variierenden Graden an recht-

---

[39] Antrag des Regierungsrates vom 9. November 2005 betreffend ein Gesetz über die Information und den Datenschutz (IDG ZH), ABl 1289, 1304.

[40] Botschaft vom 23. März 1988 des Bundesrates zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 413, 417 f.

[41] Rudin, PraKom IDG ZH (FN 6), § 3 N 20.

[42] Amédéo Wermelinger, in: Bruno Baeriswyl/Kurt Pärli (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 1. A., Bern 2015, Art. 12, N 4; David Rosenthal, in: David Rosenthal/Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 12 Abs. 2, N 14; uneinig sind sich die beiden Autoren darüber, ob es sich hierbei um eine widerlegbare Vermutung oder eine Fiktion handelt.

licher Handlungsfähigkeit mehr oder weniger eingeschränkt sind. Eine grundsätzliche Vermutung, dass Personendaten von Kindern und Jugendlichen besondere Personendaten im Sinne des Gesetzes darstellen, würde zudem jenem besonderen Schutz entsprechen, den Kinder und Jugendliche aufgrund von Art. 11 BV geniessen,[43] sowie den Zielen und Vorgaben der Kinderechtkonvention der Vereinten Nationen, welche für die Schweiz seit 1997 in Kraft ist.

2. Profiling durch Zeitdauer

a. Profile und Profiling

Neben Personendaten aus den genannten Schutzbereichen gelten gemäss § 3 Abs. 4 Bst. b IDG ZH auch Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit bestimmter oder bestimmbarer natürlicher Personen erlauben – sog. Persönlichkeitsprofile – als besondere Personendaten.

Im Bundesrecht ist die Rechtslage etwas komplizierter, zugleich aber sachgerechter, indem das künftige Datenschutzgesetz nicht mehr an das Vorliegen eines Profils, sondern an den Vorgang der Profilierung anknüpft. Dies entspricht dem modernen Verständnis von Datenschutz, wonach nicht die Daten selbst, sondern die Art und Weise der Bearbeitung ein Risiko für die Persönlichkeit und die Grundrechte darstellen.[44] Nach dieser Auffassung gilt Datenschutzrecht als (kontextsensitives) Risikorecht.[45]

In seiner Botschaft führt der Bundesrat dazu aus, dass der Wechsel von Persönlichkeitsprofilen hin zum Vorgang des Profiling als Schutzobjekt von einem statischen zu einem dynamische Datenschutzmodell gewechselt werde.[46] Für den Kanton Zürich ändert sich dadurch insofern nichts, als bereits unter dem geltenden Recht von einem dynamischen Risikobegriff ausgegangen wird: Im

---

[43] Siehe dazu die Ausführungen im Rahmen des Stellvertretungsrechts der Eltern, siehe dazu V.B.

[44] Die Botschaft spricht hier von einer «Modernisierung der Terminologie»; vgl. Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 (zit. Botschaft E-DSG), 6971; Glass (FN 36), 120.

[45] Glass (FN 36), 138 ff.

[46] Botschaft E-DSG (FN 44), 7020.

Gegensatz zum Datenschutzrecht des Bundes enthält § 3 IDG ZH Abs. 4 Bst. a IDG ZH eine allgemeine, nicht an die Aufzählung der besonderen Lebensbereiche beschränkte Definition der besonderen Personendaten, welche an eine Gefährdung der Persönlichkeit der Betroffenen anknüpft.[47] Dies gilt auch für die Bearbeitung von Personendaten, die eine gewisse Profilbildung darstellen, für sich genommen aber noch kein besonderes Personendatum im Sinne von § 3 Abs. 4 Bst. b IDG ZH darstellen.

b. Journale als Persönlichkeitsprofile

Journale bilden aufgrund ihrer verschiedenen Funktionen weite Bereiche des Lebens der Klientinnen und Klienten von Wohnheimen ab. Sie enthalten (sensible) Informationen über die persönliche Entwicklung, Beziehungen zu Freunden und Verwandten, wichtige Lebensstationen, medizinische Probleme, schulische Leistungen, Behördenkontakte sowie etwaige polizeiliche Informationen. Darüber hinaus dokumentieren sie individuell festgelegte persönliche Themen, die über die Jahre mit den Klientinnen und Klienten besprochen wurden.

Ein Journal, das über mehrere Monate oder gar Jahre geführt wurde, bildet somit grundsätzlich ein Persönlichkeitsprofil im Sinne von § 3 Abs. 4 Bst. b IDG ZH, d.h. eine Zusammenstellung von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit erlauben.

V. Rechte an den Klientendaten

A. Einsicht der minderjährigen Klientinnen und Klienten in die «eigenen» Personendaten

Aus dem Datenschutzrecht ergibt sich ein Einsichtsrecht der Kinder und Jugendlichen in jene Datenbearbeitungen des Wohnheims, welche ihre jeweiligen Personendaten betreffen. Der in § 20 Abs. 2 IDG ZH kodifizierte Anspruch bezieht sich grundsätzlich auf sämtliche Daten, welche für die Mitarbeitenden des Heims über das Kind bzw. den Jugendlichen zur Verfü-

[47] Glass (FN 36), 122.

gung gehalten werden. Dies gilt sowohl für elektronische als auch für andere Formen von Daten, etwa, Papierakten, Fotos und dergleichen – kurz: alles, was die Mitarbeitenden des Wohnheims über das Kind wissen und irgendwo in einem Dokument oder einer Akte festgehalten haben.

Das Einsichtsrecht wird durch den Ausnahmenkatalog in § 23 IDG ZH beschränkt.[48] Neben gewissen öffentlichen Interessen bilden gemäss Art. 23 Abs. 1 IDG ZH auch überwiegende private Interessen von Drittpersonen eine Grundlage für die Einschränkung der Einsichtnahme. Das Gesetz präzisiert diese Ausnahme, indem es in § 23 Abs. 3 IDG ZH die Ausnahme des überwiegenden privaten Interesses dahingehend konkretisiert, dass ein solches insbesondere dann vorliegt, wenn durch die Bekanntgabe der Information die Privatsphäre Dritter beeinträchtigt wird. Aus dem Wortlaut («insbesondere») folgt, dass weitere private Interessen denkbar sind, die im Einzelfall dem Einsichtsinteresse der Gesuchstellerin oder des Gesuchstellers entgegenstehen. Diese müssen entsprechend eine vergleichbare Persönlichkeitsnähe aufweisen.

Die weiteren Kategorien von entgegenstehenden privaten Interessen sind mit Hinblick auf die Aufgaben und das Selbstverständnis von Wohnheimen relevant, handelt es sich doch um eine Dienstleistungsbeziehung, die das Gesetz als quasi-familiär qualifiziert, indem es Wohnheime als Pflegeeltern qualifiziert.[49] Somit liegt eine Gemengelage aus beruflicher und privater Sphäre vor. Dies bedeutet, dass sog. «gemischte» Akten, welche Personendaten über Dritte, wie beispielsweise Mitarbeitende, Eltern, Lehrerinnen oder Lehrer sowie andere Kinder enthalten, entsprechend aufbereitet werden müssen, bevor das Kind Einsicht nehmen darf – soweit darin Informationen über Drittpersonen enthalten sind, die dem Kind nicht schon bekannt sind, wie dies beispielsweise bei Protokollen von Entwicklungsgesprächen mit dem Kind der Fall wäre.

In den Praxisinterviews wurde in dieser Hinsicht betont, dass die Klientinnen und Klienten über einen niederschwelligen Zugang zu ihren eigenen Journaldaten verfügen, indem sie diese beispielsweise mit der betreuenden Person

---

[48] Rudin, PraKom IDG ZH (FN 6), § 20 N 28.

[49] BK ZGB-Kurt Affolter-Fringeli/Urs Vogel, in: Kurt Affolter-Fringeli/Urs Vogel (Hrsg.), Berner Kommentar zum schweizerischen Zivilgesetzbuch, Die elterliche Sorge/der Kindesschutz, Bern 2016 (zit. BK ZGB-VerfasserIn), Art. 300 N 22.

besprechen oder damit zusammenhängende Fragen im Rahmen von Entwicklungsgesprächen thematisieren können. Dies ist insbesondere im Hinblick auf die Verwirklichung der in Art. 11 Abs. 2 BV verbrieften Autonomie sinnvoll[50] und stellt eine nachhaltige Erfüllung der datenschutzrechtlichen Informationspflichten dar.

B. Stellvertretung durch die Eltern?

Das Gesetz räumt den Eltern weitgehende Stellvertretungsrechte gegenüber Dritten ein für die Vornahme von rechtlich relevanten Handlungen im Namen ihrer Kinder. Sie werden zum einen ermächtigt, im Namen eines Kindes zu handeln und zum andern berechtigt, gewisse rechtliche Handlungen ihres Kindes zu genehmigen. Dies gilt auch für die Ausübung von Rechten der informationellen Selbstbestimmung,[51] und damit auch die Einwilligung in die Bearbeitung von Personendaten des Kindes.

Die Vertretungsmacht der Eltern wird indes durch zwei Faktoren begrenzt, namentlich durch den Umfang des Sorgerechts[52] sowie durch die Persönlichkeitsrechte des Kindes.[53]

Im Einzelnen weist Art. 304 Abs. 1 ZGB den Eltern aufgrund und im Umfang ihres Sorgerechts eine gesetzliche Vertretungsmacht im Hinblick auf Rechtsgeschäfte ihrer Kinder zu. Das Sorgerecht der Eltern gilt als Pflichtrecht[54] und umfasst insbesondere die Bestimmung des Aufenthaltsortes (Art. 301a ZGB) sowie die weltliche und religiöse Erziehung (Art. 302, 303 ZGB), kann indes durch Zuteilung der elterlichen Obhut an den anderen Elternteil auf die

---

[50] Siehe dazu sogleich folgend in V.B zum Stellevertretungsrecht der Eltern.

[51] Sandra Husi-Stämpfli, Kinder im digitalen Raum – Analoger Datenschutz in der Gesellschaft 4.0, Zürich/Basel/Genf 2021, 20.

[52] So ausdrücklich Art. 304 Abs. 1 ZGB.

[53] BSK ZGB I-Ingegeborg Schwenzer/Michelle Cottier, in: Christiana Fountoulakis/Thomas Geiser (Hrsg.), Basler Kommentar zum schweizerischen Zivilgesetzbuch I, Art. 1 – 456 ZGB, 6. A., Basel 2018 (zit. BSK ZGB I-VerfasserIn), Art. 301 N 2; BK ZGB-Affolter-Fringeli/Vogel (FN 49), Vorbemerkungen zu Art. 307–327c / II. – III. N 126.

[54] BSK ZGB I-Schwenzer/Cottier (FN 53), Art. 301 N 3; BK ZGB-Affolter-Fringeli/Vogel (FN 49), Art. 296 N 9.

«Restsorge»[55] beschränkt sein. Kennzeichnend für die elterliche Sorge als Pflichtrecht ist, dass sie (einer Amtspflicht ähnlich) im Hinblick auf einen gewissen Zweck auszuüben ist und nicht auf die Ausübung verzichtet werden kann.[56]

Die zweite Einschränkung ergibt sich im Verhältnis der Eltern zum Kind primär aus Art. 305 Abs. 1 ZGB, der dem urteilsfähigen Kind unter elterlicher Sorge das Recht zugesteht, im Rahmen des Personenrechts durch eigenes Handeln Rechte und Pflichten zu begründen und höchstpersönliche Rechte auszuüben. Diese Bestimmung wird mittlerweile durch die Selbstbestimmungsgarantie in Art. 11 BV verstärkt und erweitert. Sie verankert in Art. 11 Abs. 2 BV den Grundsatz des ZGB auf Verfassungsebene, wonach Minderjährige ihre Rechte im Rahmen ihrer Urteilsfähigkeit ausüben. Indes gilt dies auf Verfassungsebenen nicht bloss für höchstpersönliche, sondern für sämtliche Rechte und Pflichten.[57]

Dies hat zur Folge, dass die Einschränkungen der Autonomie in Art. 305 Abs. 1 ZGB als eine gesetzliche Einschränkung von Art. 11 Abs. 2 BV zu verstehen, und deren Anwendung in der Rechtspraxis entsprechend an den Voraussetzungen von Art. 36 BV zu messen ist.

Als wichtiges Element der Konkretisierung des Gehalts von Art. 11 BV kann die Kinderrechtskonvention hinzugezogen werden. Diese gesteht in Art. 12 Abs. 1 KRK «dem Kind, das fähig ist, sich eine eigene Meinung zu bilden, das Recht zu, diese Meinung in allen das Kind berührenden Angelegenheiten frei zu äussern» und garantiert, dass diese Meinung entsprechend dem Alter und der Reife des Kindes angemessen berücksichtigt wird. Ergänzend wird in Art. 12 Abs. 2 KRK ein Recht auf Anhörung verankert. Die Rechte aus diesen Bestimmungen können gemäss bundesgerichtlicher Rechtsprechung von Kindern gegenüber den Behörden in der Schweiz direkt geltend gemacht werden.[58]

---

[55] BGE 136 III 353 E. 3.2.

[56] BK ZGB-Affolter-Fringeli/Vogel (FN 49), Art. 296 N 9.

[57] BSK BV-Axel Tschentscher, in: Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Basler Kommentar, Basel 2015 (zit. BSK BV-VerfasserIn), Art. 11 N 25.

[58] Siehe die Nachweise bei Oliver Guillod/Sabrina Burgat, Droit des familles, 5. Ed., Basel 2018, 34.

Obwohl die Tragweite von Art. 11 BV noch herauszuarbeiten ist,[59] kann zumindest festgehalten werden, dass die darin verbrieften Rechte des Kindes als verfassungsmässige Rechte gegenüber der zivilrechtlichen elterlichen Sorgeplicht grundsätzlich höher zu gewichten sind, da letztere kein selbständiges Gegenrecht der Eltern darstellt, sondern vielmehr stets zur Wahrung des Kindeswohls bzw. der Durchsetzung der korrespondierenden Schutzrechte eingesetzt werden muss.[60] Zugleich aber tritt auch das Autonomierecht des Kindes regelmässig gegenüber dem öffentlichen Interesse am Kindeswohl zurück.[61] Aufgrund des Konkretisierungsmonopols der Eltern in Bezug auf das Kindeswohl[62] des unter ihrer Sorge stehenden Kindes kann sich daher eine etwas unklare Rechtslage ergeben. Eine pragmatische Auslegung gebietet wohl, dort, wo Eltern in ihrer Entscheidung einer dem Kindeswohl dienenden gesetzlichen Pflicht oder rechtlichen Obliegenheit entsprechen, der elterlichen Sorge den Vorrang zu geben und die Eltern auch gegen den Willen des Kindes entscheiden zu lassen.[63]

Im Ergebnis enthält das Gesetz für Eltern mit Sorgerecht eine Vermutung der Stellvertretungsmacht in Bezug auf das Wohl des Kindes im Rahmen ihrer jeweiligen Sorgerechte. Die Vermutung kann umgestossen werden, indem gezeigt wird, dass das betreffende Kind in diesem Bereich urteilsfähig ist und daher über das betreffende Rechtsgut bestimmen kann. Im Zweifelsfall ist jene Lösung zu suchen, von der angenommen wird, dass sie besser dem Kindeswohl dient, wobei Verfassung, Zivilgesetzbuch und Kinderrechtskonvention davon ausgehen, dass dies jene Lösung ist, welche die selbständige Entwicklung des Kindes am besten unterstützt.

---

59 BSK BV-Tschentscher (FN 57), Art. 11 N 1.

60 Siehe dazu auch Husi-Stämpfli (FN 51), 20.

61 BSK BV-Tschentscher (FN 57), Art. 11 N 34.

62 Dazu sogleich unter V.C.

63 Vgl. Husi-Stämpfli (FN 51), 21, am Beispiel der Einwilligung in die Bekanntgabe von Kindsdaten an einen Arzt oder die Schule.

C. Eigene Informationszugangsrechte der Eltern

1. Abgrenzung zur stellvertretenden Einsichtnahme

An dieser Stelle muss nun eine wichtige Unterscheidung getroffen werden. Eine Stellvertretung der Eltern in Bezug auf das Einsichtsrecht ihres Kindes liegt dann vor, wenn das Kind gestützt auf § 20 Abs. 2 IDG ZH Einsicht in seine «eigenen» Personendaten nehmen möchte und dies mangels rechtlicher Handlungsfähigkeit nicht geltend machen kann. In solchen Fällen sind die Eltern berechtigt, im Namen des Kindes handelnd ein entsprechendes Gesuch zu stellen.

Soweit aber die Eltern aus eigenem Interesse Einsicht in die Personendaten des Kindes verlangen, namentlich zur Ausübung ihres Sorgerechts, liegt hingegen keine Stellvertretung vor und handelt es sich nicht um eine Einsicht in eigene Personendaten des Kindes. In diesen Fällen stützt sich das Einsichtsgesuch der Eltern auf ihr Recht auf Informationszugang gemäss § 20 Abs. 1 IDG ZH, das auch Personendaten von Drittpersonen zum Gegenstand haben kann.

Aus Praxisinterviews ist ersichtlich, dass Gesuche um Einsicht in eigene Personendaten an das Wohnheim als Institution im Sinne von § 20 Abs. 2 IDG ZH eher gestellt werden, wenn ehemalige Klientinnen und Klienten ihre Vergangenheit aufarbeiten möchten. Aufgrund der quasi-familiären Beziehungen zwischen den Beteiligten werden solche Gesuche üblicherweise unkompliziert umgesetzt. Da Klientinnen und Klienten in solchen Fällen regelmässig nicht mehr der elterlichen Sorge unterstehen, liegt auch keine rechtliche Vermutung einer Stellvertretungsmacht der Eltern vor. Entsprechend sind Fälle, in denen Eltern ausdrücklich in Stellvertretung für ihr Kind eine Auskunft verlangen, selten anzutreffen. Somit fallen die allermeisten Fälle der Einsichtnahme in Personendaten der Kinder in die zweite, hier dargestellte Kategorie des Gesuchs um Informationszugang gemäss § 20 Abs. 1 IDG ZH, wobei es sich bei den eingeforderten Informationen um (besondere) Personendaten des Kindes handelt.

Der rechtliche Unterschied zwischen den Einsichtsrechten des Kindes und jenen der Eltern besteht darin, dass die Einsichtnahme des Kindes in die eigenen Personendaten gestützt auf § 20 Abs. 2 IDG ZH voraussetzungslos, d.h. ohne Begründung gewährt wird,[64] während für die elterliche Einsichtnahme in

[64] Rudin, PraKom IDG ZH (FN 6), § 20 N 24.

die Daten des Kindes aus eigenem Recht das Vorliegen eines Rechtsgrundes gemäss § 16 bzw. 17 IDG ZH nachgewiesen werden muss.

Von rechtlicher Bedeutung für die Beurteilung solcher Fälle erscheint hier insbesondere der Umstand, dass diese Konstellationen für die Eltern einen Interessenskonflikt bergen. Auf der einen Seite müssen sie die Interessen des Kindes vertreten, auf der anderen Seite sind sie befugt, im Rahmen des Sorgerechts eigene Interessen zu verfolgen, namentlich die Ausübung ihres «Konkretisierungsmonopols» in Bezug auf das Kindswohl, dessen Grenze aber wiederum die Verletzung des Kindswohls bildet.[65]

Wie gross der Spielraum der Eltern hier ist, erscheint indes unklar. Das Gesetz stellt zugleich die elterliche Sorge in Art. 301 Abs. 1 ZGB ausdrücklich unter den Vorbehalt der Urteilsfähigkeit des Kindes, die jedoch quasi «in erster Instanz» durch die Eltern selbst zu bestimmen ist. Der Interessenskonflikt tritt umso deutlicher zutage, je mehr das Kind an Urteilsfähigkeit gewinnt und in der Lage ist, gemäss Art. 305 Abs. 1 ZGB seine Rechte wahrzunehmen. Die ungerechtfertigte Annahme einer Stellvertretungsbefugnis der Eltern in einem Bereich, in dem das Kind aufgrund seiner Urteilsfähigkeit entscheidungsbefugt wäre, stellt wiederum eine Persönlichkeitsverletzung dar.

2. Rechtsgrundlagen für die Bekanntgabe von Kindsdaten an die Eltern

Gemäss § 16 Abs. 1 IDG ZH gibt ein öffentliches Organ Personendaten gegenüber Privaten bekannt, wenn eine rechtliche Bestimmung dazu ermächtigt, die betroffene Person im Einzelfall eingewilligt hat oder in Notfällen. Dasselbe gilt gemäss § 17 Abs. 1 IDG ZH im Grossen und Ganzen auch für besondere Personendaten, mit dem Unterschied, dass die Ansprüche an die rechtliche Grundlage in Bezug auf Normstufe und –dichte höher sind. Für die Bekanntgabe von Kindsdaten an die sorgeberechtigten Eltern bestehen gleich mehrere denkbare Rechtsgrundlagen. Ausserhalb von Notfällen, die je für sich zu entscheiden sind, sind die folgenden Rechtfertigungen denkbar.

Die Möglichkeit der Bekanntgabe aufgrund einer rechtlichen Ermächtigung i.S.v. § 16 Abs. 1 Bst. a IDG ZH (Personendaten) bzw. § 17 Abs. 1 Bst. a

[65] BSK ZGB I-Schwenzer/Cottier (FN 53), Art. 301 N 2.

IDG ZH (besondere Personendaten) setzt eine entsprechende rechtliche Bearbeitungsgrundlage der Eltern für diese (besonderen) Personendaten voraus. Dies bedeutet, dass die Bekanntgabe der Personendaten an die Eltern in einem Gesetz oder einer Verordnung geregelt sein muss.

Das ZGB enthält keine ausdrückliche, dem Sorgerecht entsprechende Datenbearbeitungsbefugnisse der Eltern in Bezug auf die Personendaten ihrer Kinder. Indes untersteht die Bearbeitung von Personendaten der Kinder durch die Eltern dem Datenschutzgesetz des Bundes. Das DSG erlaubt gemäss Art. 12 DSG (Art. 30 nDSG) grundsätzlich jegliche Datenbearbeitung zwischen Privaten, welche entweder nicht die Persönlichkeitsrechte der Betroffenen verletzen oder aber gerechtfertigt sind. Die Rechtfertigungsgründe finden sich in Art. 13 DSG (Art. 31 nDSG) und umfassen die Einwilligung des Verletzten sowie Rechtfertigung durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz.

Bei diesem letzten Rechtfertigungsgrund kann angesetzt, und die Bearbeitung von Kindsdaten durch die Eltern aufgrund ihres Sorgerechts gerechtfertigt werden. Und dies sowohl durch ein überwiegendes privates Interesse als auch durch Gesetz. Das private Interesse liegt in der Wahrnehmung des Sorgerechts der Eltern. Darüber hinaus verknüpft das Gesetz mit diesem privaten Interesse gewisse Rechtsfolgen, welche Bearbeitungen von Kindsdaten in der Regel zu rechtfertigen vermögen. Entsprechend der rechtlichen Funktion des Sorgerechts als Pflichtrecht[66] ist überdies anzunehmen, dass die Eltern die Personendaten ihrer Kinder bearbeiten müssen, soweit dies der Erledigung von Rechtsgeschäften der Kinder sowie zu deren Erziehung dient.

In Bezug auf das Recht der Eltern auf Zugang zu Information über ihr Kind gilt die elterliche Sorge folglich als rechtliche Bearbeitungsgrundlage, die keine weitergehende Begründung für die Legitimation des Informationszugangs im Einzelfall erfordert. Es ist lediglich ein plausibler Zusammenhang zwischen der Einsichtnahme und der Wahrnehmung eines bestehenden elterlichen Sorgerechts darzulegen sowie der genügende sachliche Umfang des elterlichen Sorgerechts nachzuweisen.

[66] Siehe dazu V.B.

3. Einwilligungsvorbehalt zugunsten des heranwachsenden Kindes

Soweit keine Rechtfertigung aufgrund des Sorgerechts vorliegt, besteht schliesslich die Möglichkeit der Bekanntgabe gestützt auf die Einwilligung des betroffenen Kindes i.S.v. § 16 Abs. 1 Bst. b bzw. § 17 Abs. 1 Bst. b IDG ZH. Diese Konstellation soll im Folgenden untersucht werden, wobei zunächst die Funktion des elterlichen Sorgerechts und sein Verhältnis zur zunehmenden Autonomie des Kindes im Bereich des Datenschutzrechts zu untersuchen sind. Es handelt sich hierbei um verfassungsmässige Fragen, welche insbesondere auch die Aufteilung der Schutzpflichten in Bezug auf Minderjährige zwischen Eltern und Staat betreffen. Für die Eltern ergeben sich diese aus dem Pflichtrecht der elterlichen Sorge, für den Staat aus den grundrechtlichen Garantien zugunsten der Autonomie der betreffenden Kinder. Mithin geht es demnach darum, zu prüfen, in welchen Fällen die grundrechtlich garantierte Autonomie des Kindes im Sinne von Art. 35 Abs. 3 BV geeignet ist, im privatrechtlichen Rechtsverhältnis zwischen Eltern und Kind zu wirken. Die Eignung steht insofern ausser Frage, als die Konstellation bereits im ZGB angelegt ist.[67]

a. Verfassungsmässige Grundlagen der Autonomierechte des Kindes

Die verfassungs- und zivilrechtlichen Datenschutzrechte, insbesondere das Recht auf informationelle Selbstbestimmung in Art. 13 BV, sind auf die Verhinderung und Behebung von Verletzungen der Persönlichkeit ausgerichtet.[68] Für Minderjährige wird dieser allgemeine Schutz durch die spezifischen Garantien in Art. 11 BV ergänzt.[69] Die Ziele der Bearbeitung von Personendaten von Kindern umfassen somit den allgemeinen Schutz vor Missbrauch der Daten sowie die Sicherung der informationellen Selbstbestimmung auf der einen sowie den Schutz des Kindeswohls gemäss Art. 11 Abs. 1 BV auf der anderen Seite. Vermittelnd tritt schliesslich die Sicherung der zunehmenden

---

[67] Siehe dazu V.B.

[68] Vgl. Art. 1 DSG, unverändert übernommen in Art. 1 nDSG; Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941, 7010; Art. 1 IDG ZH (Schutz der Grundrechte).

[69] OFK BV-Biaggini (FN 11), Art. 11 N 4, der insgesamt jedoch an der Sinnhaftigkeit der Norm zu zweifeln scheint (N 1).

Autonomie des heranwachsenden Kindes gemäss Art. 11 Abs. 2 BV hinzu, welche den Übergang zwischen der Phase des Kindeswohlschutzes und jener der informationellen Selbstbestimmung strukturiert, bzw. betont, dass diese Strukturierung, die bereits in der Konstellation zwischen Verfassung und Zivilgesetzbuch angelegt ist, vorzunehmen ist.[70]

b. Wahrnehmung der Persönlichkeitsrechte aus dem ZGB

Entsprechend ist die Wahrnehmung der Persönlichkeitsrechte gemäss Art. 19c ZGB nicht primär an das Alter, sondern an die Urteilsfähigkeit des Kindes gebunden.[71] Kinder sind mit anderen Worten bei der Wahrnehmung von Persönlichkeitsrechten im Rahmen ihrer Urteilsfähigkeit – von einigen gesetzlichen Ausnahmen abgesehen[72] – voll geschäftsfähig.[73] Die bedeutet auch, dass sie rechtlich in der Lage sind, selber in die Verletzung ihrer Persönlichkeit durch private Datenbearbeitung gemäss Art. 13 Abs. 1 DSG einzuwilligen. Dasselbe gilt für die Bekanntgabe von Personendaten durch öffentliche Organe im Sinne von § 3 IDG ZH gestützt auf § 16 bzw. 17 IDG ZH, inklusive der Bekanntgabe an die Eltern. Dies führt zur Notwendigkeit einer differenzierten Betrachtung der Urteilsfähigkeit von Minderjährigen in Bezug auf die Wahrnehmung entsprechender Rechte.

Klar erscheint zunächst, dass Klientinnen und Klienten von Wohnheimen je nach Urteilsfähigkeit zunehmend berechtigt sind, Einsichtnahmen der Eltern in ihre eigenen Personendaten (d.h. die Personendaten des Kindes) zu untersagen. Der Schutzauftrag der Eltern besteht indes weiterhin,[74] weshalb hier das Kindeswohl die gesetzliche Handlungsfähigkeit des Kindes beschränkt. Abgesehen von der gesetzlichen Vorschrift in Art. 303 Abs. 3 ZGB bezüglich der Urteilsfähigkeit in religiösen Fragen ab dem 16. Geburtstag bestehen nur wenige gesetzliche Altersgrenzen für die Bestimmung der Urteils- bzw.

---

70 Vgl. zur ergänzenden Funktion der Garantie OFK BV-Biaggini (FN 11), Art. 11 N 4 f. m.w.H.

71 Husi-Stämpfli (FN 51), 22.

72 KuKo ZGB-Sandra Hotz, in: Andrea Büchler/Dominique Jakob (Hrsg.), Kurzkommentar ZGB, 2. A., Basel 2018 (zit. KuKo ZGB-VerfasserIn), Art. 19c N 3.

73 KuKo ZGB-Hotz (FN 72), Art. 19c N 2.

74 KuKo ZGB-Cantieni/Vetterli (FN 72), Art. 303 Abs. 3 N 5.

Rechtsfähigkeit bei Minderjährigen.[75] Die Urteilsfähigkeit muss daher jeweils im Einzelfall bestimmt werden; allerdings wohl, aufgrund der Betonung des Kindeswohls in der Verfassung, tendenziell zugunsten der Kindesautonomie.[76]

4. Verfahren bei Urteilsunfähigkeit des Kindes

Die Geschäftsfähigkeit des Kindes im Bereich der Persönlichkeitsrechte gemäss Art. 19c ZGB umfasst auch das Recht auf Anhörung.[77] Ob eine Anhörung durchgeführt werden sollte und welche Ziele damit verbunden sind, bestimmt sich sinnvollerweise auch im öffentlich-rechtlichen Bereich analog zu den bestehenden Bestimmungen im Zivil- und Zivilprozessrecht. Diese sehen vor, dass urteilsunfähige Kinder grundsätzlich ab 6 Jahren zum Zweck der Sachverhaltsermittlung sowie zur Erfüllung der Transparenzpflicht angehört werden sollten.[78]

Dies hat auch Folgen für das Verfahren des Informationszugangs. In Fällen, da ein Kind nicht urteilsfähig ist, muss das Wohnheim in Anwendung von § 23 Abs. 1 und 3 IDG ZH eine Interessensabwägung durchführen. Dazu gehört auch eine Anhörung des Kindes gemäss § 26 IDG ZH sowie für die Bekanntgabe von besonderen Personendaten die Einholung einer ausdrücklichen Zustimmung der vertretungsbefugten Person. Entsprechend sollten hier die Vorgaben des Zivil- bzw. Zivilprozessrechts übernommen und Kinder ab 6 Jahren angehört werden. Nach dem gesagten gebieten Gesetz und Verfassung indes, in Fällen, da Kinder jünger als 6 Jahre sind, im Einzelfall zu prüfen, ob eine Anhörung sinnvoll wäre.

---

[75] Siehe die Aufzählung bei KuKo ZGB- Hotz (FN 72), Art. 11 N 4a.

[76] KuKo ZGB-Hotz (FN 72), Art. 16 N 3; bedenkenswert erscheint auch der Vorschlag, Kinder ab Eintritt in die Primarschule grundsätzlich in «Entscheide rund um den digitalen Alltag» einzubeziehen; siehe bei Sandra Husi-Stämpfli/Rita Jedelhauser, Alles für ein «like»: Sharenting vs. Kindeswohl – Kinderbilder in sozialen Medien aus Daten- und Kindesschutzsicht, in: Jusletter vom 29.04.2019, N 27 ff.

[77] KuKo ZGB-Hotz (FN 72), Art. 19c N 2; zur entsprechenden Garantie in Art. 12 KRK siehe N 55.

[78] Andrea Büchler/Luca Maranta, Das neue Recht der elterlichen Sorge – Unter besonderer Berücksichtigung der Aufgaben der Kindes- und Erwachsenenschutzbehörden, in: Jusletter vom 11.08.2014, N 92 f.

5. Zusammenfassung

Im Ergebnis bemisst sich die Zulässigkeit der Bekanntgabe von gewöhnlichen und besonderen Personendaten aus dem Journal an die Eltern an den Bestimmungen in § 16 und 17 IDG ZH über die Bekanntgabe von Information durch öffentliche Organe. Rechtsgrundlage für die Bearbeitung der Daten durch die Eltern gemäss § 16 bzw. 17 Abs. 1 Bst. a IDG ZH sind die Bestimmungen über das elterliche Sorgerecht. Entsprechend muss der Nachweis eines vorhandenen elterlichen Sorgerechts erbracht werden. Zu beachten ist, dass die Einsichtnahme gemäss § 23 Abs. 1 und 3 IDG ZH bei entgegenstehenden privaten Interessen des Kindes einzuschränken ist, wobei das Kind grundsätzlich angehört werden muss. Massgeblich ist, wie in allen Rechtsbeziehungen zwischen den Eltern und Kindern, das Kindswohl.[79]

Schliesslich ist das in Bezug auf den Einzelfall für urteilsfähig befundene Kind berechtigt, die Zustimmung zur Bekanntgabe seiner Daten an die Eltern zu verweigern. Durch die Verweigerung der Zustimmung entfällt der Rechtfertigungsgrund i.S.v. Art. 12 DSG für eine Kenntnisnahme der Kindesdaten durch die Eltern. Zudem bedeutet die Urteilsfähigkeit des Kindes, dass der Rechtsgrund der elterlichen Sorge als Voraussetzung für die Bekanntgabe der Daten wegfällt. Dem Wohnheim obliegt hier die Prüfung, ob das Kind in Bezug auf die Informationen, in die Einsicht verlangt wird, urteilsfähig ist und damit berechtigt, seine Zustimmung zu verweigern.

Da es sich hierbei um eine andauernde Entwicklung handelt, in deren Verlauf der Bereich der Einsichtsrechte der Eltern durch das Kind zunehmend eingeschränkt wird (bis sie mit Erreichen der Volljährigkeit grundsätzlich erlöschen), erscheint es sinnvoll, soweit möglich und dem Kindeswohl nicht abträglich, Eltern und Kinder periodisch zusammenzusetzen und den Umfang des Einsichtsrechts gemeinsam auszuhandeln. Dies entspricht gemäss Aussagen in den verschiedenen Interviews einer gängigen Praxis in Jugendwohnheimen.

---

[79] BSK ZGB I-Schwenzer/Cottier (FN 53), Art. 301 N 8a; BK ZGB-Affolter-Fringeli/Vogel (FN 49), Art. 296 N 12 ff.

D. Einsichtnahme durch Dritte

Soweit Wohnheime als öffentliche Organe im Sinne von § 3 IDG ZH gelten, unterstehen die bei ihnen gespeicherten Informationen grundsätzlich dem Öffentlichkeitsprinzip und können über ein Zugangsgesuch gemäss § 20 Abs. 1 IDG ZH von Privaten eingesehen werden.

Wie bereits gezeigt wurde, stützen sich Einsichtsgesuche von Eltern in die Personendaten ihrer Kinder in Bereichen der elterlichen Sorgepflicht auf dieses Zugangsrecht und unterstehen hierbei den Einschränkungen aufgrund von entgegenstehenden privaten Interessen des betroffenen Kindes. Dasselbe gilt umso mehr für Einsichtsgesuche von Personen, die gegenüber einem Kind keine elterliche Sorgepflicht tragen. Dies betrifft neben Dritten auch Eltern, deren Sorgerecht eingeschränkt oder entzogen wurde.

Zugangsgesuche gestützt auf das Öffentlichkeitsprinzip unterstehen dem weitgehenden Vorbehalt von § 24 Abs. 1 und 3 IDG ZH, der die Einschränkung oder Verweigerung des Zugangs erlaubt, wenn entgegenstehende private Interessen das öffentliche Interesse am Zugang überwiegen. Der entsprechende, weite Beurteilungsspielraum eines Wohnheims muss dabei stets im Interesse des Kindeswohls genutzt und dessen Rechte müssen gewahrt werden. Daraus ergeben sich gewisse Folgen. Erstens muss das Kind – soweit es im Hinblick auf diese Frage als urteilsfähig eingeschätzt wird – gemäss § 26 Abs. 1 IDG ZH angehört werden.

Betrifft das Einsichtsgesuch besondere Personendaten des Kindes, muss es in solchen Fällen gemäss § 26 Abs. 2 IDG ZH ausdrücklich in die Einsichtnahme zustimmen. Wird dem Kind im Hinblick auf das konkrete Einsichtsgesuch keine genügende Urteilsfähigkeit zugestanden, muss das Heim der zur Vertretung berechtigten Person die Möglichkeit zur Stellungnahme geben und auch hier das Gesuch gemäss § 26 IDG ZH ablehnen, sofern besondere Personendaten des Kindes betroffen sind und die berechtigte Person nicht ausdrücklich zustimmt.

Die Qualifikation als besondere Personendaten kann hier eine gewisse Schwierigkeit bereiten, sollte indes aufgrund des besonderen Schutzauftrags in Art. 11 BV sowie im Kindesrecht des ZGB grundsätzlich angenommen werden.

In den übrigen Fällen muss die Heimleitung entscheiden, ob die Einsicht im konkreten Fall im Interesse des Kindeswohls einzuschränken oder gar zu verweigern sei, wobei in Fällen, da eine Einsichtnahme ganz verweigert wird, davon auszugehen ist, dass die Ablehnung des Gesuchs mit einem Risiko für das Kind begründet wird, das die entsprechenden Daten sowieso als besondere Personendaten qualifiziert. Während diese Frage im Hinblick auf Einsichtsgesuche von Eltern des Kindes gewisse Schwierigkeiten bereiten kann, ist im Falle von Gesuchen von privaten Dritten das private Interesse des Kindes im Allgemeinen höher zu gewichten, insbesondere dann, wenn es sich nicht um verwandte Personen handelt. Zugangsgesuche von Dritten aufgrund des Öffentlichkeitsprinzips werden daher in der Regel aufgrund des vorrangigen Schutzes der Kinder scheitern, sofern die Gesuchsteller nicht mit dem Kind verwandt oder befreundet sind.

VI. Einzelne Verfahrensfragen

A. Einsichtsgesuche der Eltern in eigene Personendaten

Gemäss Aussagen in Praxisinterviews verlangen Eltern zuweilen gestützt auf § 20 Abs. 2 IDG ZH Zugang zu ihren eigenen Personendaten. Dies betrifft beispielsweise Protokolle von Sitzungen, an denen sie teilgenommen haben, kommt aber auch in der Form eines allgemeinen Gesuchs zur Einsicht in sämtliche über den betreffenden Elternteil gespeicherte Personendaten vor. In diesen Konstellationen sind Personendaten von Kindern der Gesuchsteller als Daten von Drittpersonen zu behandeln und ist der Zugang gegebenenfalls gestützt auf § 23 Abs. 1 und 3 IDG ZH und nach Anhörung des Kindes einzuschränken.

B. Rechtsstellung von Geschwistern

Die Rechte von Geschwistern sind im ZGB nicht ausdrücklich geregelt. Ihnen kommt zumindest kein Sorgerecht zu, und die familiäre Beistandspflicht wirkt für sie nur mittelbar[80] und damit zumindest subsidiär zu jener der Eltern.

[80] Heinz Hausheer/Thomas Geiser/Regina E. Aebi-Müller, Das Familienrecht des Schweizerischen Zivilgesetzbuches, 6. A., Bern 2018, N 17.26.

Indes können sie gewisse Ansprüche auf den in Art. 13 Abs. 1 BV garantierten Schutz des Familienlebens stützen. Dies schützt die familiäre Gemeinschaft vor äusseren Beeinträchtigungen[81] und kann entsprechend einen Rechtsgrund darstellen für erweiterte Auskünfte aus dem Gemeinderegister, wie beispielsweise den Wegzugsort ihrer Geschwister, die sie gestützt auf § 18 Abs. 2 MERG[82] von der Einwohnerkontrolle der vermuteten Wohngemeinde einholen müssen.

In Bezug auf die bei einem Wohnheim gespeicherten Kindsdaten muss daher mangels einer Rechtsgrundlage primär auf die Einwilligung gemäss § 16 Abs. 1 Bst. b bzw. § 17 Abs. 1 Bst. b IDG ZH abgestellt werden. Analog zur Einsichtnahme durch die Eltern ist das Kind, über das ein Geschwister Daten erhalten möchte, auch bei mangelnder Urteilsfähigkeit anzuhören.[83] Vorbehalten bleibt auch hier die Bekanntgabe in Notfallsituationen gestützt auf § 16 Abs. 1 Bst. c bzw. § 17 Abs. 1 Bst. c IDG ZH.

C. Interessensnachweis bei hohem Aufwand

Sofern ein Gesuch um Einsicht einen grossen Aufwand verursacht, kann das Wohnheim gemäss § 25 Abs. 2 IDG ZH einen Interessensnachweis verlangen. Dies gilt sowohl für den Informationszugang als auch für den Zugang zu eigenen Personendaten.[84] Die Voraussetzung des hohen Aufwands wird in § 15 IDV ZH[85] dahingehend präzisiert, dass ein öffentliches Organ einen Interessensnachweis verlangen kann, «wenn es das Gesuch mit seinen verfügbaren Mitteln nicht behandeln kann, ohne dass die Erfüllung seiner anderen Aufgaben wesentlich beeinträchtigt wird». In welchen Fällen diese Voraussetzung tatsächlich erfüllt ist, ergibt sich weder aus dem Gesetz noch lassen sich in Lehre und Praxis griffige Kriterien ermitteln. Allgemein wird

---

[81] René A. Rhinow/Markus Schefer/Peter Uebersax, Schweizerisches Verfassungsrecht, 3. erw. u. akt. A., Basel 2016, N 1361.

[82] Gesetz vom 11. Mai 2015 über das Meldewesen und die Einwohnerregister (MERG; ON 142.1).

[83] Siehe dazu V.C.4.

[84] Thönen, PraKom IDG ZH (FN 6), § 25 N 8.

[85] Verordnung vom 28. Mai 2008) über die Information und den Datenschutz des Kanton Zürich (IDV ZH; ON 170.41)

darauf abgestellt, ob ein öffentliches Organ aufgrund des Aufwands, den ein Einsichtsgesuch generiert, seine Kernaufgaben nicht mehr wahrnehmen kann.[86] Die Begründung des Regierungsrates zur IDV ZH nennt immerhin einige Indizien, welche das Vorliegen eines grossen Aufwandes anzeigen, namentlich komplexe Anonymisierungsbedürfnisse sowie eine besonders aufwändige Beschaffung der notwendigen Dokumente.[87]

Andere Kriterien, wie insbesondere die voraussichtliche Dauer einer solchen Beeinträchtigung, erscheinen dagegen unwesentlich zu sein. In den Tätigkeitsberichten der kantonalen und kommunalen Datenschutzbehörden sind zudem keine Fälle zu finden, die auf eine gefestigte Praxis hinsichtlich der Frage hindeuten, wann ein hoher Aufwand anzunehmen ist. Klar scheint zumindest, dass beispielsweise die Anstellung von spezialisiertem Personal zur Nutzbarmachung veralteter Datenbestände einen hohen Aufwand im Sinne des Gesetzes bedeuten würde.

Für Wohnheime bedeutet dies im Ergebnis, dass gegenüber Privaten nur in seltenen Fällen ein Interessensnachweis verlangt werden kann. Die genannten Voraussetzungen wären erst erfüllt, wenn ein Wohnheim Dienstleistungen zugunsten seiner Klientinnen und Klienten einschränken müsste, um ein Gesuch zu beantworten, oder wenn es für den ordentlichen Betrieb zusätzliches Personal bzw. spezialisiertes Personal für die Beantwortung der Anfrage benötigte.

Wird indes ein genügendes Interesse nachgewiesen, kann das Organ gemäss § 28 Abs. 2 IDG ZH die Frist zur Beantwortung des Gesuchs bzw. Gewährung des Zugangs zur verlangten Information verlängern, in Ausnahmefällen um bis zu nochmals 30 Tage.[88] Hierbei besteht nach wie vor die Möglichkeit, die Einsicht inhaltlich einzuschränken.

D. Amts- und Rechtshilfe

Die bei Wohnheimen gespeicherten Personendaten ihrer Klientinnen und Klienten können auch Gegenstand von Auskunftsgesuchen durch Dritte,

---

[86] Thönen, PraKom IDG ZH (FN 6), § 25 N 6.

[87] Begründung zur IDV, ABl 2008 916, 934.

[88] Thönen, PraKom IDG ZH (FN 6), § 28 N 5.

insbesondere von Behörden sein. Die Rechtsgrundlage für Erteilung von derartigen Auskünften, die eine Form der Bekanntgabe von Personendaten darstellen, bestimmt sich danach, wer ein Gesuch stellt, ob die Auskunft innerhalb oder ausserhalb eines Verfahrens verlangt wird.

Gemäss § 16 Abs. 2 IDG ZH bzw. § 17 Abs. 2 IDG ZH sind die öffentlichen Organe von Kanton und Gemeinden berechtigt, «anderen öffentlichen Organen sowie den Organen anderer Kantone oder des Bundes» im Einzelfall sowohl gewöhnliche als auch besondere Personendaten bekanntzugeben, «wenn das Organ, das Personendaten verlangt, diese zur Erfüllung seiner gesetzlichen Aufgaben benötigt». Diese sog. amtshilfeweise Bekanntgabe muss indes nach Lehre und Praxis verhältnismässig erfolgen.[89] Es dürfen daher nicht mehr Informationen bekanntgegeben werden, als das anfragende öffentliche Organ zur Erledigung der Aufgabe benötigt, welche den Grund für die Anfrage bildet.

Im Gegensatz zu den Gesuchen von Privaten besteht im Bereich der Amts- und Rechtshilfe wenig Spielraum für Fristen aus dem IDG ZH. Diese werden oftmals durch das Verfahrensrecht vorgegeben, welches die Rechtsgrundlage für die Datenbearbeitung des betreffenden Organs bildet. Der zweite wichtige Unterschied zu den Gesuchen von Privaten besteht darin, dass Gesuche um Amts- bzw. Rechtshilfe rechtlich begründet sein müssen. Das bekanntgebende Organ ist entsprechend verpflichtet, eine doppelte Rechtmässigkeitsprüfung durchzuführen: einmal für die eigene Bekanntgabe der Daten und dann für die Bearbeitung der Daten durch das empfangende Organ.[90]

Private Personen können aus Prozessrecht Akteneinsicht verlangen. Diese geht weniger weit als die Einsichtsrechte nach IDG ZH und beschränkt sich auf die wesentlichen Akten für ein Verfahren.[91]

---

89 Rudin, PraKom IDG ZH (FN 6), § 16 N 38.

90 Glass (FN 36), 125.

91 Siehe bei OFK BV-Biaggini (FN 11), Art. 29 N 21; BGE 125 II 473 E. 4.

VII. Journal- und Administrationssoftware

A. Notwendigkeit eines funktionierenden Datenmanagements

Der bisherige Gang der Untersuchung hat gezeigt, dass Wohnheime im Hinblick auf die bei ihnen anfallenden Personendaten der Klientinnen und Klienten vielfältige Pflichten treffen. Die Umsetzung dieser Pflichten erfordert neben der korrekten Anwendung und Umsetzung des Datenschutzrechts, der korrekten Aktenführung sowie der genügenden Datensicherung auch ein entsprechendes Datenmanagement, welches die Erfüllung unterstützt.

Wie weiter gezeigt wurde, sieht das IDG ZH einen niederschwelligen Zugang von Individuen zu den über sie gespeicherten Personendaten vor. Dieser hat grundsätzlich kostenlos zu erfolgen und kann nur in Ausnahmefällen eingeschränkt oder zeitlich aufgeschoben werden. Umso wichtiger erscheint es daher, die bei einem Wohnheim vorhandenen Daten in einer Art und Weise zu organisieren, dass die Zusammenstellung von Informationsbeständen zur Beantwortung von Einsichtsgesuchen sowie die Erfüllung der anderen gesetzlichen Pflichten in Bezug auf Personendaten möglichst problemlos erfolgen kann. Das Fundament eines solchen Datenmanagements kann die Journalsoftware bilden,[92] soweit sie dazu geeignet ist. Hierfür muss sie gewisse Funktionen bereitstellen, die im Folgenden überblicksartig dargestellt werden.

B. Hauptfunktion der Journalsoftware

1. Erfassung von Journaldaten

Die zentrale Funktion einer Journalsoftware ist die chronologische Dokumentation des Aufenthalts der Kinder und Jugendlichen im betreffenden Heim sowie sämtliche damit zusammenhängenden externen Aktivitäten. Erfasst werden jene Daten, welche für die Erfüllung des (sehr weit gefassten) gesetzlichen Auftrags benötigt werden. Aufgrund der gesetzlich vorgegebenen, quasi-familiären Bedeutung von Wohnheimen für die Klientinnen und Klienten, dürfen Daten aus sämtlichen Lebensbereichen bearbeitet werden, insbe-

[92] Die nachfolgenden Grundsätze gelten sinngemäss auch für die Führung von Papierakten.

sondere auch jenen, welche gemäss IDG ZH als besondere Personendaten zu qualifizieren sind. Vorbehalten bleibt, analog der Dateneinsicht von Eltern, die Einwilligung der Klientinnen und Klienten in Bereichen, in denen sie als urteilsfähig eingeschätzt werden.[93]

Der Einfachheit halber werden im Rahmen dieser Studie sämtliche Daten, die in das Journal aufgenommen werden, als Journaldaten bezeichnet. Hierunter sind somit sämtliche Daten und Dokumente zu verstehen, die im Zusammenhang mit dem Aufenthalt im Heim erhoben werden bzw. anfallen. Dies beinhaltet insbesondere Gesprächsprotokolle mit den Kindern und Jugendlichen, Einschätzungen der Betreuungsperson, externe Dokumente wie Zeugnisse, medizinische Berichte aber auch Kalenderdaten und Planungsnotizen.

2. Einbindung in das administrative Informationssystem

Das Journal bildet einen Teil des Informationssystems eines Wohnheims. Daneben wird ein administratives System geführt, das die personellen und organisatorischen Abläufe dokumentiert und für die Planung aufbereitet. Die beiden Systeme sind notwendigerweise miteinander verbunden. Zum einen bildet das Journal Informationen ab über die Klientinnen und Klienten des Heims, welche den Kern der Aufgabenerfüllung darstellen. Entsprechend ist die Administration um diese herum aufgebaut, insbesondere im Hinblick auf die Betreuung. Zum anderen erfordern die Pflichten der Aktenführung, die sich aus den Vorgaben von Datenschutz bzw. Datensicherheit ergeben, eine gewisse Nachvollziehbarkeit der Journalführung.[94]

Es ist demnach geboten, zwecks Nachvollziehbarkeit der Journalführung sowie zur Erfüllung der Funktionen des Journals, dieses mit anderen administrativen Daten, insbesondere Personaldaten wie Kalender, Verfügbarkeit etc. zu verknüpfen. Die Journalsoftware sollte demnach gewisse Schnittstellen zu den administrativen Informationssystemen eines Wohnheims gewährleisten. Sie kann auch ein integraler Bestandteil solcher Systeme sein.

[93] Siehe dazu V.C.3.

[94] Siehe dazu III.B.3.

Aufgrund der Sensitivität der über die Klientinnen und Klienten gespeicherten Personendaten, die überdies gesamthaft je ein Profil i.S.v. § 3 Abs. 4 Bst. b IDG ZH bilden,[95] ist überdies die Auslagerung in eine «Cloud» nicht zu empfehlen.[96]

3. Sortierungsfunktionen und Strukturierung

Voraussetzung für die Einbindung von Daten in die Bearbeitungsprozesse ist eine sinnvolle Strukturierung der Datenbestände in der Datenbank, welche mit dem Interface der Journalsoftware verbunden ist. Typische Sortierungskategorien sind die Sortierung nach Datum, Person, Dokumenttyp oder Autor eines Eintrags bzw. Dokuments.

Die in Praxisinterviews beschriebenen Funktionen der von Wohnheimen eingesetzten Software zeigen, dass diese primär mit klassischen Sortierparametern wie Datum, Person oder Dokumenttyp arbeiten. Dies funktioniert problemlos bei der Suche nach einzelnen Einträgen oder Dokumenten, kann indes bei umfangreicheren Einsichtsgesuchen an Grenzen stossen, wenn es um die gesetzlich geforderte differenzierte Abwägung geht.

C. Managementfunktionen in Bezug auf Datensicherheit und Datenschutz

Datensicherheit hat zum Zweck, Vertraulichkeit, Integrität und Verfügbarkeit von Daten bzw. der daraus ermittelbaren Information, sicherzustellen.[97] Der Fokus auf den Schutz der aus Daten ermittelbaren Information entspricht der datenschutzrechtlichen Einordnung, wonach nicht Daten, sondern deren Nutzung bzw. deren Informationen über Personen ein Risiko für deren Persönlichkeit begründen können.[98] Über die Mechanismen der Datensicherheit

---

[95] Siehe dazu IV.C.2.b.

[96] Vgl. privatim – Konferenz der schweizerischen Datenschutzbeauftragten, Merkblatt Cloud-spezifische Risiken und Massnahmen, v2.1/17.12.2019, abrufbar unter https://www.privatim.ch/wp-content/uploads/2019/12/privatim-Cloud-Papier_v2_1_20191217.pdf (Abruf 07.05.2021).

[97] Dennis-Kenji Kipker, Cybersecurity – Rechtshandbuch, München 2020, 26.

[98] Glass (FN 36), 118.

kann daher ein grosser Teil der Anforderungen des Datenschutzrechts in den Prozessablauf der Datenbearbeitung eingegliedert werden. Im Vordergrund stehen die folgenden Funktionen.

1. Zugriffsrechte und Authentisierung

Wie bereits gezeigt wurde, enthält das IDG ZH vielfältige Grundsätze zur Sicherung der rechtmässigen Bearbeitung von Daten durch die öffentlichen Organe, welche diese insbesondere auch verpflichten, Massnahmen zur Umsetzung zu ergreifen.[99] Im Hinblick auf die Frage, welche Informationen überhaupt bearbeitet werden dürfen, verlangt das Datenschutzrecht in § 8 IDG ZH eine gesetzliche Rechtfertigung für jede Bearbeitung von Personendaten durch ein öffentliches Organ.[100] Aus der Gemengelage an Pflichten folgt, dass öffentliche Organe sich auf eine Art und Weise organisieren müssen, die sicherstellt, dass Mitarbeiterinnen und Mitarbeiter nur Zugriff auf personenbezogene Informationen haben, welche sie für die Erfüllung der ihnen innerhalb des Organs zur Erledigung übertragenen öffentlichen Aufgabe benötigen.

Für Daten auf Papier bedeutet dies in der Regel eine Form des Schlüsselmanagements für den Zugriff auf die physische Ablage. Auf ähnliche Weise kann ein Zugriffsmanagement die unberechtigte Nutzung von Daten in einem elektronischen Informationssystem steuern. In diesem Fall werden Daten mittels elektronischer Schlüssel abgesichert und können nur durch Personen bearbeitet werden, die über eine entsprechende Berechtigung verfügen.

2. Rollen

Ab einer gewissen Anzahl von berechtigten Personen und verschiedenen Funktionen ist es angezeigt, diese nach Funktion zu Gruppen zusammenzufassen und jeder Gruppe eine Rolle, d.h. eine nach Funktion und Aufgaben geordnetes Bündel von Zugangsberechtigungen zuzuordnen.[101] Die Funktion von Rollen in einem Informationssystem besteht mithin in der Möglichkeit, Nutzer nach Funktionen bzw. gesetzlichen Aufgaben nach Rollen zu gruppie-

[99] Siehe dazu III.B.3.

[100] Siehe dazu IV.B.

[101] Kipker (FN 97), 28.

ren und die entsprechende standardisierte Zugriffsmatrix für die Datenbank zuzuweisen. Dadurch müssen Zugriffsrechte nicht individuell verteilt werden, was Zeit spart und Systemressourcen schont.

VIII. Ansätze für eine «best Practice»

A. Prüfung von Zugangsgesuchen

Aufgrund der bisherigen Ausführungen kann gesagt werden, dass die Einsichtnahme in Personendaten des Kindes durch die Eltern eine mehrfache rechtliche Prüfung erfordert.

- Erstens muss ermittelt werden, ob eine stellvertretende Einsichtnahme oder eine auf das Sorgerecht gestützte Einsichtnahme der Eltern in Personendaten des Kindes verlangt wird.
- Zweitens ist zu prüfen, ob der Gesuchsteller bzw. die Gesuchstellerin über eine genügende elterliche Sorge verfügt, um entweder stellvertretend für das Kind oder aber aus eigenem Recht den Zugang zu Personendaten des Kindes geltend zu machen.
- Drittens muss, soweit dies nach dem rechtlichen Massstab von Art. 11 Abs. 2 BV bzw. des Zivil- sowie Zivilprozessrechts sinnvoll erscheint, das Kind angehört werden. Dies entweder um dem Kind die Gelegenheit zu geben, die Bekanntgabe aufgrund höchstpersönlicher Rechte abzulehnen oder aber um zu ermitteln, ob seine Privatsphäre in einer Art und Weise betroffen ist, die eine Einschränkung des Zugangsrechts der Eltern erfordert.

Hierbei muss primär geprüft werden, ob das Kindswohl der Bekanntgabe der betreffenden Kindsdaten an die Eltern widerspricht. Dies wäre insbesondere von Bedeutung in Fällen, da ein Kind in Bezug auf den Gegenstand des Zugangsgesuchs eines Elternteils nicht urteilsfähig, und somit auch nicht zustimmungsfähig wäre, zugleich aber der Bekanntgabe dieser Information an den betreffenden Elternteil dem Kindswohl widerspricht.

B. Vorschläge für softwarebasierte Unterstützung zur Umsetzung von Datenschutzrechten

1. Ansätze zur Optimierung der Datenbearbeitung

Ausgangspunkt der Überlegungen zur datenschutzkonformen Ausgestaltung von Software ist der mittlerweile allgemein bekannte Slogan «code is law».[102] Damit ist nicht gemeint, dass Computercode das Recht ersetzt oder ersetzen soll – dazu fehlt grundsätzlich die rechtsstaatliche Legitimation.[103] Vielmehr formulierte Lessig damit eine Zusammenfassung seiner Beobachtung, dass viele Fragen der rechtlichen Regulierung von Prozessabläufen in Informationssystemen durch die eingesetzten Computerprogramme vorweggenommen werden.

Der Grund liegt darin, dass Code als Baustein der Systemarchitektur deterministisch auf die Funktionsweise eines Informationssystems wirkt und dadurch das Zustandekommen von computergestützten Entscheiden bzw. die Arbeitsweise von Computeranwendern entscheidend vorprägen kann. Die Programmierung von Informationssystemen und Datenbearbeitungsprogrammen definiert die Möglichkeiten von Nutzerinnen und Nutzern, im Rahmen der Systemnutzung Personendaten zu bearbeiten. Man spricht in diesem Zusammenhang von «affordances» (Möglichkeiten) und «constraints» (Beschränkungen) von Informationssystemen, wobei erstere die Möglichkeiten zur Datenbearbeitung definieren, welche die Nutzung des Systems eröffnet, und letztere die diesbezüglichen Einschränkungen.[104]

Die grundsätzliche Vorprägung der Bearbeitungsweise von Personendaten durch Computerapplikationen wurde bereits früh durch den sogenannten technischen Datenschutz thematisiert, wenn auch vorerst in der Form von Datensicherheitsvorgaben für Informationssysteme. Im Zuge der digitalen Entwicklung und im Hinblick auf den fundamentalen Wirkungszusammenhang zwischen Systemarchitektur und Datenbearbeitung, der durch «code is

---

[102] Lawrence Lessig, Code is Law, Basic Books, New York 2006.

[103] Danielle Keats Citron, Technological Due Process, Washington University Law Journal Vol. 85, 6/2008.

[104] Zu den Begriffen Woodrow Hartzog, Privacy's Blueprint, The Battle to Control the Design of New Technologies, Harvard University Press, Cambridge (MA)/London 2018, 31 f.

law» auf den Punkt gebracht wurde, entwickelte sich die Idee, die Anliegen des Datenschutzes bereits bei der Konzeption und Umsetzung von Informationssystemen einzubringen und in diese Systeme auf die Datenschutzziele auszurichten. Diese Vorgehensweise wird im schweizerischen Recht unter dem Stichwort Datenschutz durch Technik[105] bzw. «privacy by design» diskutiert.[106] Für die Schweiz werden mit Inkrafttreten des revidierten Datenschutzgesetzes des Bundes die Prinzipien Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen auf Bundesebene gesetzlich verankert werden.[107] Im Kanton Zürich ist der Grundsatz des Datenschutzes durch Technik bzw. *privacy by design* im Rahmen der Vorabkontrolle nach § 10 IDG ZH in Lehre und Praxis verankert.[108]

Für die Führung von Journalen bedeutet dies, dass die Architektur der eingesetzten Software sowie des zugrundeliegenden Informationssystems so zu strukturieren sind, dass sie die datenschutzkonforme Nutzung der darin gespeicherten Daten erleichtern und fördern. Dies gilt sinngemäss ebenso für traditionelle Papierakten.

Für die Umsetzung dieser Pflicht sind zwei Varianten denkbar. Zum einen können bestehende Systeme und oder Arbeitsabläufe entsprechend anders eingesetzt, zum anderen können sie in die entsprechende Richtung weiterentwickelt werden. Beide Varianten ermöglichen grundsätzlich eine datenschutzkonforme Bearbeitung von Journalen. Im Folgenden sollen nun einige Überlegungen zur weiteren Umsetzung von privacy by design für elektronische Journalsysteme angestellt werden.

2. Trennung von Journaldaten, Berichten und Notizen

Eine naheliegendste Lösung besteht darin, Journaldaten als Rohdaten zu behandeln und von den daraus erarbeiteten Berichten zu trennen. Dies erscheint insbesondere dort als sinnvoll, wo erfahrungsgemäss wenige Einsichtsgesu-

---

[105] So nun Art. 7 nDSG; vgl. den Schlussabstimmungstext in den Räten, abrufbar unter https://www.parlament.ch/centers/eparl/curia/2017/20170059/Schluzssabstimmungstext%203%20NS%20D.pdf (Abruf 01.07.2022).

[106] Glass (FN 36), 197 f.

[107] Vgl. Art. 7 nDSG; Botschaft E-DSG (FN 44), zu Art. 6, 7028 f.

[108] Siehe Blattmann, PraKom IDG ZH (FN 6), § 10 N 3.

che gestellt werden und diese einem berechenbaren Muster folgen, etwa die Einsicht in frühere Berichte durch ehemalige Bewohnerinnen und Bewohner.

Aus Praxisinterviews ging hervor, dass eine solche Trennung dazu führt, dass Einsichtsgesuche in der Regel auf einfache Weise beantwortet werden können. Insbesondere ehemalige Klientinnen und Klienten scheinen sich in der Regel mit der Einsicht in die Berichte zu begnügen, auch wenn ihnen eine weitergehende Einsicht in die Journaldaten angeboten wird.

Ein weiterer Vorteil dieses Vorgehens besteht darin, dass die Berichte auf eine Art und Weise verfasst werden können, welche die Persönlichkeit der Beteiligten schützt. Dies insbesondere deshalb, weil sich die Berichte auf die wesentlichen Züge der persönlichen Entwicklung konzentrieren, während die Journaldaten in der Regel eine vergleichsweise ungefilterte Dokumentation über das Leben der Betroffenen bilden.

Des Weiteren kann unter gewissen Voraussetzungen eine weitere Ablage geführt werden, welche der internen (administrativen) Kommunikation zwischen den Mitarbeitenden dient und die Möglichkeit bietet, kurzfristige persönliche Arbeitsnotizen anzulegen. Diese sind, soweit nur für die betreffende Person zugänglich, nicht Gegenstand der Einsichtsrechte des IDG ZH.[109]

Schliesslich ist zu beachten, dass eine Ablage, welche zur internen fachlichen und administrativen Kommunikation benutzt wird, eine vergleichsweise kurze Löschfrist vorsehen sollte. Das Gesetz verpflichtet dazu, Personendaten so bald wie möglich zu löschen, anonymisieren oder zumindest pseudonymisieren.[110] In Zusammenhang mit der internen Kommunikation zwischen Mitarbeitenden über Klientinnen und Klienten bedeutet dies, dass Informationen aus dieser Kommunikation, die als wichtig erachtet werden, im Journal zu vermerken sind. Die übrige Kommunikation wird danach nicht mehr benötigt und sollte innert kurzer Frist gelöscht werden.

---

[109] Beispielsweise eine persönliche Agenda, die nicht geteilt wird; vgl. Rudin, PraKom IDG ZH (FN 6), § 3 N 8; soweit solche Notizen geteilt werden, unterstehen sie jedoch dem Einsichtsrecht.

[110] Siehe dazu III.B.3.e.

3. Zuweisung von Rollen im Informationssystem

a. Aufteilung in Betreuungs- und Leitungsrollen

Hier zeigt sich nun deutlich die spezielle Lage von Wohnheimen zwischen staatlicher Aufgabenerfüllung und Familie. Die zur Erfüllung der Aufgaben gewählte Aufgabenteilung hat sich – ebenso wie die Aufgabenerfüllung selbst – primär am Kindeswohl auszurichten. Der quasi-familiäre Auftrag solcher Institutionen sowie die damit einhergehenden Strukturen legen dann auch eine weitgehende gemeinsame alltägliche Betreuung der Klientinnen und Klienten durch das Personal nahe, die nur in gewissen Fällen auf wenige Personen eingegrenzt wird.

Praxisinterviews ist zu entnehmen, dass oftmals mehr und persönlichere Daten mit den Klientinnen und Klienten besprochen werden, als dies in Familien üblich erscheint, insbesondere finden regelmässige Standort- und Entwicklungsgespräche statt. Aufgrund der besonderen Situation scheint es zudem sinnvoll, dass Mitarbeitende über eine Grundkenntnis hinsichtlich aktueller Vorkommnisse sowie des Befindens sämtlicher Klientinnen und Klienten verfügen, um diese nahtloser betreuen zu können. In Interviews wurde entsprechend deutlich, dass das Verhältnis zwischen den Institutionen und ihren Klientinnen und Klienten von Vertrauen geprägt sein muss, um die gesetzlich vorgesehenen Dienstleistungen erbringen zu können. Daraus ergebe sich nach den Aussagen der befragten Leiterinnen und Leiter insbesondere auch eine hohe gelebte Transparenz der Institution gegenüber ihren Klientinnen und Klienten bezüglich der bearbeiteten persönlichen Informationen und Daten.

Aus der beschriebenen Konstellation ergibt sich oftmals eine weitgehende Rollenteilung hinsichtlich der Betreuung der Klientinnen und Klienten, welche bloss in administrativer Hinsicht aufgebrochen wird und namentlich zwischen Mitarbeitenden und Leitungsfunktionen unterscheidet.

Diese «flache» Aufgabenteilung bringt es mit sich, dass viele Personen sich eine Rolle teilen und entsprechend Zugriff auf dieselben Kindesdaten haben. Dadurch wird ein gewisses Risiko geschaffen in Bezug auf den Missbrauch solcher Daten. Damit verbunden ist die Gefahr, im Falle einer Datenschutzverletzung die hierfür verantwortliche Person nicht identifizieren zu können. Als Massnahme zur Minderung dieses Risikos sollte daher darauf geachtet werden, dass die Bearbeitung von Daten in einem System nicht nur nach Rollen, sondern auch nach Personen dokumentiert wird.

b. Einsichtsrechte als eigene Rollenkonzepte

Einsichtsrechte begründen auf dieselbe Weise Zugriffsrechte auf Personendaten, wie dies die gesetzlichen Aufgaben tun, da sie indirekt eine Aufgabe der Behörde umschreiben, namentlich jene der Beantwortung von Gesuchen um Dateneinsicht. Der Unterschied liegt darin, dass der tatsächliche Zugriff nur mittelbar über die Einsicht gewährende Behörde erfolgen kann. Vom Standpunkt der Behörde aus betrachtet, stellt die Gewährung von Einsicht entsprechend eine eigene Aufgabe dar, welche indes auf Veranlassung von Dritten entsteht.

Im Ergebnis stellt ein Zugriff zur Gewährung von Dateneinsicht einen anderen Bearbeitungszweck dar als jener, zu dem die Daten ursprünglich erhoben wurden. Es erfolgt somit eine Zweckänderung,[111] die einer eigenen gesetzlichen Grundlage bedarf. Eine bloss mittelbare Rechtsgrundlage reicht hierzu nicht aus.[112] Zudem müssen die spezifischen datenschutzrechtlichen Bestimmungen zur Bekanntgabe von (besonderen) Personendaten in § 16 bzw. 17 IDG ZH beachtet werden.

Aufgrund dieses Wechsels in der Perspektive der Behörde, sowie der damit einhergehenden Änderung der gesetzlichen Grundlage für die Bearbeitung der Daten, erscheint es angezeigt, eine entsprechende, eigenständige Rolle zur Datenbearbeitung im System anzulegen. Dies ermöglicht es, die Aufarbeitung von Akten zwecks Einsichtsgewährung auf Personen zu beschränken, die hierzu befugt sind. Eine solche Einschränkung erscheint insbesondere dann sinnvoll, wenn Einsichtsgesuche Daten betreffen, die Informationen abbilden, die über mehrere Jahre hinweg gespeichert wurden oder aber Ereignisse betreffen, die mehrere Jahre zurück liegen. Da es sich hier um Daten handelt, die nicht mehr für die Erledigung der üblichen Aufgaben benötigt werden, sind die aktuellen Mitarbeitenden unter Umständen nicht mehr berechtigt, diese Daten ausserhalb von Einsichtnahmen zu bearbeiten.

---

[111] Vgl. Harb, PraKom IDG ZH (FN 6), § 9 N 12, wonach voraussetzungslose Bekanntgabepflichten sowie amtshilfeweise Bekanntgaben das Zweckänderungsverbot aushöhlten; im Umkehrschluss stellen sie demnach Zweckänderungen dar.

[112] Rudin, PraKom IDG ZH (FN 6), § 16 N 7; dies gilt für das Zürcher IDG, in anderen Kantonen kann die Rechtslage eine andere sein.

Die grundsätzliche Sensitivität des über längere Zeit erhobenen und strukturiert gespeicherten Bestandes an Journaldaten einer Person[113] bedeutet sodann, den Zugriff im Sinne des Zweckbindungsprinzips möglichst zu beschränken, und die Anzahl von Mitarbeitenden, die zur Bearbeitung zwecks Einsichtsgewährung berechtigt sind, möglichst klein zu halten. Hier kann es von Nutzen sein, die Einsichts- und korrespondierenden Bearbeitungsrechte an Datensätzen in einer Zugriffsmatrix abzubilden und einer spezifischen Rolle «Dateneinsicht» zuzuordnen. Die Zweckbindung wäre gewahrt, da nur auf jene Daten zugegriffen werden könnte, welche zum Zweck der Erledigung der Aufgabe «Gewährung von Einsicht in Personendaten» benötigt werden.

Wie die vorangehenden Überlegungen zeigen, müssten verschiedene, nach Art und Umfang der Einsichtsrechte differenzierte Rollen angelegt werden. Der Vorteil einer solchen Vorgehensweise ist jener, dass sie die bestehenden Funktionen des rollenbasierten Datenzugriffs nutzt und keine zusätzlichen Sonderfunktionen erfordert. Allerdings gilt hier umso mehr, dass eine solche aufwendige Rollenmatrix für ein Wohnheim nur ab einer gewissen Grösse Sinn macht.

[113] Siehe dazu IV.B.2.

Zwischen Autonomie und Angleichung

Eine Analyse zur Anwendung des neuen DSG im Lichte der DSGVO

Thomas Steiner*

Inhaltsübersicht

* Dieser Beitrag entstand auf Initiative und mit Unterstützung der ZHAW Zürcher Hochschule für Angewandte Wissenschaften.

I. Einleitung und Ausgangslage

A. Einleitung

National- und Ständerat haben am 25. September 2020 das neue Schweizer Bundesgesetz über den Datenschutz[1] (nDSG) verabschiedet. Das nDSG wird am 1. September 2023 in Kraft treten und ab dann gelten.[2]

Hauptziele[3] der Gesetzesrevision waren die Anpassung des bestehenden Bundesgesetzes über den Datenschutz (DSG)[4] an die Anforderungen des *revidierten Europarats-Übereinkommens*[5] *SEV 108*[6] und die Umsetzung der Schengen-relevanten *Richtlinie (EU) 2016/680*[7]. Zudem bezweckte die DSG-Revision eine Annäherung an die *EU-Datenschutz-Grundverordnung*

---

1 BBl 2020 7639.

2 Der Bundesrat hat am 31. August 2022 beschlossen, das nDSG per 1. September 2023 in Kraft zu setzen. Damit gewährte er Unternehmen tatsächlich eine Übergangsfrist von 12 Monaten. Das nDSG selbst sieht keine weitere Übergangsfrist vor. Das nDSG gilt daher ab Inkrafttreten. Namentlich für laufende Bearbeitungen und Verfahren bestehen Übergangsregeln (Art. 69–70).

3 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff., 6969–6970 (zit. Botschaft E-DSG).

4 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1).

5 Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Abgeschlossen in Strassburg am 10. Oktober 2018. (SEV 223; die konsolidierte Fassung nachstehend: revidiertes Europarats-Übereinkommen SEV 108).

6 Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108; SR 0.235.1).

7 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119, 4.05.2016, 89–131).

(DSGVO)[8]. Die Annäherung erachtete der Bundesrat (nebst den Anpassungen an das revidierte Übereinkommen SEV 108) als notwendig, damit die Europäische Kommission ihre Angemessenheitsentscheidung in Bezug auf das Datenschutzniveau der Schweiz aus dem Jahr 2000[9] bestätigen und auch künftig aufrechterhalten wird.[10]

B. Ausgangslage

Die Europäische Kommission überprüft ihre Angemessenheitsbeschlüsse regelmässig.[11] Im Januar 2017 ersuchte die Europäische Kommission die Schweiz, im Hinblick auf die Überprüfung des Beschlusses über die Angemessenheit des Datenschutzniveaus in der Schweiz einen Bericht zu erstellen. Der Bericht solle die datenschutzrechtliche Ausgangslage und die hauptsächlichen Gesetzesänderungen seit 2000 darlegen. Die Schweiz übermittelte den Bericht Ende 2017 nach Veröffentlichung des Entwurfs des revidierten DSG.[12]

Der Beitritt eines Drittlands zu multilateralen Übereinkünften über den Schutz von Personendaten ist eines der Kriterien, welche die Europäische Kommission bei der Beurteilung der Angemessenheit eines von einem Drittstatt gebotenen Schutzniveaus zu berücksichtigen hat (Art. 45 Abs. 2 lit. c DSGVO). Zu solchen multilateralen Übereinkünften gehören gemäss Erwägungsgrund 105 der DSGVO ausdrücklich auch das Übereinkommen SEV 108 sowie das dazugehörende Zusatzprotokoll.[13]

---

8 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; ABl. L 119, 04.05.2016, 1–88).

9 Entscheidung der Kommission vom 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl. L 215, 25.08.2000, 1 (zit. EU-Angemessenheitsbeschluss 2000).

10 Botschaft E-DSG (FN 3), 6943 f. und 6970.

11 Gemäss Art. 45 Abs. 3 DSGVO mindestens alle vier Jahre.

12 Botschaft E-DSG (FN 3), 6965.

13 Zusatzprotokoll zum Übereinkommen vom 23. Mai 2001 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108) bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (SEV 181) (zit. Zusatzprotokoll).

Der Bundesrat erachtete die *Ratifikation und Umsetzung des revidierten Übereinkommens SEV 108* daher zurecht als zentrale Voraussetzungen dafür, dass die Europäische Kommission ihre Angemessenheitsentscheidung bestätigen wird.[14] Hingegen ergibt sich aus Art. 45 Abs. 2 DSGVO nicht, dass für den Erlass oder die Bestätigung des Angemessenheitsbeschlusses darüber hinaus eine *Annäherung* des DSG an die DSGVO notwendig wäre.

Angemessenheitsentscheidungen können indes auch zum Spielball der Politik werden[15] und der EU-Angemessenheitsbeschluss zum Datenschutzniveau der Schweiz ist für die Schweizer Wirtschaft sehr bedeutsam. Insofern ist es (auch) Ausdruck einer *politischen* Risikoeinschätzung und einer dem Parlament empfohlenen politischen Entscheidung, wenn der Bundesrat in der Botschaft E-DSG ausführt, die Schweiz tue «gut daran, ihre Gesetzgebung an die europäischen Anforderungen anzupassen».[16]

Thema dieses Beitrages ist die Frage, ob und inwiefern das Parlament mit Erlass des nDSG der Empfehlung des Bundesrats gefolgt ist, das DSG – allenfalls in unterschiedlicher Art und Intensität – an das EU-Datenschutzrecht anzupassen. Der zu eruierende Wille des Gesetzgebers ist entscheidend für die Beantwortung der Forschungsfragen, denen sich dieser Beitrag widmet.

C. Forschungsfragen

Der Beitrag untersucht die folgenden Forschungsfragen:

i. Welche Art der Anpassung des DSG an die DSGVO hat der Gesetzgeber gewollt? Welche Bestimmungen sind eher von der DSGVO, welche von der Richtline (EU) 2016/680 oder vom revidierten Übereinkommen SEV 108 geprägt? Hat der Schweizer Gesetzgeber zumindest einzelne DSGVO-Bestimmungen übernommen? Wo ist der Schweizer Gesetzgeber allenfalls bewusst von der DSGVO abgewichen, um eine autonom schweizerische Lösung zu wählen?

---

[14] Botschaft E-DSG (FN 3), 6943 f.

[15] Ein Beispiel hierfür ist die Nichtverlängerung des Beschlusses der Europäische Kommission über die Börsenäquivalenz der Schweiz im Dezember 2017.

[16] Botschaft E-DSG (FN 3), 6998.

ii. Was folgt daraus für die Anwendung des nDSG? Inwiefern dürfen oder müssen rechtsanwendende Schweizer Behörden bei der Auslegung des nDSG die DSGVO und/oder die Praxis des EuGH oder der Datenschutzaufsichtsbehörden und Gerichte in EU-Mitgliedsstaaten berücksichtigen?

Zur Beantwortung dieser Fragen, entwickelt dieser Beitrag zunächst Entscheidungsgrundlagen (Teil II) und zeigt verschiedene Formen der Rezeption von EU-Recht in der Schweizer Rechtssetzung (Teil III) sowie ihre Bedeutung für die Rechtsanwendung (Teil IV) auf. Basierend darauf analysiert dieser Beitrag die Materialien der Revision des DSG daraufhin, ob und – wenn ja – in welcher Art und Intensität der Gesetzgeber sich bei der Ausgestaltung des nDSG an der DSGVO orientiert hat (Teil V), und zwar im Allgemeinen (Kapitel V.A) wie auch in Bezug auf einzelne nDSG-Bestimmungen (Kapitel V.B).

D. Abgrenzung von freiwilliger Ausrichtung am DSGVO-Standard

Der Beitrag eruiert die Möglichkeiten und Pflichten der rechtsanwendenden Schweizer Behörden bei der Auslegung des nDSG im Lichte der DSGVO. Der entsprechende Fragenkomplex ist **abzugrenzen** von einer *freiwilligen Ausrichtung* der Datenschutz-Compliance am (meist höheren) DSGVO-*Standard*.

Dieser Beitrag behandelt ausdrücklich *nicht* die Frage, ob, inwiefern und gegebenenfalls für welche Arten von Schweizer Unternehmen eine Ausrichtung am DSGVO-Standard Sinn ergibt. Auch thematisiert der Beitrag nicht Fälle, in denen DSGVO-Bestimmungen basierend auf Art. 3 Abs. 2 DSGVO direkt für Datenbearbeitungstätigkeiten von Schweizer Unternehmen gelten.

Rechtsanwendende Behörden in der Schweiz haben das Schweizer Datenschutzrecht anzuwenden. Für Unternehmen und Bundesorgane gilt das DSG und neu das nDSG. Unterschiede in der Praxis zur DSGVO sind hinzunehmen, soweit der Schweizer Gesetzgeber nicht eine grösstmögliche Parallelität von nDSG und DSGVO erwirken wollte. In der Rechtsanwendung – in der Schweizer Behörden- und Gerichtspraxis – kommt es also auf den **Willen des Gesetzgebers** an. Diesen zu eruieren ist Thema dieses Beitrags.

II. Grundlagen

A. Einleitung

Für die Beantwortung der gestellten Fragen ist entscheidend, welche Art der Rezeption von EU-Recht (DSGVO) der Schweizer Gesetzgeber wollte und bezweckte. Im Folgenden zeigt dieser Beitrag verschiedene Arten der Rezeption von EU-Recht auf. Daraus entsteht ein Prüfraster für die Beurteilung, ob und – wenn ja – in Bezug auf welche Bestimmungen des nDSG eine DSGVO-konforme Auslegung und Anwendung mit Schweizer Recht vereinbar oder sogar geboten ist.

B. Europafähige Ausgestaltung Schweizer Rechts

1. Prüfung von Gesetzgebungsvorhaben auf «Europafähigkeit»

Botschaften des Bundesrats zu Gesetzgebungsvorhaben in Bereichen mit grenzüberschreitenden Auswirkungen enthalten seit 1988 ein «Europakapitel».[17] Dieses soll Aufschluss darüber geben, wieweit das geplante Gesetzgebungsvorhaben mit europäischem Recht vereinbar ist. Das *Streben nach Parallelität der Rechtsordnungen* soll in Bereichen von grenzüberschreitender Bedeutung die Vereinbarkeit mit EU-Recht sichern und damit die *Wettbewerbsfähigkeit* der Schweizer Unternehmen stärken.[18]

Der Bundesrat ging davon aus, dass er die «Europafähigkeit» und somit die Wettbewerbsfähigkeit auf dem Binnenmarkt der damaligen Europäischen Gemeinschaft (EG) stärken kann, wenn die Rechtsvorschriften in Bereichen mit grenzüberschreitender Bedeutung im Schweizer Recht und dem Recht der EG derart parallel ausgestaltet sind, dass sie die EG und die EG-Mitgliedsstaaten *als gleichwertig anerkennen*. Zudem wollte der Bundesrat damit für alle integrationspolitischen Optionen (EWR- oder EG-Beitritt oder

[17] Vgl. Bericht des Bundesrats vom 24. August 1988 über die Stellung der Schweiz im europäischen Integrationsprozess, BBl 1988 III 249, 380; (zit. Integrationsbericht 1988).

[18] Integrationsbericht 1988 (FN 17), 380.

bilaterale Abkommen) vorbereitet sein.[19] Ziel müsse sein, in diesen Bereichen «eine *grösstmögliche Vereinbarkeit [der Schweizer] Rechtsvorschriften mit denjenigen unserer europäischen Partner*» herzustellen.[20] Hierfür sei es nicht notwendig, EG-Recht «automatisch nachzuvollziehen»[21]. Stattdessen gelte es zu verhindern, dass die Schweiz «ungewollt und unnötigerweise» neue Unterschiede zwischen den Rechtsvorschriften schaffe, die eine gegenseitige Anerkennung der Rechtsvorschriften behindern würden.[22]

2. Faktische Begründungspflicht bei abweichenden Regelungen

Seit Dezember 2003 ist der Bundesrat auch gesetzlich dazu verpflichtet, in Botschaften zu Erlassentwürfen «das Verhältnis zum europäischen Recht» zu erläutern (Art. 141 Abs. 2 lit. a ParlG[23]). Von Interesse ist dabei das EU-Recht.[24] Diese Pflicht gilt, soweit der Bundesrat substanzielle Angaben zur Europafähigkeit des Gesetzgebungsvorhabens machen kann (Art. 141 Abs. 2 ParlG). Hingegen beschränkt sich die Pflicht nicht mehr (wie noch gemäss Integrationsbericht 1988) auf Bereiche mit grenzüberschreitender Bedeutung.[25]

Daraus leitet die Bundeskanzlei in ihrem Botschaftsleitfaden eine Begründungspflicht für den Fall ab, dass die Schweizer Regelung von der europäischen Regelung abweicht.[26] Damit soll der Bundesrat das Parlament in die Lage versetzen, Unterschiede zum (für die Schweiz in der Regel unverbind-

---

[19] Zu diesem doppelten Zweck der Politik der Europaverträglichkeit: Thomas Cottier et al., Die Rechtsbeziehungen der Schweizer und der Europäischen Union Bern 2014, S. 134 N 213.

[20] Integrationsbericht 1988 (FN 17), 380.

[21] Integrationsbericht 1988 (FN 17), 380.

[22] Integrationsbericht 1988 (FN 17), 380.

[23] Bundesgesetz vom 13. Dezember 2002 über die Bundesversammlung (Parlamentsgesetz, ParlG; SR 171.10).

[24] Parlamentarische Initiative – Parlamentsgesetz (ParlG) – Bericht der SPK-N vom 1. März 2001, BBl 2001 3467, 3593.

[25] Vgl. zum Ganzen: Andreas Heinemann, Rechtliche Transplantate zwischen Europäischer Union und der Schweiz, Sonderdruck aus: Luks Fahrländer et al. (Hrsg.), Europäisierung der schweizerischen Rechtsordnung, Zürich 2013, 3–58, 20.

[26] Bundeskanzlei, Botschaftsleitfaden. Leitfaden zum Verfassen von Botschaften des Bundesrates, Stand August 2020, 35.

lichen) EU-Recht zu erkennen und abweichende Regelungen bewusst (nicht unbeabsichtigt) zu wählen.[27]

III. Formen der Rezeption von EU-Recht

A. Einleitung

Der Schweizer Gesetzgeber bedient sich verschiedener Formen der Europäisierung des Schweizer Rechts. Sie reichen von der Berücksichtigung von EU-Recht als Inspiration (*Rechtsvergleichung*) über die Schaffung von Gleichwertigkeit (*Äquivalenz*) bis zur mehr oder weniger unveränderten Übernahme von EU-Recht (*autonomer Nachvollzug*).

Die Grenzen zwischen den verschiedenen Formen der Rezeption sind fliessend. Namentlich der Begriff des autonomen Nachvollzugs wird in der Lehre teils enger, teils weiter gefasst.[28] Den Formen der Rezeption gemeinsam ist, dass das Schweizer Recht in einer Form an EU-Standards und -Regelungen *angepasst* wird oder sich daran ausrichtet – und zwar freiwillig, ohne dass die Schweiz dazu staatsvertraglich verpflichtet wäre. Zusammengefasst und vereinfacht wird diese Art der Europäisierung des Schweizer Rechts als *autonome Anpassung*[29] bezeichnet.

Ein Sonderfall der autonomen Anpassung war die Anpassung von Schweizer Recht im Rahmen des sog. *Swisslex*-Pakets. Die Anpassungen erfolgten im Nachgang zur Ablehnung des Schweizer EWR-Beitritts in der Volksabstimmung vom 6. Dezember 1992. Ursprünglich hatte der Gesetzgeber im Hinblick auf die Übernahme des *Acquis Communitaire* Anpassungen von insgesamt 61 Gesetzen vorbereitet (sog. *Eurolex*-Vorlage).

Einige ausgewählte Vorlagen nahm der Bundesrat im Rahmen eines Folgeprogramms (*Swisslex*-Paket) wieder auf. Ähnlich wie im Integrationsbericht 1988 führte der Bundesrat in der Botschaft zum *Swisslex*-Paket aus, die Herstellung

---

[27] Martin Philipp Wyss, Europakompatibilität und Gesetzgebungserfahren im Bund, in: AJP 2007, 717, 718.

[28] Vgl. nachstehend III.B.

[29] Cottier et al. (FN 19), S. 139 N 218; Heinemann (FN 25), 18 ff.

von «Kompatibilität» des Schweizer Rechts mit europäischem Recht stärke den wirtschaftlichen Wettbewerb u.a. durch Teilnahme am EG-Binnenmarkt (sowie durch angestrebte Liberalisierungen) und die Wahrung aller Optionen für eine europäische Integration der Schweiz (Beitritt oder bilaterale Abkommen).[30] Das *Swisslex*-Paket beinhaltete 27 Gesetzesrevisionen auf Bundesebene. Bedeutend waren insbesondere die Änderung von Art. 40a–40g OR (Widerspruchsrecht) und Art. 333 OR (Übergang des Arbeitsverhältnisses bei Betriebsübergängen).[31]

[30] Botschaft des Bundesrats vom 24. Februar 1993 über das Folgeprogramm nach der Ablehnung des EWR-Abkommens, BBl 1993 I 805 (zit. Botschaft Swisslex-Paket), 810; vgl. Bundesrat, Schweiz – Europäische Union. Integrationsbericht 1999 vom 3. Februar 1999, BBl 1999 IV 3935, 4104 (zit. Integrationsbericht 1999).

[31] Botschaft Swisslex-Paket (FN 30), 805 f. – Änderung des Bundesgesetzes über die Sicherheit von technischen Einrichtungen und Geräten, Änderung des Tierseuchengesetzes, Änderung des UVG, Änderung des Bundesgesetzes über die Familienzulagen in der Landwirtschaft, Änderung des SVG, Änderung des Eisenbahngesetzes, Änderung des Luftfahrtgesetzes, Bundesgesetz über die Personenbeförderung und den Zugang zu Berufen des Strassentransportunternehmers, Änderung des Bundesgesetzes über Radio und Fernsehen, Bundesgesetz über den Konsumkredit, Änderung des Bundesgesetzes über den unlauteren Wettbewerb, Bundesgesetz über Information der Arbeitnehmer in Betrieben (Mitwirkungsgesetz), Änderung des Arbeitsgesetzes, Änderung des Zollgesetzes, Änderung des Bundesgesetzes über die Ein- und Ausfuhr von Erzeugnissen aus Landwirtschaftsprodukten, Änderung des Bundesgesetzes über den Versicherungsvertrag, Änderung des Bundesgesetzes betreffend die Aufsicht über die privaten Versicherungseinrichtungen, Änderung des Bundesgesetzes über die Kautionen der ausländischen Versicherungsgesellschaften (Kautionsgesetz), Änderung des Bundesgesetzes über die Sicherstellung von Ansprächen aus Lebensversicherungen inländischer Lebensversicherungsgesellschaften, Bundesgesetz über die direkte Lebensversicherung (Lebensversicherungsgesetz), Änderung des Bundesgesetzes über die Direktversicherung mit Ausnahme der Lebensversicherung, Änderung des Bundesgesetzes über die Banken und Sparkassen, Änderung der Artikel 40b–40e des Obligationenrechts (Widerrufsrecht), Änderung des Zehnten Titels des Obligationenrechts (Der Arbeitsvertrag – Art. 333 OR), Produktehaftpflichtgesetz, Änderung des Bundesgesetzes über Messwesen, Bundesgesetz über Pauschalreisen.

Mit dem Abschluss der Bilateralen I und der Bilateralen II kamen Anpassungen von insgesamt weiteren 34 Gesetzen hinzu[32] – darunter die Änderungen im Rahmen der Assoziierung an Schengen und Dublin.[33] Gerade die Pflicht, die Weiterentwicklung des Schengen-Besitzstands im Schweizer Recht umzusetzen, prägt das Schweizer Recht – darunter das *Datenschutzrecht von Bund und Kantonen* – nachhaltig.[34]

Auch in Bereichen, in denen die Schweiz nicht zur Übernahme von EU-Recht verpflichtet ist, rezipiert die Schweiz heute regelmässig in der einen oder anderen Form EU-Recht. Solche *autonomen Anpassungen* (in der Form eines

---

[32] Botschaft des Bundesrats vom 23. Juni 1999 zur Genehmigung der sektoriellen Abkommen zwischen der Schweiz und der EG, BBl 1999 6128 (zit. Botschaft Bilaterale I), 6134–6135 – Bundesgesetz über Lebensmittel und Gebrauchsgegenstände (LMG), Änderung des Strassenverkehrsgesetzes (SVG), Änderung des Personenbeförderungsgesetzes (PBG), Änderung des Bundesgesetzes über Aufenthalt und Niederlassung der Ausländer (ANAG), Änderung des Bundesgesetzes über den Erwerb von Grundstücken durch Personen im Ausland (Lex Koller), Änderung des AHVG, Änderung des IVG, Änderung des ELG, Änderung des BVG, Änderung des KVG, Änderung des FZG, Änderung des UVG, Änderung des FLG, Änderung des Arbeitslosengesetzes, Änderung des LWG; Bundesgesetz zur Verlagerung von alpenquerendem Güterverkehr auf die Schiene, Bundesgesetz über die minimalen Arbeits- und Lohnbedingungen für in die Schweiz entsandte Arbeitnehmerinnen und Arbeitnehmer und flankierende Massnahmen: Änderung des IPRG, des OR und des AGAV; Botschaft des Bundesrats vom 1. Oktober 2004 zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II»), BBl 2004 5965 (zit. Botschaft Bilaterale II), 6233–6234 – Anpassung des RTVG, ANAG, AsylG, StGB, Verantwortlichkeitsgesetzes, Waffengesetzes, StHG, DBG, BetmG und des Zinsbesteuerungsgesetzes.

[33] Im Rahmen statischer bilateraler Abkommen zwischen der Schweiz und der EU ist die Schweiz nicht verpflichtet, EU-Recht automatisch zu übernehmen (Matthias Oesch, Die bilateralen Abkommen Schweiz – EU und die Übernahme von EU-Recht, in: AJP 2017, 638, 639). Bei solcher Rezeption von EU-Recht handelt es sich nicht um autonomen Nachvollzug. Das Abkommen zu Schengen-Dublin unterscheidet sich in diesem Punkt. Es verpflichtet die Schweiz, Schengen-relevante Rechtsakte dynamisch zu übernehmen (Oesch a.a.O. 642).

[34] Matthias Oesch, Die Europäisierung des schweizerischen Rechts, in: Thomas Cottier (Hrsg.), Die Europakompatibilität des schweizerischen Wirtschaftsrechts: Konvergenz und Divergenz, Basel 2012, 13–39, 18.

autonomen Nachvollzugs oder einer autonomen Angleichung an EU-Recht) sind mittlerweile zum Regelfall geworden.[35]

B. Autonomer Nachvollzug

Der *autonome Nachvollzug* ist die weitestgehende Form der Rezeption von EU-Recht im Schweizer Recht. In seiner Reinform bedeutet der autonome Nachvollzug die *integrale und vorbehaltslose Übernahme* von Bestimmungen des EU-Rechts.[36] Entsprechend verwenden einige Autoren den Begriff des autonomen Nachvollzugs nur für jene Form der Rezeption, in denen die Schweiz EU-Recht mehr oder weniger unverändert übernimmt.[37] Andere Autoren erfassen unter dem Begriff des autonomen Nachvollzugs auch die *Angleichung* an EU-Regelungen durch Erlass ähnlicher Normen mit gleicher Wirkung.[38]

Für die Frage der Berücksichtigung der Praxis zur DSGVO in der Anwendung des Schweizer nDSG ist entscheidend, ob der Schweizer Gesetzgeber die DSGVO oder einzelne ihrer Bestimmungen *integral und vorbehaltlos übernehmen wollte* (**autonomer Nachvollzug**), oder aber die DSGVO nur teilweise zum Modell nahm und im Übrigen *bewusst eine autonome, aber gleichwertige*

---

[35] Matthias Oesch, Europarecht Band I, 2. A., Bern 2019, § 32 Autonomer Nachvollzug, S. 522 N 942. Die folgenden Erlasse des Bundes im Bereich des Wirtschaftsrechts (wobei dies keine abschliessende Auflistung ist) enthalten zumindest in Teilen *autonome Anpassungen* an EU-Recht, d.h. Anpassungen, welche die Schweiz ohne Rechtspflicht vorgenommen hat (vgl. die Zusammenstellung bei Oesch, a.a.O., N 941): Produktehaftpflichtgesetz (PrHG; SR 221.112.944), Bundesgesetz über Pauschalreisen (SR 944.3), Obligationenrecht (OR; SR 220), Konsumkreditgesetz (KKG; SR 221.214), Bundesgesetz über die technischen Handelshemmnisse (THG; SR 946.51), Kartellgesetz (KG; SR 251), Anwaltsgesetz (BGFA; SR 935.61), Heilmittelgesetz (HMG; SR 812.21), Luftfahrtgesetz (LFG; SR 748.0), Gleichstellungsgesetz (GlG; SR 151.1), Fernmeldegesetz (FMG; SR 784.10), Nationalbankgesetz (NBG; SR 951.11), Fusionsgesetz (FusG; SR 221.301), Mehrwertsteuergesetz (MWSTG; SR 641.20), Produktesicherheitsgesetz (PrSG; SR 930.11), Kollektivanlagengesetz (KAG; SR 951.31), Gentechnikgesetz (GTG; SR 814.91), Patentgesetz (PatG; SR 232.14), Urheberrechtsgesetz (URG; SR 231.1), Lebensmittelgesetz (LMG; SR 817.0), Finanzmarktinfrastrukturgesetz (FinfraG; SR 958.1), Finanzdienstleistungsgesetz (FIDLEG; SR 950.1), Finanzinstitutsgesetz (FINIG; SR 954.1), nDSG.

[36] Vgl. Ernst A. Kramer, Juristische Methodenlehre, 6. A., Bern 2019, 353.

[37] Heinemann (FN 25), 18.

[38] Monique Sturny, Der Einfluss des EU-Rechts auf das schweizerische Kartellrecht, Bern 2014, 5; Oesch (FN 35), S. 520 N 939.

schweizerische Lösung geschaffen hat (**Angleichung/Äquivalenz**).[39] Deshalb unterscheidet der vorliegende Beitrag den autonomen Nachvollzug im engeren Sinn von der *Angleichung bzw. Äquivalenzmethode* in der Rechtsetzung.

C. Äquivalenzmethode – Angleichung – Gleichwertigkeit

1. Begriffsklärung und Regulierungsziel

Namentlich in den Bereichen des Finanzmarktrechts[40] und des Datenschutzrechts ergibt sich für die Schweiz ein *faktischer* Zwang, Äquivalenz zwischen Schweizer Recht und EU-Recht herzustellen.[41] Äquivalenz geht etymologisch auf die lateinischen Worte *aequus* («gleich») und *valere* («wert sein») zurück. Mithin bedeutet Äquivalenz Gleichwertigkeit. Die Herstellung von Gleichwertigkeit entspricht in diesem Bereich regelmässig einem gegenseitigen Interesse von Handelspartnern:

– Handelspartner möchten den Kundenschutz auch bei grenzüberschreitender Erbringung von Finanzdienstleistungen durch ausländische Anbieter für inländische Kunden sicherstellen.[42]

– Handelspartner möchten durch die Schaffung gleicher Bedingungen für inländische und ausländische Anbieter von Finanzdienstleistungen Wettbewerbsverzerrungen zwischen den Anbietern vermeiden.[43]

– Handelspartner möchten ihren Unternehmen die Bekanntgabe von Personendaten ins Ausland und somit den Zugang zu ausländischen Märkten erleichtern; gleichzeitig aber sicherstellen, dass die Persönlichkeit ihrer Bürgerinnen und Bürger auch dann geschützt ist, wenn deren Personendaten ins Ausland übermittelt und dort bearbeitet werden.[44]

---

[39] Vgl. Kramer (FN 36), 353 f.

[40] Dazu: Rolf H. Weber/Rolf Sethe, Äquivalenz als Regelungskriterium im Finanzmarktrecht, in: SJZ 110/2014, 569.

[41] Oesch (FN 35), S. 521 N 941.

[42] Bundesrat, Bericht zur Finanzmarktpolitik des Bundes, 19.12.2012, 37, abrufbar: https://www.newsd.admin.ch/newsd/message/attachments/35762.pdf (Abruf: 12.10.2022; zit. Bericht zur Finanzmarktpolitik).

[43] Bericht zur Finanzmarktpolitik (FN 42), 37.

[44] Botschaft E-DSG (FN 3), 6995.

Staaten machen den Marktzutritt ausländischer Anbieter deshalb regelmässig davon abhängig, dass die Anbieter im Heimatland äquivalenter bzw. gleichwertiger Regulierung unterliegen, wie sie auf dem einheimischen geographischen Markt gelten.[45] Dies wiederum erzeugt für die jeweiligen Gesetzgeber einen *faktischen Druck*, eine mit der Regulierung in den Staaten der wichtigsten Handelspartner gleichwertige oder zumindest vergleichbare Regulierung zu schaffen. Entsprechend ist die Gleichwertigkeitsanerkennung seitens der Europäischen Kommission in den Bereichen Finanzmarktregulierung und Datenschutz sowie in weiteren Bereichen mit sog. *Drittstaatenregime* eine Voraussetzung für den Zugang von Schweizer Unternehmen zum EU-Binnenmarkt.[46]

2. Gleichwertigkeitsbeschlüsse der Europäischen Kommission

Die Europäische Union verpflichtet ihre Handelspartner in Bereichen mit Drittstaatenregime nicht rechtlich zur Übernahme von EU-Recht. Bei den Drittstaatenregimen handelt es sich vielmehr um *einseitige Mechanismen*, mit denen die EU den Zugang zum EU-Binnenmarkt für Drittstaaten *ausserhalb gegenseitiger staatsvertraglicher Pflichten* reguliert.[47]

Das Konzept der Gleichwertigkeit oder Angemessenheit spielt dabei eine entscheidende Rolle.[48] Die Europäische Kommission befindet einseitig[49] *nach im EU-Recht verankerten Kriterien und nach eigenem Ermessen* über die Anerkennung der Gleichwertigkeit der Rechtsordnung, die im Drittstaat im

---

[45] Vgl. Weber/Sethe (FN 40), 572, zum Beispiel der Finanzmarktregulierung.

[46] Jacques Beglinger/Christa Tobler, Gleichwertigkeit, Angemessenheit, Äquivalenz, Adäquanz, in: Astrid Epiney/Petru Emanuel Zlătescu (Hrsg.), Schweizerisches Jahrbuch für Europarecht 2019/2020, 547–570, 554–559 (zur Börsenäquivalenz) und 559–565 (zur Datenschutzäquivalenz).

[47] Beglinger/Tobler (FN 46), 566 und 568.

[48] Beglinger/Tobler (FN 46), 553.

[49] Wobei Drittstaaten umgekehrt ähnliche Marktzugangsregimes aufstellen (z.B. Börsenäquivalenz und Datenschutzäquivalenz aus Sicht der Schweiz).

jeweiligen Bereich – Finanzsektor[50] oder Schutz personenbezogener Daten[51] – gilt und überprüft dies regelmässig. Die Kommission ist überdies gewillt, die Erteilung oder Bestätigung von Angemessenheitsbeschlüssen für politische Zwecke einzusetzen.[52]

Bei der Herstellung der Gleichwertigkeit bzw. Angemessenheit oder Äquivalenz im Rahmen von Drittstaatenregimes – also ausserhalb staatsvertraglicher Regelungen – geht es regelmässig um eine *Angleichung* des Rechts der Handelspartner an das EU-Recht – *nicht um eine Übernahme* von EU-Recht. Das Recht des Drittstaats muss nicht die EU-rechtlichen Bestimmungen mehr oder weniger unverändert übernehmen. Es genügt, wenn die Vorschriften und die Durchsetzungsmechanismen im Recht des Drittstaats die *Kernanforderungen*[53] der EU-rechtlichen Vorschriften erfüllen und insgesamt «der Sache nach»[54] ein *gleichwertiges* Schutzniveau bieten.

---

50 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, die Europäische Zentralbank, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Gleichwertigkeit im Bereich der Finanzdienstleistungen, COM(2019) 349 final, 29.07.2019, 4 und 9.

51 Art. 45 DSGVO (Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses); Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen, ABl. 2019 L 76, 1; EuGH, *Maximilian Schrems gegen Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650, 06.10.2015 (zit. Schrems I), N 73 f.; EuGH, Data Protection Commissioner gegen Facebook Ireland Limited und Maximilian Schrems, C-311/18, ECLI:EU:C:2020:559, 16.07.2020 (zit. Schrems II), N 162.

52 Vgl. die Nichtverlängerung des Beschlusses der Europäische Kommission über die Börsenäquivalenz der Schweiz im Dezember 2017.

53 Beglinger/Tobler (FN 46), 567.

54 EuGH, Schrems I (FN 51), N 73 («[…] nicht verlangt werden kann, dass ein Drittland ein dem in der Unionsrechtsordnung garantiertes identisches Schutzniveau gewährleistet.») und N 74 («der Sache nach gleichwertig[es]» Schutzniveau); bestätigt in Schrems II (FN 51), N 162 («der Sache nach gleichwertig[es]» Schutzniveau).

IV. Bedeutung der Rezeption für die Rechtsanwendung

A. Generelles

Die vom Schweizer Gesetzgeber gewählte Form der Rezeption von EU-Recht ist entscheidend für die Frage, welche Bedeutung die Praxis zum rezipierten EU-Recht für die Anwendung des Schweizer Rechts hat. Im Wesentlichen geht es um die Frage, *ob der Gesetzgeber autonomes Schweizer Recht schafft, das autonom ausgelegt werden soll, oder aber ob die Europakompatibilität auch im Rahmen der Rechtsfortbildung durch Gerichte und Behörden sichergestellt werden soll*.

Zur Beantwortung dieser Frage bei der Auslegung von an EU-Recht angeglichenem Schweizer Recht sind namentlich die folgenden drei Leiturteile des Bundesgerichts instruktiv:

– BGE 129 III 335 (Auslegung von Art. 333 Abs. 3 OR – Solidarhaftung von Veräusserer und Erwerber für Forderung des Arbeitnehmers bei Übergang des Arbeitsverhältnisses)
– BGE 137 II 199 (Auslegung von Art. 7 Abs. 2 lit. c KG – Erzwingung unangemessener Preise oder sonstiger unangemessener Geschäftsbedingungen)
– BGE 139 I 72 (Auslegung von Art. 7 Abs. 2 lit. b KG – Bestimmbarkeit)

B. BGE 129 III 335 (Arbeitsrecht)

1. Ausgangslage

Das Urteil BGE 129 III 335 betraf die Auslegung von Art. 333 Abs. 3 OR (solidarische Haftung des bisherigen Arbeitgebers und des Erwerbers für Forderungen des Arbeitnehmers bei Betriebsübergängen). Zu prüfen war, ob die Vorinstanz korrekt entschieden hat, Art. 333 Abs. 3 OR im Konkursfall nicht anzuwenden.[55] Gemäss Bundesgericht äussern sich weder der Wortlaut (grammatikalisches Auslegungselement) der Bestimmung noch die Materia-

[55] BGE 129 III 335 E. 3.

lien (historisches Auslegungselement) explizit zur Frage, ob der Erwerber für vor Betriebsübernahme fällig gewordene Lohnforderungen haftet.

Das Bundesgericht legte die Bestimmung nach ihrem Sinn und Zweck (teleologisches Auslegungselement) sowie gemäss ihrer systematischen Stellung im Zusammenhang mit dem Konkursrecht (systematisches Auslegungselement) aus.[56] Es kam zum Ergebnis, dass Art. 333 Abs. 3 OR im Konkursfall nicht anwendbar ist.

2. Europarechtskonforme Auslegung von Art. 333 Abs. 3 OR

Ergänzend zur klassischen Auslegung legte das Bundesgericht Art. 333 Abs. 3 OR europarechtskonform aus. Es kam dabei zum selben Ergebnis wie bei der Auslegung nach Sinn, Zweck und Systematik.

Der Schweizer Gesetzgeber hatte Art. 333 Abs. 1 OR im Rahmen der Revision vom 17. Dezember 1993 als Bestandteil des Swisslex-Pakets so abgeändert, dass Arbeitsverhältnisse, die im Zeitpunkt der Übertragung des Betriebs auf einen Dritten bestehen, von Gesetzes wegen auf den Erwerber übergehen.[57] Insoweit lag gemäss Bundesgericht eine Anpassung von Art. 333 OR an die Richtlinie 77/187/EWR[58] in der Form eines *autonomen Nachvollzugs* des europäischen Rechts vor.[59]

Gemäss Bundesgericht ist autonom nachvollzogenes Schweizer Recht mit dem europäischen Recht harmonisiertes Recht. Als solches sei es «im Zweifel europarechtskonform auszulegen».[60] In der Richtlinie 77/157/EWR blieb indes ungeregelt, ob sie im Falle des Konkurses anwendbar sei. Der Europäische Gerichtshof (EuGH) entschied, dass die Mitgliedsstaaten die Frage autonom

---

[56] BGE 129 III 335 E. 5.

[57] Botschaft Swisslex-Paket (FN 30), 880 f.

[58] Richtlinie 77/187/EWG des Rates vom 14. Februar 1977 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Wahrung von Ansprüchen der Arbeitnehmer beim Übergang von Unternehmen, Betrieben oder Betriebsteilen, ABl. L 061, 05.03.1977 (nicht mehr in Kraft).

[59] BGE 129 III 335 E. 6 (mit Hinweis auf E. 5.1).

[60] BGE 129 III 335 E. 6.

regeln dürfen.[61] Diese Rechtsprechung kodifizierte der EG-Rat später in einer Teilrevision der Richtlinie 77/187/EWR.[62] Es stellte sich die Frage, ob das Bundesgericht bei der europarechtskonformen Auslegung von Art. 333 OR und insb. Abs. 3 der Bestimmung die Anwendung der Richtlinie durch den EuGH und die Teilrevision der Richtlinie 77/187/EWR (bzw. deren Nachfolgerichtlinie 2001/23/EG[63]) durch den EG-Rat mitberücksichtigen darf. Das Bundesgericht hielt fest:

> «Wird […] die schweizerische Ordnung einer ausländischen – hier der europäischen – angeglichen, ist die Harmonisierung nicht nur in der Rechtssetzung, sondern namentlich auch in der Auslegung und Anwendung des Rechts anzustreben, soweit die binnenstaatlich zu beachtende Methodologie [d.h. die im Schweizer Recht anzuwendenden klassischen Auslegungsmethoden] eine solche Angleichung zulässt. […] Die Angleichung in der Rechtsanwendung darf sich dabei nicht bloss an der europäischen Rechtslage orientieren, die im Zeitpunkt der Anpassung des Binnenrechts durch den Gesetzgeber galt. Vielmehr hat sie auch die Weiterentwicklung des Rechts, mit dem eine Harmonisierung angestrebt wurde, im Auge zu behalten.»[64]

Das Bundesgericht entschied mit Verweis auf seine Auslegung der Bestimmungen nach teleologischer und systematischer Auslegung, dass in Bezug auf Art. 333 Abs. 3 OR ein solcher «Angleichungsspielraum» besteht.[65] Das Gericht berücksichtigte daher die EuGH-*Rechtsprechung* und die spätere *gesetzgeberische Weiterentwicklung* der europäischen Bestimmung als «Auslegungshilfe»[66] und entschied, dass Art. 333 Abs. 3 OR in Ermangelung einer gegenteiligen Regelung im Konkursfall nicht anwendbar ist.[67]

---

[61] EuGH, Rs. 135/83, 07.02.1985, *Abels*, Slg. 1985, 469; bestätigt durch Rs C-319/94, 12.03.1998, *Jules Dethier Equipements S.A.*, Slg. 1998, I–1061.

[62] Art. 4a Richtlinie 77/187/EWR, eingeführt durch Richtlinie 98/50, ABl. L 201, 17.07.1998, 88 ff.).

[63] Richtlinie 2001/23/EG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Wahrung von Ansprüchen der Arbeitnehmer beim Übergang von Unternehmen, Betrieben oder Unternehmens- oder Betriebsteilen, ABl. L 82, 22.03.2001, 16.

[64] BGE 129 III 335 E. 6 (Art. 333 OR betreffend); bestätigt in BGE 130 III 182 E. 5.5.1 (Art. 15 des Bundesgesetz über Pauschalreisen betreffend).

[65] BGE 129 III 335 E. 6.

[66] BGE 129 III 335 E. 6.

[67] BGE 129 III 335 E. 6.

C. BGE 137 II 199 (Kartellgesetz)

1. Ausgangslage

Im Urteil BGE 137 II 199 hatte das Bundesgericht Art. 7 Abs. 2 lit. c KG (Erzwingung unangemessener Preise oder sonstiger unangemessener Geschäftsbedingungen) auszulegen. Es stellte sich die Frage, welche Bedeutung darin das Wort «Erzwingung» hat.

Die Vorinstanz verneinte den Missbrauch einer marktbeherrschenden Stellung durch die Swisscom. Diese sei aufgrund der regulatorischen Rahmenordnung gar nicht in der Lage gewesen, ihre Preise oder sonstigen Geschäftsbedingungen durchzusetzen und somit zu «erzwingen». Das Volkswirtschaftsdepartement stellte sich auf den Standpunkt, Erzwingen sei kein eigenständiges Tatbestandsmerkmal. Die Swisscom habe die Höhe der Terminierungspreise allein schon aufgrund ihrer Stellung als marktbeherrschendes Unternehmen bestimmen können.[68]

2. Keine europarechtskonforme Auslegung

Das Bundesgericht hatte den Sinn von Art. 7 Abs. 2 lit. c KG durch Auslegung zu ermitteln. Das Volkswirtschaftsdepartement hielt dafür, die Bestimmung im Sinne des EU-Wettbewerbsrechts auszulegen. Dies führe zu einem restriktiveren Verständnis des Ausbeutungsmissbrauchs als jenes der Vorinstanz.[69]

Das Bundesgericht hielt fest, dass das Kartellgesetz vom EU-Recht unabhängiges Schweizer Recht sei. Als solches sei es grundsätzlich autonom auszulegen. Allerdings dränge sich der Beizug des EU-Wettbewerbsrechts als Auslegungshilfe auf, soweit der schweizerische Gesetzgeber *eine Koordination mit dem EU-Recht bezweckt habe und sich die Regelungen inhaltlich entsprechen*. Insbesondere autonom nachvollzogenes EU-Recht sei nach der Rechtsprechung europarechtskonform auszulegen. Denn beim *autonomen Nachvollzug* ginge es dem Gesetzgeber darum, eine *parallele Regelung* zu schaffen.[70]

---

[68] BGE 137 II 199 E. 4.2.

[69] BGE 137 II 199 E. 4.3.1.

[70] BGE 137 II 199 E. 4.3.1.

Mit Verweis auf die Botschaft zur Kartellgesetzrevision von 1995[71] hielt das Bundesgericht fest, die KG-Revision von 1995 habe «keinen besonderen europapolitischen Hintergrund» gehabt. Das Ziel der «EU-Kompatibilität» werde nicht genannt, auch nicht in den Ausführungen zum Missbrauch einer marktbeherrschenden Stellung. Der Gesetzgeber habe mit der Revision von 1995 somit nicht EU-Wettbewerbsrecht autonom nachvollziehen wollen.

Das Bundesgericht sah in der Formulierung der Missbrauchstatbestände eine *Anlehnung* an EU-Wettbewerbsrecht. Das Regelungsmuster des EU-Wettbewerbsrechts sei beim Erlass von Art. 7 KG aber nur insoweit berücksichtigt worden, «als nicht aus sachlichen Gründen unterschiedliche Lösungen angezeigt erschienen». Auch aus der Terminologie von Art. 7 KG liesse sich nicht ableiten, dass zwingend eine identische Regelung angestrebt war.[72]

Das Bundesgericht verwies sodann auf die Botschaft zur Kartellgesetzrevision von 2003, in welcher der Gesetzgeber direkte Sanktionen (Art. 48a KG) einführte.[73] Der Bundesrat führte darin aus, dass sich die Regelungen zur Sanktion «nur schlecht mit entsprechenden Instituten im europäischen Kontext vergleichen» liessen, da *«Unterschiede in der konzeptionellen Ausrichtung (Verbots- statt Missbrauchsprinzip in der EU)»*[74] bestünden. Immerhin erfolge eine *Annäherung* an das Schutzniveau in der EU.[75] Dieser Relativierung entnahm das Bundesgericht, dass das Schweizer Recht «nicht vollständig demjenigen der Europäischen Union entspricht» und der Schweizer Gesetzgeber mithin *nicht eine identische Regelung angestrebt* hat.[76]

---

[71] Botschaft vom 23. November 1994 zu einem Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (Kartellgesetz, KG), BBl 1995 I 468 (zit. Botschaft KG 1995).

[72] BGE 137 II 199 E. 4.3.2; Vgl. aber Sturny (FN 38). Sie beurteilt die KG-Revision von 1995 als bewusste Orientierung am EU-Wettbewerbsrecht und daher als autonomen Nachvollzug – wobei sie den autonomen Nachvollzug relativ breit versteht und ihn der blossen eklektischen Anlehnung bzw. dem zufälligen Abkupfern von EU-Recht gegenüberstellt (a.a.O. 76–77).

[73] BGE 137 II 199 E. 4.3.2.

[74] Botschaft vom 7. November 2001 über die Änderung des Kartellgesetzes, BBl 2002 2022 (zit. Botschaft KG 2003), 2051; Hervorhebung hinzugefügt.

[75] Botschaft KG 2003 (FN 74), 2051.

[76] BGE 137 II 199 E. 4.3.2.

3. Plausibilisierung des Auslegungsresultats anhand EU-Praxis

Das Bundesgericht legte Art. 7 Abs. 2 lit. c KG daher autonom in Anwendung der klassischen Auslegungsmethoden aus (grammatikalische, systematische und teleologische Auslegung).[77] Die Rechtsprechung des EuGH zog das Bundesgericht nur (aber immerhin) *rechtsvergleichend* heran: Auch nach der EuGH-Rechtsprechung folge aus der wirtschaftlichen Macht des Marktbeherrschers für sich allein noch nicht, dass dessen Preise missbräuchlich seien. Es sei vielmehr eine Gesamtwürdigung vorzunehmen.[78]

D. BGE 139 I 72 (Kartellgesetz)

1. Ausgangslage

In BGE 139 I 72 hatte das Bundesgericht zu beurteilen, ob Art. 7 Abs. 2 lit. b KG (Diskriminierung von Handelspartnern bei Preisen oder sonstigen Geschäftsbedingungen) im Sinne des strafrechtlichen Bestimmtheitsgebots genügend bestimmt sei, damit Verstösse dagegen nach Art. 49a KG («strafrechtsähnlich»[79]) direkt sanktioniert werden dürfen.

2. Erkenntnisse über den Norm-Sinn aus Praxis zu ähnlichen Bestimmungen im EU-Recht

Es scheint, als hätte das Bundesgericht in BGE 139 I 72 eine Kehrtwende vollzogen: In BGE 137 II 199 hielt es noch fest, die KG-Revision von 1995 hätte nicht zum Ziel gehabt, EU-Kompatibilität herzustellen – auch nicht mit Bezug auf den Missbrauch einer marktbeherrschenden Stellung. In BGE 139 I 72 aber hielt das Bundesgericht nun fest, dass sich das schweizerische Kartellgesetz «stark am europäischen Wettbewerbsrecht orientiert».[80]

---

[77] BGE 137 II 199 E. 4.3.3–4.3.5.

[78] BGE 137 II 199 E. 4.3.2 mit Hinweis auf das Urteil C-52/09 des EuGH vom 17.02.2011 i.S. *Konkurrensverket c. TeliaSonera Svergie AB*.

[79] BGE 139 I 72 E. 2.2.2.

[80] BGE 139 I 72 E. 8.2.3 mit Hinweis auf die Botschaft – KG 1995 (FN 71), («Parallelen bestehen beispielsweise bei der Formulierung der Tatbestände des Missbrauchs einer marktbeherrschenden Stellung»).

Gemäss Botschaft KG 1995 bestünden beispielsweise bei der Formulierung der Tatbestände des Missbrauchs einer marktbeherrschenden Stellung «Parallelen» mit der entsprechenden Regelung im EU-Wettbewerbsrecht.[81] Deshalb sei «auch die Praxis [der EU-Wettbewerbsbehörden] zu Art. 102 AEUV» bei der Auslegung von Art. 7 KG «zu berücksichtigen».[82] Aus der Praxis zu Art. 102 AEUV liessen sich «diesbezüglich» (d.h. in Bezug auf die ähnlich formulierten Tatbestände in Art. 7 KG) «Erkenntnisse über den Norm-Sinn und damit auch *Rechtssicherheit*» gewinnen.[83]

«Erkenntnisse» zu gewinnen bedeutet aber nicht, grösstmögliche Parallelität in der Rechtsanwendung anzustreben. Es ist nicht davon auszugehen, dass das Bundesgericht in BGE 139 I 72 mit dem Verweis auf die Möglichkeit, Erkenntnisse zu gewinnen, das Gebot einer europarechtskonformen Auslegung im eigentlichen Sinn gemeint hat. Sonst hätte es dies klarer (wie in BGE 129 III 335) darlegen und mit Blick auf einschlägige Praxis der EU-Behörden umsetzen müssen.

Die einschlägige Praxis der EU-Behörden analysierte das Bundesgericht indes in BGE 139 I 72 gerade nicht. Gemäss Bundesgericht musste die Publigroupe (Beschwerdeführerin) allein schon aufgrund früherer Hinweise der WEKO auf das Diskriminierungspotential der Richtlinien davon ausgehen, dass ihre Verhaltensweise unter Art. 7 KG unzulässig sein könnte.[84]

E. Regeln und Prüfraster für die Auslegung

1. Regeln

Aus den drei vorstehend besprochenen Entscheiden des Bundesgerichts ergeben sich die folgenden Regeln für die Berücksichtigung der Praxis von EU-Datenschutzaufsichtsbehörden und -Gerichten:

---

[81] BGE 139 I 72 E. 8.2.3 mit Hinweis auf die Botschaft – KG 1995 (FN 71), 531 («Parallelen bestehen beispielsweise bei der Formulierung der Tatbestände des Missbrauchs einer marktbeherrschenden Stellung»).

[82] BGE 139 I 72 E. 8.2.3.

[83] BGE 139 I 72 E. 8.2.3.

[84] BGE 139 I 72 E. 8.2.3.

- **Europarechtskonforme Auslegung:** Autonom nachvollzogenes Schweizer Recht ist im Zweifel europarechtskonform auszulegen.[85]
- **Berücksichtigung der EU-Rechtsanwendung bei europarechtskonformer Auslegung:** *Wenn es die im Schweizer Recht geltenden klassischen Auslegungselemente zulassen*, ist bei der Auslegung autonom nachvollzogenen Schweizer Rechts die Praxis der EU-Behörden und -Gerichte zum rezipierten EU-Recht autoritativ mitzuberücksichtigen.[86]
- **Berücksichtigung der EU-Rechtsanwendung als Auslegungshilfe:** Bei blosser *Angleichung des Schweizer Rechts an EU-Recht*, bei welcher der Schweizer Gesetzgeber bewusst *eine eigenständige Schweizer Regelung* schaffen wollte und z.B. eine *unterschiedliche konzeptionelle Ausrichtung*[87] gewählt hat, ist die Rechtsprechung zum rezipierten EU-Recht bloss *als Auslegungshilfe* zu berücksichtigen. Die Behörden können daraus z.B. Erkenntnisse über den Norm-Sinn der auszulegenden Bestimmung gewinnen.[88] Bei dieser Art der Berücksichtigung des EU-Rechts dient das EU-Recht nur der Bestätigung (*Plausibilisierung*) des Auslegungsergebnisses.[89]

2. Prüfung des politischen Willens des Schweizer Gesetzgebers

Bei der Wahl der anzuwendenden Regel hat die rechtsanwendende Schweizer Behörde stets zu prüfen, ob der Schweizer Gesetzgeber in Bezug auf die *einzelne auszulegende Bestimmung* den *politischen Willen* geäussert hat, EU-Recht zu übernehmen und somit autonom nachzuvollziehen, oder aber eine autonom schweizerische Lösung anstelle der EU-Lösung zu wählen – mithin die Rezeption des EU-Rechts zu begrenzen (*Umsetzung à la carte*).[90]

---

[85] BGE 129 III 335 E. 6; bestätigt in BGE 130 III 182 E. 5.5.1 und 129 III 335 E. 5.1 und 6.

[86] BGE 129 III 335 E. 6 (Art. 333 OR betreffend); bestätigt in BGE 130 III 182 E. 5.5.1.

[87] BGE 137 II 199 E. 4.3.2.

[88] BGE 139 I 72 E. 8.2.3 mit Hinweis auf Monique Sturny: Der Einfluss des europäischen Kartellrechts auf das schweizerische Kartellrecht, in: Thomas Cottier (Hrsg.), Die Europakompatibilität des schweizerischen Wirtschaftsrechts: Konvergenz und Divergenz, Basel 2012, 107 ff., 113 ff. i.V.m. 112, 124 N 90 und 127.

[89] Vgl. Marc Amstutz, Interpretatio multiplex. Zur Europäisierung des schweizerischen Privatrechts im Spiegel von BGE 129 III 335, in: Heinrich Honsell et al. (Hrsg.), Privatrecht und Methode, Festschrift für Ernst A. Kramer, Basel 2004, 67–91, 80 («blosser *Bestätigungswert* (und mithin *kein Entscheidungswert*)»).

[90] Amstutz (FN 89), 90.

Steht fest, dass es sich um autonom nachvollzogenes Recht handelt, haben Gerichte und Behörden im Einzelfall zu prüfen, ob der Gesetzgeber klar[91] den **politischen Willen** geäussert hat, das Schweizer Recht dynamisch mit dem EU-Recht zu harmonisieren und somit auch die richterliche und gesetzgeberische Weiterentwicklung des rezipierten EU-Rechts (auf dem Weg der richterlichen Rechtsfortbildung in der Schweiz) zu übernehmen.[92] Nur wenn der Nachweis dieses politischen Willens gelingt, und nur wenn der schweizerische Gesetzgeber die Umsetzung des EU-Rechts «fehlerhaft, d.h. entgegen seiner Absicht planwidrig unvollständig (*lückenhaft*) vollzogen hat»[93], haben die rechtsanwendenden Schweizer Behörden die EU-Praxis zur autonom nachvollzogenen Regelung autoritativ mitzuberücksichtigen (wovon die bloss rechtsvergleichende Berücksichtigung zu unterscheiden ist).

Grundsätzlich erfordert das Prinzip richterlicher Zurückhaltung, dass das Bundesgericht und die weiteren rechtsanwendenden Behörden einen neuerlichen Entscheid des Schweizer Gesetzgebers abwarten, anstatt EU-Praxis zu folgen, die das rezipierte EU-Recht weiterentwickelt. Etwas anderes gilt nur, wenn der Schweizer Gesetzgeber klar den Willen erkennen liess, das Schweizer Recht über richterliche Rechtsfortbildung «‹auf Gedeih und Verderb› – was auch immer der EuGH dazu judiziere!» dynamisch weiterzuentwickeln.[94]

Wenn ein solcher Wille *nicht klar erkennbar ist*, darf die rechtsanwendende Behörde die Weiterentwicklung des autonom nachvollzogenen EU-Rechts (und somit die EU-Praxis) nur *rechtsvergleichend* als *Auslegungshilfe*[95] berücksichtigen. Eine solche «**europarechtliche Orientierung der Rechtsanwendung**» drängt sich gemäss Kramer «bei grundsätzlich europakompatiblen (aber nicht i.e.S. im Wege ‹autonomen Nachvollzugs› erlassenen)» Schweizer Regelungen geradezu auf.[96]

---

[91] Emmanuel Piaget, L'influence de la jurisprudence communautaire sur l'interprétation des lois suisses relatives à la propriété intellectuelle : argument contraignant ou simple aide à l'interprétation?, in: sic! 2006, 727, 733 («de façon évidente »).

[92] Andreas Furrer, Der Einfluss der EuGH-Rechtsprechung auf das schweizerische Wirtschaftsprivatrecht, in: SZIER 2006, 311, 330.

[93] Kramer (FN 36), 353 (Hervorhebung hinzugefügt).

[94] Kramer (FN 36), 354. Vgl. Piaget (FN 91), 733.

[95] Piaget (FN 91), 733. Vgl. Kramer (FN 36), 335.

[96] Kramer (FN 36), 335 (Hervorhebung hinzugefügt).

3. Intensität der Anlehnung an EU-Recht eruieren

Das Gebot, nachvollzogenes Schweizer Recht im Zweifel europarechtskonform auszulegen, ist nicht absolut. Erstens gilt es nur in Bezug auf die *einzelne nachvollzogene Norm*. Zweitens sind «Eigenheiten oder unterschiedliche Ziele der schweizerischen Rechtsordnung»[97] zu berücksichtigen. Gerade eine *konzeptionell unterschiedliche Ausgestaltung*[98] des an das EU-Recht angeglichenen Rechts kann einer europarechtskonformen Auslegung entgegenstehen.[99]

Gemäss Heinemann haben die rechtsanwendenden Schweizer Behörden in solchen Fällen zu begründen, weshalb sie der europäischen Lösung nicht folgen.[100] Dies steht im Einklang damit, dass gemäss Botschaftsleitfaden der Bundeskanzlei bei der Ausarbeitung von Gesetzesentwürfen ein Abweichen von den europäischen Regelungen zu begründen ist.[101] Heinemann geht noch weiter und fordert, dass die rechtsanwendende Behörde vor einer abweichenden Auslegung die Vorteile eines eigenständigen Schweizer Ansatzes mit dem «Verlust an Harmonisierungsgewinnen» abwägen sollte. Dem ist entgegenzuhalten, dass der Grundsatz richterlicher Zurückhaltung erfordert, Harmonisierungsgewinne in der Rechtsanwendung nur anzustreben, wenn der Gesetzgeber diesbezüglich einen klaren Willen geäussert hat.[102]

Heinemann ist insofern zuzustimmen, dass es zwischen den Arten der autonomen Anpassung (zwischen autonomem Nachvollzug von EU-Recht und Angleichung oder allgemeiner Inspiration) Zwischenstufen gibt, die es bei der Auslegung der Schweizer Norm zu berücksichtigen gilt.[103] Die rechtsanwendende Schweizer Behörde hat somit die **Intensität der Anlehnung an EU-Recht zu bestimmen**.[104] Je intensiver der Gesetzgeber das Schweizer Regelwerk bzw. die konkret auszulegende Norm an das EU-Recht angelehnt

---

97 Heinemann (FN 25), 35.

98 BGE 137 II 199 E. 4.3.2.

99 BGE 139 I 72 E. 8.2.3; Heinemann (FN 25), 35.

100 Heinemann (FN 25), 35.

101 Heinemann (FN 25), 35.

102 Vgl. oben IV.E.2.

103 Heinemann (FN 25), 33–34.

104 Heinemann (FN 25), 31.

hat, desto relevanter wird die europarechtskonforme Auslegung oder zumindest eine Orientierung am EU-Recht wie auch seiner Weiterentwicklung durch die Praxis der EU-Behörden und -Gerichte.[105]

F. Bisherige Zurückhaltung in Praxis zum Datenschutzrecht

1. Bundesgericht

In Leitentscheiden des Bundesgerichts zum DSG findet man nur ausnahmsweise Bezüge zur Anwendung der (durch die DSGVO aufgehobenen) Richtlinien 95/46/EG:

- BGE 136 II 508 (*Logistep*) – Plausibilisierung anhand Stellungnahme der Artikel 29-Datenschutzgruppe.[106]
- BGE 138 II 346 (*Google Street View*) – keine Nennung.
- BGE 138 III 425 (*Auskunftsrecht von Bankkunden*) – keine Nennung.
- BGE 141 III 119 (*Auskunftsrecht von Mitarbeitenden*) – keine Nennung.
- BGE 142 III 263 (*Videoüberwachungssystem*) – keine Nennung.
- BGE 143 I 253 (*FINMA Watchlist*) – keine Nennung.
- BGE 144 I 126 (*Aufbewahrung von Randdaten der Telekommunikation*) – Hinweise auf Urteile des EuGH zur Vorratsdatenspeicherung, aber nicht unter Bezugnahme auf Richtlinie 95/46/EG.

2. Bundesverwaltungsgericht

Auch in der Praxis des Bundesverwaltungsgerichts finden sich nur vereinzelt Hinweise auf Bestimmungen, Praxis oder Stellungnahmen zum EU-Datenschutzrecht:

- Urteil A-3144/2008 vom 27. Mai 2009 (*Logistep*) – Hinweis auf Stellungnahme 4/2007 der Art. 29-Datenschutzgruppe.[107]

---

[105] Heinemann (FN 25), 31.

[106] BGE 136 II 508 E. 3.6.

[107] BVGer, A-3144/2008, 27.05.2009, E. 2.2.3.

– Urteil A-5225/2015 vom 12. April 2017 (*Lucency*) – keine Nennung.
– Urteil A-4232/2015 vom 18. April 2017 (*Moneyhouse*) – Hinweis[108] auf (i.c. nicht einschlägiges) EuGH-Urteil i.S. Google Spain.[109]
– Urteil A-3548/2018 vom 19. März 2019 (*Helsana*) – Hinweis auf Art. 5 Abs. 1 lit. a DSGVO, wonach Personendaten nur für «legitime» Zwecke erhoben und bearbeitet werden dürfen, und darauf, dass sich die Rechtslage gemäss DSG davon unterscheidet.[110]

V. Analyse

A. Intensität der Anlehnung an die DSGVO im Allgemeinen

1. Einleitung

Die Intensität der Anlehnung des nDSG an die DSGVO gibt Aufschluss darüber, ob und wie die Praxis der Behörden und Gerichte zur DSGVO bei der Auslegung des DSG zu berücksichtigen ist. *Je intensiver die Anlehnung, desto eher sind die DSGVO-Bestimmung und die Praxis dazu bei der Auslegung des nDSG zu berücksichtigen*. Die Skala beginnt mit der blossen Auslegungshilfe, geht über in die europarechtliche Orientierung, und reicht bis zum Gebot der europarechtskonformen Auslegung unter Berücksichtigung der EU-Praxis.[111]

Zur Eruierung der Intensität der Anlehnung des nDSG an die DSGVO sind die rechtsvergleichenden Vorarbeiten des Bundesamts für Justiz (BJ) besonders instruktiv. Der Erläuternde Bericht zum Vorentwurf des nDSG (VE-DSG)[112] enthält ein Kapitel zur «Ausgangslage auf internationaler Ebene» mit Hinweisen auf die Regelungen der EU, des Europarats und der Vereinten Nationen

---

[108] BVGer, A-4232/2015 .18.04.2017, E. 6.1 (*Moneyhouse*).

[109] EuGH, Rs. C-131/12, 13.05.2014, *Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González.*

[110] BVGer, A-3548/2018, 19.03.2019, E. 5.4.3.

[111] Vgl. oben IV.E.1.

[112] Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 21.12.2016 (zit. Erläuternder Bericht VE-DSG).

sowie auf Richtlinien der OECD.[113] In anschliessenden Kapiteln äussert sich der Erläuternde Bericht VE-DSG detailliert zu den Vorgaben der Schengen-relevanten Richtlinie (EU) 2016/680[114] und des revidierten Übereinkommens SEV 108[115]. Im Kapitel zur DSGVO erläutert das BJ die «Angleichung der schweizerischen Gesetzgebung» an die DSGVO.[116] Schliesslich enthält auch das Kapitel zu den «Ziele[n] der Revision»[117] wichtige Hinweise darauf, inwiefern mit der Revision eine Art der Anpassung an europäische Normen bezweckt wird.

Die Botschaft des Bundesrats äussert sich gleich in der Übersicht («Ausgangslage und Ziele der Vorlage») zur unterschiedlichen Bedeutung der Richtlinie (EU) 2016/680, des revidierten Übereinkommens SEV 108 und der DSGVO für das nDSG.[118] Wie bereits im Erläuternden Bericht VE-DSG, enthält das (fast identische) Kapitel «Ausgangslage auf internationaler Ebene» in der Botschaft detaillierte Hinweise zur Bedeutung der Regelungen der EU, des Europarats und der Vereinten Nationen für die Revisionsvorlage.[119] Auch das Kapitel «Ziele der Revision»[120] mit den Hinweisen auf die Art der Anpassung an europäische Normen übernimmt die Botschaft E-DSG aus dem Erläuternden Bericht VE-DSG.

In der Folge stellt dieser Beitrag für die Eruierung der Intensität der Anlehnung an die DSGVO im Allgemeinen auf den Wortlaut der genannten Kapitel in der Botschaft E-DSG ab. Dies rechtfertigt sich dadurch, dass (i) die Botschaft E-DSG aktueller ist als der Erläuternde Bericht VE-DSG und (ii) die Botschaft E-DSG durch den von der Volksvertretung (Bundesversammlung) gewählten Bundesrat veröffentlicht wurde und somit die höhere demokratische Legitimation hat. Zudem (iii) sind die Kapitel zur Ausgangslage auf internationaler Ebene und zu den Zielen der Revision im Erläuternden Bericht VE-DSG und in der Botschaft E-DSG ohnehin praktisch identisch sind.

---

113 Erläuternder Bericht VE-DSG (FN 112), 13–18.

114 Erläuternder Bericht VE-DSG (FN 112), 31–32.

115 Erläuternder Bericht VE-DSG (FN 112), 21–30.

116 Erläuternder Bericht VE-DSG (FN 112), 31–32.

117 Erläuternder Bericht VE-DSG (FN 112), 17–18.

118 Botschaft E-DSG (FN 3), 6943.

119 Botschaft E-DSG (FN 3), 6962–6969.

120 Botschaft E-DSG (FN 3), 6969–6970.

Während die erwähnten Vorarbeiten einen guten Überblick über die generelle Zielsetzung des nDSG geben, sind die Protokolle der Sitzungen der SPK von Nationalrat (SPK-N) und Ständerat (SPK-S) sowie die Mitschrift der Beratungen im Parlament unverzichtbar, um den *politischen Willen* des Gesetzgebers in Bezug auf die Revisionsvorlage insgesamt und in Bezug auf die einzelnen Bestimmungen zu eruieren. Einige davon – so die Bestimmungen zur Datenportabilität (Art. 28–29 nDSG) und die Bestimmungen zum Profiling mit hohem Risiko (Art. 5 lit. g und Art. 6 Abs. 7 lit. b nDSG) – wurden sogar erst im Zuge der Beratungen in den SPK und im Parlament in das nDSG aufgenommen.

2. Ausgangslage aus internationaler Sicht

a. Europäische Union

i. Einleitung

In Bezug auf die Ausgangslage auf Ebene der EU erwähnt der Bundesrat den Erlass der DSGVO und der Richtlinie (EU) 2016/680 vom 27. April 2016. Der Bundesrat weist auf die unterschiedliche Bedeutung dieser beiden EU-Erlasse hin: Die Richtlinie (EU) 2016/680 gehört zum Schengen-Acquis. Gemäss Art. 2 Abs. 3 des Schengen-Assoziierungsabkommens sei die Schweiz *daher verpflichtet, diese Richtlinie umzusetzen*.[121] Hingegen handle es sich bei der DSGVO nicht um eine Weiterentwicklung des Schengen-Acquis. Entsprechend sei die Schweiz *nicht verpflichtet, die DSGVO umzusetzen*.[122]

ii. Richtlinie (EU) 2016/680

Ziel der *Richtlinie (EU) 2016/680* sei es, ein angemessenes Gleichgewicht zwischen dem Interesse betroffener Personen auf Schutz ihrer Privatsphäre und den Interessen der wirksamen Strafverfolgung herzustellen. Dies soll gemäss Bundesrat namentlich durch die folgenden Änderungen erreicht werden:[123]

– Definition neuer Datenkategorien (Art. 6 der Richtlinie [EU] 2016/680);
– Stärkung des Erfordernisses einer gesetzlichen Grundlage für die Datenbearbeitung (Art. 8 der Richtlinie [EU] 2016/680);

[121] Botschaft E-DSG (FN 3), 6991.
[122] Botschaft E-DSG (FN 3), 6964, 6996 und 6998.
[123] Botschaft E-DSG (FN 3), 6989–6991.

– Einführung des Grundsatzes des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 19 und 20 der Richtlinie [EU] 2016/680);
– Einführung der Pflicht der Verantwortlichen, vor Einführung bestimmter neuer Datenverarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen und gegebenenfalls die Aufsichtsbehörde zu konsultieren (Art. 27–28 der Richtlinie [EU] 2016/680);
– Einführung der Pflicht der Verantwortlichen, Verletzungen der Datensicherheit in bestimmten Fällen der Aufsichtsbehörde und gegebenenfalls betroffenen Personen zu melden (Art. 30–31 der Richtlinie [EU] 2016/680).

iii. DSGVO

Die DSGVO thematisiert der Bundesrat als zweiten grundlegenden Datenschutzerlass auf EU-Ebene. In seinem Kurzüberblick beschreibt der Bundesrat die Regelungsbereiche der einzelnen Kapitel der DSGVO. Dabei fokussiert er auf Änderungen im Vergleich zur früheren EU-Datenschutzrichtlinie[124]. Dazu gehören:[125]

– Ausbau der Betroffenenrechte;
– Einführung des Grundsatzes des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen;
– detailliertere Regelung der Auftragsverarbeitung; Pflichten von Auftragsverarbeitern direkt aus der DSGVO;
– Pflicht, Verletzungen der Datensicherheit an Datenschutzaufsichtsbehörden und gegebenenfalls betroffene Personen zu melden;
– Pflicht, in Bezug auf gewisse geplante Verarbeitungen eine Datenschutz-Folgenabschätzung durchzuführen;
– Einführung von Geldbussen (Verwaltungsstrafen).

[124] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[125] Botschaft E-DSG (FN 3), 6996–6998.

b. Europarat

Die Schweiz hat das Übereinkommen SEV 108 sowie das Zusatzprotokoll ratifiziert. Im Hinblick auf die Ratifizierung des revidierten Übereinkommens SEV 108 ist die Schweiz verpflichtet, ihre Gesetzgebung anzupassen.[126] Der Bundesrat weist in der Botschaft E-DSG auf diese Entwicklung hin und nennt als Hauptziel der Revision des Übereinkommens SEV 108 die Stärkung des Schutzes der Privatsphäre und der Grundrechte vor dem Hintergrund der Herausforderungen, welche die technologischen Entwicklungen und die Zunahme des grenzüberschreitenden Datenverkehrs mit sich bringen würden.[127]

Diese Ziele sollen namentlich mit den folgenden *Anpassungen und Neuerungen* erreicht werden:[128]

- Pflicht des Verantwortlichen zur Meldung bestimmter Verletzungen der Datensicherheit an die zuständige Aufsichtsbehörde (Art. 7 Abs. 2 des revidierten Übereinkommens SEV 108);
- erweiterte Informationspflichten des Verantwortlichen (Art. 8 des revidierten Übereinkommens SEV 108);
- Ausbau der Betroffenenrechte, insbesondere die Einführung eines Rechts, bei automatisierten Einzelentscheiden angehört zu werden und Ausbau des Auskunftsrechts (Art. 9 des revidierten Übereinkommens SEV 108);
- Pflicht des Verantwortlichen zur Durchführung von Datenschutzfolgenabschätzungen in bestimmten Fällen (Art. 10 Abs. 2 des revidierten Übereinkommens SEV 108);
- Pflicht des Verantwortlichen zur Anwendung der Grundsätze des Datenschutzes durch Technikgestaltung (Art. 10 Abs. 2 des revidierten Übereinkommens SEV 108);
- Pflicht der Vertragsstaaten, angemessene Sanktionen bei Verletzungen der Datenschutzbestimmungen vorzusehen (Art. 10 des revidierten Übereinkommens SEV 108).

---

[126] Botschaft E-DSG (FN 3), 6996.

[127] Botschaft E-DSG (FN 3), 6966.

[128] Europarat, The Modernised Convention 108: Novelties in a Nutshell, abrufbar: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8 (Abruf: 12.10.2022); Botschaft E-DSG (FN 3), 6993–6994 .

Der Bundesrat weist darauf hin, dass das revidierte Übereinkommen SEV 108[129] der Richtlinie (EU) 2016/680 und der DSGVO «sehr ähnlich» sei. Die Europäische Kommission habe in den Verhandlungen im Europarat sehr auf die Vereinbarkeit des Inhalts des revidieren Übereinkommens SEV 108 mit dem neuen Datenschutzrecht der EU geachtet.[130] Die DSGVO regelt denn auch dieselben (und einige weitere) Anpassungen und Neuerungen, wie sie das revidierte Übereinkommen SEV 108 vorsieht; dies indes noch detaillierter als in der Richtlinie (EU) 2016/680.[131]

3. Ziele der Revision gemäss Botschaft E-DSG

Gemäss Botschaft E-DSG verfolgt das E-DSG die folgenden Ziele:

– die Anpassung des Schweizer Rechts an technogische Entwicklungen mit «erhebliche[n] Auswirkungen auf den Datenschutz»;[132]

– die Anpassung des DSG an das revidierte Übereinkommen SEV 108;[133]

– die Umsetzung der Anforderungen der Schengen-relevanten Richtlinie (EU) 2016/680 und die Umsetzung der Empfehlungen der Europäischen Kommission im Rahmen der Schengen-Evaluation des Jahres 2014;[134] sowie

– eine Annäherung des bestehenden DSG an die Anforderungen der DSGVO.

Gemäss Bundesrat führen namentlich Big Data-Analysen und Profiling auf der Basis von Algorithmen zu einem *Verlust an Kontrolle* der betroffenen Personen über ihre Daten.[135] Höhere Anforderungen an die Transparenz der Datenbearbeitung (Informationspflicht bei der Beschaffung von Personendaten und bei automatisierten Einzelentscheidungen)[136], eine Stärkung der

---

[129] Er verweist in der Botschaft noch auf den Entwurf des revidierten Übereinkommens 108. Diesen hat der Ministerrat am 18. Mai 2018 ohne substanzielle Änderungen verabschiedet.

[130] Botschaft E-DSG (FN 3), 6966.

[131] Botschaft E-DSG (FN 3), 6996–6998.

[132] Botschaft E-DSG (FN 3), 6969.

[133] Botschaft E-DSG (FN 3), 6970.

[134] Botschaft E-DSG (FN 3), 6969–6970.

[135] Botschaft E-DSG (FN 3), 6969.

[136] Botschaft E-DSG (FN 3), 6972–6973 sowie 7050–7059.

Betroffenenrechte (z.B. Ausbau des Auskunftsrechts)[137] und eine detailliertere Regelung der Voraussetzungen für eine gültige Einwilligung[138] sollen gemäss Bundesrat diesen Kontrollverlust ausgleichen. Dieser Ausgleich des Kontrollverlusts entspricht auch einer Reihe parlamentarischer Vorstösse.[139]

Die weiteren Zielsetzungen der Revision ergeben sich gemäss Bundesrat aus der Pflicht, die Richtlinie (EU) 2016/680 und die Vorgaben des revidierten Übereinkommens SEV 108 im Schweizer Recht umzusetzen. Die Ratifizierung des revidierten Übereinkommens SEV 108 liege im Interesse der Schweiz – nicht zuletzt auch, weil sie für die Aufrechterhaltung des EU-Angemessenheitsbeschlusses 2000 von grosser Bedeutung sei. Um aber das revidierte Übereinkommen SEV 108 zu ratifizieren, müsse die Schweiz ihre Gesetzgebung an dessen Neuerungen anpassen.[140]

4. Angleichung des DSG an die DSGVO

Die Überschrift zum zweiten Unterkapitel im Kapitel der Botschaft E-DSG zur DSGVO lautet «Angleichung der schweizerischen Gesetzgebung».[141] Der Bundesrat betont an dieser Stelle nochmals,[142] dass die DSGVO für die Schweiz nicht verbindlich ist, da es sich dabei nicht um eine Weiterentwicklung des Schengen-Acquis handle.[143]

Gleichzeitig betont der Bundesrat, dass die Schweiz ausserhalb der Schengen-Zusammenarbeit als Drittstaat gilt. Die Schweiz biete gemäss EU-Angemes-

---

[137] Botschaft E-DSG (FN 3), 6971–6972 sowie 7066–7070.

[138] Botschaft E-DSG (FN 3), 7027–7028.

[139] Parlamentarische Initiative Derder 14.434 «Schutz der digitalen Identität von Bürgerinnen und Bürgern» (Forderung einer Ergänzung von Art. 13 Abs. 2 BV dahingehend, dass Daten Eigentum der betreffenden Person sind); Postulat Béglé 16.3386 «Kontrolle über persönliche Daten. Informationelle Selbstbestimmung fördern»: (Forderung von Instrumenten, mit denen «Bürger die Kontrolle über ihre persönlichen Daten wiedererlangen» können); s.a. Postulat Schwaab 14.3739 «Control by Design. Die Rechte auf Eigentum im Falle von unerwünschten Verbindungen verstärken»); Hinweise auf weitere für die Revision relevante parlamentarische Vorstösse: Botschaft E-DSG (FN 3), 6959–6962.

[140] Botschaft E-DSG (FN 3), 6970.

[141] Botschaft E-DSG (FN 3), 6998.

[142] So bereits Botschaft E-DSG (FN 3), 6964 und 6996.

[143] Botschaft E-DSG (FN 3), 6998.

senheitsbeschluss 2000 ein angemessenes Datenschutzniveau. Der für die Schweizer Wirtschaft bedeutsame Beschluss könne aber jederzeit widerrufen werden und werde künftig anhand der Anforderungen der DSGVO überprüft. Für die Schweizer Wirtschaft sei es daher «von zentraler Bedeutung, dass die schweizerische Gesetzgebung einen den *Anforderungen* dieser Verordnung [DSGVO] *entsprechenden* Schutz gewährleistet.»[144] Die Schweiz tue gut daran, «ihre Gesetzgebung an die europäischen Anforderungen *anzupassen*.»[145]

Es fällt auf, dass der Bundesrat konsequent «**Angleichung**»[146] oder «**Anpassung**» (bzw. «anpassen», «anzupassen»)[147] der Schweizer Gesetzgebung an die «Anforderungen» der DSGVO schreibt.[148] Zudem betont der Bundesrat mehrfach, die Schweiz müsse die DSGVO nicht übernehmen.[149] Auch bei den Erläuterungen zu den einzelnen Bestimmungen des E-DSG schreibt der Bundesrat nie von einer Übernahme einer DSGVO-Bestimmung. Stattdessen verwendet er bei Bezugnahme auf DSGVO-Bestimmungen regelmässig das Wort «**ähnlich**»[150], oder er schreibt (in einem Fall) «anpassen»[151] oder (in einem Fall) «Angleichung»[152]. In der Ratsdebatte sprach die Justizministerin von einer «**Annäherung**»[153] des DSG an die DSGVO.

---

144 Botschaft E-DSG (FN 3), 6965 (Hervorhebungen hinzugefügt).

145 Botschaft E-DSG (FN 3), 6968 (Hervorhebung hinzugefügt).

146 Botschaft E-DSG (FN 3), 6998 (Hervorhebung hinzugefügt) und (bei der Erläuterung der Bestimmungen zur Bekanntgabe von Personendaten ins Ausland) 7037.

147 Botschaft E-DSG (FN 3), 6998, 6970, 6998, 7021 (Verzicht auf Anpassung des Begriffs «Bearbeiten» an «Verarbeiten») und 7182.

148 Botschaft E-DSG (FN 3), 6964, 6996 und 6998.

149 Botschaft E-DSG (FN 3), 6964, 6996 und 6998.

150 Botschaft E-DSG (FN 3), 7020 (in Bezug auf die neuen Datenkategorien genetische und biometrische Daten; vgl. dazu unten I.D.1 und 2.a., 7029 (in Bezug auf den Grundsatz des Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen), 7031 (Datensicherheit), 7050 (Informationspflicht bei der Beschaffung von Personendaten; vgl. dazu unten III.B.4.), 7056 (Informationspflicht bei einer automatisierten Einzelentscheidung), 7059 (Datenschutz-Folgenabschätzung), 7063 (Meldung von Verletzungen der Datensicherheit), 7077 (Recht auf Löschung), 7088 (Wiederernennung der Aufsichtsbehörde) und 7182 (das E-DSG enthalte «ähnliche Massnahmen» wie die DSGVO).

151 Botschaft E-DSG (FN 3), 7021 (Verzicht auf Anpassung des Begriffs «Bearbeiten» an «Verarbeiten») und 7182.

152 Botschaft E-DSG (FN 3), 7037 (Bekanntgabe von Personendaten ins Ausland).

153 Votum BR Keller-Sutter, AB 2019 N 1781 und AB 2019 S 1238–1239 (Hervorhebung hinzugefügt).

In Bezug auf die *Richtlinie (EU) 2016/680* verwendet der Bundesrat hingegen konsequent den Begriff «Übernahme» bzw. «übernehmen».[154] Diese konsequente *Unterscheidung in der Begriffswahl* – Angleichung, Anpassung oder Ähnlichkeit einerseits und Übernahme andererseits – ist ein deutliches Zeichen dafür, dass der Bundesrat bei der Rezeption von EU-Recht *unterschiedliche Ziele* verfolgte: Eine Angleichung an die DSGVO einerseits und die Übernahme der Bestimmungen der Richtlinie (EU) 2016/650 andererseits.

5. Übernahme der Richtlinie (EU) 2016/680 und Aufrechterhaltung der EU-Angemessenheit

a. Übernahme nur der Richtlinie (EU) 2016/680 im SDSG

Der Gesetzgeber behandelte das Revisionsvorhaben in zwei Etappen.[155] Die Zweiteilung erfolgte, um:[156]

– die Richtlinie (EU) 2016/680 rechtzeitig umzusetzen; und um

– die Totalrevision des DSG angesichts der «grossen Komplexität der Thematik»[157] «ohne Zeitdruck»[158] beraten zu können.

---

[154] Botschaft E-DSG (FN 3), 6941, 6943, 6946, 6950, 6951 (zwei Erwähnungen), 6955, 6971 und 6976 (Übernahme von Begriffen aus dem europäischen Recht – Begriffe aus der Richtlinie (EU) 2016/650 namentlich), 6975, 6991 (drei Erwähnungen), 6992 (zwei Erwähnungen), 6993 (drei Erwähnungen), 6996, 7007, 7170, 7184 (5 Erwähnungen). In Bezug auf die Terminologie verwendet die Botschaft E-DSG an einer Stelle explizit, dass die Schweizer Bestimmung die Terminologie («Standarddatenschutzklauseln») der DSGVO «übernimmt» (Botschaft E-DSG (FN 3), 7040). Dies ist jedoch kein Hinweis auf eine Übernahme der Regelung der DSGVO, sondern vielmehr eine Massnahme zur Herstellung der Vergleichbarkeit im Bereich des Datentransfers ins Ausland, wo die Angemessenheit der Schweizer Gesetzgebung massgebend ist.

[155] SPK-N, Revision des Datenschutzrechtes in zwei Etappen, Medienmitteilung, 12.01.2018 (zit. SPK-N, Etappen); SPK-N, Protokoll der Sitzung vom 11. Januar 2018. So auch SPK-N, Protokoll der Sitzung vom 29. Juni 2018.

[156] SPK-N, Etappen (FN 155).

[157] SPK-N, Etappen (FN 155).

[158] SPK-N, Etappen (FN 155).

Die Schweiz war verpflichtet, die Richtlinie (EU) 2016/680 bis zum 1. August 2018[159] umzusetzen. Mit der Herauslösung der Schengen-relevanten Bestimmungen aus dem E-DSG und dem Erlass des SDSG am 28. September 2018 als Übergangsgesetz wollte sich das Parlament Zeit verschaffen, um der Komplexität der Materie gerecht zu werden und bei der Totalrevision des DSG (so der Kommissionssprecher) «sorgfältig [zu] legiferieren».[160]

Die Begründung der Zweiteilung der Revisionsvorlage und der Erlass des SDSG als Übergangsgesetz zeigen, dass der Gesetzgeber zwar eine Übernahme (recte: Umsetzung) der Richtlinie (EU) 2016/680 bezweckte, nicht aber eine Übernahme (im Sinne eines autonomen Nachvollzugs) der DSGVO. Denn wenn der Gesetzgeber die DSGVO hätte autonom nachvollziehen wollen – ohne autonome Schweizer Lösungen zumindest bei einigen Bestimmungen zu wählen –, dann hätte er die DSGVO einfach eins-zu-eins ins nDSG überführen und mithin ein totalrevidiertes DSG rasch behandeln und verabschieden können. Eine solche **blosse Kopie der DSGVO wollte der Gesetzgeber klar nicht**. Vielmehr wollte er sorgfältig legiferieren und der Komplexität der Materie (generell oder in Bezug auf einzelne Bestimmungen) durch eine Schweizer Lösung gerecht werden.

b. Aufrechterhaltung der EU-Angemessenheit

Bei der Beratung der Totalrevision des nDSG (zweite Etappe) konzentrierte sich die Diskussion in den SPK[161] wie auch im Parlament früh auf die Frage, welche Anpassungen des DSG zur Aufrechterhaltung der EU-Angemessenheit notwendig sind. Man erhält den Eindruck, die Umsetzung des revidierten

---

[159] Die Mitgliedsstaaten waren verpflichtet, die Richtlinie (EU) 2016/680 bis zum 6. Mai 2018 im nationalen Recht umzusetzen. Die Schweiz war verpflichtet, diese Richtlinie bis zum 1. August 2018 in der Schweizer Rechtsordnung umzusetzen. Vgl. Notenaustausch vom 1. September 2016 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (Weiterentwicklung des Schengen-Besitzstands), von der Bundesversammlung am 28. September 2018 genehmigt, in Kraft getreten am 18. Januar 2019, AS 2019 359; BBl 2017 6941.

[160] Votum Jauslin, AB 2018 N 959–960. Vgl. auch SPK-N, Etappen (FN 156) und Protokoll der Sitzung der SPK-N vom 11. Januar 2018.

[161] SPK-N, Protokoll der Sitzung vom 11. Januar 2018; Protokoll der Sitzung vom 18. Oktober 2018.

Übereinkommens SEV 108 sei zweitrangig, oder aber bei der Angleichung zwecks Aufrechterhaltung der EU-Angemessenheit einfach mitgedacht.

Dies zeigen namentlich die Voten aus den Debatten in Ständerat bzw. Nationalrat:

– «[…] wäre es von Vorteil, wenn wir unsere Datenschutzbestimmungen der DSGVO angleichen würden, um auch in Zukunft das Kriterium der Angemessenheit zu erfüllen, **aber nur so weit wie unbedingt nötig, mit Augenmass und ohne Swiss Finish**.»[162]
– «[…] verlangen wir [die SP] die Sicherstellung der **Äquivalenz** – also nicht die Übernahme der DSGVO».[163]
– «Das totalrevidierte Gesetz muss schlussendlich mit dem neuen EU-Datenschutzrecht **als äquivalent deklariert werden**. Wir wollen keine hundertprozentige Übernahme des EU-Rechts, sondern nur die Übernahme der **Grundsätze, der Standards und der Mechanismen, welche die Äquivalenz garantieren**.»[164]
– «Dabei liessen wir uns vor allem von der Frage leiten, wie die nötige Äquivalenz mit dem europäischen Datenschutzrecht [gemeint: DSGVO] erreicht werden kann.»[165]
– «Erstens soll die neue Gesetzgebung **äquivalent** sein mit der europäischen Datenschutz-Grundverordnung.»[166]
– «[…] deren [jene von DSGVO und DSG] **Äquivalenz** ja nun hergestellt werden soll – das ist die grundlegende Zielsetzung dieser Gesetzesrevision».[167]
– «**Äquivalenz** zum europäischen Recht zu konsolidieren.»[168]

Der Gesetzgeber entschied sich somit für die Äquivalenzmethode anstelle des autonomen Nachvollzugs als Form der Rezeption von EU-Recht.

---

[162] Votum Jauslin, AB 2018 N 959 (Hervorhebung hinzugefügt).
[163] Votum Wermuth, AB 2019 N 1776 (Hervorhebung hinzugefügt).
[164] Votum Romano, AB 2019 N 1777 (Hervorhebung hinzugefügt).
[165] Votum Fässler, AB 2020 S 290 (Hervorhebung hinzugefügt).
[166] Votum Silberschmid, AB 2020 N 142 (Hervorhebung hinzugefügt).
[167] Votum Glättli, AB 2020 N 1597 (Hervorhebung hinzugefügt).
[168] Votum Romano, AB 2020 N 144 (Hervorhebung hinzugefügt).

6. Zwischenfazit: Äquivalenz statt autonomer Nachvollzug

Generell lässt sich die Frage danach, wie intensiv der Gesetzgeber sich an das EU-Recht anlehnen wollte, wie folgt beantworten:

– Der Gesetzgeber lässt nicht den Willen erkennen, die DSGVO autonom nachzuvollziehen.

– Der Gesetzgeber wollte die Äquivalenz des Schweizer Datenschutzrechts und der DSGVO herstellen.

– Die Äquivalenz – mithin die EU-Angemessenheit – wollte der Gesetzgeber insbesondere durch Umsetzung der Anforderungen des revidierten Übereinkommens SEV 108 erreichen.

– Nur in Bezug auf die Schengen-relevanten Bestimmungen des E-DSG bestand – im Rahmen dessen, was im SDSG beschlossen wurde – der gesetzgeberische Wille, EU-Recht im Schweizer Recht umzusetzen.

B. Analyse einzelner Bestimmungen des nDSG

1. Räumlicher Geltungsbereich

a. Regelung im Gesetz

Die DSGVO und das nDSG regeln den räumlichen Anwendungsbereich wie folgt:[169]

Art. 3 DSGVO

(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer **Niederlassung** eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

[169] Hervorhebungen hinzugefügt.

a. **betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten**, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b. das Verhalten betroffener Personen zu **beobachten, soweit ihr Verhalten in der Union erfolgt.**

(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt

Art. 3 nDSG

(1) Dieses Gesetz gilt für Sachverhalte, die sich in der Schweiz **auswirken**, auch wenn sie im Ausland veranlasst werden.

(2) Für privatrechtliche Ansprüche gilt das Bundesgesetz vom 18. Dezember 1987 über das **Internationale Privatrecht**. Vorbehalten bleiben zudem die Bestimmungen zum räumlichen Geltungsbereich des **Strafgesetzbuchs**.

b. Analyse

i. Art. 3 Abs. 1 DSGVO: Niederlassungsprinzip

Gemäss Art. 3 Abs. 1 DSGVO gilt die DSGVO für in der EU oder im EWR niedergelassene Unternehmen und Organisationen in Bezug auf die Verarbeitungen personenbezogener Daten, die im Zusammenhang mit den Tätigkeiten dieser Niederlassung erfolgen. Die DSGVO übernimmt damit Art. 4 lit. a der EG-Datenschutzrichtlinie[170] und statuiert im Bereich des Datenschutzrechts das **Niederlassungsprinzip**.[171]

---

[170] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[171] Die einzige Neuerung in Art. 3 Abs. 1 DSGVO besteht darin, dass das Niederlassungsprinzip nun ausdrücklich auch für Datenverarbeitungen im Rahmen der Tätigkeit von in der EU oder im EWR niedergelassenen Auftragsverarbeitern gilt – selbst wenn der jeweilige Auftraggeber (Verantwortlicher) nicht in der EU oder im EWR niedergelassen ist. Dan Jerker B. Svantesson, in: Christopher Kuner et al. (Hrsg.), The EU General Data Protection Regulation (GDPR). A Commentary, Oxford 2020 (zit. Oxford Commentary GDPR–VerfasserIn), Art. 3, 74–99, 86; Manuel Klar, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung. Kommentar, 3. A., München 2020 (zit. VerfasserIn, DS-GVO BDSG), Art. 3 N 2.

Das Niederlassungsprinzip gilt für Auftragsverarbeiter auch dann, wenn für den Verantwortlichen in Bezug auf die von ihm veranlasste Auftragsverarbeitung nicht die Vorgaben der DSGVO, sondern z.B. jene des DSG (bzw. nDSG) gelten. Umgekehrt fallen Datenverarbeitungen eines Verantwortlichen in der Schweiz nicht allein deshalb in den Anwendungsbereich der DSGVO, weil er einen in der EU oder im EWR niedergelassenen Auftragsbearbeiter beizieht.[172]

ii. Art. 3 Abs. 2 DSGVO: Prinzip der Zielgerichtetheit

Art. 3 Abs. 2 lit. a DSGVO statuiert für den Bereich des Datenschutzrechts das **Marktortprinzip**.[173] Das Marktortprinzip will gleich lange Spiesse unter den Marktteilnehmern auf dem EU-Binnenmarkt sicherstellen, indem ausserhalb der EU oder des EWR niedergelassene Unternehmen denselben Regeln unterstehen, wie in der EU oder des EWR niedergelassene Unternehmen, wenn sie ihr Angebot *erkennbar*[174] an den EU-Binnenmarkt ausrichten. In anderen Worten: Mein Markt – meine Regeln!

Das Marktortprinzip ist eine besondere Ausprägung des Prinzips der **Zielgerichtetheit** (*targeting*): Ein Unternehmen ausserhalb der EU oder des EWR *zielt* mit seinem Angebot erkennbar auf EU/EWR-Endkunden.[175] Auch Art. 3 Abs. 2 lit. b DSGVO implementiert das Prinzip der Zielgerichtetheit: Die DSGVO gilt für Datenverarbeitungen bei Verhaltensbeobachtung, die auf das Verhalten natürlicher Personen *abzielt*, die sich in der EU oder im EWR befinden.

---

[172] EDSA, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3), Vers. 2.0, 12.11.2019, 13.

[173] Vgl. Oxford Commentary GDPR–Svantesson (FN 171), Art. 3, 89–90; EDSA, Leitlinien 3/2018, 15.

[174] Ob sich ein Angebot erkennbar auf den EU-Endkundenmarkt ausrichtet, ist sowohl anhand objektiver Kriterien als auch unter Berücksichtigung der (subjektiver) Absichten des Unternehmens zu bestimmen. Vgl. DSGVO, Erwägungsgrund 23; vgl. auch Oxford Commentary GDPR–Svantesson, (FN 171), Art. 3, 90 und Klar, DS-GVO BDSG (FN 171), Art. 3 N 80–89.

[175] Vgl. Oxford Commentary GDPR–Svantesson, (FN 171), Art. 3, 89–90.

iii. Räumlicher Anwendungsbereich des nDSG: Übersicht

Art. 3 Abs. 1 nDSG stellt klar, dass für die Untersuchungskompetenz des EDÖB das **verwaltungsrechtliche Auswirkungsprinzip** gilt. Art. 3 Abs. 2 nDSG verweist in Bezug auf die privatrechtlichen Ansprüche auf das **international-privatrechtliche Auswirkungsprinzip** (Art. 139 IPRG) und in Bezug auf die strafrechtliche Durchsetzung auf das **strafrechtliche Territorialitätsprinzip** (Art. 3 StGB).[176]

iv. Kodifikation des verwaltungsrechtlichen Auswirkungsprinzips

Gemäss Rechtsprechung des Bundesgerichts (*Google Street View*) gilt das DSG für Datenbearbeitungen, die sich **auf die Persönlichkeit und Grundrechte von Personen in der Schweiz auswirken**. Der EDÖB ist somit heute schon zuständig für die Untersuchung von Sachverhalten, wenn sich die Personen, deren Persönlichkeit oder Grundrechte durch die untersuchte Datenbearbeitung gefährdet sind, in der Schweiz befinden bzw. wenn eine Persönlichkeitsverletzung in der Schweiz eintritt.[177]

Somit kodifiziert Art. 3 Abs. 1 nDSG im Bereich des öffentlichen Datenschutzrechts das verwaltungsrechtliche **Auswirkungsprinzip**, wie es beispielsweise im Schweizer Kartellrecht gemäss Art. 2 Abs. 2 KG gilt.[178]

v. Vergleich zum Auswirkungsprinzip im Kartellrecht

Die Praxis der Wettbewerbskommission sowie die Rechtsprechung des Bundesverwaltungsgerichts und des Bundesgerichts zu Art. 2 Abs. 2 KG ori-

[176] Für die Anwendung der Strafbestimmungen des nDSG auf Auslandsachverhalte ist demnach entscheidend, ob der Täter die Tat in der Schweiz begangen hat. Demgegenüber ist Art. 7 StGB (passives Territorialitätsprinzip) in Bezug auf die Strafbestimmungen im nDSG nicht relevant. Die in Art. 60–64 nDSG aufgeführten Delikte sind keine Verbrechen (Art. 10 Abs. 2 StGB) oder Vergehen (Art. 10 Abs. 3 StGB), sondern Übertretungen (Art. 103 StGB).

[177] BGE 138 II 346 E. 3.3 (*Google Street View*).

[178] Gl.M. David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter vom 16. November 2020, N 88–89.

entieren sich stark an objektiven Kriterien.[179] Dies im Unterschied zu den in Erwägungsgrund 23 DSGVO genannten Kriterien. Letztere entspringen der Rechtsprechung des EuGH zur gerichtlichen Zuständigkeit und der Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen.[180] Sie zielen alle darauf ab, herauszufinden, ob der Verantwortliche *beabsichtigt*, betroffenen Personen in der EU/im EWR Waren oder Dienstleistungen anzubieten.[181] Die gestützt darauf vom EDSA entwickelten, auf die (*subjektive*) Absicht des Verantwortlichen abzielenden Kriterien[182] kontrastieren mit den primär *objektiven* Kriterien, die für die Anwendung des Schweizer Kartellrechts auf ausländische Sachverhalte gelten.

---

[179] Offensichtliche Absicht, natürlichen Personen in EU/EWR-Mitgliedsstaaten Waren oder Dienstleistungen anzubieten. Nicht ausreichend: blosse Zugänglichkeit einer Website in der EU, E-Mail-Adresse, andere Kontaktdaten oder die Verwendung einer Sprache, in Drittland, indem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist. Aber: In Verbindung mit Faktoren wie der Erwähnung von Kunden oder Nutzern, die sich in der EU befinden, kann die Verwendung einer in der EU verwendeten Sprache oder Währung «darauf hindeuten, dass der Verantwortliche beabsichtigt, den Personen in der Union Waren oder Dienstleistungen anzubieten» (DSGVO, Erwägungsgrund 23).

[180] Namentlich EuGH, in Rs. C-585/08 und C-144/09, 07.12.2010, *Pammer / Reederei Karl Schlüter GmbH & Co und Hotel Alpenhof / Heller*. Zu den in *Pammer* entwickelten Kriterien gehören die Verwendung eines/r in einem Mitgliedsstaat gebräuchlichen internationalen Telefon-Landescodes, Sprache, Währung oder Top-Level-Domain gebräuchlich sind. Vgl. Oxford Commentary GDPR–Svantesson (FN 171), Art. 3, 89–90.

[181] Vgl. auch EDSA, Leitlinien 2018/3, 19.

[182] EDSA, Leitlinien 2018/3, 20–21: «Die EU oder mindestens ein Mitgliedstaat wird unter Bezugnahme auf die angebotene Ware oder Dienstleistung benannt; der Verantwortliche oder der Auftragsverarbeiter bezahlt einen Suchmaschinenbetreiber für einen Internetreferenzierungsdienst, um den Zugang zu seiner Website durch Verbraucher in der Union zu erleichtern, oder der Verantwortliche oder der Auftragsverarbeiter hat eine Marketing- und Werbekampagne gestartet, die sich an das Publikum in einem EU-Land wendet; die internationale Natur der in Rede stehenden Tätigkeit, wie bestimmte touristische Aktivitäten; die Angabe spezieller Adressen oder Telefonnummern, die von einem EU-Land zu erreichen sind; die Verwendung eines anderen Top-Level-Domain-Namens als desjenigen des Drittlands, in dem der Verantwortliche oder der Auftragsverarbeiter niedergelassen ist, z. B. «de», oder die Verwendung neutraler Top-Level-Domain-Namen wie «.eu»; die Angabe eines internationalen Kundenkreises, der aus Kunden mit Sitz in verschiedenen EU-Mitgliedstaaten besteht, insbesondere durch die Rechnungslegung durch diese Kunden; die Verwendung einer anderen Sprache oder einer anderen Währung als der im Land des Gewerbetreibenden üblichen, insbesondere einer Sprache oder Währung eines oder mehrerer EU-Mitgliedstaaten; der Verantwortliche bietet die Lieferung von Waren in EU-Mitgliedstaaten an.»

Das Bundesverwaltungsgericht folgt bei der Auslegung von Art. 2 Abs. 2 KG der *Anknüpfungstheorie der sachlichen Rückkoppelung*.[183] Demnach wirkt sich ein ausländischer Sachverhalt auf die Schweiz aus, wenn das Marktverhalten einen materiellen Tatbestand des Schweizer KG erfüllt.[184]

Das Bundesgericht hat diese Qualifikation des Auswirkungsprinzips bestätigt. Dies mit der Begründung, das Schutzgut «schweizerische Wettbewerbsordnung» sei unteilbar; Art. 2 Abs. 2 KG stelle sicher, dass Verhalten, das sich negativ auf den Wettbewerb in der Schweiz auswirkt oder auswirken kann, unterbunden werden kann – auch wenn sich das Verhalten im Ausland abspielt.[185] Wann ein Verhalten sich auf die Schweiz auswirke oder auswirken könne, ergebe sich daraus, dass das Verhalten im Ausland einen materiellen Tatbestand des KG (z.B. eine unzulässige Wettbewerbsabrede gemäss Art. 5 KG) in der Schweiz erfüllt. Es schliesst also von der Tatbestandsmässigkeit zurück (Rückkoppelung) auf die Auswirkung in der Schweiz. Damit sei genügender Konnex zur Schweiz hergestellt. Die Intensität der Auswirkung sei im Rahmen von Art. 2 Abs. 2 KG nicht zu prüfen.[186]

vi. Folgerungen für die Auslegung von Art. 3 Abs. 1 nDSG

Übertragen auf das Datenschutzrecht und die Auslegung von Art. 3 Abs. 1 nDSG bedeutet dies, dass der EDÖB einen Auslandssachverhalt dann zu untersuchen hat, wenn die betreffende Datenbearbeitung (voraussichtlich) **die Persönlichkeit von Personen in der Schweiz verletzt**. Dies stimmt im Übrigen überein mit der Regelung in Art. 3 Abs. 2 Satz 1 nDSG bzw. Art. 139 Abs. 3 IPRG, wonach Schweizer Recht (nDSG) anwendbar ist, wenn die Persönlichkeitsverletzung (Erfolg der verletzenden Handlung) in der Schweiz eintritt.

---

[183] Dazu: Anton K. Schnyder, Wirtschaftskollisionsrecht, Sonderanknüpfung und extraterritoriale Anwendung wirtschaftsrechtlicher Normen unter besonderer Berücksichtigung von Marktrecht, Zürich 1990, N 6–10.

[184] BVGer, B-581/2012, 17.09.2016 E. 4.3 (*Nikon*); Vgl. Marc Amstutz/Ramin Silvan Gohari, in: Marc Amstutz/Mani Reinart (Hrsg.), Kartellgesetz, Basler Kommentar, 2. A., Basel 2021 (zit. BSK KG–VerfasserIn), Art. 2 N 187–188.

[185] BGE 143 II 297 E. 3.3 (*Gaba*).

[186] BGE 143 II 297 E. 3.7; Vgl. zum Ganzen: BSK KG–Amstutz/Gohari (FN 184), Art. 2 N 190.

vii. Keine Übernahme des Marktortprinzips im nDSG

Art. 3 Abs. 1 nDSG **übernimmt nicht das EU-rechtliche Marktortprinzip**.[187] Denn Art. 3 Abs. 1 nDSG erfasst Datenbearbeitungen mit Auswirkungen auf die Persönlichkeit Betroffener in der Schweiz unabhängig davon, ob die Datenbearbeitung, die sich in der Schweiz auswirkt, im Zusammenhang mit einem Angebot an Schweizer Endkunden erfolgt oder nicht. Somit geht Art. 3 Abs. 1 nDSG potentiell weiter als Art. 3 Abs. 2 lit. a DSGVO. Praktisch aber wird eine Datenbearbeitung im Ausland vor allem dann spürbare Auswirkungen in der Schweiz zeitigen, wenn sie im Zusammenhang mit der Inanspruchnahme einer Dienstleistung durch Betroffene in der Schweiz erfolgt.

Vereinzelte Wortmeldungen in den SPK-N[188], wonach Art. 3 nDSG das Marktortprinzip einführen solle, sind zu unreflektiert, als dass daraus gefolgert werden könnte, Art. 3 Abs. 1 nDSG übernehme Art. 3 Abs. 2 lit. a DSGVO. Wenn der Gesetzgeber das Marktortprinzip oder das Prinzip der Zielgerichtetheit hätte übernehmen wollen, dann hätte er dies in der Ratsdebatte selbst klar zum Ausdruck bringen müssen – z.B. durch stärkere Orientierung am Wortlaut von Art. 3 Abs. 2 DSGVO. Im Vergleich zu Art. 3 Abs. 1 nDSG hat sich der Gesetzgeber z.B. in Art. 14 nDSG (Vertretung) stark am Wortlaut von Art. 27 DSGVO (Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern) und in Art. 28 nDSG (Recht auf Datenherausgabe oder -übertragung) an Art. 20 DSGVO (Recht auf Datenübertragbarkeit) orientiert. Im Unterschied dazu hat der Gesetzgeber bei Art. 3 Abs. 1 nDSG klar eine *autonome Schweizer Lösung* gewählt.

Art. 3 Abs. 1 nDSG **übernimmt auch nicht das Prinzip der Zielgerichtetheit** bei der Verhaltensbeobachtung. Denn relevant sind (anders als bei Art. 3 Abs. 2 lit. b DSGVO) die (spürbaren) Auswirkungen in der Schweiz; nicht aber, ob eine Verhaltensbeobachtung auf Personen in der Schweiz abzielt.

---

[187] Gl.M. Rosenthal (FN 178), N 88–89. A.M. (Übernahme des Marktortprinzips) Bruno Baeriswyl, Der «grosse Bruder» DSGVO und das revDSG: Ein vergleichender Überblick, in: SZW 1/2021, 8, 11 (der allerdings in seinem Kurzüberblick die augenscheinlichen Unterschiede im Wortlaut der Bestimmungen und die einschlägige Bundesgerichtspraxis nicht thematisiert).

[188] SPK-N, Protokoll der Sitzung vom 16. August 2018.

c. Folgerungen für die Auslegung von Art. 3 nDSG

Aus dem Vorstehenden resultiert das Folgende für den Einfluss der EU-Praxis auf die Auslegung von Art. 3 nDSG:

– Für die Auslegung von Art. 3 Abs. 1 nDSG ist primär die **Praxis der Schweizer Behörden und Gerichte zur Auslegung des verwaltungsrechtlichen Auswirkungsprinzips** in Erlassen zu berücksichtigen, die das Auswirkungsprinzip kodifizieren – namentlich die Praxis der Wettbewerbskommission, des Bundesverwaltungsgerichts und des Bundesgerichts zu Art. 2 Abs. 2 KG. Die **Praxis der EU-Behörden** zu Art. 3 Abs. 2 DSGVO **eignet sich nicht** zur Auslegung von Art. 3 nDSG. Sie stellt mitunter auf subjektive Kriterien (Absicht des Verantwortlichen) ab und nicht darauf, wo die Persönlichkeitsverletzung eintritt.

– Für die Auslegung von Art. 3 Abs. 2 nDSG gilt in Bezug auf die privatrechtlichen Ansprüche die **Praxis der Schweizer Gerichte zu Art. 139 Abs. 3 IPRG**. Die **Praxis der EU-Behörden** zu Art. 3 Abs. 2 DSGVO ist **unerheblich**.

– Für die Auslegung von Art. 3 Abs. 2 nDSG gilt im Bereich der strafrechtlichen Durchsetzung des nDSG die **Praxis der Schweizer Gerichte zu Art. 3 Abs. 1 StGB**. Die **Praxis der EU-Behörden** zu Art. 3 Abs. 2 DSGVO ist **unerheblich**.

2. Genetische Daten und biometrische Daten

a. Regelung im Gesetz

Das nDSG führt in Art. 5 lit. c Ziff. 3 die Datenkategorie «genetische Daten» und in Art. 5 lit. c Ziff. 4 die Datenkategorie «biometrische Daten» ein. Die Einführung dieser neuen Datenkategorien ist eine Anforderung sowohl der Richtlinie (EU) 2016/680[189] als auch des revidierten Übereinkommens SEV 108[190]. Zur Umsetzung der Richtlinie (EU) 2016/680 hat der Gesetzgeber die Datenkategorien bereits in Art. 3 lit. a Ziff. 3–4 SDSG als weitere Kategorien besonders schützenswerter Personendaten eingeführt. Art. 5 lit. c Ziff. 3–4 nDSG übernehmen die Regelung aus dem SDSG unverändert.

[189] Art. 10 Richtlinie 2016/680.

[190] Art. 6 des revidierten Übereinkommens SEV 108.

Auch in der DSGVO hat die EU den Katalog der besonderen Kategorien von Daten (besonders schützenswerte personenbezogene Daten) um die Datenkategorien «genetische Daten» und «biometrische Daten» erweitert. Die Begriffsdefinitionen in Art. 4 Ziff. 13–14 DSGVO sind identisch mit jenen in Art. 3 Ziff. 12–13 der Richtlinie (EU) 2016/680.

Die Bestimmungen lauten wie folgt:[191]

DSGVO

Art. 4 Ziff. 13 DSGVO (genetische Daten)

«genetische Daten» personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden

Art. 4 Ziff. 14 DSGVO (biometrische Daten)

«biometrische Daten» mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten

Richtlinie (EU) 2016/680

Art. 3 Ziff. 12 Richtlinie (EU) 2016/680 (genetische Daten)

«genetische Daten» personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden

[Identisch mit Art. 4 Ziff. 13 DSGVO]

[191] Hervorhebungen hinzugefügt.

Art. 3 Ziff. 12 Richtlinie (EU) 2016/680 (genetische Daten)

«biometrische Daten» mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten

[Identisch mit Art. 4 Ziff. 14 DSGVO]

Revidiertes Übereinkommen SEV 108

[Das revidierte Übereinkommen SEV 108 definiert den Begriff «genetische Daten» nicht; stellt aber in Art. 6 besondere Anforderungen an deren Bearbeitung.]

[Das revidierte Übereinkommen SEV 108 definiert den Begriff «biometrische Daten» nicht; stellt aber in Art. 6 besondere Anforderungen an deren Bearbeitung.]

nDSG

Art. 5 lit. c Ziff. 3 (genetische Daten)

[Das nDSG listet den Begriff «genetische Daten» als Teil der abschliessenden Auflistung besonders schützenswerter Personendaten in Art. 5 lit. c Ziff. 3 auf, definiert ihn aber nicht. Demgegenüber enthält Art. 3 lit. l GUMG resp. Art. 3 lit. k nGUMG die folgende Definition: «genetische Daten: Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden, einschliesslich des DNA-Profils.»]

Art. 5 lit. c Ziff. 4 (biometrische Daten)

[Das nDSG listet den Begriff «biometrische Daten» als Teil der abschliessenden Auflistung besonders schützenswerter Personendaten in Art. 5 lit. c Ziff. 4 auf, definiert ihn aber nicht; bzw. nur mit dem Zusatz «[…] die eine natürliche Person eindeutig identifizieren.»]

b. Analyse

Es fällt auf, dass das nDSG die Begriffe «genetische Daten» und «biometrische Daten, die eine natürliche Person eindeutig identifizieren» als Kategorien besonders schützenswerter Daten einführt bzw. vom SDSG übernimmt, diese aber im Gesetz nicht definiert. Demgegenüber enthalten die Richtlinie (EU) 2016/680 und die DSGVO (im Wortlaut identische) Begriffsdefinitionen für diese Datenkategorien. Es liegt nahe, dass sich rechtsanwendende Behörden in der Schweiz mangels Regelung im nDSG an den Begriffsdefinitionen im EU-Recht orientieren werden.

Zumindest für den *Schengen-relevanten Bereich* ist das Fehlen einer Begriffsbestimmung im SDSG und (künftig) im nDSG eine planwidrig unvollständige Umsetzung der Regelung in Richtlinie (EU) 2016/680. Diese Lücke gilt es zu füllen. Im Anwendungsbereich des SDSG handelt es sich um eine Umsetzung von EU-Recht. Entsprechend sind die Begriffsdefinitionen der Richtlinie (EU) 2016/680 zumindest bei der Beurteilung von Bearbeitungen genetischer und biometrischer Daten im Rahmen der Schengen-relevanten Strafverfolgung im Sinne einer *europarechtskonformen Auslegung* beizuziehen.

Ausserhalb der Schengen-relevanten Bereiche der Bearbeitung von Personendaten (namentlich im Bereich der für Private geltenden Bestimmungen des nDSG) ist die Schweiz nicht an die Begriffsdefinitionen in der Richtlinie (EU) 2016/680 gebunden. Denn diesbezüglich handelt es sich bei Art. 3 lit. a Ziff. 3–4 nDSG lediglich um eine Anpassung an eine Vorgabe des revidierten Übereinkommens SEV 108, das von den Vertragsstaaten keine Begriffsdefinition verlangt.

Die Botschaft E-DSG verweist im Zusammenhang mit Erklärungen zum Begriff der genetischen Daten auf die Definition in Art. 3 lit. l des GUMG.[192] Dies ist ein Hinweis darauf, dass es dem Willen des Gesetzgebers entspricht, den Begriff «genetische Daten» in Art. 3 lit. a Ziff. 3 nDSG gleich auszulegen wie in Art. 3 lit. l GUMG. Mehrere Voten in der Ratsdebatte bestätigen dies. Die Bezüge zur Verwendung des Begriffs im Bereich der «Life Science[s]» wurden in der Ratsdebatte erkannt.[193] In der Debatte wurde der Begriff zudem mit Bezügen auf die Gesundheit einer natürlichen Person («Gesundheitszustand»[194], «Gesundheitsdaten»[195], «Gendefekte»[196], «medizinische Prädispositionen»[197]) erläutert. Entsprechend sollten rechtsanwendende Schweizer Behörden ausserhalb des Schengen-Bereichs den Begriff der «genetischen Daten» in Übereinstimmung mit der Praxis zum GUMG interpretieren und die Praxis zur DSGVO in diesem Bereich nur zur Plausibilisierung (Bestätigung) des Auslegungsresultats beiziehen.

---

[192] Botschaft E-DSG (FN 3), 7020.

[193] Votum Silberschmid, AB 2020 N 142; vgl. auch Votum Flach, AB 2020 N 139.

[194] Votum Flach, AB 2020 N 146.

[195] Votum BR Keller-Sutter, AB 2020 N 146.

[196] Votum BR Keller-Sutter, AB 2020 N 146.

[197] Votum Flach, AB 2020 N 146.

Bei den «biometrische[n] Daten» ist bei der Auslegung methodisch ebenfalls zwischen Schengen-relevanter Datenbearbeitung und Datenbearbeitungen in anderen Bereichen zu unterscheiden. Allerdings verweisen diesbezüglich weder der Bundesrat noch das Parlament auf eine Definition in einem anderen Schweizer Gesetz. Vielmehr übernimmt der Bundesrat für seine Umschreibung des Begriffs in der Botschaft E-DSG im Wesentlichen die Begriffsdefinition in der Richtlinie (EU) 2016/680 bzw. in der DSGVO.[198] Dies spricht dafür, den Begriff im gesamten Anwendungsbereich des nDSG europarechtskonform unter Berücksichtigung der Definition in der Richtlinie (EU) 2016/680 auszulegen. Allerdings ist ausserhalb des Schengen-Bereichs grössere Zurückhaltung angezeigt als bei der Berücksichtigung der Praxis der EU-Behörden. Denn dort handelt es sich nicht um eine Umsetzung von EU-Recht.

c. Folgerungen für die Auslegung der Begriffe im nDSG

Aus dem Vorstehenden resultiert das Folgende für den Einfluss der EU-Praxis auf die Auslegung der Begriffe «genetische Daten» und «biometrische Daten»:

– Die Begriffe «genetische Daten» und «biometrische Daten» sind im Schengen-Bereich europarechtskonform, mithin richtlinienkonform auszulegen. Entsprechend sind die Begriffe im nDSG für diesen Bereich wie in der Richtlinie (EU) 2016/680 definiert auszulegen.

– Die Praxis der EU-Behörden zur Auslegung der Begriffe «genetische Daten» und «biometrische Daten» ist für die Schweizer Behörden auch im Schengen-Bereich nicht verbindlich, ist aber eine sehr bedeutende Auslegungshilfe – sie ist schon im Sinne einer staatsvertragskonformen bzw. richtlinienkonformen Auslegung mehr als nur zur Plausibilisierung einer auf der Grundlage der Begriffsdefinition gefundenen (Schweizer) Auslegung zu berücksichtigen.

---

[198] Botschaft E-DSG (FN 3), 7020 («Unter biometrischen Daten sind hier Personendaten zu verstehen, die durch ein *spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen*. Es handelt sich dabei beispielsweise um einen digitalen Fingerabdruck, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme. Diese Daten müssen zwingend auf einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt. Dies ist beispielsweise grundsätzlich nicht der Fall bei gewöhnlichen Fotografien»; Hervorhebung hinzugefügt).

– Ausserhalb des Schengen-Bereichs (ausserhalb der polizeilichen Zusammenarbeit und der Strafverfolgung, namentlich bei der Datenbearbeitung durch Private) besteht kein Raum für eine europarechtskonforme bzw. richtlinienkonforme Auslegung. Die EU-Praxis ist aber immerhin zur Orientierung zu berücksichtigen.
– Für die Auslegung des Begriffs «genetische Daten» ist ausserhalb des Schengen-Bereichs die Anwendung der Begriffsdefinition im GUMG für die Schweizer Behörden verbindlich. Auch im Schengen-Bereich ist sie aber mitzuberücksichtigen.

3. Rechtsgrundlagen und Rechtfertigungsgründe

a. Regelung im Gesetz

Die DSGVO und das nDSG enthalten die folgenden Bestimmungen zu Rechtsgrundlagen bzw. Rechtfertigungsgründen:[199]

Art. 6 DSGVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a. Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b. die Verarbeitung ist für die **Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist**, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c. die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** [aus EU oder EU-Mitgliedsstaatsrecht] erforderlich, der der Verantwortliche unterliegt;

d. die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im **öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt** erfolgt, die dem Verantwortlichen übertragen wurde;

[199] Hervorhebungen hinzugefügt.

f. die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten** erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Art. 31 nDSG

(1) Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch **Einwilligung** der betroffenen Person, durch ein **überwiegendes privates oder öffentliches Interesse** oder durch **Gesetz** *gerechtfertigt* ist.

(2) Ein überwiegendes Interesse des Verantwortlichen fällt insbesondere in folgenden Fällen in Betracht:

a. Der Verantwortliche bearbeitet die Personendaten über die Vertragspartnerin oder den Vertragspartner in **unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags**

[Im Unterschied zur Regelung in Art. 6 DSGVO (Buchstabe a) nennt das nDSG die Notwendigkeit zur Vertragserfüllung nicht als separaten Rechtfertigungsgrund, sondern als ein Beispiel eines (möglicherweise) überwiegenden Interesses des Verantwortlichen.]

b. Der Verantwortliche steht mit einer anderen Person in wirtschaftlichem Wettbewerb oder wird in wirtschaftlichen Wettbewerb treten und bearbeitet zu diesem Zweck Personendaten, die Dritten nicht bekanntgegeben werden; nicht als Dritte im Rahmen dieser Bestimmung gelten Unternehmen, die zum selben Konzern gehören wie der Verantwortliche.

c. Der Verantwortliche bearbeitet Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person, wobei die folgenden Voraussetzungen erfüllt sind: […]

d. Der Verantwortliche bearbeitet die Personendaten beruflich und ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums oder die Daten dienen ihm, falls keine Veröffentlichung erfolgt, ausschliesslich als persönliches Arbeitsinstrument.

e. Der Verantwortliche bearbeitet die Personendaten für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung oder Statistik, wobei die folgenden Voraussetzungen erfüllt sind: […]

f. Der Verantwortliche sammelt Personendaten über eine Person des öffentlichen Lebens, die sich auf das Wirken dieser Person in der Öffentlichkeit beziehen.

Art. 34 nDSG

(1) Bundesorgane dürfen Personendaten nur bearbeiten, wenn dafür eine **gesetzliche Grundlage** besteht.

(4) In Abweichung von den Absätzen 1–3 dürfen Bundesorgane Personendaten bearbeiten, wenn eine der folgenden Voraussetzungen erfüllt ist:

a. Der **Bundesrat hat die Bearbeitung bewilligt**, weil er die Rechte der betroffenen Person für nicht gefährdet hält.

b. Die betroffene Person hat **im Einzelfall in die Bearbeitung eingewilligt** oder hat ihre Personendaten **allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt**.

c. Die Bearbeitung ist **notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen**, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.

b. Analyse

DSGVO und nDSG folgen im Bereich der Datenbearbeitung durch private Verantwortliche **unterschiedlichen Regelungskonzepten**:

– *Ausgangslage unter der DSGVO:* Jegliche (von der DSGVO erfasste[200]) Verarbeitung personenbezogener Daten ist **grundsätzlich verboten**. Die Datenverarbeitung ist aber erlaubt, wenn mindestens einer der in Art. 6 Abs. 1 DSGVO aufgeführten Erlaubnistatbestände erfüllt ist, wenn also eine **Rechtsgrundlage** besteht (sog. Verbotsprinzip mit Erlaubnisvorbehalt[201]). Die Rechtsgrundlagen sind im Bereich der Verarbeitung durch Private ein Korrektiv dafür, dass das Verbotsprinzip auch für private Verantwortliche (also nicht nur für die Verarbeitung durch Behörden) gilt.[202]

---

[200] Jede ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten und die Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 2 DSGVO).

[201] Buchner/ Petri, DS-GVO BDSG (FN 171), Art. 6 N 1 und 11; Sebastian Schulz, in: Peter Gola, Datenschutz-Grundverordnung VO (EU) 2016/679, Kommentar, 2. A., München 2018 (zit. VerfasserIn, DS-GVO), Art. 6 N 2; Oxford Commentary GDPR–Kotschy (FN 171), Art. 6, 325.

[202] Schulz, DS-GVO (FN 201), Art. 6 N 3.

Verantwortliche müssen im Einzelfall aufzeigen können, dass für die in Frage stehende Datenverarbeitung mindestens eine der Rechtsgrundlagen gilt.[203] Die Auflistung der Rechtsgrundlagen in Art. 6 Abs. 1 DSGVO ist abschliessend.[204] Es gibt keine Rangfolge unter den Rechtsgrundlagen in dem Sinne, dass gewisse Rechtsgrundlagen prioritär zu wählen wären.[205]

– *Ausgangslage im nDSG* im Bereich der *Bearbeitung durch private Verantwortliche:* Die Bearbeitung von Personendaten ist **grundsätzlich erlaubt** (keine Rechtsgrundlage erforderlich). Die Bearbeitung ist nur dann verboten, wenn sie **die Persönlichkeit der betroffenen Person widerrechtlich verletzt** (Art. 30 Abs. 1 nDSG).[206] Anders als in der Konzeption der DSGVO stellt die Bearbeitung von Personendaten unter dem DSG und dem nDSG somit allein noch keine Persönlichkeitsverletzung dar. Umgekehrt bedeutet dies, dass der private Verantwortliche – anders als unter der DSGVO – nicht für jede Datenbearbeitung darlegen muss, dass eine Rechtsgrundlage oder Rechtfertigung vorliegt. Nur wenn die Datenbearbeitung im Einzelfall die Persönlichkeit verletzt, muss geprüft werden, ob die Persönlichkeitsverletzung allenfalls gerechtfertigt und somit nicht widerrechtlich ist.[207]

– Eine **Persönlichkeitsverletzung** liegt gemäss Art. 30 Abs. 2 nDSG insbesondere vor, wenn der Verantwortliche (i) sich nicht an die Bearbeitungsgrundsätze nach Art. 6 (Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckbindung, Datenminimierung, Speicherbegrenzung, Richtigkeit) und 8 (Datensicherheit) nDSG hält, (ii) Personendaten wei-

---

[203] Vgl. Oxford Commentary GDPR–Kotschy (FN 171), Art. 6, 329.

[204] Buchner/Petri, DS-GVO BDSG (FN 171), Art. 6 N 1; Oxford Commentary GDPR–Kotschy (FN 171), Art. 6, 329.

[205] Oxford Commentary GDPR–Kotschy (FN 171), 329.

[206] Corrado Rampini, in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ), Basler Kommentar. 3. A., Basel 2014 (zit. BSK DSG–VerfasserIn), Vorbemerkungen zu Art. 12–15 N 4.

[207] David Rosenthal, in: David Rosenthal/Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich 2008 (zit. VerfasserIn, Handkommentar), Art. 12, N 1; Rosenthal (FN 178), N 7; BSK DSG–Rampini (FN 206), Art. 13 N 1; BGE 136 II 508 E. 6.3.2. Nicht zutreffend ist daher die zuweilen vom EDÖB vertretene Auffassung, wonach jede Datenbearbeitung einer Rechtfertigung bedarf – so z.B. EDÖB, Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz. Für die Privatwirtschaft, September 2013, 5; und EDÖB, Kundenbindungsprogramm Supercard. Schlussbericht (überarbeitet), 14.12.2015, 8.

terbearbeitet, nachdem die betroffene Person ausdrücklich zum Ausdruck gebracht hat, dass sie dies nicht (mehr) möchte (z.B. eine Einschränkung der Bearbeitung oder Löschung der Personendaten verlangt), oder wenn (iii) der Verantwortliche besonders schützenswerte Personendaten an einen Dritten (Auftragsbearbeiter sind keine Dritte in diesem Sinne) *weitergibt*.

– Persönlichkeitsverletzungen nach Art. 30 nDSG sind jedoch nur dann widerrechtlich, wenn kein **Rechtfertigungsgrund** (Art. 31 nDSG) vorliegt. Dieses Regelungskonzept (Art. 30–31 nDSG) **übernimmt das nDSG von Art. 12–13 DSG**.[208] Art. 31 Abs. 1 nDSG (derzeit Art. 13 Abs. 1 DSG) ist somit das **Pendant zum Konzept des Art. 28 Abs. 2 ZGB**, wonach eine Persönlichkeitsverletzung nur dann widerrechtlich ist, wenn sie nicht durch Einwilligung des Verletzten, ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.[209]

– *Im öffentlichen Bereich (Bearbeitung durch Bundesorgane)* gilt das **Legalitätsprinzip** (Art. 5 Abs. 1 BV). Bundesorgane müssen sicherstellen, dass sie Personendaten nur basierend auf einer Grundlage im Gesetz (**Rechtsgrundlage**) bearbeiten (Art. 34 nDSG).[210]

– Für einige Datenbearbeitungen ergibt sich die Rechtsgrundlage direkt aus dem **nDSG** (vgl. Art. 35–39). In der Regel stützt sich die Bearbeitung von Personendaten durch Bundesorgane hingegen **direkt** (Ermächtigung in einer spezialgesetzlichen Norm[211]) oder **indirekt** (Notwendigkeit zur Erfüllung einer gesetzlich festgelegten Aufgabe[212]) auf eine Grundlage aus

---

[208] Rosenthal (FN 178), N 7.

[209] BGE 136 II 508 E. 6.3.2 («Art. 13. Abs. 1 DSG übernimmt in diesem Sinne den in Art. 28 Abs. 2 ZGB verankerten Grundsatz»); BSK DSG–Rampini (FN 206), Art. 12 N. 1. Vgl. auch Botschaft E-DSG (FN 3), 7070 («Die Vorschriften zum Bearbeiten von Personendaten durch private Personen konkretisieren den Schutz der Persönlichkeit nach Art. 28 ZGB in Bezug auf den Datenschutz. […] Artikel 26 E-DSG [Art. 30 nDSG] konkretisiert Persönlichkeitsverletzungen im Bereich des Datenschutzes, Art. 27 E-DSG [Art. 31 nDSG] definiert spezifische Rechtfertigungsgründe»).

[210] Vgl. BSK DSG–Ballenegger (FN 206), Art. 17 N 1–4; Jöhri, Handkommentar DSG (FN 207), Art. 17 N 1–3.

[211] Vgl. BSK DSG–Ballenegger (FN 206), Art. 17 N 3 und 6–7; Jöhri, Handkommentar DSG (FN 207), Art. 17 N 4 und 8–10.

[212] Vgl. BSK DSG–Ballenegger (FN 206), Art. 17 N 26–27; Jöhri, Handkommentar DSG (FN 207), Art. 17 N 76–77.

einem **anderen Bundesgesetz** oder (ausser bei besonders schützenswerten Personendaten) aus einer Verordnung[213] des Bundes.

c. Folgerungen für die Auslegung von Art. 31 nDSG

i. Bewusstes Abweichen vom Regelungskonzept der DSGVO – keine europarechtskonforme Auslegung

Die Wahl eines Regelungskonzepts, das sich wesentlich vom Regelungsansatz der DSGVO unterscheidet, **entspricht dem Willen des Schweizer Gesetzgebers**. Instruktiv hierzu ist das folgende Votum von Nationalrat Balthasar Glättli in der Herbstsession 2020:[214]

> «[…] vor Augen führen, dass die beiden Gesetzeswerke, die EU-Datenschutz-Grundverordnung einerseits und das schweizerische Datenschutzgesetz andererseits, deren Äquivalenz ja nun hergestellt werden soll – […] einen **völlig unterschiedlichen Ansatz** haben. Bei der EU-Datenschutz-Grundverordnung gilt grundsätzlich jede Verarbeitung von personenbezogenen Daten als rechtswidrig. Sie ist also nicht erlaubt, es sei denn, man kann sich auf einen Rechtsgrund stützen. […] **In der Schweiz haben wir eigentlich das umgekehrte Prinzip**. Eine Verarbeitung von Daten ist immer zulässig, es sei denn, es liegen Ausnahmetatbestände vor. Das heisst, es müssen sich zwei Rechtsordnungen irgendwo in der Mitte finden, von denen **die eine sagt, alles sei verboten, ausser […], und die andere, unsere, sagt, alles sei erlaubt, ausser […]**»

Das bewusste Abweichen vom Regelungskonzept der DSGVO bedeutet, dass die entsprechenden Regelungen im rezipierten EU-Recht sich kaum mit entsprechenden Regelungen im Schweizer Recht vergleichen lassen. Entsprechend sollten rechtsanwendende Schweizer Behörden sehr zurückhaltend sein bei Vergleichen der Rechtfertigungsgründe gemäss Art. 31 nDSG bzw. (im Behördenbereich) der Rechtsgrundlagen in Art. 34 nDSG mit den Rechtsgrundlagen gemäss Art. 6 Abs. 1 DSGVO. Die EU-Praxis zu Art. 6 Abs. 1 DSGVO sollten rechtsanwendende Schweizer Behörden somit (wenn überhaupt) **nur zur Plausibilisierung** eines autonomen Schweizer Auslegungsresultats heranziehen.[215]

---

[213] Jöhri, Handkommentar DSG (FN 207), Art. 17 N 59.

[214] Vgl. z.B. Votum Glättli AB 2020 N 1597 (Hervorhebungen hinzugefügt).

[215] Vgl. oben IV.E.1.

ii. Wesentliche Unterschiede in der Ausgestaltung der Rechtfertigungsgründe und Rechtsgrundlagen – Zurückhaltung bei der Berücksichtigung der EU-Praxis

Es bestehen wesentliche Unterschiede bei der Ausgestaltung der einzelnen Rechtfertigungsgründe in Art. 31 nDSG im Vergleich zu Art. 6 Abs. 1 DSGVO. Diese sollen Schweizer Behörden beachten:

– Der Rechtfertigungsgrund, wonach die Datenbearbeitung zur **Einhaltung eines Gesetzes** gerechtfertigt ist, bezieht sich in Art. 31 Abs. 1 nDSG auf Schweizer Gesetze und Verordnungen des Bundes und der Kantone,[216] in Art. 6 Abs. 1 lit. c DSGVO auf Gesetze der EU und der Mitgliedsstaaten,[217] denen der Verantwortliche unterliegt.

– Das nDSG (Art. 31 Abs. 1 i.V.m. Art. 6 Abs. 6 nDSG) stellt weniger strenge Anforderungen an die **Gültigkeit einer Einwilligung** als die DSGVO (Art. 6 Abs. 1 lit. a i.V.m. Art. 7 DSGVO). Art. 6 Abs. 6 nDSG übernimmt im Wesentlichen Art. 4 Abs. 5 Satz 1 DSG. Demgegenüber finden die folgenden Anforderungen von Art. 7 DSGVO an eine gültige Einwilligung **nicht** für das nDSG Anwendung:

  – Erfordernis, dass das Ersuchen um **Einwilligung** in einer *klaren und einfachen Sprache* und *getrennt von Informationen zu anderen Sachverhalten* erfolgen muss (Art. 7 Abs. 2 DSGVO); obschon es auch unter Schweizer Recht ratsam und gute Praxis ist, Einwilligungen in die Bearbeitung von Personendaten nicht zusammen mit der Einwilligung zu anderen Sachverhalten (z.B. Zustimmung zu AGB) zu verknüpfen, dürfen rechtsanwendende Schweizer Behörden Art. 6 Abs. 6 nDSG nicht europarechtskonform auslegen und solches unter Berücksichtigung von Art. 7 Abs. 2 DSGVO fordern;[218] sie können aber Art. 6 Abs. 6 nDSG da-

---

[216] BGE 138 I 331 E. 8.4; BSK DSG–Rampini (FN 206), Art. 13 N 17 und 19; Rosenthal, Handkommentar DSG (FN 207), Art. 13 N 26.

[217] Art. 6 Abs. 3 DSGVO.

[218] Entsprechend sollten rechtsanwendende Schweizer Behörden Zurückhaltung walten lassen bei der Berücksichtigung von Anforderungen an eine gültige Einwilligung, wie sie z.B. der EuGH im Urteil *Google LLC gegen Commission national de l'informatique et des libertés (CNIL)*, Rs. C-507/17, 24.09.2019 oder der EDSA in seinen Leitlinien 05/2020 zur Einwilligung gemäss Verordnung 2016/679 (Version 1.1, 04.05.2020) stellen.

hingehend – konform mit dem revidierten Übereinkommen SEV 108[219] – so auslegen, dass eine Einwilligung nur gültig ist, wenn sie *eindeutig* erfolgt, was die erwähnte Trennung eben ratsam erscheinen lässt.

– Pflicht zur *Information über das Recht, die Einwilligung jederzeit zu widerrufen*; und zwar so einfach wie es war, die Einwilligung zu erteilen (Art. 7 Abs. 3 DSGVO); Verantwortliche richten ihre Datenschutzerklärungen (freiwillig oder aus Pflicht) regelmässig am DSGVO-Standard aus. Entsprechend informieren sie über das Recht, Einwilligungen zu widerrufen. Dennoch dürfen rechtsanwendende Schweizer Behörden Art. 6 Abs. 6 nDSG nicht europarechtskonform auslegen und solches unter Berücksichtigung von Art. 7 Abs. 3 DSGVO fordern.

– Erfordernis, bei der Beurteilung der Freiwilligkeit der Einwilligung dem Umstand «grösstmöglich» Rechnung zu tragen, ob der Verantwortliche die Erfüllung eines Vertrags und die Erbringung einer Dienstleistung davon abhängig macht, dass die betroffene Person in die betreffende(n) Datenbearbeitung(en) einwilligt; rechtsanwendende Schweizer Behörden dürfen Art. 6 Abs. 6 nDSG nicht europarechtskonform auslegen und solches unter Berücksichtigung von Art. 7 Abs. 3 DSGVO fordern.

– Der Anwendungsbereich des Rechtfertigungsgrunds der **Vertragserfüllung** und der diesbezüglichen Leistungserbringung ist im nDSG (Art. 31 Abs. 2 lit. a) nicht dahingehend auszulegen, dass nur sehr eng mit der geschuldeten (Dienst-) Leistung verknüpfte Datenverarbeitungen gerechtfertigt sind. Dies gilt umso mehr, als die Vertragserfüllung im nDSG ein Anwendungsbeispiel eines privaten Interesses ist; es ist eine Interessenabwägung notwendig – wobei sich das Interesse des Verantwortlichen nicht darin erschöpft, die für die Leistungserbringung absolut notwendigen Datenbearbeitungen vorzunehmen (so

[219] Gemäss Art. 5 des revidierten Übereinkommens SEV 108 sollen Vertragsstaaten ihr Recht so ausgestalten, dass nur eine freiwillige, spezifische und eindeutige Einwilligung («free, specific, informed and *unambiguous* consent»; Hervorhebung hinzugefügt) eine gültige Einwilligung ist.

aber der Wortlaut von Art. 6 Abs. 1 lit. b DSGVO – erforderlich – und das Verständnis des EDSA).[220]

– Unter der DSGVO muss bei der Bearbeitung besonders schützenswerter Personendaten (sog. besondere Kategorien personenbezogener Daten) zusätzlich zum Vorliegen einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO eine der **Voraussetzungen von Art. 9 Abs. 2 DSGVO** erfüllt sein; weil dort nur wenige Fälle einer Vertragserfüllung aufgelistet sind, führt dies dazu, dass im Bereich der Bearbeitung besonders schützenswerter Personendaten der Anwendungsbereich der Rechtsgrundlage der Vertragserfüllung sehr eingeschränkt und häufiger die Einwilligung der betroffenen Person notwendig ist;[221] während gemäss nDSG auch ein anderer Rechtfertigungsgrund (z.B. Vertragserfüllung) für eine Weitergabe (die Bearbeitung an sich braucht in der Regel nicht gerechtfertigt zu werden) besonders schützenswerter Personendaten an Dritte in Frage kommt und in der Regel geeigneter ist.

– Unter dem nDSG (Art. 31 Abs. 1) können sich auch private Verantwortliche auf den Rechtfertigung des **überwiegenden öffentlichen Interesses** (Dritter) berufen (z.B. das Informationsbedürfnis der Öffentlichkeit[222]); demgegenüber können sich nur Behörden oder Private, denen die Wahrnehmung einer Aufgabe im öffentlichen Interesse gemäss dem Recht des jeweiligen Mitgliedsstaats *übertragen* wurde, auf die Rechtsgrundlage des öffentlichen Interesses i.S.v. Art. 6 Abs. 1 lit. e DSGVO berufen;[223] allerdings ist das Bundesgericht sehr zurückhaltend bei der Annahme eines (selbständigen) öffentlichen Interesses des privaten Verantwortlichen als Rechtfertigungsgrund – was nicht mit dem EU-Datenschutzrecht, sondern vielmehr damit zusammenhängt, dass öffentliche Interessen oft schon in gesetzlichen Regelungen umgesetzt

---

[220] EDSA, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäss Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, 08.10.2019, N 26–39; vgl. dazu Oxford Commentary GDPR–Kotschy (FN 171), Art. 6, 331 und Buchner/Petri, DS-GVO BDSG (FN 171), Art. 6 N 38–46.

[221] Oxford Commentary GDPR–Kotschy (FN 171), Art. 6, 335.

[222] BGE 132 III 641 E. 3; BGE 129 III 529 E. 3.1; Rosenthal (FN 178), N 22.

[223] Art. 6 Abs. 3 DSGVO; DSGVO-Erwägungsgrund 45; Oxford Commentary GDPR–Kotschy (FN 171), Art. 6, 335; Buchner/Petri, DS-GVO BDSG (FN 171), Art. 6 N 111 und 117.

sind oder das Gericht stark auf die privaten wirtschaftlichen Interessen des Verantwortlichen fokussiert.[224]

4. Informationspflicht bei der Beschaffung von Personendaten

a. Regelung im Gesetz

Die DSGVO, das revidierte Übereinkommen SEV 108 und das nDSG implementieren im Vergleich zum alten Recht höhere Anforderungen an die Transparenz. Dazu gehört die Pflicht, betroffene Personen bereits bei der Beschaffung bzw. nach Erhalt von Personendaten über die Beschaffung und Bearbeitung von Personendaten zu informieren. Dies soll es betroffenen Personen ermöglichen, Bearbeitungen ihrer Personendaten zu erkennen und ihre Betroffenenrechte (z.B. Recht auf Auskunft, Berichtigung oder Löschung) auszuüben.

Die Regelungen im Gesetz lauten wie folgt:[225]

Art. 13–14 DSGVO

(1) […] so teilt der Verantwortliche der betroffenen Person [Art. 13(1): zum Zeitpunkt der Erhebung dieser Daten] Folgendes mit:

a. [von Art. 13(1) und 14(1)] den **Namen** und die **Kontaktdaten des Verantwortlichen** sowie gegebenenfalls seines **Vertreters**;

b. [von Art. 13(1) und 14(1)] die Kontaktdaten **des Datenschutzbeauftragten**;

c. [von Art. 13(1) und 14 (1)] die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die **Rechtsgrundlage** für die Verarbeitung;

d. [von Art. 13(1) und Art. 14 (2) b] wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die **berechtigten Interessen**, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

---

[224] BSK DSG–Rampini (FN 206), Art. 13 N 47; BGE 138 II 346 E. 10.6.1 (*Google Street View* – öffentliches Informationsinteresse an der Nutzung von Google Street View überwiegt nicht die Interessen der auf Bildern erkennbaren Personen); BGE 136 II 508 E. 6.3.3 *Logistep* – öffentliches Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen mag die Tragweite der Persönlichkeitsverletzung durch Logistep nicht rechtfertigen).

[225] Hervorhebungen hinzugefügt.

[von Art. 14 Abs. 1] […] d)] die **Kategorien personenbezogener Daten**, die verarbeitet werden.

e. [von Art. 13(1) und 14(1)] gegebenenfalls die **Empfänger oder Kategorien von Empfängern der personenbezogenen Daten** und

f. [von Art. 13(1) und 14(1)] gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein **Drittland** oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich […]

a. [von Art. 13(2) und 14(2)] die **Dauer**, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b. [von Art. 13(2) und Art. 14 (2)(c)] das Bestehen eines **Rechts auf Auskunft** seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c. [von Art. 13(2) und Art. 14(1)(d)] wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines **Rechts, die Einwilligung jederzeit zu widerrufen**, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d. [von Art. 13(2) und Art. 14(2)(e)] das Bestehen eines **Beschwerderechts bei einer Aufsichtsbehörde**;

e. [von Art. 13(2)] ob die Bereitstellung der personenbezogenen Daten **gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich** ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte;

f. [von Art. 13(2) und Art. 14(2)(g)] das **Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling** gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

f. [von Art. 14(2)] aus welcher **Quelle** die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

Art. 13 Richtlinie (EU) 2016/680

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche der betroffenen Person zumindest die folgenden Informationen zur Verfügung stellt:

a. den **Namen** und die **Kontaktdaten des Verantwortlichen**,

b. gegebenenfalls die **Kontaktdaten des Datenschutzbeauftragten**,

c. die **Zwecke**, für die die personenbezogenen Daten verarbeitet werden,

d. [das Bestehen eines **Beschwerderechts bei einer Aufsichtsbehörde**; sowie deren Kontaktdaten]

e. das Bestehen eines **Rechts auf Auskunft und Berichtigung oder Löschung** personenbezogener Daten und Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch den Verantwortlichen.

(2) […] sehen die Mitgliedsstaaten durch Rechtsvorschriften [für besondere Fälle die Mitteilung der folgenden zusätzlichen Informationen] vor:

a. die **Rechtsgrundlage** der Verarbeitung.

b. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

c. […] gegebenenfalls die **Kategorien von Empfängern der personenbezogenen Daten**, auch der **Empfänger in Drittländern** oder in internationalen Organisationen,

d. erforderlichenfalls **weitere Informationen**, insbesondere wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben werden.

Art. 8 revidiertes Übereinkommen SEV 108 (Transparency of processing)

(1) Each Party shall provide that the controller informs data subjects of

a. his or her **identity** and **habitual residence or establishment**;

b. the **legal basis** and the **purposes** of the intended processing;

c. the **categories of personal data** processed;

d. the **recipients or categories of recipients** of the personal data, if any; and

e. the means of **exercising the rights** set out in Article 9,

as well as **any necessary additional information** in order to ensure fair and transparent processing of the personal data.

Art. 19–20 nDSG (Informationspflicht bei der Beschaffung von Personendaten)

(1) [von Art. 19] Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

(2) Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die **erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist**; er teilt ihr mindestens mit:

a. die **Identität** und die **Kontaktdaten des Verantwortlichen** [Art. 14 Abs. 3: und gegebenenfalls seiner **Vertretung**];

[Art. 10(3)(d) Der Verantwortliche veröffentlicht die **Kontaktdaten der Datenschutzberaterin** oder des Datenschutzberaters und teilt diese dem EDÖB mit.]

b. den **Bearbeitungszweck**;

c. gegebenenfalls die **Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern**, denen Personendaten bekanntgegeben werden.

(3) Werden die Daten nicht bei der betroffenen Person beschafft, so teilt er ihr zudem die **Kategorien der bearbeiteten Personendaten** mit.

(4) Werden die Personendaten ins Ausland bekanntgegeben, so teilt er der betroffenen Person auch **den Staat oder das internationale Organ** und gegebenenfalls die **Garantien** nach Artikel 16 Absatz 2 oder die Anwendung einer Ausnahme nach Artikel 17 mit.

[Art. 21(1) Informationspflicht bei einer automatisierten Einzelentscheidung] Der Verantwortliche informiert die betroffene Person über eine **Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht** und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt […]]

[Art. 20 Ausnahmen von der Informationspflicht und Einschränkungen]

b. Analyse

Art. 13 und 14 DSGVO enthalten Listen von Pflichtinformationen. Diese führen die erforderlichen Informationen *abschliessend* auf,[226] und zwar aufgeteilt (jeweils Abs. 1 und 2) in zwei Kataloge von Informationen.

Die Verteilung der Liste der Pflichtinformationen auf jeweils zwei Absätze verleitet zur Annahme, gewisse Basisinformationen seien immer mitzuteilen, weitere Informationen aber nur unter besonderen Umständen. Dies war im Ratsentwurf tatsächlich so gemeint und würde sich mit Erwägungsgrund 60 («besondere Umstände und Rahmenbedingungen») decken.[227] Eine solche Auslegung würde aber dem klaren Wortlaut von Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO widersprechen. Aus der Formulierung «[…] stellt der Verantwortliche […] folgende [weitere] Informationen zu Verfügung» ergibt sich, dass der Verantwortliche betroffenen Personen die in Abs. 2 und Abs. 1 aufgelisteten Kategorien von Informationen **unabhängig von den konkreten Umständen** gleichermassen mitteilen muss.[228]

Die Erwähnung der Notwendigkeit (Art. 13 Abs. 2 DSGVO) bzw. Erforderlichkeit (Art. 14 Abs. 2 DSGVO) zur Gewährleistung einer fairen und transparenten Verarbeitung ist vielmehr ein Hinweis darauf, dass der Gesetzgeber

---

[226] Oxford Commentary GDPR–Zanfir-Fortuna (FN 171), Art. 13, 426; Bäcker, DS-GVO BDSG (FN 171), Art. 13 N 19; Oxford Commentary GDPR–Zanfir-Fortuna (FN 171), Art. 14, 444; Bäcker, DS-GVO BDSG (FN 171), Art. 14 N 13. Zur Verwirklichung des Transparenzgebots (Art. 5 Abs. 1 DSGVO) könnten in Einzelfällen zusätzliche Informationen erforderlich sein. Dieser Fall scheint aber eher theoretisch und nicht vereinbar mit der Rechtssicherheit, die durch die Auflistung in Art. 13–14 DSGVO hergestellt werden soll.

[227] Bäcker, DS-GVO BDSG (FN 171), Art. 13 N 20.

[228] Oxford Commentary GDPR–Zanfir-Fortuna (FN 171), Art. 13, 428; Bäcker, DS-GVO BDSG (FN 171), Art. 13 N 20; Oxford Commentary GDPR–Zanfir-Fortuna (FN 171), Art. 14, 444; Bäcker, DS-GVO BDSG (FN 171), Art. 14 N 13.

diese Informationen namentlich hinsichtlich der Fairness und Transparenz für notwendig bzw. erforderlich hält.[229]

Im Unterschied zu Art. 13–14 DSGVO unterscheidet *Art. 13 der Richtlinie (EU) 2016/680* klar zwischen **Basisinformationen** (Abs. 1) und nur «in besonderen Fällen» mitzuteilenden **Zusatzinformationen** (Abs. 2).

Art. 8 Abs. 1 des revidierten Übereinkommens SEV 108[230] und *Art. 19 Abs. 2 nDSG* implementieren ein **anderes Konzept**. Beide Rechtsakte statuieren einen **Katalog von Mindestinformationen** und ergänzen diesen mit einer **Generalklausel**. Die Mindestinformationen sind immer mitzuteilen, weitere Informationen (Generalklausel) hingegen nur, wenn es für die Wahrnehmung der Betroffenenrechte und zur Gewährleistung einer transparenten Bearbeitung erforderlich ist.

Mit diesem Konzept folgt der Gesetzgeber einer *etablierten Schweizer Rechtsetzungsmethode*, mit allgemeinen Grundsätzen zu arbeiten und diese mit Beispieltatbeständen[231] oder Mindestanforderungen[232] zu ergänzen, welche die allgemeinen Grundsätze konkretisieren.[233]

Bereits unter dem geltenden DSG besteht eine Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 14 DSG). Auch in Bezug auf allgemeine Personendaten besteht (indirekt) eine Informationspflicht für den Fall, dass nur eine vorgängige oder nachträgliche Information eine faire (Art. 4 Abs. 2 DSG; Treu und Glauben) und transparente bzw. erkennbare (Art. 4 Abs. 4 Abs. 4 DSG) Datenbearbeitung sicherstellen kann. Für Bundesbehörden gelten gemäss Art. 18 DSG bei systematischen Erhebungen und gemäss Art. 18a DSG generell für die Beschaffung jeglicher Arten von Personendaten weitergehende Informations-

---

[229] Oxford Commentary GDPR–Zanfir-Fortuna (FN 171), Art. 13, 428.

[230] «[…] as well as any necessary additional information in order to ensure fair and transparent processing of the personal data» (Art. 8 Abs. 1 letzter Teilsatz des revidierten Übereinkommens SEV 108).

[231] Vgl. z.B. die Generalklausel in Art. 2 UWG, ergänzt durch Beispiele unlauteren Verhaltens in Art. 3 UWG; Art. 7 Abs. 1 KG, ergänzt durch Beispiele missbräuchlichen Verhaltens marktbeherrschender Unternehmen in Art. 7 Abs. 2.

[232] Vgl. z.B. Art. 10a Abs. 2 DSG.

[233] Botschaft E-DSG (FN 3), 7051.

pflichten.[234] Art. 19 nDSG führt die Art. 14, 18 und 18a DSG in einer Norm zusammen[235] und schafft eine einheitliche Regelung, die für Bundesbehörden wie auch für private Verantwortliche gilt.[236]

Art. 19 Abs. 2–4 nDSG statuiert die meisten der Pflichtinformationen gemäss Art. 8 des revidierten Übereinkommens SEV 108 als Mindestinformationen. Es bestehen drei Abweichungen.

Die erste Abweichung – Angabe nur des Bearbeitungszwecks anstelle von Rechtsgrundlage und Bearbeitungszweck[237] – von der Bestimmung im revidierten Übereinkommen SEV 108 ergibt sich daraus, dass das nDSG für die Datenbearbeitung durch private Verantwortliche keine Rechtsgrundlage verlangt.[238] Die zweite Abweichung besteht darin, dass gemäss Art. 19 Abs. 3 nDSG (im Gegensatz zu Art. 8 Abs. 1 lit. c des revidierten Übereinkommens SEV 108) die Angabe der Kategorien der bearbeiteten Personendaten nur erforderlich ist, wenn die Personendaten nicht bei der betroffenen Person beschafft werden.

Schliesslich (dritte Abweichung) verlangt Art. 8 Abs. 1 lit. e des revidierten Übereinkommens SEV 108, dass Verantwortliche die betroffenen Personen darüber aufklären, wie sie ihre Betroffenenrechte ausüben können. Eine solche Pflicht zur Aufklärung über Betroffenenrechte ist im Katalog der Mindestinformationen gemäss Art. 19 Abs. 2–4 nDSG nicht enthalten. Der Nationalrat hatte es abgelehnt, eine vom Ständerat vorgeschlagene Liste von Betroffe-

---

234 Im Vergleich zu Art. 14 DSG schreiben Abs. 2 lit. d (Information über das Auskunftsrecht) und Abs. 2 lit. e (Folgen einer Weigerung der betroffenen Person, die verlangten Personendaten anzugeben) von Art. 18a DSG für Bundesbehörden weitere Mindestinformationen vor.

235 Im Vergleich zu Art. 14 Abs. 2 lit. c, Art. 18a Abs. 2 lit. c und Art. 18 DSG (Kategorien von Datenempfängern) kann der Verantwortliche gemäss Art. 19 Abs. 2 lit. c nDSG wählen, ob er die Empfängerinnen namentlich nennen oder nur Kategorien von Empfängerinnen angeben möchte.

236 Botschaft E-DSG (FN 3), 7050. Allerdings enthält Art. 19 nDSG nicht mehr explizit die in Bezug auf Bundesbehörden unter Art. 18 DSG bei systematischen Erhebungen geltende Pflicht, die Rechtsgrundlage der Bearbeitung bekannt zu geben.

237 «[T]he legal basis and the purposes of the intended processing» (Art. 8 Abs. 1 lit. b des revidierten Übereinkommens SEV 108); «den Bearbeitungszweck» (Art. 19 Abs. 2 lit. b nDSG).

238 Vgl. oben V.B.3.b.

nenrechten als Mindestinformation in Art. 19 Abs. 2 nDSG aufzunehmen.[239] Allerdings ergibt sich die Pflicht darüber aufzuklären, *wie* eine betroffene Person ihre Rechte wahrnehmen kann, zumindest implizit aus dem ersten Teil der Generalklausel in Art. 19 Abs. 2 nDSG. Demnach muss der Verantwortliche Informationen mitteilen, «die erforderlich sind, damit sie [die betroffene Person] ihre Rechte nach diesem Gesetz [nDSG] geltend machen kann […]»).[240]

Art. 18a DSG ist seit dem 1. Dezember 2010 in Kraft. Die Bestimmung wurde im Rahmen der Vorgängerregelung[241] zur der Richtlinie (EU) 2016/680 (Rahmenbeschluss 2008/977/JI) eingeführt.[242] Insofern als Art. 19 nDSG Art. 18a DSG integriert, handelt es sich somit – im *Schengen-relevanten Bereich* – bei Art. 19 nDSG auch um eine zur **Umsetzung der Richtlinie (EU) 2016/680** erforderliche Regelung.[243]

Ausserhalb des Schengen-Bereichs und namentlich im Bereich der Bearbeitung durch private Verantwortliche handelt es sich bei Art. 19 nDSG aber um eine Umsetzung der Anforderungen gemäss Art. 8 des revidierten Übereinkommens SEV 108.[244] Der Gesetzgeber baut in Art. 19 nDSG auf der Regelung in Art. 14 DSG auf und ergänzt sie mit weiteren Pflichtinformationen gemäss **Vorgaben des revidierten Übereinkommens SEV 108**.

Dieses Analyseergebnis deckt sich mit den Aussagen des Bundesrats in der Botschaft E-DSG, wonach Art. 17 E-DSG (Art. 19 nDSG) Anforderungen des Art. 7bis E-SEV 108 (Art. 8 revidiertes Übereinkommen SEV 108) und

---

239 AB 2020 N 152 (Ablehnung der lit. d und e von Art. 17 Abs. 2 E-DSG im Nationalrat). Vgl. Votum Jauslin, AB 2020 N 149.

240 Im Vergleich zu Art. 14 Abs. 2 lit. c, Art. 18a Abs. 2 lit. c und Art. 18 DSG (Kategorien von Datenempfängern) kann der Verantwortliche gemäss Art. 19 Abs. 2 lit. c nDSG wählen, ob er die Empfängerinnen namentlich nennen oder nur Kategorien von Empfängerinnen angeben möchte.

241 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350, 30.12.2008, 60

242 Ziff. 3 des Bundesgesetzes über die Umsetzung des Rahmenbeschlusses 2008/977/JI über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.

243 So auch: Botschaft E-DSG (FN 3), 7050.

244 Vgl. z.B. Votum BR Keller-Sutter, AB 2019 N 1805; Votum BR Keller-Sutter, AB 2020 N 147.

des Art. 13 der Richtlinie (EU) 2016/680 entspreche. Nur ergänzend weist der Bundesrat in diesem Zusammenhang darauf hin, dass die Art. 13–14 DSGVO «eine ähnliche Regelung» enthalten.[245] Diese Formulierung («ähnliche Regelung») verdeutlicht, dass der Bundesrat auch in diesem Punkt keine Übernahme der DSGVO-Regelung, sondern eine vom Konzept der DSGVO abweichende, eigene **Schweizer Lösung** vorschlug.

Ziel war es, eine *flexibel handhabbare Informationspflicht* zu schaffen. Die Bestimmung soll es Verantwortlichen ermöglichen, je nach Kategorie der bearbeiteten Personendaten sowie Art und Umfang der Datenbearbeitung unterschiedlich ausführlich und detailliert zu informieren.[246] Insofern lässt die Regelung in **Art. 19 nDSG einen risikobasierten Ansatz** zu.

Dies kontrastiert stark mit der Regelung in Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO. Diese sehen (wie oben erwähnt) gerade nicht vor, dass die dort aufgelisteten Informationen nur bei besonderem Bedarf mitzuteilen wären. Also lassen **Art. 13–14 DSGVO keine risikobasierte Anwendung** zu – ganz im Gegensatz zu Art. 19 nDSG.[247]

Voten in der Ratsdebatte bestätigen, dass der Gesetzgeber mit Art. 19 nDSG eine flexible, vom Konzept der DSGVO abweichende, den Anforderungen des revidierten Übereinkommens SEV 108 genügende und mit den Anforderungen des EU-Rechts «kompatib[le]» Regelung der Informationspflicht einführen wollte.[248]

c. Folgerungen für die Auslegung von Art. 19 nDSG

Es liegt *in der Unternehmenspraxis* nahe, die Einhaltung der Generalklausel von Art. 19 Abs. 2 nDSG dadurch sicherzustellen, dass Datenschutzerklärungen nach nDSG nebst den Mindestinformationen weitere Angaben enthalten, die Art. 13–14 DSGVO (im Unterschied zu Art. 19 Abs. 2–4 nDSG) als Pflichtinformationen auflisten. Ohnehin werden Verantwortliche, für deren Datenbearbeitungen sowohl die Vorgaben der DSGVO als auch jene des

---

[245] Botschaft E-DSG (FN 3), 7050.

[246] Botschaft E-DSG (FN 3), 7051.

[247] Gl.M. Bäcker, DS-GVO BDSG (FN 171), Art. 13 N 20.

[248] Votum Noser, AB 2020 S 292 («auch mit den EU-Datenschutzvorgaben kompatibel»). Vgl. Votum BR Keller-Sutter, AB 2019 N 1805; Votum BR Keller-Sutter, AB 2020 N 147.

nDSG gelten, sämtliche Pflichtinformationen gemäss Art. 13–14 DSGVO in die Datenschutzerklärung aufnehmen und diese mit (Swiss-Finish) Angaben zu Empfängerstaaten (oder zumindest einer Umschreibung, z.B. Europa oder weltweit) ergänzen.

Dennoch: Art. 19 nDSG übernimmt nicht Art. 13–14 DSGVO, sondern implementiert eine **bewusst vom Konzept der DSGVO abweichende Schweizer Lösung**. Die Bestimmung lässt daher eine europarechtskonforme Auslegung nicht zu. Infolgedessen dürfen rechtsanwendende Schweizer Behörden aus der in der Unternehmenspraxis zu erwartenden Angleichung des nDSG an die DSGVO im Bereich der Datenschutzerklärungen nicht folgern, die ergänzenden Angaben aus Art. 13–14 DSGVO seien in jedem Fall erforderlich (Pflichtinformation), um im Sinne der Generalklausel von Art. 19 Abs. 2 nDSG eine transparente Datenbearbeitung zu gewährleisten. Ohne besondere Umstände (z.B. hohes Risiko für Betroffene) werden die in Abs. 2 aufgelisteten Mindestangaben in der Regel genügen, um Transparenz im Sinne der Generalklausel herzustellen.[249] Wenn überhaupt, so dürfen rechtsanwendende Schweizer Behörden die EU-Praxis zu Art. 13–14 DSGVO **nur zur Bestätigung** (Plausibilisierung) eines autonomen Schweizer Auslegungsresultats heranziehen.[250]

5. Recht auf Datenherausgabe oder -übertragung

a. Regelung im Gesetz

DSGVO und nDSG führen beide ein Recht auf Datenherausgabe oder -übertragung (sog. Datenübertragbarkeit oder Datenportabilität) ein.

Die Regelungen im Gesetz lauten wie folgt:[251]

[249] So auch Rosenthal (FN 178), N 98.

[250] Vgl. oben IV.E.1. Zur wichtigen Unterscheidung zwischen Unternehmenspraxis und Behördenpraxis bei der Anwendung des nDSG im Lichte der DSGVO – namentlich bei der Anwendung von Informationspflichten – vgl. auch Rosenthal (FN 178), N 11.

[251] Hervorhebungen hinzugefügt.

Art. 20 DSGVO

(1) Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen **bereitgestellt** hat, **in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten**, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern:

a. die Verarbeitung auf einer **Einwilligung** gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a oder auf einem **Vertrag** gemäß Artikel 6 Absatz 1 Buchstabe b beruht und

b. die Verarbeitung mithilfe **automatisierter Verfahren** erfolgt.

(2) Bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Absatz 1 hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten **direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist**.

(3) Die Ausübung des Rechts nach Absatz 1 des vorliegenden Artikels lässt Artikel 17 unberührt. Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

(4) [Ausnahme]

Art. 28 nDSG

(1) Jede Person kann vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm **bekanntgegeben** hat, in einem gängigen elektronischen Format verlangen, wenn:

a. der Verantwortliche die Daten **automatisiert bearbeitet**; und

b. die Daten mit der **Einwilligung** der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines **Vertrags** zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden.

(2) Die betroffene Person kann zudem vom Verantwortlichen verlangen, dass er ihre Personendaten **einem anderen Verantwortlichen überträgt**, wenn die Voraussetzungen nach Absatz 1 erfüllt sind und dies **keinen unverhältnismässigen Aufwand erfordert**.

(4) [Kostenlosigkeit]

[Art. 29 Einschränkungen des Rechts auf Datenherausgabe oder -übertragung]

b. Analyse

i. Einführung des Datenportabilitäts-Rechts in SPK-N und Nationalrat

Das Recht auf Datenherausgabe oder -übertragung (hier auch Datenportabilität genannt) fand erst im Laufe der Beratungen in SPK und Parlament Eingang ins nDSG. Der Bundesrat hingegen hatte im VE-DSG wie auch im E-DSG auf die Einführung dieses neuen Betroffenenrechts verzichtet, weil es in erster Linie wettbewerbspolitische Ziele verfolge, einem Konsumentenanliegen entspreche und nicht (oder nur indirekt) dem Schutz der Persönlichkeit betroffener Personen diene.[252]

In der Vernehmlassung bedauerten Konsumentenschutzorganisationen, die Grünliberale Partei (GLP), die Sozialdemokratische Partei (SP) und eine grosse Anzahl Kantone den Verzicht auf die Einführung des Rechts auf Datenherausgabe oder -übertragung.[253] Auch der EDÖB hätte die Einführung dieses neuen Betroffenenrechts begrüsst.[254] Der Bundesrat aber hielt im E-DSG an seinem Entscheid fest, auf die Einführung dieses neuen Betroffenenrechts zu verzichten. Er wollte «die Ergebnisse der Erfahrungen innerhalb der Europäischen Union abwarten, bevor die Einführung eines Rechts auf Datenportabilität in Betracht gezogen»[255] werde. Die Frage werde auch im Rahmen der Strategie «Digitale Schweiz» weiter geprüft.[256]

Im Parlament wollte dann aber eine Mehrheit ein Datenportabilitäts-Recht ins nDSG aufnehmen. Federführend war der Nationalrat. Auf entsprechende Anträge in der SPK-N hin erarbeitete das EJPD einen Vorschlag (Art. 25a E-DSG[257]). Dieser war näher an der Regelung in der DSGVO (Art. 20) als die in die SPK-N eingebrachten Vorschläge. Letztere hatten gefordert, den

---

[252] «[N]ach Auffassung des Bundesrats ist dieses Recht mehr darauf ausgerichtet, den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen, um den Wettbewerb spielen zu lassen, als ihre Persönlichkeit zu schützen» (EJPD, Erläuternder Bericht VE-DSG, 22).

[253] Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz. Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens, 10.08.2017, Ziff. 5.3.2.

[254] Vgl. Botschaft E-DSG (FN 3), 6985.

[255] Botschaft E-DSG (FN 3), 6984–6985.

[256] Botschaft E-DSG (FN 3), 6984–6985.

[257] Siehe AB 2019 N 1819. Entspricht der Fassung in Art. 26 nDSG.

Anspruch auf Datenportabilität auf jegliche vom Verantwortlichen gespeicherten und verarbeiteten Personendaten über die Antragstellerin auszudehnen.[258] Demgegenüber erfasste der Vorschlag des EJPD – entsprechend der Regelung in Art. 20 DSGVO – nur von der betroffenen Person an den Verantwortlichen bekanntgegebene Personendaten.

ii. Ausgestaltung des Gegenstands der Datenherausgabe oder -übertragung nach Vorbild der DSGVO

Bundesrätin *Keller-Sutter* stellte in der Ratsdebatte klar, dass mit bekanntgegebenen Personendaten nicht nur von der Antragstellerin *überlassene* Personendaten, sondern auch vom Verantwortlichen *beobachtete* Personendaten gemeint sind. Nicht erfasst seien indes Personendaten, die aus «grösseren Datenanalysen oder aus Auswertungen», mithin aus «Eigenleistung» des Verantwortlichen entstehen.[259] Die Justizministerin bezog sich mit dieser Verdeutlichung des Anwendungsbereichs von Art. 28 nDSG auf das Verständnis zum Anwendungsbereich von Art. 20 DSGVO.[260]

Nach herrschender Auffassung zu Art. 20 DSGVO erfasst auch diese Bestimmung überlassene (*provided data*) sowie beobachtete Personendaten (*observed data*)[261], nicht aber vom Verantwortlichen durch Datenanalyse oder «Auswertung»[262] basierend auf den überlassenen oder beobachteten Personendaten «entwickelte»[263] oder auf andere Weise davon «abgeleitete» (*derived data*)[264] Personendaten.[265] Dies wird damit begründet, dass «Bereitstellen»

---

[258] Vgl. Protokoll der Sitzung der SPK-N vom 23. Mai 2019; Votum BR Keller-Sutter, AB 2019 N 1816; Votum Glättli, AB 2019 N 1814–1815 («ein umfassendes Recht auf Kopie», «Auskunftsrecht 2.0»,; «alle Daten, die irgendwo auf einer dieser Riesenplattformen über sie [die betroffene Person] gespeichert sind […] – also nicht nur diejenigen, die sie selbst geliefert hat, sondern auch diejenigen, die über sie errechnet wurden.»).

[259] Votum BR Keller-Sutter, AB 2019 N 1816.

[260] Gl.M. Lena Götzinger/David Vasella, Datenportabilität und ihre Umsetzung, in: SZW 1/2021, 40, 43.

[261] Oxford Commentary GDPR–Lynskey (FN 171), Art. 20, 503; Art. 29-Arbeitsgruppe, Guidelines on the right to data portability, 05.04.2017 (WP-242rev.01; bestätigt vom EDSA in seiner ersten Plenarsitzung), 10.

[262] Herbst, DS-GVO BDSG (FN 171), Art. 20 N 11 (Hervorhebung weggelassen).

[263] Oxford Commentary GDPR–Lynskey (FN 171), Art. 20, 503.

[264] Art. 29-Arbeitsgruppe (FN 261), 10.

[265] Götzinger/ Vasella (FN 260), 43.

(«provided by») im Sinne von Art. 20 Abs. 1 DSGVO «einer aktiven und wissentlichen Handlung»[266] der betroffenen Person bedarf. Beispielsweise erfasst dies auch die *von einer betroffenen Person* bei der Nutzung einer Dienstleistung generierten und vom Verantwortlichen beobachteten Tracking- oder Messdaten (z.B. aus einem *wearable*), nicht aber von Verantwortlichen basierend darauf erstellte Auswertungen (z.B. medizinische Diagnose oder automatisiert durch technische Analyse erstellte Berichte).[267]

Auf das Erfordernis des *bewussten und aktiven Bereitstellens* bezog sich auch Bundesrätin Keller-Sutter in der Ratsdebatte.[268] Überdies wies die Justizministerin (Keller-Sutter) deutlich darauf hin, dass die Lösung der Minderheit, das neue Betroffenenrecht auf sämtliche vom Verantwortlichen über die betroffene Person bearbeiteten Personendaten auszudehnen, «über den EU-Datenschutzstandard hinausgehen» würde.[269]

Art. 20 Abs. 2 der neuen Datenschutzverordnung (**DSV**) vom 31. August 2022 verdeutlicht, dass der Anspruch auf Datenherausgabe oder -übertragung nur bereitgestellte oder beobachtete Personen erfasst, nicht aber basierend darauf erstellte eigene Auswertungen des Verantwortlichen. Abs. 1 lit. a von Art. 20 DSV wiederum enthält den Aspekt des bewussten und aktiven Bereitstellens («wissentlich und willentlich zur Verfügung stellt»).

iii. Ausgestaltung der Voraussetzungen der Datenherausgabe oder -übertragung nach Vorbild von Art. 20 DSGVO

Die Lösung der Mehrheit orientiert sich auch in den Anwendungsvoraussetzungen an Art. 20 DSGVO:

– Art. 28 Abs. 1 lit. a nDSG wie auch Art. 20 Abs. 1 lit. b DSGVO setzen für die Datenherausgabe oder -übertragung voraus, dass es sich bei den

---

[266] Piltz, DS-GVO (FN 201), Art. 120 N 14.

[267] Center for Information Policy Leadership (CIPL), Comments on the Article 29 Data Protection Working Party's «Guidelines on the Right to Data Portability» Adopted on 13 December 2016, 15.02.2017, 33; vgl. Oxford Commentary GDPR–Lynskey (FN 171), Art. 20, 503; Götzinger/Vasella (FN 260), 43; Herbst, DS-GVO BDSG (FN 171), Art. 20 N 11.

[268] Votum BR Keller-Sutter, AB 2019 N 1816 (von einer «betroffene[n] Person dem Verantwortlichen *bewusst und aktiv* zur Verfügung gestellt[e]» Personendaten).

[269] Votum BR Keller-Sutter, AB 2019 N 1816.

herausverlangten Personendaten um *automatisiert* bearbeitete Personendaten handelt.

– Art. 28 Abs. 1 lit. b nDSG wie auch Art. 20 Abs. 1 lit. a DSGVO setzen für die Datenherausgabe oder -übertragung voraus, dass der Verantwortliche die herausverlangten Personendaten entweder basierend auf der Einwilligung der betroffenen Person oder im Zusammenhang mit der Erfüllung eines Vertrags mit der betroffenen Person bearbeitet.

Aus der ersten Voraussetzung (automatisierte Bearbeitung) folgt, dass der Anspruch auf Datenportabilität nur elektronisch-digitale Personendaten erfasst, nicht aber Papieraufzeichnungen oder anonymisierte Daten.[270] Dies deckt sich mit dem Verständnis zu Art. 20 Abs. 1 lit. b DSGVO. Demnach muss es sich um personenbezogene Daten handeln. Das heisst, Art. 20 DSGVO ist nicht anwendbar, wenn der Verantwortliche die betroffene Person nicht oder nur unter Bezugnahme auf von der betroffenen Person zusätzlich bereitgestellte Informationen (re-)identifizieren kann.[271] Der Verantwortliche muss sodann auch unter Art. 20 DSGVO keine Anstrengungen unternehmen, Papieraufzeichnungen zu digitalisieren und maschinenlesbar zu machen.[272]

Auch die zweite Voraussetzung (Bearbeitung basierend auf Einwilligung oder Vertrag mit der betroffenen Person) hat der Schweizer Gesetzgeber von der Bestimmung in der DSGVO übernommen. Nach der Regelung in Art. 20 Abs. 1 lit. a DSGVO ist die *Rechtsgrundlage* der Verarbeitung der herausverlangten personenbezogenen Daten massgebend dafür, ob der Anspruch auf Herausgabe oder Übertragung besteht. Der Anspruch besteht nur, wenn der Verantwortliche die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) oder die Erfüllung eines Vertrags mit der betroffenen Person (Art. 6 Abs. 1 lit. b DSGVO) als Rechtsgrundlage für die Verarbeitung bestimmt hat.

Diese Art der Einschränkung des Datenportabilitätsrechts funktioniert im Konzept der DSGVO, weil der Verantwortliche (i) die betroffene Person vorgängig über die Rechtsgrundlage der Verarbeitung informieren muss[273] und (ii) in

---

[270] Christian Laux, Das Recht auf Datenportabilität, in: digma 2019, 166, 167.

[271] Oxford Commentary GDPR–Lynskey (FN 171), Art. 20, 503.

[272] Herbst, DS-GVO BDSG (FN 171), Art. 20 N 13.

[273] Art. 13 Abs. 1 lit. c bzw. Art. 14 Abs. 1 lit. c DSGVO.

der Lage sein muss, im Einzelfall aufzeigen zu können, dass für die in Frage stehende Datenverarbeitung mindestens eine der Rechtsgrundlagen gilt.[274]

Die in Art. 28 Abs. 1 lit. b nDSG statuierte Voraussetzung orientiert sich an Art. 20 Abs. 1 lit. a DSGVO. Die Formulierung der Voraussetzungen im nDSG ist zugleich der Versuch einer Anpassung des DSGVO-Datenportabilitätsrechts an die Konzeption des nDSG. Das nDSG verpflichtet private Verantwortliche nicht dazu, für jede Datenbearbeitung eine Rechtsgrundlage nachweisen zu können. Das Rechtfertigungskonzept von Art. 31 nDSG folgt vielmehr dem Konzept von Art. 28 Abs. 2 ZGB: Demnach braucht es nur für *persönlichkeitsverletzende Datenbearbeitungen* überhaupt eine Rechtfertigung.[275]

Nun entspricht es aber bestimmt **nicht dem Willen des Gesetzgebers, den Anspruch auf Herausgabe oder Übertragung nur bei persönlichkeitsverletzenden**, aber durch Einwilligung (Art. 31 Abs. 1 nDSG) oder Notwendigkeit zur Abwicklung eines Vertrags mit der betroffenen Person (Art. 31 Abs. 2 lit. a nDSG) gerechtfertigten **Datenbearbeitungen zu bejahen**.[276] Stattdessen ist der Hinweis auf die *Einwilligung* der betroffenen Person in Art. 28 Abs. 2 lit. b nDSG so auszulegen, dass der Herausgabe- bzw. Übertragungsanspruch für dem Verantwortlichen **freiwillig überlassene** Personendaten gilt.[277] Der Hinweis auf den unmittelbaren *Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags* mit der betroffenen Person ist so auszulegen, dass es sich bei den herausverlangten Daten um Personendaten handeln muss, welche die betroffene Person bei der Inanspruchnahme einer Dienstleistung (z.B. Nutzung einer Online-Plattform) **freiwillig und selbstbestimmt** generiert oder von der jeweiligen Dienste-Anbieterin (Verantwortlichen) im Rahmen dieser **selbstgewählten Vertragssituation** hat beobachten lassen.

Dies knüpft nahtlos an der Auslegung von «Bekanntgeben» im Sinne von Art. 28 Abs. 1 nDSG bzw. «Bereitstellen» im Sinne von Art. 20 Abs. 1 DSGVO an. Bekanntgeben erfordert gemäss Erklärungen von Bundesrätin Keller-Sutter eine *bewusste und aktive* – mithin selbstbestimmte – Handlung

---

[274] Vgl. Oxford Commentary GDPR–Kotschy (FN 171), Art. 6, 329.

[275] Vgl. oben V.B.3.b.

[276] Gl.M. Götzinger/Vasella (FN 260), 44.

[277] Gl.M. Götzinger/Vasella (FN 260), 44.

einer betroffenen Person.[278] Ähnlich impliziert Bereitstellen im Sinne von Art. 20 Abs. 1 DSGVO ein **freiwilliges, bejahendes Element**.[279]

Die Auslegung im Sinne von Freiwilligkeit und Selbstbestimmtheit folgt überdies der *ratio legis* von Art. 20 DSGVO, die informationelle Selbstbestimmung zu fördern und die betroffene Person zu ermächtigen, die Verwendung von Plattformen mit möglichst geringen Wechselkosten (*switching costs*) selbst zu bestimmen.[280] Diese *ratio legis* deckt sich mit jener von Art. 28 Abs. 1 nDSG: Es sollte ein «neues Gleichgewicht» zwischen der Macht grosser Plattformbetreiber und dem Recht der Personen hergestellt werden, «autonom» (selbstbestimmt) über die Verwendung ihrer Daten zu entscheiden.[281]

Auch Art. 20 DSV enthält die Elemente der Selbstbestimmung und des freiwilligen Überlassens (bereitgestellt oder beobachten lassen) von Personendaten. Erfasst vom Anspruch sind nämlich einerseits «wissentlich und willentlich» bereitgestellte Personendaten (Art. 20 Abs. 1 lit. a DSV) und andererseits «über die betroffene Person und ihr Verhalten im Rahmen der Nutzung eines Diensts oder Geräts» (Art. 20 Abs. 1 lit. b DSV) erhobene (bzw. beobachtete) Daten.

Bei Auslegung im Lichte der Selbstbestimmung lässt sich das Datenportabilitätsrecht nach Art. 28 Abs. 2 lit. b nDSG tatsächlich als **datenschutzrechtliches Informations- und Kontrollrecht** zum **Schutz der Persönlichkeit** denken: Eine Nutzerin eines Online-Diensts vertraut der Anbieterin des Dienstes ihre Personendaten an. Sie investiert – freiwillig und selbstbestimmt – in den Aufbau ihres Profils und bezahlt die zunehmende Personalisierung des Angebots mit Einschränkungen ihrer Privatsphäre. Entsprechend dient das Datenportabilitätsrecht auch datenschutzrechtlichen (nicht nur wettbewerbspolitischen) Zielen, nämlich dem **Schutz der Persönlichkeit vor übermässiger Bindung (Art. 27 Abs. 2 ZGB) an eine Anbieterin**, die durch Investition in den Aufbau von Profilen und die entsprechende Umständlichkeit eines Anbieterwechsels entstehen kann.

---

[278] Votum BR Keller-Sutter, AB 2019 N 1816 (von einer «betroffene[n] Person dem Verantwortlichen *bewusst und aktiv* zur Verfügung gestellt[e]» Personendaten).

[279] CIPL (FN 267), 8; vgl. Oxford Commentary GDPR–Lynskey (FN 171), Art. 20, 503.

[280] Vgl. Oxford Commentary GDPR–Lynskey (FN 171), Art. 20, 449.

[281] Votum Glättli, AB 2019 N 1815.

iv. Autonomer Nachvollzug von Art. 20 DSGVO

Insgesamt zeigt die vorstehende Analyse, dass der Gesetzgeber mit der Einführung des Rechts auf Datenherausgabe oder -übertragung gemäss Art. 28 nDSG im Wesentlichen **Art. 20 DSGVO autonom nachvollziehen wollte**. Dafür spricht zusammengefasst:

– Die Mehrheit der SPK-N stimmte einem Vorschlag des EJPD zu, der näher an der DSGVO liegt (nur bekanntgegebene Personendaten) als der Vorschlag der Minderheit (alle Personendaten).

– Dem Entwurf des EJPD (Art. 25a E-DSG) hat der Nationalrat, wie von der Mehrheit der SPK-N beantragt, zugestimmt; er entspricht dem heutigen Art. 28 nDSG.

– Der Ständerat hat dem Vorschlag des EJPD ebenfalls zugestimmt.

– Die Justizministerin verdeutlichte in ihren Erläuterungen zu Art. 25a E-DSG ein Verständnis des Anwendungsbereichs der Bestimmung (überlassene und beobachtete Daten, nicht aber abgeleitete Daten), das dem Verständnis zu Art. 20 DSGVO entspricht.

– Die Justizministerin wies in der Ratsdebatte darauf hin, dass die Lösung der Minderheit (Herausgabe aller Personendaten) über das hinausgehen würde, was Art. 20 DSGVO regelt.

– Eine vom Gesetzgeber gewollte Auslegung der Anwendungsvoraussetzungen Einwilligung oder Vertrag, die sich an der Freiwilligkeit der Bekanntgabe und der Selbstbestimmtheit (bewusst und aktiv) des Handelns der betroffenen Person orientiert, entspricht der *ratio legis* der entsprechenden Anwendungsvoraussetzungen in Art. 20 Abs. 1 lit. a DSGVO.

Im Ergebnis zeigt dies, dass der Vorschlag des Bundesrats (EJPD), dem das Parlament zustimmte, Art. 20 DSGVO in Art. 28 nDSG **übernimmt** und somit **autonom nachvollzieht**. Der Gesetzgeber entschied sich **gegen einen Swiss-Finish, mithin gegen eine eigene Schweizer Lösung** (mit Ausnahme der Anpassungen an das unterschiedliche Rechtfertigungskonzept).

c. Folgerungen für die Auslegung von Art. 28 nDSG

Art. 28 nDSG rezipiert Art. 20 DSGVO im Sinne des autonomen Nachvollzugs. Insofern ist es gerechtfertigt und es liegt nahe, Art. 28 nDSG europarechtskonform auszulegen. Dabei sind aber die Besonderheiten zu beachten, die sich aus dem **unterschiedlichen Rechtfertigungskonzept** von DSGVO und nDSG ergeben.

Art. 28 Abs. 1 lit. b nDSG sollte gerade *nicht* so ausgelegt werden, als bestünde der Anspruch nur bei Datenbearbeitungen, in die eine betroffene Person eingewilligt hat. Denn die wenigsten Datenbearbeitungen bedürfen unter dem nDSG einer Einwilligung. Vielmehr ist der Verweis auf die Einwilligung in Art. 28 Abs. 1 lit. b nDSG als Verweis auf die Freiwilligkeit der Datenbekanntgabe an den Verantwortlichen zu verstehen. Auch sollte Art. 28 Abs. 1 lit. b nDSG *nicht* dahingehend ausgelegt werden, dass alternativ zur Einwilligung ein Vertrag als Bearbeitungsgrund den Herausgabe- oder Übertragungsanspruch eröffnet. Stattdessen sollte die Nennung des Vertragszusammenhangs als Hinweis auf eine freiwillig und selbstbestimmt eingegangene Vertragsbeziehung betreffend eins von der betroffenen Person selbst gewählten Diensts (z.B. Online-Plattform) gelesen werden.

So entsteht auch die Abgrenzung zu vom Gesetz geforderten Datenerhebungen oder vom Verantwortlichen in eigenem Interesse mit Eigenleistung erhobenen oder abgeleiteten Daten, die nicht dem Herausgabe- oder Übertragungsrecht unterstehen.

6. Vereinbarung über die Auftragsbearbeitung

a. Regelung im Gesetz

Art. 9 nDSG verpflichtet Verantwortliche, die Kontrolle über ihre Auftragsbearbeiter vertraglich sicherzustellen. Auch die DSGVO (Art. 28 Abs. 3) und die Richtlinie (EU) 2016/680 (Art. 22 Abs. 3) setzen für die Verarbeitung durch Auftragsverarbeiter eine Vereinbarung voraus.

Die Bestimmungen lauten wie folgt:[282]

[282] Hervorhebungen hinzugefügt.

Art. 28 Abs. 3 DSGVO

«Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter:

a. die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c. alle gemäß Artikel 32 [Datensicherheit] erforderlichen Maßnahmen ergreift;

d. die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e. angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g. nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

h. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Art. 22 Abs. 3 Richtlinie (EU) 2016/68

Die Mitgliedstaaten sehen vor, dass die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erfolgt, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und der den Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a. nur auf Weisung des Verantwortlichen handelt,

b. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen,

c. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten,

d. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen – nach Wahl des Verantwortlichen – zurückgibt bzw. löscht und bestehende Kopien vernichtet, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht, 4.5.2016 L 119/114 Amtsblatt der Europäischen Union DE,

e. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt,

f. die in den Absätzen 2 und 3 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält.

Art. 9 nDSG

(1) Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

(2) Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

(3) Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

b. Analyse

i. Art. 9 nDSG übernimmt Art. 10a DSG

Art. 9 nDSG übernimmt Art. 10a DSG im Wesentlichen unverändert. Terminologisch hat der Gesetzgeber die Bestimmung an die neuen Begriffe «Verantwortlicher» und «Auftragsbearbeiter» angepasst (Abs. 1, 2 und 4).[283]

In Abs. 1 verwendet der Gesetzgeber neu den Begriff «vertraglich» («contrat», «contratto») statt «Vereinbarung» («convention», «convenzione). Damit ändert sich materiell nichts. Der Beizug von Auftragsbearbeitern setzt bereits unter aktuellem Recht eine vertragliche Regelung voraus, die namentlich die Weisungsgebundenheit (Art. 10a Abs. 1 lit. a DSG) und die Pflicht zur Gewährleistung der Datensicherheit (Art. 10a Abs. 2 DSG) absichert.[284]

Materiell bringt einzig Abs. 3 von Art. 9 nDSG eine Neuerung. Auftragsbearbeiter sind künftig von Gesetzes wegen dazu verpflichtet, für den Beizug von Unterauftragsbearbeitern vorgängig die Genehmigung des Verantwortlichen einzuholen. Diese Neuerung erfolgt gemäss Botschaft E-DSG zur Umsetzung der entsprechenden Anforderung in Art. 22 Abs. 2 der Richtlinie

[283] Botschaft E-DSG (FN 3), 7031–7032.

[284] Thomas Steiner, Digitalisierter Arztbesuch und Cloud-Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, in: sic! 2020, 377 ff., 680; Rosenthal (FN 178), N 17.

(EU) 2016/680.[285] Gemäss Art. 7 Abs. 1 DSV (und wie schon in der Botschaft E-DSG ausgeführt[286]) kann die Genehmigung spezifischer oder allgemeiner Art sein. Hat der Verantwortliche dem Beizug von Unterauftragsbearbeitern im Allgemeinen zugestimmt, muss ihn der Auftragsbearbeiter über jede Änderung (Hinzuziehen neuer oder Ersatz bestehender Auftragsbearbeiter) informieren und dem Verantwortlichen ein Widerspruchsrecht gewähren (Art. 7 Abs. 2 DSV).

Art. 9 nDSG stimmt mit dem vom Bundesrat entworfenen Art. 8 E-DSG überein. Das Parlament diskutierte die Bestimmung weder in den Sitzungen ihrer SPK noch in den Ratsdebatten. Somit entspricht die Beibehaltung des bereits in Art. 10a DSG implementierten Konzepts in Art. 9 nDSG dem Willen des Gesetzgebers.

ii. Kontrollziele und zwei Mindestregelungspunkte

Mit Art. 9 Abs. 1 lit. a nDSG (Weisungsgebundenheit) und Art. 9 Abs. 2 nDSG (Gewährleistung der Datensicherheit) gibt der Gesetzgeber unverändert vor, *was* der Verantwortliche (Auftraggeber) zu kontrollieren hat. Er gibt aber nicht vor, *wie* – d.h. mit welchen vertraglichen (oder gesetzlichen) Regelungen und in welchem Detaillierungsgrad – der Verantwortliche sich die Kontrollmöglichkeit zuzusichern hat.

Implizit – entsprechend den **Kontrollzielen** – gilt unter Art. 9 nDSG (unverändert) der folgende **Mindestinhalt** einer Vereinbarung über die Auftragsbearbeitung: (i) der Verantwortliche muss den Auftragsbearbeiter untersagen, die der Auftragsbearbeitung unterliegenden Personendaten (weisungswidrig) zu eigenen Zwecken zu verwenden (Art. 9 Abs. 1 lit. b nDSG); und (ii) der Auftragsbearbeiter muss sich zur Einhaltung ausreichender technischer und organisatorischer Massnahmen zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der Personendaten verpflichten (Art. 9 Abs. 2 nDSG). Somit fokussiert Art. 9 nDSG stark auf Kontrollziele und überlässt es den Unternehmen, *wie* sie die Zielerreichung vertraglich absichern.

---

[285] Botschaft E-DSG (FN 3), 7031–7032.

[286] Botschaft E-DSG (FN 3), 7032.

iii. Kataloge von Mindestregelungspunkten – inhaltliche Vorgaben

Demgegenüber legen Art. 22 Abs. 3 der Richtlinie (EU) 2016/680 wie auch Art. 28 Abs. 3 DSGVO gleich einen ganzen **Katalog** von Regelungspunkten fest und enthalten zumindest teilweise **inhaltliche Vorgaben** für die Ausgestaltung der entsprechenden vertraglichen Regelungen.

Die **Kataloge von Mindestregelungspunkten** sind in der DSGVO und in der Richtlinie (EU) 2016/680 weitgehend identisch. In Art. 22 Abs. 3 der Richtlinie (EU) 2016/680 fällt die Formulierung der Anforderungen an die Regelungspunkte teilweise (insb. in Bezug auf die Weisungsgebundenheit) etwas weniger detailliert aus als in Art. 28 Abs. 3 DSGVO. Überdies sind zwei Regelungspunkte (Unterstützung bei der Einhaltung der Datensicherheit sowie Unterstützung bei der Durchführung von Datenschutzfolgenabschätzungen wie auch bei vorherigen Konsultationen der Datenschutzaufsichtsbehörden) aus Art. 28 Abs. 3 DSGVO keine Mindestregelungspunkte gemäss Art. 22 Abs. 3 Richtlinie (EU) 216/680.

iv. Keine Übernahme von Art. 28 Abs. 3 DSGVO

Es fällt auf, dass Art. 9 nDSG im Wesentlichen Kontrollziele vorgibt und es den Verantwortlichen überlässt, wie sie die Erreichung dieser Kontrollziele vertraglich absichern. Der gewählte Ansatz ist vergleichbar mit dem in Art. 19 nDSG (Informationspflichten) gewählten Ansatz: Generell-abstrakte Regel – ergänzt mit wenigen Mindestanforderungen.

Diese Schweizer Lösung **unterscheidet sich konzeptionell stark** vom Ansatz gemäss Art. 22 Abs. 3 Richtlinie (EU) 2016/680 und Art. 28 Abs. 3 DSGVO. Die EU-Regelungen enthalten einerseits einen langen Katalog von Mindestregelungspunkten, die über die blosse Regelung der Weisungsgebundenheit und der Datensicherheit hinausgehen. Andererseits enthält vor allem Art. 28 Abs. 3 DSGVO auch inhaltliche Vorgaben zur Ausgestaltung der Vereinbarung über die Auftragsverarbeitung. Beispielsweise ergänzt Art. 28 Abs. 3 DSGVO (nicht aber Art. 22 Abs. 3 lit. e Richtlinie (EU) 20216/680) das Informationsrecht des Verantwortlichen mit dem Recht auf Überprüfung durch eigene oder beauftragte Prüfer.[287]

[287] Art. 28 Abs. 3 lit. h DSGVO.

c. Folgerungen für die Auslegung von Art. 9 nDSG

Schweizer Unternehmen werden sich bei der Ausgestaltung von Vereinbarungen über die Auftragsbearbeitung regelmässig am *Standard* gemäss Art. 28 Abs. 3 DSGVO ausrichten. Dies entspricht entweder einer Rechtspflicht (unter Art. 28 Abs. 3 DSGVO, wo anwendbar) des Verantwortlichen in der Schweiz oder eines in der EU niedergelassenen Auftragsverarbeiters; oder aber es entspricht der Erwartung unter Geschäftspartnern (*best practice*) an eine sorgfältige Auswahl, Instruktion und Kontrolle von Auftragsbearbeitern.

Tatsächlich entspricht es heute schon **guter Praxis**, die Kontrolle über Auftragsbearbeiter mit weitergehenden vertraglichen Regelungen abzusichern als es Art. 10a DSG erfordern würde. Dazu gehören namentlich Zusicherungen in Bezug auf die Information und die Ausübung des Widerspruchsrechts beim Austausch von Unterauftragsbearbeitern, Informations-, Kooperations- und Vertraulichkeitspflichten des Auftragsbearbeiters, Prüfrechte des Verantwortlichen und Regelungen in Bezug auf den Ort der Bearbeitung sowie zur Bekanntgabe von Personendaten ins Ausland.[288]

Was aber Unternehmen tun, weil sie selbst oder ihre Vertragspartner dazu gesetzlich unter der DSGVO verpflichtet sind, oder aber weil Geschäftspartner es im Sinne der guten Praxis von ihnen erwarten, entspricht nicht sogleich einer Pflicht unter Art. 9 nDSG. Der zur Sicherstellung der Kontrolle über Auftragsbearbeiter im Sinne von Art. 9 nDSG erforderliche Vertragsinhalt ergibt sich **aus den Umständen und den involvierten Risiken für betroffene Personen** – nicht aus Art. 28 Abs. 3 DSGVO.

Entsprechend dürfen der EDÖB und die Schweizer Gerichte *nicht* dieselben hohen Ansprüche an die Ausgestaltung solcher Vereinbarungen stellen, wie dies Datenschutzaufsichtsbehörden in der EU zuweilen tun.[289] Eine solche Ausrichtung an der Praxis und den Empfehlungen der EU-Datenschutzaufsichtsbehörden wäre nur zulässig, wenn der Schweizer Gesetzgeber den Willen geäussert hätte, in der Rechtsanwendung in Bezug auf die konkret

---

[288] Vgl. Steiner (FN 284), 858–887.

[289] Vgl. z.B. EDSA, Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), Adopted on 9 July 2019 (vgl. z.B. zur Beschreibung der Auftragsverarbeitung: «This description should be made in the most detailed possible manner», a.a.O. N 50).

auszulegende Norm (hier Art. 9 nDSG) auf Gedeih und Verderb der EU-Praxis zu folgen – was gerade nicht der Fall ist.

Entsprechend haben der EDÖB und Schweizer Gerichte Art. 9 nDSG **autonom auszulegen**. Art. 28 Abs. 3 DSGVO kann allenfalls als **Auslegungshilfe** zur Plausibilisierung des Schweizer Auslegungsresultats dienen.

VI. Zusammenfassung und Folgerung für die Auslegung des nDSG

Die nachstehende Übersicht fasst links die Regeln zusammen, die für die Berücksichtigung von EU-Recht bei der Auslegung von Schweizer Recht gelten. In der rechten Spalte folgt eine Zuordnung der *in diesem Beitrag analysierten* Bestimmungen des nDSG.

Auslegungsregeln	**Anwendung auf nDSG-Bestimmungen**
Europarechtskonforme Auslegung: Autonom *nachvollzogenes* Schweizer Recht ist *im Zweifel europarechtskonform* auszulegen.	– Art. 28 nDSG (Datenportabilität), unter Berücksichtigung des unterschiedlichen Rechtfertigungskonzepts; und – Art. 14 (Vertretung) [in diesem Beitrag nicht analysiert], unter Berücksichtigung der unterschiedlichen Regelung des räumlichen Geltungsbereichs in Art. 3 nDSG bzw. Art. 3 Abs. 2 DSGVO.

Auslegungsregeln	**Anwendung auf nDSG-Bestimmungen**
Berücksichtigung der EU-Rechtsanwendung bei europarechtskonformer Auslegung: *Wenn es die im Schweizer Recht geltenden klassischen Auslegungselemente zulassen*, ist bei der Auslegung autonom nachvollzogenen Schweizer Rechts die Praxis der EU-Behörden und -Gerichte zum rezipierten EU-Recht autoritativ mitzuberücksichtigen.	– Es gibt in den Materialien selbst in Bezug auf die autonom nachvollzogenen Bestimmungen, Art. 28 nDSG und Art. 14 nDSG, *keine* Hinweise darauf, dass der Gesetzgeber über den Nachvollzug der Gesetzgebung hinaus die richterliche Weiterentwicklung der rezipierten DSGVO-Bestimmungen autoritativ mitzuberücksichtigen wollte.
Berücksichtigung der EU-Rechtsanwendung als Auslegungshilfe: Bei blosser *Angleichung des Schweizer Rechts an EU-Recht*, bei welcher der Schweizer Gesetzgeber bewusst *eine eigenständige Schweizer Regelung* schaffen wollte und z.B. eine *unterschiedliche konzeptionelle Ausrichtung* gewählt hat, ist die Rechtsprechung zum EU-Recht bloss *als Auslegungshilfe* zu berücksichtigen. Die Behörden können daraus z.B. Erkenntnisse über den Norm-Sinn der auszulegenden Bestimmung gewinnen. Bei dieser Art der Berücksichtigung des EU-Rechts dient das	– Art. 5 lit. c Ziff. 3 nDSG (genetische Daten); Auslegung nach Art. 1 lit. l GUMG, Berücksichtigung der EU-Rechtsanwendung zur Bestätigung des Auslegungsresultats; – Art. 5 lit. c Ziff. 4 nDSG (biometrische Daten); – Art. 19 nDSG (Informationspflicht bei Beschaffung von Personendaten), unter Berücksichtigung der im Vergleich zu Art. 13–14 DSGVO unterschiedlichen Konzeption;

Auslegungsregeln	**Anwendung auf nDSG-Bestimmungen**
EU-Recht nur der Bestätigung (*Plausibilisierung*) des Auslegungsergebnisses.	– Art. 31 nDSG (Rechtfertigungsgründe), unter Berücksichtigung des unterschiedlichen Rechtfertigungskonzepts und wesentlicher Unterschiede bei der Ausgestaltung der einzelnen Rechtfertigungsgründe (im Vergleich zu den DSGVO-Rechtsgrundlagen); und – Art. 9 nDSG (Vereinbarung über die Auftragsbearbeitung)
EU-Rechtsanwendung unbeachtlich bei autonomen Schweizer Regelungen Bei autonomen Schweizer Regelungen, die keine Entsprechung im rezipierten EU-Rechtsakt finden, ist die EU-Rechtsanwendung unbeachtlich.	– Art. 3 Abs. 1 nDSG (räumlicher Geltungsbereich – Verwaltungsrecht); Auslegung gemäss kodifiziertem verwaltungsrechtlichem Auswirkungsprinzip, wie z.B. Art. 2 Abs. 2 KG; – Art. 3 Abs. 2 nDSG (räumlicher Geltungsbereich – Privatrecht), etablierte Auslegung von Art. 139 IPRG; und – Art. 3 Abs. 2 nDSG (räumlicher Geltungsbereich – Strafrecht), etablierte Auslegung von Art. 3 StGB.

VII. Schlussbemerkungen

Schweizer Unternehmen werden sich in der **Unternehmenspraxis** aus guten Gründen am Standard der DSGVO ausrichten – etwa in Bezug auf Datenschutzerklärungen oder Vereinbarungen über die Auftragsbearbeitung.

Ein Grund dafür kann sein, dass für dieselbe Datenbearbeitung des Schweizer Unternehmens sowohl das nDSG als auch die DSGVO gelten. In solchen

Fällen ist es nachvollziehbar, dass das Schweizer Unternehmen im EU-Markt wie auch im Schweizer Markt einheitliche Datenschutzerklärungen und Vereinbarungen über die Auftragsbearbeitung verwenden möchte.

Ein anderer Grund für eine Orientierung am DSGVO-Standard können Erwartungen von Kundinnen oder Geschäftspartnern des Schweizer Unternehmens sein (z.B. Erwartungen an die Ausgestaltung einer Vereinbarung über die Auftragsbearbeitung). Zudem gibt es Bereiche, in denen Geschäftspartner oder Lieferanten ihrerseits verpflichtet sind, Unternehmen in der Schweiz Pflichten aus der DSGVO vertraglich zu überbinden (z.B. die Pflicht von in der EU niedergelassenen Auftragsverarbeitern, eine Vereinbarung über die Auftragsverarbeitung nach Massgabe von Art. 28 Abs. 3 DSGVO abzuschliessen).

Überdies werden viele Schweizer Unternehmen bei Inkrafttreten des nDSG bereits Erfahrungen im Umgang mit der DSGVO gesammelt haben. Zur DSGVO werden auch mehr Lehrmeinungen als zum nDSG vorliegen. Zudem gibt es zur DSGVO bereits eine umfangreiche Behörden- und Gerichtspraxis. Es ist somit (leider) davon auszugehen, dass Schweizer Unternehmen (und Behörden) die zur DSGVO entwickelten Ansichten (z.B. Lehrmeinungen zur DSGVO oder Interpretationen von EU-Datenschutzaufsichtsbehörden in Leitlinien und Entscheidungen) zuweilen unreflektiert übernehmen werden.

In Untersuchungen durch den EDÖB oder der Staatsanwaltschaften sowie in Streitfällen vor Gericht sind hingegen Einzelfälle zu beurteilen. Dabei ist eine gewisse **Resistenz der rechtsanwendenden Schweizer Behörden** gegenüber der Behörden- und Gerichtspraxis zur DSGVO gefragt. Die rechtsanwendenden Schweizer Behörden sollen (i) den Sachverhalt selbst abklären (und nicht die Schilderungen von EU-Behörden in allfälligen Parallelverfahren unreflektiert übernehmen), (ii) eigene Lösungen aus dem nDSG heraus entwickeln und (iii) die Praxis zur DSGVO in der Regel (wie in diesem Beitrag aufgezeigt) höchstens zur Plausibilisierung solcher autonomer Lösungen heranziehen.

Von der Praxis zur DSGVO abweichende Schweizer Praxis zum nDSG ist **hinzunehmen – und zwar ungeachtet dessen, dass eine solche Praxis bei der Prüfung eines EU-Angemessenheitsbeschlusses zum politischen Spielball werden könnte**. Politik ist Sache des Parlaments – nicht der rechtsanwendenden Schweizer Behörden.

Im Zweifelsfall haben Behörden und Gerichte in der Schweiz einen neuerlichen Entscheid des Schweizer Gesetzgebers abzuwarten. Sonst hätte der Schweizer Gesetzgeber die DSGVO gleich ganz kopieren und den rechtsanwendenden Schweizer Behörden die Pflicht auferlegen können, in der Rechtsanwendung eine grösstmögliche Parallelität zur DSGVO zu erreichen. Der vorliegende Beitrag zeigt, dass dies gerade *nicht* der Wille des Gesetzgebers war.

Zusammenspiel informationsrechtlicher Bestimmungen in der schulinternen Logopädie und Sozialarbeit

Rechtsgrundlagen und Anwendungsbeispiele

Tobias Fasnacht

Inhaltsübersicht

I. Einleitende Bemerkungen

Die Weitergabe von Informationen im schulischen Bereich ist für die unterschiedlichsten Funktionsträger im Schulwesen eine wohl teilweise selbstverständliche, weil in der Regel notwendige Handlung. Im Rahmen des Schulalltags werden die Schülerinnen und Schüler von Tag zu Tag beobachtet – und auch beurteilt. Um sie in ihrem Alltag zu begleiten, scheint es zunächst unabdingbar, dass die im Schulbetrieb involvierten Personen über einen «vollständigen» Kenntnisstand verfügen, um den Kindern das zu geben, was ihnen von Verfassung wegen zusteht: Bildung.

Während ihrer Schulkarriere kommen die Kinder bzw. die Jugendlichen mit den verschiedensten Fachkräften in Kontakt. Zusammen mit Anderen oder in Einzelsettings treffen sie auf die Hausmeisterin oder den Hausmeister, das im Zentrum stehende Lehrpersonal, die Schulleitung, Sozialarbeiterinnen und Sozialarbeiter, Logopädinnen und Logopäden, Schulpsychologinnen und Schulpsychologen etc. Alle genannten Personen übernehmen im Schulbetrieb ihre eigene Funktion und sehen die Kinder demzufolge aus ihrer eigenen Perspektive.

Die vorliegende Arbeit verfolgt das Ziel, den involvierten Personen – allen voran Logopädinnen und Logopäden sowie Sozialarbeiterinnen und Sozialarbeitern – einen Überblick über die informationsrechtlichen Grundlagen für ihre Tätigkeit zu geben. Mit dieser Hilfestellung soll bestimmt werden, was hinsichtlich der Bearbeitung und Weitergabe von Informationen über Schülerinnen und Schüler erlaubt ist und was nicht. Die informationsrechtlichen Rahmenbedingungen sind aber auch ein dienliches Instrument, um den Entscheidungsprozess betreffend die Weitergabe von Information zu strukturieren und zu vereinfachen; d.h. zu entscheiden, ob eine Information weitergegeben werden darf oder nicht.

Oft geben informationsrechtliche Bestimmungen nur den Handlungsrahmen wieder, was aus Perspektive der Fachperson nicht bedeutet, dass im konkreten Fall keine Informationen bearbeitet bzw. weitergegeben werden dürfen. Dort, wo sich im Gesetz keine spezifischen Handlungsleitlinien für die jeweilige Situation finden lassen, ist eine vertiefte Auseinandersetzung und Begründung seitens der Fachperson erforderlich; die Verantwortung wird mit anderen Worten in die Hände der Adressatin oder des Adressaten der informations-

rechtlichen Bestimmungen gelegt. Sie oder er hat in der konkreten Situation die Pflicht, Handlungen zu überdenken und zu begründen. Der Aufwand dafür soll nicht den Schulbetrieb unnötig verkomplizieren. Er zeugt von Respekt gegenüber den Persönlichkeitsrechten aller Beteiligter, insbesondere der Kinder.

Dies lässt sich ganz einfach an zwei erfundenen[1] Fallbeispielen illustrieren, in denen sich informationsrechtliche Fragen stellen. Es handelt sich um ein Fallbeispiel aus der Logopädie mit dem Schwerpunkt Kommunikation zwischen Fachpersonen untereinander und Fachpersonen mit den Eltern. Das zweite Fallbeispiel ist im Bereich Sozialarbeit angesiedelt mit dem Schwerpunkt Meldepflichten und -rechte gegenüber der Kindesschutzbehörde. Die Fallbeispiele werden nach dem Grundlagenteil ausgeführt und aus informationsrechtlicher Perspektive näher besprochen.[2]

II. Rechtliche Rahmenbedingungen

Logopädinnen oder Sozialarbeiterinnen befinden sich aus informationsrechtlicher Perspektive in einem Spannungsfeld, das sich auch in anderen staatlichen Bereichen, wie etwa auf dem Standesamt, bei der Einwohnerkontrolle oder dem Strassenverkehrsamt, wiederfindet; ein Spannungsverhältnis zwischen dem Wissen über Personendaten, um den gesetzlich vorgesehenen Auftrag erfüllen zu können und den Persönlichkeitsrechten der Betroffenen. Akzentuiert wird das Spannungsfeld im Schulbereich, weil mit sehr persönlichen Personendaten gearbeitet wird und eine Vielzahl an Personen – Kinder, Eltern, Lehrpersonen etc. – involviert ist.

---

[1] Die Fallbeispiele sind nach Gesprächen mit Fachpersonen entstanden bzw. vom Verfasser erfunden und im Hinblick auf einen (hoffentlich) relevanten Mehrwert für die Leserin bzw. den Leser abgeändert worden.

[2] Vgl. unten III.

Die Bearbeitung[3] «besonderer» Personendaten[4] und auch deren Weitergabe werden im Datenschutzrecht regelmässig an weitergehende Voraussetzungen geknüpft.

Es gilt somit in einem ersten Schritt aufzuzeigen, wie sich dieses Spannungsfeld ausgestaltet. Dargestellt wird im vorliegenden Kapitel zunächst der Auftrag der Logopädinnen und Sozialarbeiter, wie er sich aus den einschlägigen Rechtsgrundlagen ableiten lässt. Sodann wird auf die anwendbaren «informationsrechtlichen» Bestimmungen eingegangen. Informationsrechtlich werden diese Bestimmungen genannt, weil sie nicht nur aus den «Datenschutzgesetzen» bestehen, sondern sich aus einem teils durchaus komplexen Zusammenspiel von verschiedenen anwendbaren (kantonal unterschiedlichen) Gesetzen ergeben. Vorliegend wird auf die anwendbaren Gesetze und Verordnungen des Kantons Zürich eingegangen.

A. Schweizerische Bundesverfassung

Das Schulwesen ist nach Art. 62 Abs. 1 BV Sache der Kantone. Im Bereich der Sonderschulung besteht ein Handlungsauftrag an die Kantone: «Die Kantone sorgen für eine ausreichende Sonderschulung aller behinderten Kinder und Jugendlichen bis längstens zum vollendeten 20. Lebensjahr.» (Art. 62 Abs. 3 BV). Die Sonderschulung gilt als Teil des Schulwesens, womit sie gemäss Art. 62 Abs. 1 BV ebenfalls in die Kompetenz der Kantone fällt und auch

[3] «Bearbeiten ist jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten.» (§ 3 Abs. 5 des Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz des Kantons Zürich, Informations- und Datenschutzgesetz, IDG ZH; ON 170.4).

[4] «Besondere Personendaten sind: a. Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, wie Informationen über 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, 2. die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten, 3. Massnahmen der sozialen Hilfe, 4. administrative oder strafrechtliche Verfolgungen oder Sanktionen.» (§ 3 Abs. 4 IDG ZH).

von diesen finanziert wird.[5] Im Ergebnis wird aus Art. 62 Abs. 3 BV in der Lehre (teilweise[6]) ein verfassungsrechtlicher Anspruch auf ein angemessenes, ausreichendes Sonderschulungsangebot an öffentlichen Schulen bis zum vollendeten 20. Lebensjahr abgeleitet. Ob sich (auch) der Auftrag der Logopädie – wie er vorliegend besprochen wird – zumindest teilweise aus Art. 62 Abs. 3 BV oder aus dem Anspruch auf Grundschulunterricht, Art. 19 BV ableiten lässt, kann vorliegend offen bleiben. Dies gilt auch für die verfassungsrechtliche Grundlage der Sozialarbeit, die allenfalls aus Art. 19 BV (Anspruch auf Grundschulunterricht) in Verbindung mit Art. 11 BV (Schutz der Kinder und Jugendlichen) abgeleitet werden könnte.[7]

Auch ohne die verfassungsrechtlichen Grundlagen abschliessend zu klären, können nämlich die (kantonalen) Vereinbarungen, Gesetze und Verordnungen beigezogen werden. Der Auftrag für die Logopädie und die Sozialarbeit ist somit vorliegend in den kantonalen Gesetzen und Verordnungen zu suchen, wobei hieraus abgeleitet werden kann, in welchem Rahmen die Arbeit der Logopädinnen und Sozialarbeiterinnen stattfindet. Die massgeblichen Bestimmungen werden nachfolgend aufgezeigt.

B. Interkantonale Vereinbarung im Bereich Sonderpädagogik vom 25. Oktober 2007

Die Vereinbarung über die interkantonale Zusammenarbeit im Bereich der Sonderpädagogik ist am 25. Oktober 2007 im Namen der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK) unterzeichnet worden (nachfolgend: IKV). Der Kanton Zürich ist der Vereinbarung beigetreten.[8] Sie ist zu verstehen als Folge von Art. 62 Abs. 3 BV, wonach die ausreichende Sonderschulung als Auftrag an die Kantone definiert worden ist, und dem

---

5 BSK BV-Peter Hänni in: Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015 (zit. BSK BV-Verfasserin), Art. 62 N 35 f.

6 Die Frage, ob ein Individualanspruch vorliegt, ist allerdings umstritten, vgl. BSK BV-Hänni (FN 5), Art. 62 N 37.

7 Vgl. BSK BV-Tschentscher (FN 5), Art. 11 N 23.

8 Bis zum 30.06.2014 sind die nachfolgenden Kantone der Vereinbarung beigetreten (gemäss Beitrittsdatum): VS, SH, OW, GE, LU, VD, FR, TI, AR, BS, BL, UR, GL, NE, JU und ZH.

Wunsch nach Harmonisierung, was sich bereits aus dem ersten Artikel der Interkantonalen Vereinbarung ergibt: Um ihrem Verfassungsauftrag nachzukommen, legen die Kantone in der Interkantonalen Vereinbarung das Grundangebot fest. Namentlich soll die Integration der Kinder und Jugendlichen im Bereich Sonderpädagogik gefördert werden und die Kantone verpflichten sich zur Anwendung gemeinsamer Instrumente (Art. 1 IKV). Es wird mit anderen Worten in der Vereinbarung «ein gesamtschweizerischer Rahmen für die wichtigsten Massnahmen sowie für die Entwicklung und Anwendung von gemeinsamen Instrumenten […] im sonderpädagogischen Bereich festgelegt […].»[9] Das sonderpädagogische Grundangebot (als Leistungsauftrag) umfasst (auch) die Logopädie (Art. 4 Abs. 1 lit. a IKV), nicht aber die Sozialarbeit.

C. Volksschulgesetz des Kantons Zürich

Im Volksschulgesetz des Kanton Zürich[10] finden sich die einschlägigen Bestimmungen zu den sonderpädagogischen Massnahmen in § 33 ff. VSG ZH. Die Bestimmungen des Volksschulgesetzes bzw. die Einzelheiten zu den sonderpädagogischen Massnahmen werden in der Verordnung über die sonderpädagogischen Massnahmen[11] präzisiert.

Die Logopädie ist eine Form der Therapie,[12] die ihrerseits eine sonderpädagogische Massnahme ist (§ 34 Abs. 1 VSG ZH i.V.m. § 9 Abs. 1 VSM ZH). Therapie ist die individuelle Unterstützung von Schülerinnen und Schülern mit spezifischen pädagogischen Bedürfnissen (§ 34 Abs. 3 VSG ZH),[13] die von den Gemeinden angeboten wird (§ 35 VSG ZH).

---

[9] Interkantonale Vereinbarung über die Zusammenarbeit im Bereich der Sonderpädagogik vom 25. Oktober 2007, Kommentar zu den einzelnen Bestimmungen, EDK, 04.12.2007, 3.

[10] Volksschulgesetz vom 7. Februar 2005 des Kantons Zürich (VSG ZH; ON 412.100).

[11] Verordnung vom 11. Juli 2007 über die sonderpädagogischen Massnahmen des Kantons Zürich (VSM ZH; ON 412.103).

[12] § 9 Abs. 1 VSM ZH.

[13] § 2 Abs. 2 VSM ZH: «Besondere pädagogische Bedürfnisse entstehen vor allem aufgrund ausgeprägter Begabung, von Leistungsschwäche, des Erlernens von Deutsch als Zweitsprache, auffälliger Verhaltensweisen oder von Behinderungen.».

Die Entscheidung, ob und welche sonderpädagogische Massnahme stattfinden soll, wird von den Eltern, der Lehrperson und der Schulleitung gemeinsam getroffen (§ 37 Abs. 1 VSG ZH). Kann keine Einigung erzielt werden oder bestehen Unklarheiten, wird (unter Umständen auch gegen den Willen der Eltern) eine schulpsychologische Abklärung durchgeführt (§ 38 Abs. 1 VSG ZH). Besteht auch nach dieser Abklärung keine Einigung unter den Beteiligten, beschliesst die Schulpflege das weitere Vorgehen (§ 39 VSG ZH). Die Gemeinden sorgen für die Überprüfung der angeordneten Massnahmen auf ihre Notwendigkeit und Wirksamkeit hin (§ 40 VSG ZH).

Die Logopädinnen und Logopäden im Sinne von § 34 Abs. 3 VSG ZH arbeiten mit den Schülerinnen und Schülern einzeln oder in Gruppen und beraten bei Bedarf die Lehrpersonen in Bezug auf Therapiebedürftige und Fragen der Prävention im Regelklassenunterricht (§ 10 Abs. 1 und 2 VSM ZH). Es wird in der Verordnung ein Minimum an Volllzeiteinheiten für die einzelnen Schulstufen als Auftrag an die Gemeinden festgelegt (§ 11 VSM ZH).

Logopädinnen und Logopäden arbeiten in der Schule somit im Rahmen ihres gesetzlich vorgesehenen Auftrages.

D. Kinder- und Jugendhilfegesetz des Kantons Zürich

Die Sozialarbeit wird im Volksschulgesetz nicht erwähnt. Sie hat ihre gesetzliche Grundlage in § 19 KJHG ZH[14], wo festgehalten wird, dass die Gemeinden für ein bedarfsgerechtes Angebot an Schulsozialarbeit sorgen. Auch die Sozialarbeiterinnen und Sozialarbeiter arbeiten somit im Rahmen ihres gesetzlich vorgesehenen Auftrages.

In der Folge ist auf informationsrechtliche Bestimmungen auf Bundes- und kantonaler Ebene einzugehen, die im Bereich der Logopädie und der Sozialarbeit zu beachten sind.

[14] Vgl. Kinder- und Jugendhilfegesetz vom 14. März 2011 des Kantons Zürich (KJHG ZH, ON 852.1).

E. Amts- und Berufsgeheimnisse auf Bundes- und kantonaler Ebene

Logopädinnen und Logopäden sowie Sozialarbeiterinnen und Sozialarbeiter unterstehen bei ihrer Arbeit an der Schule dem *Amtsgeheimnis*. Das Amtsgeheimnis dient dem Schutz staatlicher Geheimhaltungsinteressen und schützt die Privatsphäre des Einzelnen, wenn dieser der Verwaltung Informationen offenbart.[15] Das Amtsgeheimnis ergibt sich aus § 15 Abs. 1 des Personalgesetzes:[16] «Die Angestellten sind zur Verschwiegenheit über dienstliche Angelegenheiten verpflichtet, soweit an der Geheimhaltung ein überwiegendes öffentliches oder privates Interesse gemäss § 23 IDG ZH[17] besteht oder wenn eine besondere Vorschrift dies vorsieht.» Die Verpflichtung zur Bewahrung des Amtsgeheimnisses bleibt auch nach Beendigung des Arbeitsverhältnisses bestehen (§ 15 Abs. 2 Personalgesetz).

Die (vorsätzliche) Missachtung des Amtsgeheimnisses wird gemäss Art. 320 StGB[18] mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Keine Bestrafung erfolgt, wenn das Geheimnis mit schriftlicher Einwilligung der vorgesetzten Behörde offenbart wird (Art. 320 Abs. 2 StGB). Geheim ist eine Tatsache, wenn sie nicht allgemein bekannt oder zugänglich ist, ein berechtigtes Interesse und auch ein Wille an deren Geheimhaltung besteht.[19] Die geheime Tatsache wird sodann zum Amtsgeheimnis, wenn sie einer Person in der Eigenschaft als Mitglied der Verwaltung anvertraut oder diese im Rahmen der amtlichen Stellung wahrgenommen wird.[20]

Neben dem Amtsgeheimnis ist im Gesundheitsbereich («Personen, die einen Beruf im Gesundheitswesen ausüben») auch das Berufsgeheimnis zu beach-

---

[15] Matthias Michlig/Eva Wyler, in: Damian K. Graf (Hrsg.), StGB, Annotierter Kommentar, Bern 2020 (zit. VerfasserIn, StGB), Art. 320 N 1.

[16] Personalgesetz vom 27. September 1998 (ON 177.10).

[17] Gesetz vom 12. Februar 2007 über die Information und den Datenschutz des Kantons Zürich (Informations- und Datenschutzgesetz, IDG ZH; ON 170.4).

[18] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB; SR 311.0).

[19] Michlig/Wyler, StGB (FN 15), Art. 320 N 3.

[20] Michlig/Wyler, StGB (FN 15), Art. 320 N 5.

ten; es wird in § 15 GesG ZH statuiert.[21] Es gilt für Personen, die im Kanton Zürich selbständig einen Gesundheitsberuf ausüben und somit der Bewilligungspflicht zur Berufsausübung unterstehen (§ 3 GesG ZH). Der Bewilligungspflicht unterstehen *selbständig* tätige Logopädinnen und Logopäden.

Die Verletzung des Berufsgeheimnisses ist gemäss Art. 321 StGB strafbewehrt. Es soll dem Einzelnen ermöglichen, bestimmten Berufsgruppen (die in Art. 321 StGB genannt werden) medizinische Geheimnisse anzuvertrauen, ohne dass diese an unbefugte Dritte weitergegeben werden.[22] Wenn somit im Rahmen der obligatorischen Schule tätige Logopädinnen und Logopäden dem Amtsgeheimnis unterstehen, ist dennoch auf die Frage einzugehen, ob diese auch dem *Berufsgeheimnis* unterstehen, insbesondere weil sie im Rahmen ihrer Tätigkeit bei der Anamnese gesundheitliche Aspekte abfragen, die bspw. auch von Ärztinnen und Ärzten abgefragt werden.

Zunächst ist festzustellen, dass die angedrohte Strafe nach Art. 320 StGB (Amtsgeheimnisverletzung) mit derjenigen in Art. 321 StGB (Berufsgeheimnisverletzung) identisch ist. Abweichungen sind dahingehend auszumachen, dass sich Art. 321 StGB auch auf das Studium bezieht, das heisst, dass auch Studierende bestraft werden können, die Geheimnisse offenbaren, welche sie in ihrem Studium wahrnehmen. Ferner ist die Berufsgeheimnisverletzung dann nicht strafbar, wenn eine Einwilligung der berechtigten Person vorliegt oder das Geheimnis auf der Grundlage einer schriftlichen Bewilligung der Aufsichtsbehörde offenbart worden ist.

Abgesehen von diesen Unterschieden ist auszumachen, dass die Logopädinnen bzw. Logopäden in Art. 321 StGB nicht erwähnt werden, und zwar auch nach einer Ergänzung des besagten Artikels im Rahmen einer Revision des Bundesgesetzes über die Gesundheitsberufe, die seit dem 1. Februar 2020 in Kraft ist.[23]

---

[21] Gesundheitsgesetz vom 2. April 2007 des Kantons Zürich (GesG ZH; ON 810.1); § 15 Abs. 1: «Personen, die einen Beruf des Gesundheitswesens ausüben, und ihre Hilfspersonen wahren Stillschweigen über Geheimnisse, die ihnen infolge ihres Berufes anvertraut worden sind oder die sie in dessen Ausübung wahrgenommen haben.»

[22] Michlig/Wyler, StGB (FN 15), Art. 321 N 1.

[23] Neu genannt werden in Art. 321 StGB Pflegefachpersonen, Physiotherapeuten, Ergotherapeuten, Ernährungsberater, Optometristen und Osteopathen; Berufsfelder, die durch das angepasste Bundesgesetz über die Gesundheitsberufe einer Regelung hinsichtlich der Ausbildung unterworfen worden sind.

Die Logopädie als Berufszweig sowohl im sonderpädagogischen als auch im Gesundheitsbereich ist in der Botschaft zur Änderung des Bundesgesetzes über die Gesundheitsberufe vom 18. November 2015 thematisiert worden. Es sei in der Vernehmlassung die Aufnahme dieses Berufs in das Gesetz gefordert worden. Im Ergebnis sei die Logopädie aber schweizweit reglementiert[24] und dies habe sich bewährt; «eine parallele Regelung durch den Bund oder eine Teilung der Regelung in zwei Zuständigkeiten (pädagogisch-therapeutisch durch die EDK, medizinisch-therapeutisch durch den Bund) [sei] weder sinnvoll noch erwünscht.»[25]

Dass Logopädinnen und Logopäden nicht dem Berufsgeheimnis unterstellt werden sollen bzw. worden sind, und zwar nur, weil die Regelung des Berufsfeldes sich aufgrund bereits bestehender interkantonaler Regelungen nicht aufdrängt, scheint vor dem Hintergrund der anderen (neu) genannten Berufsgruppen nicht ganz nachvollziehbar. Grundsätzlich ist nämlich bekannt, dass auch Logopädinnen und Logopäden im Rahmen der Anamnese medizinische Geheimnisse offenbart werden, die an sich mit den Geheimnissen, die einer Ärztin oder einem Arzt offengelegt werden, identisch sind.[26]

Dennoch ist eine Bestrafung im Rahmen logopädischer Aufgaben nach Art. 321 StGB aufgrund des Grundsatzes *nulla poena sine lege* (keine Bestrafung ohne Gesetz, Art. 1 StGB[27]) ausgeschlossen. Anders verhält es sich, wenn die Logopädin oder der Logopäde als Hilfsperson einer in Art. 321 StGB genannten Berufsgattung tätig wird oder, wie eingangs erwähnt, die Logopädie fachlich eigenverantwortlich bzw. selbständig anbietet und somit der Bewilligungspflicht zur Berufsausübung gemäss dem Gesundheitsgesetz des Kantons Zürich unterstellt ist.

---

[24] Vgl. Interkantonale Vereinbarung über die Anerkennung von Ausbildungsabschlüssen vom 18. Februar 1993 durch die Schweizerische Konferenz der kantonalen Erziehungsdirektoren (EDK).

[25] Botschaft vom 18. November 2015 zum Bundesgesetz über die Gesundheitsberufe. BBl 2015 8715, 8729 f.

[26] Ob es sinnvoll wäre, auch die Logopädinnen und Logopäden unter das Berufsgeheimnis zu stellen, soll vorliegend nicht beantwortet werden.

[27] Vgl. etwa Graf, StGB (FN 15), Art. 1 N 1 ff.

F. Meldepflichten und -rechte

Art. 314*c* f. ZGB, die am 1. Januar 2019 in Kraft getreten sind, regeln Melderechte und Meldepflichten gegenüber der Kindesschutzbehörde. Gemäss Art. 314*c* Abs. 1 ZGB *kann* jede Person der Kindesschutzbehörde Meldung erstatten, wenn die körperliche, psychische oder sexuelle Integrität eines Kindes gefährdet erscheint. Personen, die an das Berufsgeheimnis gebunden sind, können eine Meldung machen, wenn die Meldung «im Interesse des Kindes» ist.[28]

Melde*pflichten* werden in Art. 314*d* Abs. 1 ZGB statuiert für Personen, die *nicht* dem Berufsgeheimnis unterstehen. Eine Meldepflicht liegt vor, «wenn konkrete Hinweise dafür bestehen, dass die körperliche, psychische oder sexuelle Integrität des Kindes gefährdet ist und (die meldepflichtigen Personen) nicht im Rahmen ihrer Tätigkeit Abhilfe schaffen können.» Folgende (meldepflichtigen) Personen werden in Art. 314*d* Abs. 1 ZGB explizit genannt: Zunächst Fachpersonen aus den Bereichen Medizin, Psychologie, Pflege, Betreuung, Erziehung, Bildung, Sozialberatung, Religion und Sport, die beruflich regelmässig Kontakt zu Kindern haben (Art. 314*d* Abs. 1 Ziff. 1 ZGB). Sodann Personen, welche in ihrer amtlichen Tätigkeit von «einem solchen Fall erfahren» (Art. 314*d* Abs. 1 Ziff. 2 ZGB). Die Meldepflicht gilt als erfüllt, wenn die Meldung an die vorgesetzte Person gerichtet ist; die Kantone können darüber hinaus noch weitere Meldepflichten vorsehen (Art. 314*d* Abs. 2 und 3 ZGB).

Im Kanton Zürich wird eine Meldepflicht im kantonalen Recht in § 51 VSG ZH statuiert: Hiernach informiert die Schulpflege die für Kindesschutzmassnahmen zuständige Behörde, wenn das Wohl einer Schülerin oder eines Schülers im Sinne von Art. 307 ZGB gefährdet ist. Es wird lediglich die Schulpflege verpflichtet, eine Meldung zu machen. Die kantonale Bestimmung geht insoweit weniger weit als die Bestimmungen des ZGB, die eine Meldepflicht direkt an die individuelle Fachperson adressiert.

Die rechtliche Situation für an der Schule praktizierende Logopädinnen und Logopäden sowie Sozialarbeiterinnen und Sozialarbeiter gestaltet sich somit

[28] Nicht aber deren Hilfspersonen, vgl. Art. 314*c* Abs. 2 ZGB, zweiter Satz.

einheitlich: Da sie alle – wie im vorangehenden Abschnitt aufgezeigt[29] – «nur» dem Amtsgeheimnis (und nicht dem Berufsgeheimnis) unterstehen, haben sie sowohl das Recht als auch die Pflicht, Vorkommnisse den Kindesschutzbehörden mitzuteilen, welche die körperliche, psychische oder sexuelle Integrität eines Kindes zu gefährden scheinen. Aus Sicht der Meldepflichtigen ist allerdings festzustellen, dass diese ihrer Pflicht nachkommen, wenn die Meldung an die vorgesetzte Person gerichtet ist (Art. 314*d* Abs. 2 ZGB). Eine Meldung an die vorgesetzte Person hindert die Meldepflichtigen aber nicht daran, (zusätzlich) von ihrem Melderecht (direkt gegenüber den Kindesschutzbehörden) Gebrauch zu machen.

G. Anwendbare datenschutzrechtliche Bestimmungen

1. Völker- und verfassungsrechtlicher Rahmen

«Datenschutz» ist ein Grundrecht. Es schützt (vereinfacht gesagt) vor ungerechtfertigter Bearbeitung und Weitergabe von Personendaten. Einschlägige, für die Schweiz (teilweise) anwendbare Bestimmungen finden sich unter anderem in der Schweizerischen Bundesverfassung, der Europäischen Menschenrechtskonvention,[30] in der Datenschutzkonvention des Europarates[31] und in der inzwischen schon nicht mehr ganz neuen Datenschutzgrundverordnung der Europäischen Union.[32] Insbesondere die Datenschutzgrundverordnung hat mannigfaltigen Einfluss auf das neue Datenschutzgesetz in

---

[29] Vgl. oben, II.E.

[30] Konvention zum Schutze der Menschenrechte und Grundfreiheiten, abgeschlossen in Rom am 4. November 1950 (SR 0.101).

[31] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abgeschlossen in Strassburg am 28. Januar 1981 (SR 0.235.1).

[32] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung); vgl. zum völker- und europarechtlichen Rahmen das (inzwischen nicht mehr umfassend aktuelle, aber eine gute Übersicht bietende) Kapitel, Belser, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011 (zit. VerfasserIn, Datenschutzrecht Grundlagen), 53 ff.

der Schweiz.[33] Vorliegend ist nicht genauer auf die internationalen Vorgaben einzugehen, sondern lediglich daran zu erinnern, dass der Schutz der Grundrechte im Bereich der Bearbeitung persönlichkeitsrelevanter Daten (durch staatliche Behörden) international anerkannt wird.

Staatliche Datenbearbeitung (als Eingriff in das Grundrecht «Datenschutz») ist grundsätzlich rechtfertigungsbedürftig[34] bzw. es braucht aus Perspektive der Verwaltung einen hinreichenden Grund, persönlichkeitsrelevante Daten zu bearbeiten. Ganz allgemein geregelt ist der Mechanismus der Rechtfertigung von Grundrechtseingriffen in Art. 36 BV, der die Marginalie «Einschränkungen von Grundrechten» trägt. Demgemäss bedürfen Einschränkungen einer gesetzlichen Grundlage (Abs. 1), müssen durch ein öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt (Abs. 2) und verhältnismässig sein (Abs. 3).[35] Vorliegend interessiert vor allen Dingen die gesetzliche Grundlage und die Verhältnismässigkeit:[36] Diese zwei Aspekte kommen in der Bundes- und in den kantonalen Datenschutzgesetzgebungen zum Ausdruck bzw. müssen in den besagten Bestimmungen aus verfassungsrechtlicher Sicht zum Ausdruck kommen. Das öffentliche Interesse an der Bearbeitung persönlichkeitsrelevanter Daten von Schülerinnen und Schülern ergibt sich aus den Zweckbestimmungen der jeweiligen Volksschulgesetze,[37] insbesondere dem Bildungsauftrag.

2. Anwendungsbereich

Wenn vorliegend, wie bisher, auf die anwendbaren (datenschutzrechtlichen) Bestimmungen im Kanton Zürich eingegangen wird, ist zunächst der *Anwendungsbereich* zu prüfen: Das Gesetz über die Information und den Datenschutz

---

[33] Vgl. zum Fortschritt der Revision auf der Homepage des Bundesamtes für Justiz, https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html (Abruf 29.08.2022).

[34] Vgl. Belser, Datenschutzrecht Grundlagen (FN 32), N 122 mit Verweis auf die kritische Lehre, 378 f.

[35] Ebenso darf der Kerngehalt nicht verletzt werden, vgl. Belser, Datenschutzrecht Grundlagen (FN 32), 393 f, der allerdings erst dann zum Tragen kommt, wenn die Menschenwürde verletzt würde, etwa, so die Autorin, wenn die Datenerfassung so umfassend ist, dass der Einzelne für den Staat zu einer durchsichtigen Person würde.

[36] Zum öffentlichen Interesse sogleich.

[37] Vgl. bspw. § 1 ff. VSG ZH.

vom 12. Februar 2007 (nachfolgend: IDG ZH) regelt gemäss § 1 den Umgang öffentlicher Organe mit Informationen. Öffentliche Organe des Kantons Zürich sind zu dessen Anwendung verpflichtet (§ 2 IDG ZH). Es bezweckt, die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Daten bearbeiten (§ 1 Abs. 2 lit. b IDG ZH). Logopädinnen und Logopäden sowie Sozialarbeiterinnen und Sozialarbeiter unterstehen somit im Rahmen ihrer Tätigkeit an öffentlichen Schulen dem kantonalen Datenschutzrecht.

3. «Bearbeitung» von «Personendaten»

Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen (§ 3 Abs. 3 IDG ZH). Der Begriff scheint schwammig, ist aber mit Blick auf das vorliegende Thema durchaus konkretisierbar: Es geht um Informationen, die einer Schülerin oder einem Schüler zugeordnet werden können. Geht es um Informationen, die sich in den Akten der Schülerinnen oder Schüler befinden, sind sie «bestimmt», geht es um einen Brief an die Eltern einer Schulkasse oder an eine Fachstelle und es geht dabei um ein Kind X, das zwar nicht namentlich genannt aber anhand spezifischer Aussagen erkannt werden kann, betreffen diese Informationen unter Umständen eine «bestimmbare» Person.

Die Bearbeitung[38] «besonderer» Personendaten wird aufgrund der stärkeren Eingriffsintensivität in die Grundrechte von Gesetzes wegen an weitere Voraussetzungen geknüpft, beispielsweise bei deren Weitergabe:[39] Es sind dies – für vorliegenden Beitrag am relevantesten – Informationen über religiöse und weltanschauliche Ansichten, über die Gesundheit, die Intimsphäre, die ethnische Herkunft oder Massnahmen der sozialen Hilfe (§ 3 Abs. 4 lit. a IDG ZH). Diese Personendaten werden im IDG ZH – anders als in der Bundesdatenschutzgesetzgebung – «besonders» genannt.[40]

---

[38] Vgl. FN 3.

[39] Vgl. § 3 Abs. 4 lit. a IDG ZH: «Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht […]».

[40] In der Bundesdatenschutzgesetzgebung werden sie «besonders schützenswert» genannt, vgl. Art. 3 lit. c des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1).

Logopädinnen und Logopäden sowie die Sozialarbeiterinnen und Sozialarbeiter bearbeiten mitunter Personendaten, die «besonders» sind.[41]

4. Datenschutzrechtliche Grundsätze

Es gilt nun, auf die zu beachtenden informationsrechtlichen Grundsätze einzugehen, wobei sich eine Kurzübersicht anhand der Systematik des IDG ZH aufdrängt:

Zunächst hat das öffentliche Organ den Umgang mit Informationen so zu gestalten, dass es rasch, umfassend und sachlich informieren kann (*Transparenzprinzip*, § 4 IDG ZH).

Das öffentliche Organ bzw. die Schule regelt die Verantwortlichkeiten der Datenbearbeitung. In Schulen des Kantons Zürich wird für die Datenbearbeitung regelmässig die Schulleitung *verantwortlich* sein, obliegt doch ihr die administrative Führung der Schule (§ 44 Abs. 1 VSG ZH). Das öffentliche Organ sorgt für den Schutz der Informationen durch *organisatorische und technische Massnahmen* (§ 7 IDG ZH).

Das öffentliche Organ darf Personendaten nur bearbeiten, soweit dies zur Erfüllung seiner *gesetzlich umschriebenen Aufgabe* (öffentliches Interesse) geeignet, erforderlich und zumutbar ist. Das Bearbeiten «besonderer» Personendaten bedarf einer hinreichend bestimmten Regelung in einem formellen Gesetz (*gesetzliche Grundlage*, § 8 IDG ZH).[42]

Bei der gesetzlichen Grundlage ist zu beachten, dass bei der *Bekanntgabe von Personendaten* an Dritte weitere, spezifische Anforderungen zu beachten sind. Das öffentliche Organ gibt Personendaten bekannt, wenn eine rechtliche Bestimmung es dazu ermächtigt, die betroffene Person im Einzelfall eingewilligt hat oder es im Einzelfall zur Abwendung einer drohenden Gefahr für Leib und Leben unentbehrlich oder der notwendige Schutz anderer wesent-

---

[41] Es handelt sich nicht um Auftragsdatenbearbeitung im Sinne von § 6 IDG ZH. Die genannten Personen bearbeiten die Personendaten als «Teil» eines staatlichen Organes, der Schule.

[42] Vgl. Bruno Baeriswyl, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zürich 2012 (zit. VerfasserIn, PraKom IDG ZH), § 8 N 3: «Grundsätzlich ist die Aufgabe eines öffentlichen Organs in einer Rechtsgrundlage umschrieben.».

licher Rechtsgüter höher zu gewichten ist (§ 16 Abs. 1 IDG ZH). Anderen öffentlichen Organen (des Kantons oder des Bundes) können sodann im Einzelfall und auf Verlangen Personendaten bekannt gegeben werden, wenn diese wiederum einen Auftrag von Gesetzes wegen haben, die Personendaten zu bearbeiten (§ 16 Abs. 2 IDG ZH). Bei «besonderen» Personendaten sind diese Anforderungen wiederum höher: Zur Bekanntgabe ist eine «*hinreichend bestimmte Regelung in einem formellen Gesetz*» erforderlich (§ 17 Abs. 1 lit. a IDG ZH) und eine allfällige Einwilligung hat «im Einzelfall ausdrücklich» zu erfolgen (§ 17 Abs. 1 lit. b IDG ZH).[43]

Schulen des Kantons Zürich bzw. die praktizierenden Logopädinnen und Logopäden sowie Sozialarbeiterinnen und Sozialarbeiter können sich bei der Bearbeitung von Personendaten auf § 3a VSG ZH stützen: Hiernach bearbeitet «die Schule» für die Erfüllung ihrer Aufgaben Personendaten, auch «besondere» (§ 3a Abs. 1 VSG ZH). «Besondere» Personendaten werden im zweiten Absatz des besagten Artikels aufgelistet, wobei auch das Sozialverhalten (Sozialarbeit) und sonderpädagogische Massnahmen gemäss § 34 VSG ZH (Logopädie) explizit genannt werden.[44] Vorliegend soll keine Prüfung stattfinden, ob § 3a VSG ZH vor dem Hintergrund von § 8 IDG ZH als «hinreichend bestimmte Regelung» zu qualifizieren ist. Im Volksschulgesetz finden sich – in Ergänzung der allgemeinen gesetzlichen Grundlage zur Bearbeitung von Personendaten in § 3a VSG ZH – sodann für einzelne Situationen spezifische Grundlagen für die Bekanntgabe von Personendaten. Es handelt sich um Meldepflichten beim Schulwechsel, bei dem die alte der neuen Schule oder der Gemeinde für die Aufnahme «notwendige» Personendaten und besondere Personendaten von Schülerinnen und Schülern bekannt gibt (§ 3b VSG ZH). Sodann besteht eine gesetzliche Grundlage zur Bekanntgabe von (auch «besonderen») Personendaten zwischen Tagesstrukturen und Schulen (§ 3c VSG ZH).[45]

---

[43] Zur Einwilligung sogleich weiter unten im gleichen Kapitel.

[44] Vgl. schliesslich § 3d VSG ZH, wobei es sich um die gesetzliche Grundlage für den elektronischen Zugriff durch die Direktion und die schulpsychologischen Dienste auf (auch «besondere» Personendaten) der Schule handelt.

[45] Vgl. ebenfalls vergleichbare informationsrechtliche Bestimmungen in § 6a ff. KJHG ZH.

Ebenfalls in § 8 Abs. 1 IDG ZH findet sich das Gebot der *Verhältnismässigkeit*.[46] Die Datenbearbeitung muss in der Folge geeignet sein, den damit verfolgten Zweck (öffentliches Interesse) zu erreichen (Geeignetheit). Es dürfen bei einer Gesamtsicht (in sachlicher, zeitlicher, räumlicher und personeller Hinsicht) keine weniger einschneidenden Massnahmen möglich sein (bspw. die Bekanntgabe von «weniger» Personendaten), um den besagten Zweck zu erreichen (Erforderlichkeit). Schliesslich muss ein ausgewogenes Verhältnis zwischen der Datenbearbeitung und dem angestrebten Zweck bzw. zwischen dem öffentlichen Nutzen und der privaten Last bestehen (Zumutbarkeit oder Verhältnismässigkeit «im engeren Sinne»).[47]

Aus dem in § 9 Abs. 1 IDG ZH fliessenden *Zweckbindungsgebot* ist sodann abzuleiten, dass das öffentliche Organ Personendaten nur zu dem Zweck bearbeiten darf, zu dem sie erhoben worden sind, soweit nicht eine rechtliche Bestimmung ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall eingewilligt hat.

Im Zusammenhang mit dem Zweckbindungsgebot ist (auch vor dem Hintergrund der Anforderung an eine gesetzliche Grundlage[48]) auf das *Konstrukt der Einwilligung* einzugehen: Die Einwilligung als im Ergebnis Ersatz für eine «gesetzliche Grundlage» zur Datenbearbeitung wird in verschiedenen Bestimmungen des IDG ZH angesprochen. Bei der Bekanntgabe von Personendaten soll sie ausnahmsweise eine gesetzliche Grundlage ersetzen (§ 16 Abs. 1 lit. b und 17 Abs. 1 lit. b IDG ZH). Sodann wird die Einwilligung beim Zweckbindungsgebot erwähnt (§ 9 Abs. 1 IDG ZH). Das öffentliche Organ soll, wenn die betroffene Person einwilligt, Personendaten auch zu einem Zweck bearbeiten dürfen, der ursprünglich, bei der Datenerhebung, nicht vorgesehen war. Die Einwilligung ist mit anderen Worten nicht für jede Datenbearbeitung notwendig, sondern kann da zum Einsatz kommen, wo eine gesetzliche Grundlage fehlt.

---

[46] § 8 Abs. 1 IDG ZH: «[…] soweit dies zur Erfüllung seiner gesetzlich umschriebenen Aufgabe *geeignet und erforderlich* ist.».

[47] Vgl., m.w.H. Baeriswyl, PraKom IDG ZH (FN 42), § 8 N 6 ff.; Müller, Verhältnismässigkeit als Grundsatz der Rechtsetzung und Rechtsanwendung, 17. Jahrestagung des Zentrums für Rechtsetzungslehre, Zürich/St. Gallen 2019, 16.

[48] Vgl. § 16 Abs. 1 und 17 Abs. 1 lit. b IDG ZH.

Die Einwilligung der betroffenen Person hat *freiwillig* und *vor* der Datenbearbeitung (Bekanntgabe oder Zweckänderung) zu erfolgen, ausserdem muss sie *aktiv* erfolgen und ist nur *im Einzelfall* möglich.[49]

Die Einwilligung ist im Verwaltungsrecht als problematisch bzw. unzulässig anzusehen, wenn sie dazu dient, das Zweckbindungsgebot oder die gesetzliche Grundlage bei der Datenbekanntgabe «auf Vorrat» zu «*überspannen*», indem sie systematisch und so offen wie möglich ausgestaltet daherkommt. Es muss gerade umgekehrt sein: Die Einwilligung hat – wenn sie durch die Behörde eingefordert wird – stets zweckgebunden zu sein und sich am Prinzip der Verhältnismässigkeit zu orientieren. Andernfalls widerspräche das Vorgehen einerseits dem Konstrukt der Einwilligung als solchem. Die einwilligende Person will nämlich (vor der Datenbearbeitung) darüber aufgeklärt werden, zu welchem (zukünftigen) Zweck die Datenbearbeitung geeignet und erforderlich ist und sie den Eingriff in ihre Grundrechte (im Einzelfall) duldet. Andererseits ist das Prinzip der Verhältnismässigkeit für sämtliches staatliches Handeln, mitunter auch die Einholung einer Einwilligung bei der von der Datenbearbeitung betroffenen Person, zwingend zu beachten (Art. 5 BV).

Im Grundsatz nachvollziehbar (und im IDG ZH vorgesehen) ist die Einwilligung dann, wenn sie *tatsächlich im Einzelfall* und auf der Grundlage der einschlägigen Bestimmungen im Datenschutzrecht eine nicht vorhersehbare Zweckänderung ermöglichen oder eine gesetzliche Grundlage zur Bekanntgabe von (besonderen) Personendaten an Dritte ersetzen bzw. ergänzen soll. Im Ergebnis können nämlich durch die informationsrechtlichen Bestimmungen nicht sämtliche Informationsflüsse einer Verwaltung durch rechtliche Grundlagen definiert werden; das ist schlicht lebensfremd.

Diese im Ergebnis «Erweiterung» der gesetzlichen Grundlage lässt sich aus dem Selbstbestimmungsrecht ableiten, das sich wiederum aus der Bundesverfassung ableiten lässt (Art. 10 Abs. 2 BV und Art. 13 Abs. 2 BV), *eigene* Personendaten im Rahmen eines Auskunftsrechts erhältlich zu machen und an Dritte weiterzugeben. Freilich sind in dieser Situation die Anforderungen an eine Einwilligung im Einzelfall vollumfänglich einzuhalten, wobei die Frei-

[49] Rudin, PraKom IDG ZH (FN 42), § 16 N 14 f.; vgl. zu den Anforderungen von Art. 4 Abs. 5 der Bundesdatenschutzgesetzgebung Tobias Fasnacht, Die Einwilligung im Datenschutzrecht, Zürich 2017, N 222 ff.

willigkeit – gerade im Verwaltungsrecht – einen hohen Stellenwert einnimmt: Gibt es nämlich keine gesetzliche Grundlage, ist der Staat rechtlich und somit faktisch vollumfänglich auf eine Einwilligung des Einzelnen angewiesen, die den einschlägigen Anforderungen entspricht, andernfalls er ohne gesetzliche Grundlage handelt. Ob eine gültige Einwilligung vorliegt, lässt sich im Ergebnis nur im konkreten Einzelfall feststellen und ist anhand der einschlägigen – bereits erwähnten[50] – Anforderungen an eine datenschutzrechtliche Einwilligung zu prüfen.

Ein wesentlicher Pfeiler des Datenschutzrechts ist sodann das *Auskunftsrecht*, welches sich direkt aus der Bundesverfassung ableiten lässt.[51] Jede Person hat gemäss § 20 Abs. 2 IDG ZH Anspruch auf Zugang zu den *eigenen* Personendaten.[52] Das Auskunftsrecht kann aus Perspektive der Verwaltung im Einzelfall aufgrund einer – im Gesetz definierten – Prüfung bzw. Abwägung der involvierten öffentlichen und privaten Interessen verweigert werden (§ 23 IDG ZH). Das Verfahren auf Zugang zu Personendaten wird in den § 24 ff. IDG ZH definiert.

Im Hinblick auf die erwähnten Leitlinien und Prinzipien, die sich aus den einschlägigen datenschutzrechtlichen Bestimmungen ableiten lassen, ist abschliessend zu thematisieren, wann diese zu beachten (und einzuhalten) sind. Welche Rolle spielt das Datenschutzgesetz, wenn gleichzeitig andere informationsrechtliche Bestimmungen anwendbar sind (wie bspw. die Melderechte und -pflichten oder das Amtsgeheimnis)?

5. Datenschutz als Querschnittsmaterie

Regelmässig wird Datenschutzrecht als Querschnittsmaterie umschrieben. Dies ist insofern zutreffend, als Datenschutzgesetze immer dann anwendbar sind, wenn Personendaten durch die Verwaltung bearbeitet werden und keine

---

[50] Vgl. oben im gleichen Kapitel.

[51] Vgl. Belser, Datenschutzrecht Grundlagen (FN 32), 368 f.

[52] Darüber hinaus stehen der betroffenen Person von Gesetzes wegen verschiedene am Auskunftsrecht angehängte Rechte zu: Sie kann verlangen, dass unrichtige Personendaten berichtigt oder vernichtet werden, die widerrechtliche Datenbearbeitung unterlassen wird, die Folgen der widerrechtlichen Bearbeitung beseitigt werden, die Widerrechtlichkeit der Datenbearbeitung festgestellt (§ 21 Abs. 1 IDG ZH) oder die Bekanntgabe ihrer Personendaten an Private gesperrt wird (§ 22 Abs. 1 IDG ZH).

anderen gesetzlichen Grundlagen einen Informationsfluss regeln. Im Datenschutzgesetz werden mit anderen Worten alle Datenbearbeitungsvorgänge auf einer abstrakten Ebene geregelt, so dass sämtliche Informationsflüsse der Verwaltung darunterfallen können, wenn nicht speziellere Bestimmungen (sog. «lex specialis») anwendbar sind.

So sind beispielsweise (nur) Verwaltungsverfahrensgesetze oder die Strafprozessordnung als «Datenschutzgesetze» anwendbar, solange ein Verwaltungs- oder Strafverfahren läuft.[53] Der Informationsfluss wird dann durch die einschlägigen Verfahrensgesetze (teilweise sehr unterschiedlich) geregelt; vor dem Verfahren und sobald das Verfahren beendet ist, sind wieder die (allgemeinen) Datenschutzgesetze anwendbar. Vorliegend interessiert insbesondere das Zusammenspiel zwischen dem Datenschutzgesetz und Amts- und Berufsgeheimnissen einerseits sowie Melderechten und -pflichten andererseits:

Die Bekanntgabe von Personendaten erfordert eine Rechtsgrundlage und muss verhältnismässig sein (§ 8 Abs. 1 IDG ZH). Sind diese Voraussetzungen gegeben, handelt es sich um rechtmässiges staatliches Handeln.[54] Werden Amtsgeheimnisse auf der Grundlage einer spezifischen Gesetzesgrundlage, wie bspw. einem Datenschutzgesetz, Dritten bekannt gegeben, kann dies keine Amtsgeheimnisverletzung darstellen. Dies lässt sich aus dem allgemeinen Prinzip des Strafrechts ableiten, wonach kein Vorgang unter Strafe stehen kann, der rechtmässig erfolgt.[55] Liegt allerdings keine gesetzliche Grundlage vor bzw. ist die Datenbekanntgabe an Dritte «unverhältnismässig» und erfolgt sie vorsätzlich, das heisst willentlich, gegenüber einem unbefugten Dritten, ist diese als Amtsgeheimnisverletzung zu werten und gegebenenfalls strafbar.

Dasselbe gilt für die Situation, in der eine Sozialarbeiterin oder ein Sozialarbeiter bzw. eine Logopädin oder ein Logopäde von ihren zivilrechtlichen Melderechten oder -pflichten Gebrauch macht.[56] Werden die Voraussetzungen der besagten Bestimmungen eingehalten, erfolgt die Datenbekanntgabe auf der Grundlage einer spezifischen Bestimmung; die Bekanntgabe ist somit

---

[53] Vgl. § 2b Abs. 1 IDG ZH.

[54] Vgl. oben II.G.4.

[55] Art. 14 StGB: «Wer handelt, wie es das Gesetz gebietet oder erlaubt, verhält sich rechtmässig, auch wenn die Tat nach diesem oder einem anderen Gesetz mit Strafe bedroht ist.».

[56] Vgl. oben II.F.

auch gemäss der allgemeineren Bestimmung in § 16 f. IDG ZH zulässig und folglich auch nicht strafbar. Auch hier entfällt grundsätzlich eine Amtsgeheimnisverletzung.

H. Das Kind im Informationsrecht

Es geht bei den Personendaten, die in der Schule bearbeitet werden, wohl zu einem überwiegenden Teil um Daten, die in Bezug zu einer Schülerin und einem Schüler stehen. Es stellt sich folglich die Frage, inwiefern das Kind in der Lage ist, auf die «Informationsflüsse» selbständig Einfluss zu nehmen. Die Frage kann auch aus einer anderen Perspektive gestellt werden: Gibt es im Datenschutzrecht Handlungsbereiche des Kindes bzw. der Schülerin oder des Schülers, auf welche die Eltern im Rahmen ihrer gesetzlichen Vertretungsmacht der elterlichen Sorge keinen Einfluss haben? Was bedeutet es beispielsweise, wenn ein Kind den Willen äussert, dass weder die Eltern oder die Kindesschutzbehörde informiert oder involviert werden sollen? Oder was sind die Folgen, wenn es will, dass die Mutter oder der Vater nicht in eine spezifische Angelegenheit involviert werden, wie im Beispiel bei der Abklärung, ob eine logopädische Behandlung notwendig ist? Wie ist sodann mit der Situation umzugehen, wenn zwischen einem Elternteil und dem Kind ein Interessenskonflikt vorliegt?

Dies sind relevante Fragen, weil nicht auszuschliessen ist, dass die Sozialarbeiterin oder der Sozialarbeiter sich in der Lage befindet, dass sie die Sachverhaltsdarstellung des Kindes erfährt, aber nicht die der Eltern oder die Logopädin bzw. der Logopäde als Vertrauensperson des Kindes persönlichkeitsrelevante Dinge erfährt, die selbst die Eltern nicht erfahren etc. Sind die genannten Personen in dieser Situation verpflichtet, sich an die Wünsche und Aussagen des Kindes zu halten oder befugt, sich über solche im Sinne der «Klärung eines Sachverhaltes», bspw. bei einer Kindswohlgefährdung, hinwegzusetzen? Wie sieht es aus, wenn eine Sozialarbeiterin oder ein Sozialarbeiter eigene Interessen verfolgt, etwa wenn sie das Vertrauensverhältnis mit dem Kind durch ein Nichtinvolvieren der Eltern schützen will, um ihre *eigene* Aufgabenerfüllung nicht zu gefährden? Die Fragen können nicht abstrakt beantwortet werden, sondern erfordern eine Klärung im konkreten Einzelfall; die rechtlichen Rahmenbedingungen geben dabei Anhaltspunkte und Leitlinien:

Kinder und Jugendliche haben gemäss Art. 11 BV einen Anspruch auf besonderen Schutz ihrer Unversehrtheit und auf Förderung ihrer Entwicklung. Im besagten Artikel wird im zweiten Absatz ausgeführt, dass sie «ihre Rechte im Rahmen ihrer Urteilsfähigkeit aus[üben]».[57]

Im Hinblick auf das Informationsrecht ist dieser Artikel wie folgt zu verstehen: Die sogenannten «Datenschutzgrundrechte» ergeben sich aus Art. 10 Abs. 2 BV (Recht auf persönliche Freiheit) und Art. 13, insbesondere Abs. 2 BV («Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten»).[58]

Die Konkretisierung dieser verfassungsmässigen Rechte finden sich für die Bearbeitung von Personendaten *durch kantonale Organe* in den kantonalen Datenschutzgesetzen und für die Bundesverwaltung im Datenschutzgesetz des Bundes.[59] Aus diesen einschlägigen Datenschutzbestimmungen ergeben sich keine ausdrücklichen Hinweise, ab wann oder unter welchen Umständen Kinder ihre Rechte im Rahmen ihrer Urteilsfähigkeit ausüben (Art. 11 Abs. 2 BV).

Anders verhält es sich im *privaten Datenschutzrecht*, wo das Datenschutzgesetz des Bundes im Ergebnis eine Konkretisierung der Generalklausel betreffend die Persönlichkeitsverletzung (Art. 28 ZGB) darstellt;[60] für Kinder lässt sich die Frage somit anhand der entwickelten Prinzipien des Zivilrechts beantworten. Diese Konkretisierung der Urteilsfähigkeit ist vor dem Hintergrund von Art. 11 BV, wegen dem Grundsatz der Einheit der Rechtsordnung, aber unter Berücksichtigung der Situation, dass Schülerinnen und Schüler in einem besonderen Näheverhältnis zum Staat stehen, m.E. auch im Verwaltungsrecht zu berücksichtigen:

Gemäss Art. 19*c* Abs. 1 ZGB üben urteilsfähige handlungs*un*fähige[61] Personen ihre Rechte selbständig aus, *die ihnen um ihrer Persönlichkeit willen zustehen*. «Datenschutzrechte», zumindest das Auskunftsrecht, im Sinne von

---

[57] Vgl. zum Ganzen: BSK BV-Tschentscher (FN 5), Art. 11 N 24 ff.

[58] Vgl. für einen Überblick Belser/Epiney/Waldmann (FN 32), 319 ff.

[59] Vgl. oben II.A.

[60] BGE 138 II 346 E. 8.

[61] Art. 13 ZGB: «Die Handlungsfähigkeit besitzt, wer volljährig und urteilsfähig ist.» Handlungs*un*fähig ist im Sinne von Art. 19*c* ZGB, wenn jemand urteilsfähig aber noch nicht volljährig ist.

Persönlichkeitsrechten gemäss Art. 28 ff. ZGB, sind relativ höchstpersönliche Rechte.[62] Die Frage, inwiefern eine minderjährige Person ihre Datenschutzrechte gegenüber Dritten geltend machen kann, hängt somit einzig von deren *Urteilsfähigkeit* ab. Urteilsfähig im Sinne des Gesetzes ist jede Person, der nicht wegen ihres Kindesalters, infolge geistiger Behinderung, psychischer Störung, Rausch oder ähnlicher Zustände die Fähigkeit mangelt, vernunftgemäss zu handeln (Art. 16 ZGB).

Die Urteilsfähigkeit orientiert sich im jeweiligen Sachverhalt anhand der Willensbildungsfähigkeit und Willensumsetzungsfähigkeit des minderjährigen Kindes.[63] Das Kind soll einerseits die Fähigkeit haben, sich einen eigenen Willen zu bilden, was voraussetzt, die Vor- und Nachteile einer Persönlichkeitsverletzung zu erkennen und auch beurteilen zu können, und diesen schliesslich gegen aussen kundzutun. Andererseits wird vorausgesetzt, dass die Entscheidung von der minderjährigen Person auch umgesetzt werden kann, was beinhaltet, einen gewissen Widerstand gegenüber Fremdbeeinflussung leisten zu können.[64]

Wichtig erscheint erneut zu betonen, dass die Urteilsfähigkeit einer Schülerin oder eines Schülers immer im konkreten Einzelfall zu beurteilen ist, sich die Urteilsfähigkeit mit anderen Worten nicht bspw. an einem gewissen Alter festlegen lässt (sog. *Relativität der Urteilsfähigkeit*).[65] Im Ergebnis kann somit die Frage nach der Urteilsfähigkeit einer Schülerin oder eines Schülers im Hinblick ihrer Datenschutzrechte nicht abstrakt beantwortet werden. Vielmehr ist anhand der konkreten Situation die Willensbildungs- und Willensumsetzungsfähigkeit des minderjährigen Kindes von dessen *peers* zu beurteilen.

Es ist im Grundsatz nicht ganz von der Hand zu weisen, dass die einzelne Schülerin oder der einzelne Schüler in einem jungen Alter aufgrund diverser mehr

---

[62] Vgl. zur Abgrenzung zwischen «absolut» und «relativ» höchstpersönlichen Rechten etwa BSK ZGB I-Roland Fankhauser, in: Christiana Fountoulakis/Thomas Geiser (Hrsg.), Basler Kommentar zum schweizerischen Zivilgesetzbuch I, Art. 1 – 456 ZGB, 6. A., Basel 2018 (zit. BSK ZGB I-VerfasserIn), Art. 19c N 5 ff.

[63] Relativität der Urteilsfähigkeit, vgl. BSK ZGB I-Roland Fankhauser (FN 62), Art. 16 N 6 ff., 15, 34 ff.

[64] Fasnacht (FN 49), N 628, m.w.H.

[65] Wie dies beispielsweise beim Entscheid über das religiöse Bekenntnis ab 16 Jahren der Fall ist, vgl. Art. 303 Abs. 3 ZGB.

oder weniger starker Abhängigkeiten im jeweiligen sozialen Umfeld – Familie und Schule – Mühe haben dürfte, die Tragweite ihrer bzw. seiner einzelnen (datenschutzrechtlichen) Handlungsanweisungen zu erfassen. Nichtsdestotrotz ist die Prüfung der Urteilsfähigkeit im Einzelfall unter Berücksichtigung sämtlicher Umstände vorzunehmen. Zumindest darf die Aussage des Kindes im konkreten Einzelfall keinesfalls ausser Acht gelassen werden, sondern ist zu protokollieren und eine Nichtberücksichtigung zu begründen. Aussagen eines Kindes sind mit anderen Worten in einer Gesamtinteressenabwägung zu berücksichtigen, damit sichergestellt wird, dass sie ihre Rechte im Rahmen ihrer Urteilsfähigkeit ausüben können (Art. 11 Abs. 2 BV). Ist ein Kind im Hinblick auf einen informationsrechtlichen Vorgang urteilsfähig, nimmt es seine Rechte selbständig wahr.

I. Zusammenfassung

Zusammenfassend sind aus den vorangehenden Absätzen für Sozialarbeiterinnen und Sozialarbeiter sowie für Logopädinnen und Logopäden die nachfolgenden informationsrechtlichen grundsätzlichen Überlegungen abzuleiten:

Sozialarbeiterinnen und Sozialarbeiter sowie Logopädinnen und Logopäden, die im Rahmen einer Schule tätig werden, handeln mit ihrer Arbeit im Namen und Auftrag des Staates. Ihre (auch informationsbezogene) Tätigkeit bedarf mithin einer gesetzlichen Grundlage.

Sie unterstehen dem *Amtsgeheimnis*, aber nicht dem Berufsgeheimnis. Geheime Tatsachen, die eine Person in der Eigenschaft eines Mitglieds der Verwaltung erfährt, dürfen somit nicht an Dritte bekannt gegeben werden. Die (vorsätzliche) Verletzung des Amtsgeheimnisses ist eine strafbare Handlung, die mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft wird.

Gemäss Schweizerischem Zivilgesetzbuch haben Sozialarbeiterinnen und Sozialarbeiter sowie Logopädinnen und Logopäden ein *Melderecht* gegenüber den Kindesschutzbehörden, wenn die körperliche, psychische oder sexuelle Integrität eines Kindes gefährdet erscheint. Weil sie nicht dem Berufsgeheimnis unterstehen, haben sie zudem eine *Meldepflicht*, «wenn konkrete Hinweise dafür bestehen, dass die körperliche, psychische oder sexuelle Integrität des Kindes gefährdet ist und (die meldepflichtigen Personen) nicht im Rahmen

ihrer Tätigkeit Abhilfe schaffen können». Die Pflicht gilt als erfüllt, wenn die Meldung an die vorgesetzte Person gerichtet ist. Kommen sie einer Meldepflicht nach, indem sie ihre Vorgesetzten damit konfrontieren, bleibt das Melderecht bestehen.

Staatliche Datenbearbeitung ist im Rahmen verwaltungsrechtlichen Handelns immer rechtfertigungsbedürftig; die Bearbeitung von Personendaten bedarf mithin immer einer *gesetzlichen Grundlage* und sie muss *verhältnismässig* erfolgen. Sozialarbeiterinnen und Sozialarbeiter sowie Logopädinnen und Logopäden haben sich bei der Datenbearbeitung an das kantonale Datenschutzrecht zu halten. Sie können sich hierbei auf das Volksschulgesetz und das Informations- und Datenschutzgesetz des Kantons Zürich stützen: Erlaubt ist zur Erfüllung der Aufgaben sowohl die Bearbeitung «normaler» als auch «besonderer» Personendaten. Spezifische Anforderungen sind zu beachten, wenn Personendaten *an Dritte bekannt gegeben werden*. Die Bekanntgabe ist nur erlaubt, wenn eine rechtliche Bestimmung dazu ermächtigt, die betroffene Person im Einzelfall eingewilligt hat oder sie zur Abwendung einer drohenden Gefahr für Leib und Leben unentbehrlich oder der notwendige Schutz anderer Rechtsgüter höher zu gewichten ist. Bei «besonderen» Personendaten ist eine «hinreichend bestimmte Regelung in einem formellen Gesetz» erforderlich und eine allfällige Einwilligung hat «im Einzelfall ausdrücklich» zu sein.

Ein wichtiger Pfeiler des Datenschutzrechts ist sodann das *Auskunftsrecht*. Jede Person hat Anspruch auf Zugang zu den eigenen Personendaten. Es ist die Grundlage, dass die betroffene Person von ihren weiteren Rechten Gebrauch machen kann: Sie kann die Widerrechtlichkeit der Datenbearbeitung feststellen oder die Bekanntgabe ihrer Personendaten an Dritte sperren lassen.

Das Datenschutzrecht ist sodann eine *Querschnittsmaterie* bzw. immer dann anwendbar, wenn Personendaten bearbeitet werden. Die Bekanntgabe von Personendaten an Dritte darf nur auf der Grundlage eines Rechtssatzes erfolgen und muss verhältnismässig sein. Liegt eine Rechtsgrundlage vor, handelt es sich um ein rechtlich zulässiges Vorgehen. Liegt keine gesetzliche Grundlage vor, ist die Datenbekanntgabe unzulässig. Solche Datenbekanntgaben sind ausserdem unter Umständen aufgrund einer Amtsgeheimnisverletzung strafbar. Melderechte und -pflichten sind, wenn deren rechtliche Voraussetzungen eingehalten werden, als gesetzliche Grundlage für eine Datenbekanntgabe zu qualifizieren, womit diese nicht strafbar sein können.

Zu beachten ist schliesslich, dass Kinder und Jugendliche aufgrund von Art. 11 BV einen Anspruch auf besonderen Schutz ihrer Unversehrtheit und auf Förderung ihrer Entwicklung haben; sie üben ihre Rechte im Rahmen ihrer Urteilsfähigkeit aus. Dies hat direkt zur Folge, dass grundsätzlich auch das Kind mitbestimmt, was mit seinen Personendaten geschieht. Damit ein Kind gehört wird, ist allerdings die Urteilsfähigkeit desselben in Betracht zu ziehen. Als urteilsfähig im Hinblick auf seine Informationsrechte gilt es, wenn es die Fähigkeit hat, sich einen eigenen Willen zu bilden und diesen gegen aussen kundzutun. Ebenfalls wird vorausgesetzt, dass die Entscheidung vom Kind umgesetzt werden kann, was auch beinhaltet, einen gewissen Widerstand gegen Fremdbeeinflussung leisten zu können. Die Urteilsfähigkeit lässt sich in der Folge nur im konkreten Einzelfall beurteilen, wobei die Beurteilung im Einzelfall durch seine *peers* bzw. durch die Sozialarbeiterinnen und Sozialarbeiter sowie die Logopädinnen und Logopäden erfolgt. Die Aussagen des Kindes sind in der Folge nicht unbeachtlich und sind im Einzelfall in einer Interessensabwägung zu berücksichtigen.

III. Anwendung auf die einleitend erwähnten Fallbeispiele

A. Fallbeispiel 1 – Sachverhalt

Ein Kind, 11 Jahre, wird logopädisch abgeklärt. Insbesondere im Singunterricht war auffällig, dass das Kind die Töne nicht trifft, aber auch vom Lehrer und der Sozialarbeiterin wird seit einiger Zeit berichtet, dass die Schülerin sich flüsternd, teilweise sogar tonlos und nur auf Nachfrage hin am Unterricht beteiligt. Der Logopäde der Schule trifft sich mit dem Vater des Kindes und es scheint, als ob soziale Faktoren Ursache für die Stimmstörungen seien. Nach Aussagen des Vaters wird klar, dass das Kind wohl im häuslichen Umfeld aufgrund der Überlastung der Eltern (beide sind berufstätig und haben Beschwerden psychologischer Art) oft in schwere Konflikte mit den Eltern gerät. Die Rede ist von heftigen verbalen Auseinandersetzungen, indirekt erwähnt werden teilweise (verbal) übergriffige Situationen gegenüber dem Kind durch die Mutter. Die Eltern sind in Paartherapie, beide Elternteile sind separat in psychologischer, teilweise psychiatrischer Behandlung; der Vater hat die Be-

handlung komplett abgebrochen. Der Logopäde trifft sich auch mit dem Kind, das ihm mitteilt, es wolle nicht, dass die Mutter in die Angelegenheit involviert werde. Auf Nachfrage nach den Gründen hierfür bricht das Kind in Tränen aus und spricht nicht mehr über den Vorfall. Auch in den nachfolgenden Treffen antwortet das Kind ausweichend. Der Logopäde informiert seinen Vorgesetzten in der Angelegenheit und schlägt eine Unterstützung im geschützten Rahmen in Form einer logopädischen Therapie der Stimmstörung vor. Die Klassenlehrerin des Kindes ist aufgrund der inzwischen fortgeschrittenen Lücke beim Schulstoff der Meinung, ein regelmässiger Besuch des Unterrichts sei unumgänglich; die angesetzte logopädische Unterstützung von je drei Wochenstunden, die allesamt aufgrund terminlicher Knappheit beim Logopäden in wichtige Unterrichtsfächer fallen, seien dem schulischen Fortkommen der Schülerin abträglich. Im Pausenraum will die Klassenlehrerin über die Hintergründe der logopädischen Behandlung informiert werden, «man sei ja hier im geschützten Raum der Schule». Ebenso will die Mutter über das Vorgehen informiert werden. Was darf der Logopäde mit der Klassenlehrerin besprechen und muss die Mutter informiert werden?

B. Fallbeispiel 1 – Anwendung der informationsrechtlichen Bestimmungen

1. Fragestellung

Im ersten Beispiel geht es um die Frage, ob Personendaten bekannt gegeben werden dürfen, die eine logopädische Anamnese und die daraus folgende Behandlung betreffen, und zwar in zwei verschiedenen Konstellationen: Einerseits der Mutter des Kindes und andererseits der Klassenlehrerin des Kindes innerhalb des Schulbetriebs. Der Logopäde hat sich an den einschlägigen informationsrechtlichen Bestimmungen zu orientieren: Anwendbar ist das Informations- und Datenschutzgesetz des Kantons Zürich, allenfalls stellt sich auch die Frage nach einer Amtsgeheimnisverletzung. Da es sich bei den Informationen im Zusammenhang der Schülerin um «besondere» Personendaten handelt (insbesondere Personendaten über die Gesundheit), sind die besonderen Anforderungen an die Datenbekanntgabe zu beachten.[66]

[66] Vgl. oben II.G.3.

2. Bekanntgabe der Personendaten an die Mutter

Es ist dem Grundsatz nach davon auszugehen, dass die Mutter als gesetzliche Vertreterin ihres Kindes im Rahmen ihrer elterlichen Sorge (Art. 304 Abs. 1 ZGB) Anspruch auf Auskunft über Personendaten ihres Kindes hat. In der Folge ist ihr grundsätzlich vollumfängliche Auskunft über die Personendaten ihres Kindes bzw. über die Vorkommnisse zu erteilen, weil eine gesetzliche Grundlage zur Datenbekanntgabe vorliegt.

Dieser Auskunftsanspruch kann aus Perspektive der Schule bzw. des Logopäden auf der Grundlage von § 23 IDG ZH im Einzelfall aufgrund überwiegender privater Interessen Dritter eingeschränkt werden. Wenn nun das urteilsfähige[67] Kind sein Interesse bekundet, es wolle, dass die Mutter davon nichts erfährt, stellt sich die Frage, ob das Auskunftsrecht aufgrund der Interessen des Kindes und folglich auf der Grundlage von § 23 IDG ZH gegenüber der Mutter eingeschränkt werden kann.

Diese Herangehensweise ist aber technisch nicht korrekt. Die Antwort auf diese Frage ist somit im Zivilrecht, genauer bei den Bestimmungen zur elterlichen Sorge und der Vertretungsmacht der Eltern, zu suchen. Gemäss Art. 304 Abs. 1 ZGB haben die Eltern von Gesetzes wegen die Vertretung des Kindes gegenüber Drittpersonen «im Umfang der ihnen zustehenden elterlichen Sorge» inne.

Grenzen der elterlicher Vertretungsmacht finden sich u.a. in Art. 305 Abs. 1 ZGB. Dieser statuiert, dass das urteilfähige Kind unter elterlicher Sorge im Rahmen des Personenrechts durch eigenes Handeln Rechte und Pflichten begründen und höchstpersönliche Rechte selbst ausüben kann.[68] «Datenschutzrechte» sind höchstpersönliche Rechte, weshalb das *urteilsfähige* Kind sie selber ausüben kann.[69]

---

[67] Vgl. oben II.H.

[68] Vgl. aus Perspektive von Art. 304 ZGB: BSK ZGB I-Schwenzer/Cottier (FN 62), Art. 304/305 N 6: «Nur mit der Einwilligung des Kindes können die Eltern das urteilsfähige Kind vertreten, wo es um die Ausübung von Rechten geht, die ihm um seiner Person willen zustehen, sofern das jeweilige Recht nicht per se vertretungsfeindlich ist […].»

[69] Vgl. oben II.H.

Im Ergebnis führt das dazu, dass die Mutter gar keinen Auskunftsanspruch hinsichtlich der Personendaten ihres Kindes gemäss IDG ZH hat, sofern das Kind in der fraglichen Situation urteilsfähig ist.

Besteht die konkrete Möglichkeit, dass die Tochter durch die Mutter einer gefährlichen Situation ausgesetzt wird (unabhängig von der Urteilsfähigkeit der Tochter), hat dies eine Interessenskollision im Sinne von Art. 306 Abs. 3 ZGB zur Folge,[70] wobei die Vertretungsmacht der Mutter von Gesetzes wegen ganz entfällt. Auch in dieser Situation hat die Mutter somit keinen Auskunftsanspruch, selbst wenn ihre Tochter *nicht urteilsfähig* ist; es besteht m.a.W. keine gesetzliche Grundlage, die Personendaten der Mutter bekanntzugeben.

Es ist folglich zu prüfen, ob die Tochter urteilsfähig ist im Hinblick auf die Unterbindung des Informationsflusses zwischen der Schule und ihrer Mutter oder ob eine Interessenskollision vorliegt.

Dies ist, wie schon erläutert, im Einzelfall einer Prüfung zu unterziehen: Ob die Schülerin im konkreten Einzelfall urteilsfähig ist, hängt von ihrer Willensbildungs- und Willensumsetzungsfähigkeit ab. Im vorliegenden Sachverhalt hat sich die Schülerin ihren eigenen Willen gebildet und gegen aussen kundgetan. Es ist somit abzuklären, ob die Schülerin aufgrund ihrer persönlichen Entwicklung in der Lage war, diesen (eigenen) Willen zu bilden bzw. die Vor- und Nachteile zu erkennen und auch beurteilen zu können. Dies kann nicht abstrakt beantwortet werden. Die Abklärung obliegt im konkreten Einzelfall dem Logopäden, allenfalls in Zusammenarbeit mit seinen Vorgesetzten. Ebenso ist abzuklären, ob die Schülerin angesichts ihres jungen Alters sich der Konsequenzen ihrer Aussagen bewusst ist. Ist sie sich mit anderen Worten der Folgen einer Nichtkommunikation bewusst?

Bei einer ersichtlichen möglichen Gefährdung der Tochter durch die Mutter liegt eine Interessenskollision vor, insbesondere wenn sich die Tochter konkret hinsichtlich gefährdender Vorkommnisse äussert oder andere Anhaltspunkte für eine Gefährdung bestehen. Dies erfordert allerdings, dass die Tochter solche gegenüber Dritten auch äussert. Weitere Abklärungen durch den Logopäden mit der Tochter wären vor dem Hintergrund möglicher Gefährdungen angebracht.

---

[70] «Bei Interessenkollision entfallen von Gesetzes wegen die Befugnisse der Eltern in der entsprechenden Angelegenheit.» (Art. 306 Abs. 3 ZGB).

Zu prüfen ist schliesslich, ob aufgrund von Art. 314*d* Abs. 1 ZGB der Logopäde verpflichtet ist, der Kindesschutzbehörde eine Meldung zu machen. Im konkreten Sachverhalt hat er die Vorkommnisse seinem Vorgesetzten geschildert, womit er seiner zivilrechtlichen Informationspflicht nachgekommen ist.

3. Bekanntgabe der Personendaten an die Lehrerin

Die zweite Fragestellung betrifft die Kommunikation zwischen dem Logopäden und der Klassenlehrerin. Der Logopäde und die Klassenlehrerin können sich bei ihrer schulinternen Kommunikation auf die gesetzlichen Grundlagen in § 3a Abs. 1 und 2 VSG ZH stützen.[71] Sie können für die Erfüllung ihrer Aufgaben (auch «besondere») Personendaten bearbeiten bzw. Informationen hinsichtlich der Schülerin austauschen.

Allerdings muss eine derartige Weitergabe von Personendaten auch verhältnismässig sein (§ 8 IDG ZH): Verhältnismässigkeit bedeutet, dass die Datenbearbeitung einem spezifischen Ziel (öffentliches Interesse) dient, dieses durch die Datenbearbeitung auch erreicht werden kann und bei einer Gesamtabwägung der Interessen keine weniger einschneidenden Massnahmen gibt, um dieses Ziel zu erreichen.

Die Klassenlehrerin macht sich aufgrund der inzwischen fortgeschrittenen Lücke beim Schulstoff Sorgen; ein regelmässiger Besuch des Unterrichts der Schülerin sei unumgänglich. Sie will informiert werden über die Hintergründe der logopädischen Behandlung. Es wird sich bei dem Interesse der Lehrperson nicht um reine «Neugier» handeln, schliesslich muss sie als Lehrperson ihren Bildungsauftrag wahrnehmen, ist dazu arbeitsvertraglich verpflichtet und auch gegenüber ihren Vorgesetzten Rechenschaft schuldig, warum einzelne ihrer Schülerinnen oder Schüler nicht in der Lage sind, dem Schulstoff nachzukommen. Hierbei handelt es sich um das öffentliche Interesse, zu dessen Erreichung der Austausch über die Hintergründe der logopädischen Behandlung allenfalls *geeignet* sein könnte.

Aufgrund des Wissens des Logopäden über die Eltern bzw. das familiäre Umfeld der Tochter besteht allerdings ein klassischer Interessenskonflikt zwischen

[71] «Die zuständigen öffentlichen Organe bearbeiten für die Erfüllung ihrer Aufgaben nach diesem Gesetz Daten, einschliesslich Personendaten und besonderer Personendaten von Schülerinnen und Schülern.» (§ 3a Abs. 1 VSG ZH).

dem Informationsinteresse der Klassenlehrerin im Hinblick auf die eingeleiteten logopädischen Massnahmen einerseits und die Privatsphäre der Eltern andererseits. Der Vater hat im Gespräch mit dem Logopäden offengelegt, dass es zuhause oft zu Konflikten mit der Tochter kommt, gesprochen wird ebenfalls von einer Paartherapie der Eltern sowie von separaten psychologischen, teilweise psychiatrischen Behandlungen. Bei einer Interessensabwägung muss somit dem Logopäden klar sein, dass er grundsätzlich nicht befugt ist, mit Lehrpersonen über medizinische Angelegenheiten der Eltern zu sprechen, weil diese Angaben im Hinblick auf das Ziel, die Lehrperson über die Gründe der logopädischen Behandlung zu informieren, nicht notwendig ist, sondern darüber hinaus gehen (Erforderlichkeit). In einer Gesamtabwägung ist eine Information über die Grundzüge der Entscheide des Logopäden wohl eine verhältnismässige Lösung: Es ist angesichts des Rechts auf Privatsphäre und den Geheimhaltungsinteressen der Eltern diesen nicht zumutbar, dass ihre gesundheitsrelevanten Personendaten offengelegt werden, weil dadurch kein zusätzlicher Nutzen entsteht (Verhältnismässigkeit im engeren Sinne). Im Fazit ist ein Gespräch durchaus möglich, sollte aber so geführt werden, dass nur effektiv erforderliche Informationen weitergegeben werden.

Selbstverständlich besteht ein Informationsbedürfnis der Klassenlehrerin hinsichtlich sämtlicher (auch familiärer) Umstände der eigenen Schülerinnen und Schüler. Das Informationsbedürfnis und die -bereitschaft haben sich allerdings im Schulalltag am Prinzip der Verhältnismässigkeit zu orientieren. Dies hat *nicht* zur Folge, dass sich die Mitarbeiterinnen und Mitarbeiter einer Schule gegenseitig nicht vertrauen, sondern manifestiert sich im Auftrag der Beteiligten, die Persönlichkeitsrechte der Betroffenen zu schützen.

C. Fallbeispiel 2 – Sachverhalt

Bei einem Jungen in der 6. Klasse wird ein Leistungsabfall beobachtet. Er wurde bereits im vergangenen Jahr im Zusammenhang mit Vorfällen von der Sozialarbeiterin betreut; auch die Polizei war involviert. Die Klassenlehrperson spricht bei dem Jungen aufgrund der Vorfälle von einem «verlorenen Schuljahr». Im Gespräch mit dem Jungen ergibt sich, dass die Eltern regelmässig eheliche Konflikte vor den Kindern austragen und gegenüber dem Jungen handgreiflich werden, möglicherweise kommt es auch zu Schlägen.

Die Eltern werden durch die Sozialarbeiterin im Rahmen eines Gesprächs miteinbezogen und aufgefordert, gemeinsam eine Elternberatung zu besuchen. Der Vater stellt der Sozialarbeiterin während des Gesprächs die Frage, weshalb die Elternberatung denn notwendig sei. Ihm wird geantwortet, dass «sei halt nötig wegen der Konflikte zwischen den Eheleuten». Dass der Junge physische Gewalt angedeutet hat, wird ihm bzw. den Eltern nicht mitgeteilt. Die Sozialarbeiterin berät sich mit ihrer Vorgesetzten und informiert diese über die Andeutungen des Jungen betreffend der Schläge. Die Vorgesetzte sieht «im Moment» keinen weiteren Handlungsbedarf. Die Elternberatung findet statt, der Vater nimmt daran nicht teil. Der Junge gibt der Sozialarbeiterin in der Zwischenzeit bekannt, dass er vom Vater im Rahmen einer Auseinandersetzung gegen eine Tischkante gestossen wurde, was in einer Platzwunde resultierte. Die Sozialarbeiterin ist sich nicht sicher, was sie tun soll. Die Eltern miteinbeziehen will sie nicht, hat sie doch von einer erfahrenen Kollegin bei einem privaten Treffen erfahren, dass «in solchen Fällen» ein Einbezug der Eltern die Situation für das Kind nur verschlimmern würde. Ebenso befürchtet sie, dass die Konfrontation der Eltern mit den Aussagen des Kindes das Vertrauensverhältnis zu dem Jungen zerstören könnte, obwohl dieser gesagt hat, er wolle, dass die Eltern involviert werden. Dies scheint ungewöhnlich, zeigt doch die persönliche Erfahrung der Sozialarbeiterin, dass die Kinder die Eltern regelmässig nicht involvieren wollen, aufgrund damit einhergehender Loyalitätskonflikte. Hätten die Eltern von Anfang an vollständig über die Aussagen des Kindes informiert werden müssen und kann die Sozialarbeiterin jetzt – nachdem die Vorgesetzte über alle Anhaltspunkte informiert worden ist – eine Gefährdungsmeldung überhaupt noch vornehmen?

D. Fallbeispiel 2 – Anwendung der informationsrechtlichen Bestimmungen

1. Fragestellung

Vorliegend geht es um die Frage, ob die Sozialarbeiterin die Meldepflichten gegenüber der Kindesschutzbehörden (Art. 314*d* ZGB) verletzt hat. Zudem ist der Kontakt zwischen der Sozialarbeiterin und den Eltern zu prüfen. Die Sozialarbeiterin hat sich an den einschlägigen informationsrechtlichen Bestimmungen zu orientieren: Anwendbar ist das Informations- und Daten-

schutzgesetz des Kantons Zürich. Es ist nicht ganz eindeutig, ob es sich im vorliegenden Sachverhalt um «besondere» Personendaten[72] handelt; da es sich unter Umständen um medizinische Informationen handeln könnte (§ 3 Abs. 4 IDG ZH), sind die besonderen Anforderungen an eine Datenbekanntgabe zu beachten. Ebenso anwendbar sind die einschlägigen Bestimmungen zu den Melderechten und -pflichten gemäss Art. 314*c* f. ZGB.

2. Information der Eltern

Zunächst ist auf die Tatsache einzugehen, dass die Eltern von der Sozialarbeiterin nicht darüber informiert worden sind, dass das Kind von Handgreiflichkeiten der Eltern gesprochen hat. Die Eltern haben – wie bereits im ersten Fallbeispiel thematisiert – im Rahmen ihrer elterlichen Sorge im Grundsatz einen Informationsanspruch gegenüber der Schule über sämtliche Vorkommnisse betreffend ihr Kind. Vorliegend sind allerdings zwei Besonderheiten zu beachten:

Erstens stellt sich die Frage, ob zwischen den Interessen des Kindes und der Eltern eine Interessenskollision vorliegt. Läge eine solche vor, haben die Eltern keinen Informationsanspruch gegenüber der Schule, weil ihre Vertretungsbefugnis und somit auch der genannte Anspruch von Gesetzes wegen aufgrund einer Interessenskollision entfällt (Art. 306 Abs. 3 ZGB[73]).

Zweitens hat das Kind seinen Wunsch geäussert, die Eltern seien zu involvieren. Ob dieser Wunsch zu berücksichtigen ist, muss vor dem Hintergrund der konkreten Entwicklung des Kindes bzw. seiner Urteilsfähigkeit[74] durch die Sozialarbeiterin und ihre Vorgesetzten beurteilt werden.

Im vorliegenden Fallbeispiel ist die Möglichkeit zu berücksichtigen, dass die Interessen des Kindes von keiner einzigen Partei mehr unabhängig vertreten werden: Es könnte mit anderen Worten die Situation entstehen, dass die Eltern aufgrund eines Interessenskonfliktes ihre Vertretungsmacht (und damit den Informationsanspruch) verlieren und – gleichzeitig – dem Schüler (von der Schule) die Urteilsfähigkeit abgesprochen wird. In dieser Situation

---

[72] Vgl. oben II.G.3.

[73] Vgl. auch hierzu bereits im vorangehenden Kapitel.

[74] Vgl. oben II.H.

ist der Schüler auf die Wahrung seiner Interessen durch die Sozialarbeiterin und ihre Vorgesetzten bzw. die Schule angewiesen. Letztere könnten aber unter Umständen (auch) ihre eigenen Interessen verfolgen. Dies zeigt sich im Beispiel an der Überlegung der Sozialarbeiterin, durch das Involvieren der Eltern das Vertrauensverhältnis zum Kind (und damit ihre Arbeitsgrundlage) zu zerstören. Die Sozialarbeiterin muss sich die Frage stellen, ob sie in der konkreten Situation die Interessen des Kindes oder ihre eigenen vertritt bzw. ob sich diese vermischen.

Aus dieser (möglichen) Ausgangslage können sich zweierlei Probleme ergeben: Erstens würden die Interessen des Schülers von niemandem mehr unabhängig vertreten und zweitens ist fraglich, ob die Schule die richtige bzw. zuständige Institution ist, um die Interessen des Kindes in dieser Situation gegenüber Dritten (den Eltern) zu wahren, auch wenn dies aus schulischer Perspektive nachvollziehbar zu sein scheint.

Meines Erachtens wäre die Wahrung der Interessen des Kindes in einer solchen Konstellation nicht bei der Schule selbst, sondern bei der Kindesschutzbehörde zu suchen, deren gesetzlicher Auftrag es ist, die Interessen des Kindes gegenüber Dritten – und somit unter Umständen auch gegenüber der Schule – zu vertreten.

Die Schule hat von Gesetzes wegen keinen Auftrag, die Interessen des Kindes gegenüber den Eltern zu vertreten: Dies zeigt sich in § 2 VSG ZH, wonach die Aufgabe der Volksschule sich grundsätzlich auf Bildungs- und Erziehungsaufgaben beschränkt; die Interessensvertretung von Kindern – gegenüber den Eltern sowie Dritten – ist als Aufgabe von Volksschulen nicht vorgesehen.

Besteht eine Interessenskollision zwischen dem Kind und seinen Eltern einerseits und zwischen dem Kind und der Schule andererseits, ist somit zu prüfen, ob die Interessen des Kindes durch die Kindesschutzbehörde vertreten werden *müssen*.[75] Die Prüfung dieser Umstände obliegt freilich zunächst der Sozialarbeiterin bzw. ihren Vorgesetzten, welche die Frage allfälliger Interessenskollisionen (auch eigenen) und der Urteilsfähigkeit des Kindes beurteilen müssen.

[75] Art. 306 Abs. 2 ZGB: «Sind die Eltern am Handeln verhindert oder haben sie in einer Angelegenheit Interessen, die denen des Kindes widersprechen, so ernennt die Kindesschutzbehörde einen Beistand oder regelt diese Angelegenheit selber.»

3. Meldepflicht

Schliesslich wird im Beispiel die Frage aufgeworfen, ob Meldepflichten verletzt worden sind: Zu unterscheiden ist im Sachverhalt die Gefährdungsmeldung *vor und nach* der Elternberatung. Jede Person, mithin auch die Sozialarbeiterin, kann die Kindesschutzbehörde informieren, wenn die körperliche, psychische oder sexuelle Integrität eines Kindes *gefährdet erscheint* (Art. 314*c* Abs. 1 ZGB). Weil die Sozialarbeiterin nicht an das Berufsgeheimnis gebunden ist, ist die Meldung, unabhängig, ob dies der geäusserte Wunsch bzw. Wille des Kindes ist, zulässig.[76] Es handelt sich hierbei um eine klare gesetzliche Grundlage gemäss § 8 IDG ZH, die eine allfällige Meldung aus informationsrechtlicher Perspektive rechtfertigt.

Meldepflichtig ist die Sozialarbeiterin,[77] «wenn *konkrete Hinweise* dafür bestehen, dass die körperliche, psychische oder sexuelle Integrität des Kindes gefährdet ist und (die meldepflichtige Person) nicht im Rahmen ihrer Tätigkeit Abhilfe schaffen können.» (Art. 314*d* Abs. 1 ZGB). Die Meldepflicht gilt als erfüllt, wenn sich die Meldung an die vorgesetzte Person richtet (Art. 314*d* Abs. 2 ZGB). Liegt eine Meldepflicht vor, handelt es sich um eine klare gesetzliche Grundlage gemäss § 8 IDG ZH, die eine Meldung aus informationsrechtlicher Perspektive rechtfertigt.

Im konkreten Beispiel hat sich die Sozialarbeiterin nach den ersten Erkenntnissen über allfällige häusliche Gewalt an ihre Vorgesetzte gewendet. Sie ist damit ihrer Meldepflicht gemäss Art. 314*d* Abs. 2 ZGB nachgekommen. Nach der Elternberatung erfährt die Sozialarbeiterin vom Schüler, dass dieser gegen eine Tischkante gestossen wurde. Aufgrund dieses Vorkommnisses ist davon auszugehen, dass die Meldepflicht der Sozialarbeiterin gemäss Art. 314*d* ZGB wieder auflebt. Sie ist mit anderen Worten erneut meldepflichtig gegenüber der Kindesschutzbehörde; zumindest hat sie ihre Vorgesetzte erneut über die (neuen) Erkenntnisse zu informieren. Darüber hinaus ist sie auch berechtigt, die Kindesschutzbehörde direkt zu kontaktieren (Art. 314*c* Abs. 1 ZGB).

---

[76] Vgl. oben II.F.

[77] Die Sozialarbeiterin ist zwar nicht explizit in Art. 314*d* Abs. 1 Ziff. 1 ZGB erwähnt, sie ist aber wohl zumindest einer der Fachpersonen aus den Bereichen Betreuung, Erziehung, Bildung oder Sozialberatung zuzuordnen.

IV. Schluss – Handlungsempfehlungen

Informationsrechtliche Bestimmungen – vorliegend die kantonalen Datenschutzgesetze, Amts- und Berufsgeheimnisse sowie zivilrechtliche Melderechte und -pflichten – stellen zunächst einen Handlungsleitfaden für staatliche Angestellte, wie das Personal von öffentlichen Schulen, dar. Wenn Logopäden und Logopädinnen sowie Sozialarbeiterinnen und Sozialarbeiter bessere Kenntnisse über die rechtlichen Grundlagen haben, dann hilft dies, informationsrechtliche Lösungen zu finden, welche die Persönlichkeitsrechte der Schülerinnen und Schüler nachhaltiger und besser schützen. Informationsrechtliche Kenntnisse helfen ihnen aber auch, ihren komplexen Aufgaben umfassend und kompetent nachzukommen. Um effektiv informationsrechtliche Fragestellungen zu beantworten, ist der nachfolgende Handlungsleitfaden hilfreich:

1. Handle ich im Rahmen eines staatlichen Auftrages?
2. Ist diese Handlung vom Anwendungsbereich der informationsrechtlichen Bestimmungen (kantonale Datenschutzgesetze, Amts-, Berufsgeheimnisse, Melderechte und -pflichten) erfasst?
3. Welche Informationen sollen bearbeitet werden bzw. sind darunter sogenannte «besondere» Personendaten, wie bspw. Personendaten über die Gesundheit, Religionszugehörigkeit etc. (§ 3 Abs. 4 IDG ZH)?
4. An welche Personen oder Entitäten sollen die Personendaten bzw. Informationen weitergegeben werden?
5. Was ist die gesetzliche Grundlage zur Bekanntgabe von Personendaten: kantonales Datenschutzgesetz, allgemeine Bestimmungen (§ 8 IDG ZH); Volksschulgesetz (§ 3a VSG ZH); Auskunftsrecht der Eltern im Rahmen ihrer Vertretungsmacht (§ 20 Abs. 2 IDG ZH); Melderecht bzw. -pflicht (Art. 314*c* f. ZGB)?
6. Liegen im Einzelfall Gründe für Einschränkungen des Auskunftsrechts vor, weil überwiegende Interessen gegen eine Bekanntgabe sprechen (§ 23 IDG ZH)?
7. Ist die Bekanntgabe von Personendaten verhältnismässig bzw. geeignet und erforderlich im Hinblick auf das Ziel und den Zweck derselben (§ 8 IDG ZH)?

8. Liegt keine gesetzliche Grundlage vor oder ist die Bekanntgabe nicht verhältnismässig im Sinne von § 8 IDG ZH und könnte in der Folge eine Amtsgeheimnisverletzung gemäss Art. 320 StGB begangen werden?
9. Parallel sind die Interessen des Kindes zu prüfen. Bestehen Interessenskollisionen zwischen dem Kind und den Eltern oder der Schule und stellt sich somit die Frage der Interessensvertretung durch eine Kindesschutzbehörde?

Während die ersten zwei Fragen wohl regelmässig bejaht werden können, entscheidet sich anhand der nachfolgenden Fragen, ob ein Informationsaustausch zulässig und wie weiter vorzugehen ist. Im Ergebnis obliegt es den zuständigen Fachpersonen, die jeweiligen Interessenabwägungen selbst vorzunehmen. Eine umfassende Aktenführung hinsichtlich der Überlegungen ist Pflicht. Aus praktischer Perspektive werden informationsrechtliche Bestimmungen oft als Hindernis gesehen. Mit den notwendigen Grundlagenkenntnissen stellen sie aber bei der täglichen Arbeit kein solches (mehr) dar; eine fast vollständige Mehrheit der Informationsflüsse in der Schule war schon immer (berechtigterweise) vorhanden und wird es auch bleiben. Das Hindernis zu überwinden, ist angesichts des Schutzes der Persönlichkeitsrechte sämtlicher von der Datenbearbeitung Betroffener im Umfeld der Schule ohnehin der einzige gangbare Weg.

Datenschutzrecht für künstliche Intelligenz in der öffentlichen Verwaltung

Eine Auslegeordnung am Beispiel des Kantons Zürich

Philip Glass

Inhaltsübersicht

I. Künstliche Intelligenz und damit verbundene Risiken[1]

A. Eine grosse Diversität an Definitionen von KI

1. Klassische begriffliche Unterscheidungen

Die Erfassung des Phänomens der künstlichen Intelligenz («KI») bereitet gewisse Schwierigkeiten, weil bisher keine schlüssige Definition existiert. Dies ist einerseits historisch begründet, da das Ziel einer intelligent handelnden Maschine auf verschiedene Arten verfolgt wurde.[2] Andererseits liegt es auch daran, dass trotz Jahrhunderten der Nachforschung und des Überlegens nach wie vor keine anerkannte allgemeine Theorie von «Intelligenz» existiert und insgesamt unklar ist, was man unter dem Begriff der Intelligenz verstehen soll.[3] In Bezug auf «künstliche Intelligenz» besteht immerhin ein gewisser Konsens, dass es (vorerst) lediglich um die Simulation der von aussen beobachtbaren Attribute von Intelligenz geht, sogenannte *weak AI*,[4] insbesondere

---

[1] An dieser Stelle möchte ich Dr. Sc. (ETH Zürich) Colin W. Glass für die kritische Durchsicht des Manuskripts und Besprechung der technischen Aspekte der Untersuchung danken.

[2] Stuart Russel/Peter Norvig, Artificial Intelligence – A Modern Approach, Global Edition, 4. Ed., Pearson Education 2022, Introduction; vgl. dazu die Zusammenfassung der gängigsten Konzepte und Methoden bei Alfred Früh/Dario Haux, Foundations of Artificial Intelligence and Machine Learning, Weizenbaum Series 29, Berlin 2022, https://www.weizenbaum-institut.de/media/Publikationen/Weizenbaum_Series/Weizenbaum_Series_29.pdf (Abruf 06.09.2022), *passim*.

[3] Mark Coeckelbergh, Ai Ethics, Cambridge (MA)/London 2020, Kapitel 3; Yann Le Cun, Quand la machine apprend – La révolution des neurones artificiels et de l'apprentissage profond, Paris 2019, 374; Melanie Mitchell, Artificial Intelligence – A Guide for Thinking Humans, Pelican Books 2019, 6 f.; Stuart Russell, Human Compatible – AI and the Problem of Control, Penguin Books 2019, 13. f.; Stan Franklin, History, motivations, and core themes, in: Keith Frankish/William R. Ramsey (Eds.), The Cambridge Handbook of Artificial Intelligence, Cambridge University Press 2014, 15; für ein Beispiel der technischen Quantifizierung der universellen Intelligenz eines Systems siehe Jörg Zimmermann/Armin B. Cremers, Foundations of Artificial Intelligence and Effective Universal Induction, in: Joachim von Braun/Margaret S. Archer/Gregory M. Reichberg/Marcelo Sánchez Sorondo (Eds.), Robotics, AI, And Humanity – Science Ethics, and Policy, Springer Open Access 2021, 37.

[4] Zur Unterscheidung zwischen *weak AI* und *strong AI* siehe Russel/Norvig (FN 2), 1032 f.

Sprachverständnis, Wissensrepräsentation, automatisierte Schlussfolgerung – erweitert durch kognitive Werkzeuge der Simulation von Sinneswahrnehmung durch Sensoren wie beispielsweise die Bilderkennung.[5] Konkret einsatzfähige KI-Systeme müssen im Einzelnen jeweils für die Aufgabe programmiert bzw. trainiert werden, für die sie vorgesehen sind. Ob und gegebenenfalls wann eine allgemeine KI, *artificial general intelligence (AGI),* verschiedentlich auch *strong AI* oder *human level intelligence* genannt, für welche dies nicht mehr zwingend notwendig wäre, verfügbar sein wird, ist unklar.[6]

Im Kern geht es bei KI um konkrete Problemlösung durch Algorithmen als anpassbares, zunehmend intelligentes Verhalten.[7] Künstliche Intelligenz ist somit ein technologisches Querschnittskonzept, dessen methodische Konkretisierung mit dem Fortschritt der technologischen Entwicklung ändert. Entsprechend werden KI-Probleme, die als «gelöst» gelten, «in die Schublade der klassischen Werkzeuge versorgt» und mit der Zeit als *good old fashioned AI* (GOFAI) bezeichnet.[8] Aktuell bezeichnet der Begriff jene KI-Systeme, die auf der Grundlage von logischer Verknüpfung von formalen Regeln arbeiten.[9] Solche Methoden werden auch *symbolic AI* genannt, da ihre Wissensbasis aus symbolischen Repräsentationen für Aspekte der Maschinenumwelt be-

---

[5] Russel/Norvig (FN 2), 20; aus rechtlicher Sicht zuletzt Wolfgang Hoffmann-Riem, Recht im Sog der Digitalisierung – Herausforderungen, Tübingen 2022, 39 ff. m.w.H.

[6] Micheal Wooldridge, The Road to Conscious Machines – The Story of AI, Pelican Books 2021, 303 ff.; Le Cun (FN 3), 372 f.; Mitchell (FN 3), 363; Margaret A. Boden, Artificial Intelligence – A Very Short Introduction, Oxford University Press 2018, 47 f.; skeptisch gegenüber der Möglichkeit einer hierzu notwendigen «Intelligenzexplosion» Erik J. Larson, The Myth of Artificial Intelligence – Why Computers Can't Think the Way We Do, Cambridge MA/London 2021, 37 f.

[7] Wooldridge (FN 6), 22.

[8] Le Cun (FN 3), 17 f. (Übersetzung durch den Verfasser); Nadja Braun Binder/Matthias Spielkamp/Catherine Egli/Laurent Freiburghaus/Eliane Kunz/Nina Laukenmann/Michele Loi/Anna Mätzener/Liliane Obrecht/Jessica Wulf, Einsatz Künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen – Schlussbericht vom 28. Februar 2021 zum Vorprojekt IP6.4, Staatskanzlei des Kantons Zürich 2021, 10, hier: «Basistechnologie».

[9] Le Cun (FN 3), 384; Russel/Norvig (FN 2), 1033; Margaret A. Boden, GOFAI, in: Keith Frankish/William R. Ramsey (Eds.), The Cambridge Handbook of Artificial Intelligence, Cambridge University Press 2014, 89 ff.; zu den Kognitiven Grenzen des Ansatzes zusammenfassend Manuela Lenzen, Natürliche und künstliche Intelligenz – Einführung in die Kognitionswissenschaft, Frankfurt a.M. 2002, 63 ff.

steht.[10] Demgegenüber sind neue Methoden des *machine learning* in der Lage, «lernende» Algorithmen zu erzeugen, die auf ihr Lernziel hin optimiert werden können. Heutige KI-Systeme sind vielfach Mischungen verschiedener Technologien, oftmals GOFAI in Kombination mit maschinellem Lernen.[11] Aufgrund der Vielfalt der methodischen Zugänge enthalten wissenschaftliche, politische und rechtliche Stellungnahmen zum Thema je eigene Umschreibungen des Phänomens.

2. Definitionen der OECD und des Europarates

Auf einen offenen, technologieneutralen Begriff von KI legte sich die AI Expert Group der OECD fest. Die Definition besteht aus drei Elementen. Demnach handelt es sich bei KI-Systemen zunächst um *Maschinen-basierte Systeme*, die in der Lage sind, im Rahmen von Zielen, die durch Menschen definiert werden, Voraussagen zu treffen, Empfehlungen zu generieren oder auch ihre reale bzw. virtuelle Umgebung zu beeinflussen. Sodann nutzen solche Systeme begriffsnotwendig durch Menschen oder Maschinen generierte Inputdaten, um reale oder virtuelle Umgebungen wahrzunehmen und diese in statistische Modelle umzuwandeln. Bei der Anwendung auf neue Daten sind sie schliesslich in der Lage, auf der Grundlage dieser Modelle mittels *model inference*[12] Optionen und Informationen für Handlungen zu formulieren. Dabei verfügen solche Systeme über unterschiedliche Grade an Autonomie.[13]

---

[10] Boden (FN 6), 5, 19 ff.; Mitchell (FN 3), 9 ff.; Wooldridge (FN 6), 42 ff.: «This approach is called symbolic AI, because it makes use of symbols that stand for things that the system is reasoning about.»; vgl. auch die Erläuterung anhand von *natural language processing* bei Markus Christen/Clemens Mader/Johann Čas/Tarik Abou-Chadi/Abraham Bernstein/ Nadja Braun Binder/Daniele Dell'Aglio/ Luca Fábián/Damian George/Anita Gohdes/Lorenz Hilty/ Markus Kneer/Jaro Krieger-Lamina/Hauke Licht/Anne Scherer/Claudia Som/Pascal Sutter/Florent Thouvenin, Wenn Algorithmen für uns entscheiden: Chancen und Risiken der künstlichen Intelligenz, TA-Swiss 72/2020, 84.

[11] Le Cun (FN 3), 2: «tricotage d'apprentissage-machine, de GOFAI et d'informatique classique».

[12] Vgl. dazu Paul DeBeasi, Training versus Inference, blogs.gartner.com, 14.02.2019, https://blogs.gartner.com/paul-debeasi/2019/02/14/training-versus-inference/ (Abruf 06.09.2022).

[13] Siehe die Definition bei OECD, Artificial Intelligence in Society, Paris 2019, https://doi.org/10.1787/eedfee77-en (Abruf 02.04.2022), 22.

Etwas abstrakter formuliert dies der Europarat im Rahmen seiner Studie über die Machbarkeit sowie mögliche Elemente eines rechtlichen Rahmens für die Entwicklung, das Design und den Einsatz von KI-Systemen im Hinblick auf den Schutz der Menschenrechte, der Demokratie und der Verwirklichung von Rechtsstaatlichkeit.[14] Als künstliche Intelligenz wird hier die Entdeckung von Mustern und Trends in grossen Datensets durch statistische Methoden bezeichnet. Hierdurch ermöglichten intelligente Algorithmen die Erkennung von Bildern und Tönen, das *streamlining* von Produkten und Dienstleistungen sowie grosse Effizienzgewinne bei der Verwirklichung komplexer Aufgaben.[15] Es handelt sich somit um einen Begriff von künstlicher Intelligenz, der mit *machine learning* gleichzusetzen ist und eine enge Verwandtschaft zum Konzept *big data* aufweist. Es war denn auch der Aufstieg von Big Data-Systemen, bestehend aus grossen Speichern, grossen Datenmengen und schnellen Prozessoren, welche im Nachgang zum Aufkommen des *world wide web* die Entwicklung neuer Methoden zur Entwicklung von Algorithmen beschleunigte, auf deren Grundlage probabilistische Modelle erstellt und trainiert werden können.[16]

3. «Big Algo» und «algorithmische Systeme»

In der Literatur wird deshalb auch der Begriff «Big Algo» vorgeschlagen, was den Fokus von den Daten zu Art und Kontext der Bearbeitung verschieben soll.[17] Soweit ersichtlich, hat sich der Begriff noch nicht durchgesetzt. Derweil scheint sich der Fokus der KI-Entwicklung aus verschiedenen Gründen eher weg von grossen Mengen hin zu qualitativ hochwertigen Datensets (*good data*) zu verlagern,[18] sowie zu optimierten simplen Regelmodellen.[19] Mit an-

---

[14] Ad Hoc Committee on Artificial Intelligence, Feasibility Study, CAHAI (2020)23, N 4.

[15] Feasibility Study 2020 (FN 14), N 4.

[16] Siehe dazu Russel/Norvig (FN 2), 43 ff.

[17] Siehe den Hinweis bei Hoffmann-Riem (FN 5), 38.

[18] Siehe dazu das Interview von Eliza Strickland, Andrew Ng: Unbiggen AI, IEEE Spectrum, 09.02.2022, abrufbar unter https://spectrum.ieee.org/andrew-ng-data-centric-ai (Abruf 06.09.2022); bzw. «smart data», Rolf H. Weber, Big Data: Herausforderung für das Datenschutzrecht, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Big Data und Datenschutzrecht, Zürich/Basel/Genf 2016, 18 f.

[19] Zu dieser Entwicklung siehe Brian Christian, The Alignment Problem: Machine Learning and Human Values, New York City 2020, 98 ff.

deren Worten wird versucht, die Auswahl der Parameter für KI-Modelle besser empirisch abzustützen.

In eine ähnliche Richtung wie «Big Algo» geht die *Digital Society Initiative* der Universität Zürich, die in ihrem Positionspapier zur Regulierung von künstlicher Intelligenz anstelle von KI von «algorithmischen Systemen» spricht. Dies soll nicht bestimmte Technologien bezeichnen, sondern «auf die Anwendung dieser Technologien in einem sozialen Kontext [verweisen]».[20] Auch hier wird der Kontext der Anwendung in den Vordergrund gestellt und als primäre Grundlage für eine mögliche Regulierung gesehen. Der Begriff ist indes in mehrfacher Hinsicht problematisch, denn er erscheint sehr weit gefasst und enthält keine inhärenten Hinweise auf die (zusätzlichen) Bedeutungen, die ihm beigemessen werden.

Erstens bezeichnet der Begriff «Algorithmus» klar strukturierte Handlungsanweisungen, die zunächst einmal nicht als künstlich intelligent bezeichnet werden, beispielsweise Kochrezepte und andere Abläufe logischer Deduktion.[21] Mithin wird als Algorithmus «jede eindeutige Handlungsanweisung gekennzeichnet, die dafür eingesetzt wird, bestimmte Probleme in definierten Einzelschritten zu lösen».[22] Das Moment der künstlichen Intelligenz besteht denn auch nicht im Algorithmus, sondern im Modell, das durch den Algorithmus umgesetzt wird.[23] Mithin muss ein algorithmisches System nicht begriffsnotwendig künstlich intelligente Funktionen aufweisen.

Zweitens ist mit der Bezeichnung als System in der klassischen Bedeutung des Begriffs nicht ein sozio-technisches (Gesamt-)System gemeint, sondern ein Informationsverarbeitungssystem. Entsprechend bezeichnet der Begriff des algorithmischen Systems – analog zum verwandten, aber nicht identischen

---

[20] Florent Thouvenin/Markus Christen/Abraham Bernstein/Nadja Braun Binder/Thomas Burri/Karsten Donnay/Lena Jäger/Mariela Jaffé/Michael Krauthammer/Melinda Lohmann/Anna Mätzener/Sophie Mützel/Liliane Obrecht/Nicole Ritter/Matthias Spielkamp/Stephanie Volz, Positionspapier: Ein Rechtsrahmen für künstliche Intelligenz, DSI 2021, https://www.zora.uzh.ch/id/eprint/211386/ (Abruf 01.03.2022), 1.

[21] Russel/Norvig (FN 2), 27.; Vgl. beispielsweise den Herzstillstand-Algorithmus bei Hans Rickli (Hrsg.), Kardiovaskuläres Manual Kantonsspital St. Gallen, https://www.kssg.ch/sites/default/files/2016-05/kv-manual2011.pdf (Abruf 01.03.2022), 12.

[22] Hoffmann-Riem (FN 5), 36.

[23] Siehe III.A.1.

Begriff des KI-Systems[24] – ein Informationsverarbeitungssystem, das auf Basis von Algorithmen arbeitet.[25]

Aus rechtsmethodischer Sicht lassen die Überlegungen hinter den Begriffen «Big Algo» und «algorithmisches System» bzw. «algorithmisches/automatisiertes Entscheidungssystem» insofern aufhorchen, als sie an eine ähnliche Entwicklung im Datenschutzrecht erinnern. Hier hat sich mittlerweile durchgesetzt, dass sich der rechtliche Schutz nicht primär nach dem Inhalt der Daten richtet, sondern nach dem Kontext der Datenbearbeitung und den damit verbundenen Risiken für die Betroffenen.[26] Der Grund liegt zunächst darin, dass der Informationsgehalt von Daten, aufgrund dessen Entscheidungen letztlich getroffen werden, stets eine kontextbezogene Interpretativleistung darstellt.[27] Parallel dazu zeigt sich zunehmend deutlich, dass der Wert der erweiterten Persönlichkeitssphäre als Gegenstand der informationellen Selbstbestimmung – das primäre Schutzgut des Datenschutzrechts – ebenfalls kontextsensibel ist.[28] Indes blieb der Rechtsbegriff des Datums unverändert technisch.

Der Verweis auf die sozialen Auswirkungen ist aus dieser Perspektive von Bedeutung, als KI-Instanzen ein komplexes Zusammenspiel von Algorithmen

---

[24] Dazu Martin Ebers, Regulierung von KI und Robotik, in: Martin Ebers/Christian Heinze/Tina Krügel/Björn Steinrötter (Hrsg.), Künstliche Intelligenz und Robotik – Rechtshandbuch, München 2020, § 3 N 4.

[25] Hoffmann-Riem (FN 5), 195 ff.

[26] Zuletzt Joel Drittenbass, Regulierung von autonomen Robotern – Angewendet auf den Einsatz von autonomen Medizinrobotern: Eine datenschutzrechtliche und medizinproduktrechtliche Untersuchung, Diss. Univ. St. Gallen, Zürich/St. Gallen 2021, N 140; Philip Glass, Die rechtstaatliche Bearbeitung von Personendaten in der Schweiz – Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, zugl. Diss Univ. Basel 2016, Zürich/St. Gallen 2017, 125 ff. m.w.H.; Thomas Gächter/Gregori Werder, Einbettung ausgewählter Konzepte in das schweizerische Datenschutzrecht, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2013, 88; Eva Maria Belser, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht – Grundlagen und öffentliches Recht, Bern 2011 (zit. VerfasserIn, Datenschutzrecht Grundlagen), 27 f. N 50 u. 53.

[27] Marion Albers, Informationelle Selbstbestimmung, Baden-Baden 2005, 95.

[28] Grundlegend Helen Nissenbaum, Privacy in Context – Technology, Policy, and the Integrity of Social Life, Stanford 2010, 129 ff.; vgl. zum Zweckbindungsgrundsatz IV.A.1.b.

bilden, und solche technischen Systeme über einzelne Nutzer(gruppen) zunehmend auf die Gesellschaft insgesamt wirken.[29] Dennoch sollte begrifflich weiterhin zwischen Algorithmen als Regulierungsgegenstand auf der einen und deren Einbettung in den sozialen Kontext als Zielgrösse der Regulierung auf der anderen Seite getrennt werden. Der Grund liegt darin, dass sowohl der Regulierungsgegenstand als auch die Regulierung desselben je eigene, individuelle wie gesellschaftliche Risiken erzeugen, deren Auswirkungen auch je separat zu beachten sind.

Besonders problematisch erscheint damit die gleichsetzende Umdeutung des Begriffs des algorithmischen Systems als sozio-technisches KI-System schliesslich deshalb, weil die Automatisierung von Prozessen durch einen in Software codierten Algorithmus und die Lernfunktion von künstlich intelligenten Modellen je eigene intrinsische Risiken bergen.[30] Der Begriff «algorithmisches System» verweist in seiner üblichen Bedeutung auf die Risiken von Automatisierung, während der Begriff «KI-System» darüber hinaus die spezifischen Risiken der Umsetzung von Ergebnissen der maschinellen Modellbildung mitumfasst. Daher erscheint der Begriff des algorithmischen Systems nicht als geeigneter Ersatz für den Begriff des KI-Systems. Dies gilt auch für verwandte Begriffe, wie «algorithmisches Entscheidungssystem»[31] oder «automatisiertes Entscheidungssystem»[32]. Immerhin wird hier durch den Fokus auf Entscheidungen eine gewisse Verbindung zu gesellschaftlichen Systemen hergestellt. Eine diesbezügliche Abgrenzung kann an dieser Stelle indes nicht geleistet werden.

---

[29] Hoffmann-Riem (FN 5), 35 ff.; Mario Martini, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, Berlin 2019, 64 f.

[30] Siehe I.D.

[31] Vgl. dazu Julia Krüger/Konrad Lischka, Damit Maschinen den Menschen dienen – Lösungsansätze, um algorithmische Entscheidungen in den Dienst der Gesellschaft zu stellen, Arbeitspapier im Auftrag der Bertelsmannstiftung, Mai 2018, abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Algorithmenethik-Loesungspanorama.pdf (Abruf 01.03.2022).

[32] Vgl. dazu das Positionspapier der Digitalen Gesellschaft zur Regulierung von automatisierten Entscheidungssystemen vom 21. Februar 2022, abrufbar unter https://www.digitale-gesellschaft.ch/uploads/2022/02/Position-der-Digitalen-Gesellschaft-zur-Regulierung-von-automatisierten-Entscheidungssystemen-1.0.pdf (Abruf 01.03.2022).

4. Definition der EU

Einen konkreteren Begriff verwendet schliesslich die EU in ihrem Entwurf zur KI-Regulierung, indem sie neben einer ähnlich abstrakten Definition verschiedene Kategorien von Technologien bezeichnet, die ein KI-System konstituieren können. Dies steht in einem gewissen Gegensatz zur Entwicklung in der Schweiz. Hier wird eher eine technologieneutrale Regulierung angestrebt bzw. empfohlen.[33] Indes ist der vorgeschlagene Begriff trotz der enumerativen Elemente sehr weit gefasst. Als KI-System nach der Konzeption des EU-Entwurfs kommt demgemäss Software in Frage, die unter Verwendung gewisser, im Anhang der Regulierung beschriebenen methodischen bzw. technologischen Ansätzen entwickelt wurde. Solche Software soll indes nur dann als künstlich intelligent gelten, wenn sie dazu geeignet sind, zur Verwirklichung vorgegebener menschlicher Ziele sinnvollen Output zu generieren, insbesondere Inhalte, Prognosen, Empfehlungen oder Entscheidungen mit Auswirkungen auf die Umgebung, mit der sie interagieren.

B. Ein einfaches Modell einer *learner*-KI

1. Elemente und zyklische Phasen des Lernens

Moderne künstlich intelligente Systeme bestehen aus einem mehr oder weniger komplexen Algorithmus (*KI-Funktion*), der ein mathematisches Modell (*Transformationsregel*) an eingegebenen Daten (*Input*) abarbeitet, unter Umständen mittels Resultat-Feedback verbessert (*Lernfunktion*), und dessen Resultate (*Output*) Aussagen über statistisch belastbare Zusammenhänge in den Inputdaten (*Korrelationen*) erlauben. Hieraus lassen sich Tatsachenbehauptungen generieren, die mit einer gewissen Wahrscheinlichkeit zutreffend sind, beispielsweise in der Form von Prognosen, aufgrund derer geplant oder Empfehlungen, aufgrund derer gehandelt werden kann. Soweit diese als Daten erfasst und gespeichert werden, handelt es sich um *probabilistische*

[33] Herausforderungen der künstlichen Intelligenz – Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» an den Bundesrat, SBFI Forschung und Innovation, Dezember 2019, 10; Christen et al. (FN 10), 291 f.; Thouvenin et al. (FN 20), 2.

Daten, also nicht um empirisch erhobene Daten.[34] Darüber hinaus kann die Auswahl der nachfolgenden Handlung ebenfalls automatisiert werden, etwa zur Begründung, Änderung oder Aufhebung von Rechten oder Pflichten einer Person oder zur Steuerung des Verkehrsflusses mittels Verkehrsanalyse mit automatisierten Geschwindigkeitsbeschränkungen. Je nachdem, ob schlussendlich Mensch oder Maschine entscheidet, spricht man von *Teilautomation* oder *Vollautomation* eines Entscheidungsprozesses.[35]

KI-Systeme sind demnach Informationsverarbeitungsmaschinen, die stets weiter optimiert werden können. Die Möglichkeit der fortlaufenden Verbesserung führt zu einer zyklischen Betrachtungsweise von solchen Systemen, dem sogenannten *Lebenszyklus* einer KI, der in diskrete Phasen unterteilt wird. Die Unterteilung erfolgt üblicherweise in die Phasen der Erstellung (Auswahl und Zusammenstellung der KI-Technologien), des Trainings, der Anwendung oder des Einsatzes sowie des Feedbacks, das den Lernprozess auslöst.[36] Während des Trainings, in der Anwendung sowie in der Feedbackphase können Personendaten bearbeitet werden, was je eigene Datenschutzfragen aufwirft. Bei der Auswahl und Zusammenstellung der KI-Technologien für eine geplante KI-Instanz ergeben sich die Datenschutzrisiken indes aus der gewählten Architektur, die opak oder transparent – also interpretier und erklärbar – ausgestaltet sein kann.[37]

2. Überwachtes versus unüberwachtes Lernen

Ziel einer KI ist die Berechnung von sinnvollen, prädiktiven Outputdaten. Der Sinn von Outputdaten ergibt sich wiederum aus dem Einsatzzweck der KI. Der Lernprozess, aufgrund dessen solche Programme als «intelligent» bezeichnet werden, besteht in der Optimierung einer sog. Transformationsregel, welche

---

[34] Dies birgt Fragen in Bezug auf die Datenrichtigkeit, siehe dazu IV.A.3.

[35] Braun Binder et al. (FN 8), 11.

[36] Vgl. dazu die übersichtliche Darstellung für neuronale Netze bei Samuel Klaus, KI trifft Datenschutz: Risiken und Lösungsansätze, in: Astrid Epiney/Sophia Rovelli (Hrsg.), Künstliche Intelligenz und Datenschutz – L'intelligence artificielle et protection des données, Zürich/Basel/Genf 2021, 83 f.

[37] Vgl. dazu die Liste möglicher Risiken und Lösungsansätze pro Phase bei Klaus (FN 36), 92 ff.; Zur Frage der Transparenz und Erkennbarkeit siehe IV.A.1.c. u. d.

auf Inputdaten nützliche Outputdaten abbildet.[38] Diese wird zunächst anhand von repräsentativen Trainingsdaten in Hinblick auf den Einsatzzweck trainiert. Beispielsweise können dies Bilder von Katzen und Hunden sein,[39] die der Algorithmus voneinander unterscheiden bzw. jeweils korrekt bezeichnen soll. Im Rahmen des Trainings werden diese Daten als Bilddateien in das System eingelesen. Je nach Automatisierungsgrad der KI sind die Inputdaten von Menschen vorsortiert, d.h. als Hundebilder und Katzenbilder beschriftet oder nicht. Man spricht hier von überwachtem Lernen (*supervised learning)* bzw. unüberwachtem Lernen (*unsupervised learning)*.[40]

Von den Daten, die für das Training zur Verfügung stehen, sollte ein zufällig ausgewählter Teil vor dem Training heraussortiert, als getrenntes Datenset gespeichert und vorerst zurückbehalten, d.h. nicht für das Training der Transformationsregel verwendet werden. Es handelt sich hierbei um jene Daten, die dazu benutzt werden, den fertigen Algorithmus anhand von «neuen», d.h. nicht im Trainingsset enthaltenen Daten zu testen oder auch zu validieren. Die Daten in diesem Set werden daher Test- oder Validierungsdaten genannt.[41]

Soweit mit *supervised learning* gearbeitet wird, besteht das Ziel der Transformationsregel darin, die Daten des Trainingsdatensets den jeweils korrekten Labels zuzuweisen (die Anwendung auf die Testdaten folgt später). Im Rahmen von *unsupervised learning* besteht das Ziel darin, dass die KI unterschiedliche diskrete Kategorien von Daten in den Trainingsdaten bildet und neue Daten nach diesen Kriterien sinnvoll unterscheiden kann, z.B. dahinge-

---

[38] Andreas Kaminski/Colin W. Glass, Das Lernen der Maschinen, in: Kevin Liggieri/Oliver Müller (Hrsg.), Mensch-Maschinen-Interaktion – Handbuch zu Geschichte – Kultur – Ethik, Berlin 2019, 130, 132.

[39] Offenbar ein beliebtes Beispiel; vgl. dazu die Grafik bei Klaus (FN 36), 83.

[40] Kaminski/C.W. Glass (FN 38), 130 f.; mittlerweile wird an sehr grossen und unspezifizierten Modellen geforscht, sog. *foundation models*; siehe dazu die Übersicht bei https://research.ibm.com/blog/what-are-foundation-models/ (Abruf 11.06.2022).

[41] Andriy Burkov, The Hundred-Page Machine Learning Book, Eigenpublikation 2019, 49, der hier zusätzlich den Begriff *holdout set* verwendet, weil die Daten *zurückbehalten* werden; Kaminski/C.W. Glass (FN 38), 131.

hend, ob sie Bilder von Katzen und Hunden enthalten. Es existieren Ansätze, die diesbezügliche Qualitätsprüfung ebenfalls zu automatisieren.[42]

Die Ergebnisse des Trainings sind nicht notwendigerweise empirisch belastbare Kausalzusammenhänge. Vielmehr handelt es sich beim Output des KI-Trainings um stochastische Daten, also um Daten, die in einem gegebenen Datensatz eine Wahrscheinlichkeitsverteilung in Bezug auf bestimmte Merkmale in den Daten beschreiben. Wird festgestellt, dass der Algorithmus die Trainingsdaten gut voraussagt, kann ein Testlauf mit den Testdaten starten. Hier werden klassische Fehlerquellen, insbesondere eine mögliche Überanpassung an die Trainingsdaten geprüft.

3. Klassische Trainings-«Fehler»

a. Underfitting

«Fehler» im Sinne von unerwünschten Ergebnissen können entstehen, wenn Abkürzungen genommen werden, indem beispielsweise das Modell einfacher angelegt wird, als der gewünschte Output erfordert oder die benutzten Features für die gesuchte Funktion nicht informativ genug sind, um sinnvolle, regelhafte Unterscheidungen zu ermöglichen. Es handelt sich um eine Form von hohem Bias.[43]

b. Overfitting

Umgekehrt besteht im Rahmen des überwachten Lernens immer die Gefahr, dass ein Modell zu komplex ist, d.h. über zu viele Freiheitsgrade verfügt, und in der Folge zu präzise für die spezifische Anwendung auf die Trainingsdaten optimiert wird.[44] Dies kann darin resultieren, dass der Algorithmus idiosynkratische Muster des Trainingsdatensets als verallgemeinerbare Unterscheidungsmerkmale übernimmt, wodurch das Modell in der allgemeinen Anwendung

---

[42] Beispiel für eine automatisierte Überprüfung sind *generative adversarial networks* (GAN). Hier generiert ein neuronales Netzwerk Bilder, beispielsweise von Katzen, während ein zweites Netzwerk diese Bilder mit echten Bildern von Katzen vergleicht und Feedback gibt; Vgl. dazu Martin Giles, The GANfather: The man who's given machines the gift of imagination, Technology Review 21.02.2018.

[43] Burkov (FN 41), 51.

[44] Kaminski/C.W. Glass (FN 38), 130.

schlechte Resultate zeigen wird.[45] Es liegt mit anderen Worten eine *Überanpassung* des Modells an die Trainingsdaten vor.[46]

c. Benachteiligender Bias (und Diskriminierung)

Als Bias im technischen Sinn werden gemeinhin Verzerrungen des KI-Modells relativ zu den realen Begebenheiten der KI-Umwelt bezeichnet. Es handelt sich um architektonisch bedingte Effekte von Lernalgorithmen.[47] Diese können eine moralische Bedeutung[48] sowie eine aus rechtlicher Sicht signifikante Form annehmen, indem sie Unterscheidungen treffen oder nicht treffen, und daraus eine unsachliche bzw. ungerechtfertigte Ungleichbehandlung oder Diskriminierung resultiert. Obwohl der Grund für das Entstehen von Bias in der logischen Architektur von Lernalgorithmen zu finden ist, liegt die Quelle von rechtlich signifikanten Verzerrungen oftmals in den Trainingsdaten, indem diese unsorgfältig ausgesucht wurden. Da sich technischer Bias kaum vermeiden lässt, müssen KI-Systeme in der Anwendung stets mit Blick auf mögliche rechtsungleiche oder gar diskriminierende Auswirkungen in der realen Welt im Auge behalten werden.

Je nach Algorithmus kann es indes schwierig bis unmöglich sein, die diskriminierende Wirkung eines Bias *ex post* rechtsgenüglich zu belegen. Lässt sich nämlich eine strukturelle Benachteiligung in den Ergebnissen statistisch nachweisen, wird dadurch zunächst nur erkennbar, dass der KI eine tendenziell diskriminierende Entscheidungsstruktur antrainiert wurde. Damit ist nicht belegt, dass diese diskriminierende Verzerrung in einem Einzelfall für das Ergebnis ausschlaggebend war, da andere Faktoren «KI-intern» höher gewichtet worden sein könnten. Vor allem lässt sich möglicherweise nicht erkennen, ob die Vermutung einer Diskriminierung, welche aufgrund des Nachweises des Bias entstanden ist, innerhalb der internen Logik des Algorithmus durch eine

---

[45] Burkov (FN 41), 52.

[46] Kaminski/C.W. Glass (FN 38), 130 f.; Burkov (FN 41), 23 f.

[47] Stefan Bauberger/Birgit Beck/Aljoscha Burchardt/Petter Remmers, Ethische Fragen der künstlichen Intelligenz, in: Günther Görz, Ute Schmid, Tanya Braun (Hrsg.), Handbuch der künstlichen Intelligenz, 6. A. Berlin Boston 2021, 918; Batya Friedman/Helen Nissenbaum, Bias in Computer Systems, ACM Transactions on Information Systems, Vol. 14, No. 03.07.1996, abgedruckt in: John Weckert (Hrsg.), Computer Ethics, London New York 2007 (2018), 220.

[48] Friedman/Nissenbaum (FN 47), 217.

besonders qualifizierte sachliche Begründung entkräftet und die Entscheidung dadurch gerechtfertigt wurde.[49] In solchen Fällen müsste die qualifizierte Rechtfertigung scheitern.

Das klassische Beispiel für einen technischen Bias, der zu diskriminierenden Entscheidungen führen kann, stammt aus der Gesichtserkennung.[50] Idealerweise sucht man hierfür ein KI-System, das grundsätzlich in der Lage wäre, jedes Gesicht der Welt zu erkennen, egal welchen Alters, Geschlechts oder Hautfarbe. Aufgrund der Tatsache, dass Erkennungsalgorithmen oft mit Bildern von Gesichtern trainiert werden, die überwiegend männlich und hellhäutig sind, zeigen KI-Systeme immer wieder Schwächen bei der Erkennung von Gesichtern von Frauen bzw. von dunkler Hautfarbe, was in einer schlechteren Trefferquote für die Erkennung von dunkelhäutigen weiblichen Gesichtern resultieren kann. Je nach Verwendung des KI-Systems entstehen hierdurch Nachteile für die Betroffenen.[51] Der Schlüssel zur Vermeidung von benachteiligendem Bias liegt in diesen Fällen in der sorgfältigen Auswahl von repräsentativen Trainingsdaten.

---

[49] Zur Diskriminierungsprüfung siehe René Rhinow/Markus Schefer/Peter Uebersax, Schweizerisches Verfassungsrecht, 3. erw. u. akt. Aufl., Basel 2016, N 1891; Giovanni Biaggini, in: Giovanni Biaggini (Hrsg.), BV Kommentar, 2. A., Zürich 2017 (zit. OFK BV-Biaggini), Art. 8 N 22; Bernhard Waldmann, in: Bernhard Waldmann/Eva Maria Belser/Astrid Epiney (Hrsg.), Schweizerische Bundesverfassung, Basler Kommentar, Basel 2015, Art. 8 BV N 87; Rainer Schweizer, St. Galler Kommentar zu Art. 8 BV, in: Bernhard Ehrenzeller/Benjamin Schindler/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die Schweizerische Bundesverfassung, St. Galler Kommentar, 3. A. St. Gallen 2014, (zit. SGK BV-VerfasserIn) N 54; Vincent Martenet, Commentaire sur article 8 Cst., in: Vincent Martenet/Jacques Dubey (Hrsg.), Constitution fédérale, Commentaire Romand, Basel 2021 (zit. CR Cst.-VerfasserIn), N 98.

[50] Zu den weiteren Herausforderungen der Gesichtserkennung siehe VII.A.3.

[51] Notorisch ist das «Gorilla»-Debakel von Google Photos: Mitchell (FN 3), 123 ff.; Tom Simonite, When It Comes to Gorillas, Google Photos Remains Blind, Wired.com 11.01.2018; Marco Metzler, Wie Computer lernen, uns zu diskriminieren, NZZ vom 04.03.2017; Richard Nieva, Google apologizes for algorithm mistakenly calling black people ‹gorillas›, cnet.com 01.07.2015; Maggie Zhang, Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software, Forbes.com 01.07.2015.

Probleme können aber dennoch (oder erst recht) auftauchen, wenn sorgfältig ausgewählte Daten eine in der Gesellschaft vorhandene, gruppenspezifische Benachteiligungen korrekt transportieren.[52] In diesem Zusammenhang sorgt es für Verwirrung, dass der Begriff «Bias» mit einer anderen Bedeutung verwendet wird, die jener des technischen Bias aber sehr ähnlich ist. Von einem vorbestehenden Bias (*pre-existing bias*[53] oder *societal bias*[54]) wird gesprochen, wenn die Ergebnisse der KI tatsächliche, unerwünschte Ungleichbehandlung in der Gesellschaft widerspiegeln.[55] Hier bezieht sich die Verzerrung nicht auf die realen Tatsachen, wie sie sind, sondern auf die realen Tatsachen, wie sie aus rechtlicher oder moralischer Sicht sein sollten. Aus technischer Sicht ist anzumerken, dass der nicht-technische, vorbestehende Bias sich auf die Ergebnisse der KI als Abbild gesellschaftlicher Zustände bezieht und nicht auf die korrekte Funktionsweise der KI.

Die Vermeidung von Bias mit rechtlich relevanten negativen Folgen kann demnach auf mindestens zwei konzeptionell nachvollziehbare Arten angegangen werden. Zum einen kann durch sorgfältige Auswahl der Trainingsdaten darauf geachtet werden, dass das zu analysierende Phänomen in repräsentativer Weise wiedergeben wird.[56] Zum anderen ist es denkbar, dass mittels Bias in KI-Systemen tatsächliche Benachteiligungen in der Gesellschaft identifiziert und der politischen Diskussion zugeführt werden.[57] Die erste

---

[52] Bauberger et al. (FN 47), 919; siehe die Beispiele bei Coeckelbergh (FN 3), 127 ff.; vgl. dazu den «Referenzfall COMPAS» bezüglich Strafaussetzung auf Bewährung in den USA bei Martini (FN 29), 55 f.; sowie Julia Angwin/Jeff Larson/Surya Mattu/Lauren Kirchner, Machine Bias, ProPublica.org, 23.05.2016.

[53] Friedman/Nissenbaum (FN 47), 218.

[54] Russel/Norvig (FN 2), 1043 f.

[55] Bauberger et al. (FN 47), 918 f.; a.M. Coeckelbergh (FN 3), AI Ethics, Cambridge (MA)/London 2020, 126, der mit *bias* offenbar Bias mit rechtlich relevanten Unterscheidungsfehlern (z.B. Diskriminierung) meint; ebenso Friedman/Nissenbaum (FN 47), 217.

[56] Zu den diesbezüglichen Herausforderungen Ben Schneiderman, Human-Centered AI, Oxford University Press 2022, 161 ff.

[57] Vgl. dazu Aria Khademi/David Foley/Sanghack Lee/Vasant Honavar, Fairness in algorithmic decision making: An excursion through the lens of causality, Proceedings of the World Wide Web Conference, ACM 2019, 2907-2914, arXiv:1903.11719; Christian (FN 19), 47 ff.

Vorgehensweise betrifft den Datenschutz direkt, indem über die Qualität der Daten grundrechtliche Risiken der Betroffenen vermindert werden. Die zweite Methode ist dagegen primär eine Frage der politischen und verfassungsrechtlichen Entwicklung im Umgang mit KI. Sie betrifft Datenschutzfragen insofern, als die zur entsprechenden KI-Analyse notwendigen Daten personenbezogene Daten sein werden.

C. Überprüfbarkeit in der Anwendung

Um herauszufinden, wie gut ein KI-System die gestellte Aufgabe in der Anwendung meistert, müssen dessen Resultate in irgendeiner Form überprüfbar sein.[58] Dabei ist zu unterscheiden, ob sich der zu prüfende Algorithmus im Trainingsstadium oder in jenem der Anwendung befindet. Im Training dient die Überprüfung dazu, den *Lernerfolg* zu messen, während in der Anwendung die *Nützlichkeit* des Algorithmus in Bezug auf die ihm gestellte Aufgabe im Vordergrund steht. Der Lernerfolg kann auf strukturell benachteiligenden oder diskriminierenden Bias untersucht,[59] die Nützlichkeit der jeweiligen Prognose dagegen im Einzelfall angefochten werden.

Die Überprüfung erfolgt grundsätzlich mithilfe der durch Menschen in einem Datenset feststellbaren Tatsachen, bzw. festgelegten Ein- und Ausgabewerte, der sog. *ground truth*.[60] In dem vorhin benutzten Beispiel sind dies die Tatsachen darüber, welche Bilder tatsächlich Hunde zeigen, welche Bilder tatsächlich Katzen zeigen. So kann festgestellt werden, ob und gegebenenfalls inwieweit die Transformationsregel, welche durch den Algorithmus gebildet wurde, das Verhältnis zwischen Ein- und Ausgabedaten korrekt abbildet.

---

[58] Siehe zum Transparenzprinzip IV.A.1.c.

[59] Siehe I.B.3.c.

[60] Kaminski/C.W. Glass (FN 38), 128.

Schwierig wird der Vergleich dort, wo die tatsächlichen Gegebenheiten nur schwer feststellbar sind. In solchen Fällen kann möglicherweise mittels statistischer Evidenz ermittelt werden, ob die individuellen, wie gesellschaftlichen Auswirkungen der Verwendung von Ergebnissen einer KI-Instanz den damit verfolgten Zweck erfüllen oder nicht.[61] Auf diese Weise könnte in manchen Fällen auch ein benachteiligender bzw. diskriminierender Bias nachgewiesen werden.[62] Ein statistischer Prüfungsansatz bedingt indes, dass sinnvolle Messwerte sowie eine Bandbreite von akzeptablen Resultaten festgelegt werden können.

D. Nicht-lernende KI-Systeme

Als künstlich intelligent gelten neben Lernalgorithmen nach wie vor Systeme aus den ersten Jahrzehnten der KI-Forschung, die auf unveränderlichen, deterministischen Entscheidungsalgorithmen basieren. Im Gegensatz zu Lern-KI arbeiten einfache logische Agenten mit vorprogrammierten Regeln und nicht mit erlernten Wahrscheinlichkeiten. Sie sind daher grundsätzlich berechenbar und transparent.[63] Ein gutes Beispiel sind einfache Expertensysteme, deren Programm aus einer Sammlung von logisch verknüpften Aussagen bestehen, die jeweils Expertenwissen in einer Domäne wiedergeben.

Die intrinsischen Datenschutzprobleme solcher Algorithmen erscheinen aufgrund ihrer Architektur als weit weniger weitreichend wie jene von Lernalgorithmen. Soweit KI-Systeme indes nicht-lernende Elemente enthalten, werden diese – wie andere Software auch – in die datenschutzrechtliche Beurteilung des Gesamtsystems einbezogen werden müssen.

---

[61] Joanna J. Bryson, The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation, in: Markus D. Dubber/Frank Pasquale/Sunit Das (Hrsg.), The Oxford Handbook of Ethics of AI, Oxford University Press 2020, 9.

[62] OECD (FN 13), 92.

[63] Siehe IV.A.1.d.

II. Vorüberlegungen zu KI und Datenschutz

A. KI-Wertung versus Selbstwertung

Die Möglichkeit von künstlicher Intelligenz, Entscheidungsprozesse zu automatisieren, steht in einem gewissen Widerspruch zum Kerngedanken des Datenschutzes, wonach jedem Menschen ein verfassungsmässiges Recht auf informationelle Selbstbestimmung zukommt. Der Grund liegt darin, dass die Automatisierung eine Einflussnahme der Betroffenen auf das Ergebnis im Einzelfall verunmöglichen oder zumindest in unzumutbarer Weise erschweren und zudem zu einer unübersichtlichen Datenlage hinsichtlich der «eigenen» Personendaten führen kann.[64]

Weitere Risiken für die Grundrechte der Betroffenen entstehen, wenn KI-Systeme ihnen gewisse Persönlichkeitsaspekte wie etwa «erhöhte Gefährlichkeit»[65] oder Emotionen[66] zuweisen, insb. wenn diese Zuweisung die Grundlage für eine (hier: staatliche) Entscheidung bildet. Die (implizite) Verknüpfung mit besonders geschützten Merkmalen von Art. 8 BV kann zudem zu einer (mittelbaren) Diskriminierung durch einen benachteiligenden Bias im verwendeten Algorithmus führen.[67] Schliesslich ist ebenso bedenklich, dass die Ergebnisse der Ausforschung von Personen durch KI als Hebel für Manipulation verwendet werden können, und zwar auf einer individuellen wie auch auf einer gesellschaftlichen bzw. demokratischen Ebene.[68]

---

[64] Thomas Wischmeyer, Regierungs- und Verwaltungshandeln durch KI, in: Martin Ebers/Christian Heinze/Tina Krügel/Björn Steinrötter (Hrsg.), Künstliche Intelligenz und Robotik – Rechtshandbuch, München 2020, § 20 N 51 ff.

[65] Beispielsweise im Rahmen von *predictive policing,* siehe VII.A.6.

[66] Catrin Misselhorn, Künstliche Intelligenz und Empathie – Vom Leben mit Emotionserkennung, Sexrobotern & Co., Reclam Ditzingen 2021, 20 ff.

[67] Siehe I.B.3.c.

[68] Zum Ganzen BVerfG, 06.11.2019 – 1 BvR 16/13 – Recht auf Vergessen I, N 85; Nadja Braun Binder/Thomas Burri/Melinda Florina Lohmann/ Monika Simmler/ Florent Thouvenin/Kerstin Noëlle Vokinger, Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, in: Jusletter vom 28.06.2021, N 31 ff.; Dirk Helbling, Societal, Economic, Ethical and Legal Challenges of the Digital Revolution – From Big Data to Deep Learning, Artificial Intelligence, and Manipulative Technologies, in: Jusletter IT vom 21.05.2015, N 40; Sami Coll, Big Data, Big Problem?, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Big Data und Datenschutzrecht, Zürich/Basel/Genf 2016, 26 f.

Datenschutz ist einer jener Bereiche, in denen das sogenannte *value alignment problem* der KI-Technologien sehr deutlich zum Vorschein kommt. Der Begriff bezeichnet die Schwierigkeit, die Wertvorstellungen der menschlichen Nutzerinnen – inklusive jenen Werten, die durch die Normen des Rechts transportiert werden – mit den durch die Automatisierungsfunktion der KI tatsächlich beförderten Werten in Einklang miteinander zu bringen.[69] Aus technischer Sicht zeigt sich das Problem dort, wo die *utility function,* d.h. die internalisierte Werteskala bzw. -gewichtung der KI in ihrer Lösungsstrategie gesellschaftliche und individuelle Wertvorstellungen bezüglich des zu lösenden Problems nicht miterfasst.[70] Gerade weil KI-Systeme laufend verfeinert und vergrössert werden und in der Form von sog. *foundation models* mittlerweile mit Millionen von automatisch generierten Parametern operieren können,[71] ist die Auflösung dieses Zielkonflikts alles andere als trivial, zumal die Erarbeitung der Parameter für die internalisierte Werteskala oftmals als Geschäftsgeheimnis aufgefasst und entsprechend intransparent und entkoppelt von Nutzern bzw. gesellschaftlichen Entscheidungsstrukturen erfolgt.[72] Soweit öffentliche Organe solche KI-Produkte nutzen, kann dies die demokratische Legitimation von Normgebungs- oder anderen staatlichen Entscheidungsprozessen unterwandern, so etwa, wenn Beurtei-

---

[69] Le Cun (FN 3), 370 ff.; zur Problemstellung in Bezug auf Moral Lukas Brand, Künstliche Tugend – Roboter als moralische Akteure, Regensburg 2018, 80 ff.

[70] Russel/Norvig (FN 2), 1054 f.; dies kann sich in einem diskriminierenden Bias zeigen, siehe I.B.3.c.

[71] Siehe beispielsweise Suman Bhattacharyya, Meta Unveils New AI Supercomputer, WSJ vom 24.01.2022; zum Begriff siehe FN 40; zur Problematik siehe auch Briefing, Huge «foundation models» are turbo-charging AI progress, The Economist, 11.07.2022, https://www.economist.com/interactive/briefing/2022/06/11/huge-foundation-models-are-turbo-charging-ai-progress (Abruf 12.06.2022); Rishi Bommasani/Percy Liang, Reflections on Foundation Models, Stanford HAI, 18.10.2021, https://hai.stanford.edu/news/reflections-foundation-models (Abruf 01.06.2022).

[72] Martini (FN 29), 33 ff.; Glass (FN 26), 214 f.

lungsspielräume der Verwaltung durch Entscheidungen eines KI-Systems konkretisiert werden.[73]

Schliesslich ist zu bedenken, dass die internalisierte Werteskala im Hinblick auf ihre Nützlichkeit in Bezug auf das Zielergebnis der KI optimiert wird. Letzteres kann moralisch signifikante Auswirkungen in der KI-Umwelt zeitigen, wird aber auf absehbare Zeit nicht von einer KI-Funktion moralisch bewertet werden können.[74] Damit bleibt auch die Möglichkeit einer rechtlichen Selbstkontrolle durch die betreffende KI vorerst auf die Anwendung von entscheidbaren Regelnormen bzw. die Erkennung von klar definierten Sachverhaltselementen (beispielsweise die Identifikation eines Nummernschildes) beschränkt.

B. Selbstbestimmung in Bezug auf personenbezogene Daten

In Zusammenhang mit der Digitalisierung im Allgemeinen und künstlicher Intelligenz im Besonderen wird in der Literatur erneut darauf hingewiesen, dass das Recht auf informationelle Selbstbestimmung durch die technische Entwicklung obsolet geworden oder gar von Beginn an eine Fehlkonstruktion gewesen sei.[75] Diese Kritik wurde bereits nach der Entwicklung des Rechts durch das Bundesverfassungsgericht im Volkszählungsurteil vorgebracht,[76]

---

[73] Danielle Keats Citron, Technological Due Process, 85 WASH. U. L. REV. 1249 (2008), https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2 (Abruf 07.02.2022), 1294 ff.; zur Opazität von COMPAS bezüglich Rückfallwahrscheinlichkeit Monika Simmler/Giulia Canova, Smart Government in der Strafrechtspflege: Wann ist Smart Criminal Justice smart?, in: Monika Simmler (Hrsg.), Smart Criminal Justice – Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege, Basel 2021, 50.

[74] Catrin Misselhorn, Grundfragen der Maschinenethik, Reclam Ditzingen 2018, 70 ff.; Brand (FN 69), 89 f.

[75] Hinweise bei Braun Binder et al. (FN 68), N 17.; Vgl. auch die vorgeschlagene Neukonzeption für das deutsche Recht bei Marion Albers, Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in: Michael Friedewald/Jörn Lamla/Alexander Rossnagel (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, 21 ff.

[76] Siehe die Hinweise bei Glass (FN 26), 154 f.; Hanspeter Bull, Informationelle Selbstbestimmung – Vision oder Illusion? – Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, Tübingen 2009, 45 ff.; Florent Thouvenin, Informational Self-Determination: A Convincing Rationale for Data Protection Law?, JIPITEC 4/2021, N 4 ff.

sowie nach der Übernahme des Grundrechts als Teilgehalt der persönlichen Freiheit[77] in das schweizerische Recht durch das Bundesgericht.[78] Aus verschiedenen Gründen ist hier Vorsicht geboten.

Zunächst ist die Idee, ein Grundrecht aufgrund mangelnder Wirksamkeit infrage zu stellen, mit Gefahren für den Bestand des Grundrechts und damit auch für die geschützten Personen verbunden. Die Relativierung eines Grundrechts in seinem materiellen Gehalt aufgrund einer festgestellten mangelhaften Umsetzung käme einer Kapitulation gegenüber den betreffenden Verletzungskonstellationen gleich. Als legitim erscheint dagegen, die Wirkungsweise eines Grundrechts in Bezug auf die Verwirklichung von dessen Schutzgehalt zu hinterfragen und gegebenenfalls anzupassen.[79]

Das Konzept eines Rechts auf informationelle Selbstbestimmung wurde im Volkszählungsurteil des deutschen Bundesverfassungsgerichts begründet und war eine Reaktion auf einen drohenden Kontrollverlust,[80] den das Gericht in Bezug auf persönliche Informationen sowie das Bild, welches Dritte sich von der eigenen Person machen, diagnostiziert hatte.[81] Als Ausdruck eines informationellen Persönlichkeitsschutzes war es nie als «absolute Verfügungsbefugnis»[82] über «eigene» Personendaten konzipiert.[83]

Die aktuelle Rechtsprechung des Bundesverfassungsgerichts bekräftigt dies: Die ursprüngliche Formel aus dem Volkszählungsurteil, entwickelt als Abwehrrecht gegen den Staat,[84] wonach das Grundrecht eine Befugnis des Einzelnen gewährleiste, «grundsätzlich selbst über die Preisgabe und Ver-

---

77 Beat Rudin, in: Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich/Basel/Genf 2014 (zit. VerfasserIn, PraKom IDG BS), Grundlagen, N 2.

78 Dazu Rudin, PraKom IDG BS (FN 77), Grundlagen, N 5 ff.

79 Vgl. dazu Eva Maria Belser, Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Bern 2013, 27.

80 Zu aktuellen Formen des drohenden Kontrollverlustes Albers (FN 75), 27.

81 BVerfGE, 65,1 (42 f.).

82 Belser (FN 79) 25; Albers (FN 75), 16.

83 Für das schweizerische Recht Beat Rudin, Kollektives Gedächtnis und informationelle Integrität, AJP 1998, 248 f.; Glass (FN 26), 155.

84 Albers (FN 75), 19.

wendung seiner persönlichen Daten zu bestimmen»[85] wurde im Verhältnis zwischen Privaten präzisierend ergänzt. Hier entfalte sie eine mittelbare Drittwirkung im Sinne einer «Gewährleistung, über der eigenen Person geltende Zuschreibungen selbst substanziell mitzuentscheiden».[86] Diese neue Formel eines «Rechts auf substanzielle Mitentscheidung» entspricht nach wie vor der ursprünglichen Funktion der informationellen Selbstbestimmung als ergänzendem Schutz der Privatheit in Bezug auf Daten über die eigene Person, welche sich ausserhalb des Herrschaftsbereichs des Individuums bei Dritten befinden.[87]

Es erscheint daher nach wie vor als sachgerecht, im schweizerischen Recht die informationelle Selbstbestimmung als Teilgehalt bzw. informationelle Dimension des in Art. 10 Abs. 2 BV garantierten Rechts auf persönliche Freiheit aufzufassen,[88] und als eigenständigen Aspekt des in Art. 13 Abs. 2 BV garantierten Missbrauchsschutz gegen grundrechtsverletzende Datenbearbeitungen beizubehalten.[89] Als solcher tritt es gleichsam als Recht auf «informationelle Integrität»[90] neben den körperlichen und geistigen Integritätsschutz. Der Schutzbereich erstreckt sich hierbei zunächst auf Personendaten, welche Informationen über elementare Erscheinungsformen der Persönlichkeitsentfaltung abbilden – unabhängig davon, wo sich diese befinden.[91] Da nun aber das allgemeine Persönlichkeitsrecht in enger Beziehung zu den übrigen Grundrechten steht, indem es als «verfassungsrechtliche Grundgarantie zum Schutz der Persönlichkeit» gilt, welche «hinter die speziellen Garantien zurücktritt»,[92] können die aus den speziellen Garantien fliessenden informationsspezifischen Teilgehalte umgekehrt als Ausbildungen eines so verstandenen informationel-

---

85 BVerfGE 65, 1 (43).

86 BVerfG, 06.11.2019 – 1 BvR 16/13 – Recht auf Vergessen I, N 86 f.; siehe auch Braun Binder et al. (FN 68), FN 31.

87 Glass (FN 26), 178 f.

88 Belser (FN 79), 27 ff..; Zur historischen Entwicklung dieser Verbindung und der diesbezüglichen bundesgerichtlichen Rechtsprechung siehe Belser (FN 26), Datenschutzrecht Grundlagen, 322 f.; Vgl. die Hinweise bei Rudin (FN 83), 248; SGK BV-Breitenmoser (FN 49), Art. 13 BV, N 4.

89 Im Ergebnis ähnlich Belser (FN 26), Datenschutzrecht Grundlagen, 378 N 121.

90 Rudin, PraKom IDG BS (FN 77), Grundlagen, N 4.

91 Glass (FN 26), 164 f.

92 OFK BV-Biaggini (FN 49), Art. 10 N 17.

len Persönlichkeitsschutzes verstanden werden. Dies bringt die ursprüngliche, vom Bundesgericht bestätigte Funktion der persönlichen Freiheit als Garantin der übrigen Rechte zum Ausdruck.[93]

Ein auf diese Schutzfunktion der persönlichen Freiheit bezogenes Recht auf informationelle Selbstbestimmung ist Garantin der übrigen Verfassungsrechte in Bezug auf die damit zusammenhängenden Informationen bzw. Personendaten. Als solche erstreckt sie sich über den Schutzbereich der Grundrechte insgesamt und kann auch als Grundlage und Massstab[94] dienen, um über das Verwirklichungsgebot in Art. 35 BV entsprechende Schutzpflichten der Datenbearbeiter festzulegen. Damit wird auch deutlich, dass die informationelle Selbstbestimmung primär gegenüber dem Staat wirksam und für Informationsvorgänge zwischen Privaten in der Regel konkretisierungsbedürftig ist. Mithin ist die «informationelle Integrität» als Persönlichkeitsgut im Sinne des zivilrechtlichen Persönlichkeitsschutzes zu betrachten.[95] Die in der Literatur beklagte faktische Wirkungslosigkeit oder auch Inhaltsleere der informationellen Selbstbestimmung[96] wird damit primär zum Thema für den Gesetzgeber,[97] die Gerichte, den eidgenössischen Datenschutzbeauftragten sowie die Lehre und die Anbieter von Rechtsdienstleistungen.[98]

Eine so verstandene informationelle Selbstbestimmung korrespondiert mit der Gesetzgebung in der Schweiz, soweit Datenschutzgesetze ausdrücklich den Schutz der Grundrechte der betroffenen Personen als Gesetzeszweck nennen,

---

93 BGE 90 I 29 E. 3a: «En d'autres termes, elle (die persönliche Freiheit; Anm. d. Verfassers) vise à garantir l'existence des conditions de fait indispensables pour que l'homme puisse effectivement exercer ces autres libertés»; siehe auch bei Belser (FN 26), Datenschutzrecht Grundlagen, 322 N 9.

94 Glass (FN 26), 161.

95 Dazu Philip Glass, Die Schutzparameter des zivilrechtlichen und des verfassungsrechtlichen Persönlichkeitsrechts, datalaw.ch, 28.05.2018, N 4 ff. m.w.H.

96 Belser (FN 79), 27 m.w.H.; Gächter/Werder (FN 26), 88.

97 Vgl. dazu Drittenbass (FN 26), N 144.

98 Ähnlich Gächter/Werder (FN 26), 95, allerdings nicht als Ausdruck der informationellen Selbstbestimmung, sondern als konkretisierungsbedürftige «justiziable Minimalgarantie» des verfassungsrechtlichen Datenschutzes.

insbesondere Art. 1 DSG bzw. Art. 1 nDSG[99], sowie für den Kanton Zürich § 1 Abs. 2 Bst. b IDG ZH[100].[101]

Schliesslich sollte nicht vergessenen gehen, dass die Datenschutzidee aus der Beobachtung entstand, dass die Verletzung von Grundrechten durch die moderne Bearbeitung von Personendaten einfacher, leichter skalierbar und zugleich für den Einzelnen weniger durchschaubar geworden war. Mittlerweile droht das Ausmass an Ausforschung der Persönlichkeitsstruktur des Einzelnen in ein Übergewicht der Fremd- gegenüber der Eigenwahrnehmung zu münden. Damit verbunden besteht das Risiko der Zurechnung bzw. Übernahme eines datafizierten, d.h. aus quantifizierten Datenmustern zusammengesetzten,[102] unterkomplexen und aus der Drittperspektive entwickelten Selbst.[103] Die informationelle Selbstbestimmung im Sinne des datenschutzrechtlichen Grundrechtsschutzes betrifft daher stets nur die Bearbeitung von personenbezogenen Daten, d.h. insbesondere Erhebung, Aufbewahrung, Nutzung, Veränderung,

---

[99] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1); zum neuen Datenschutzgesetz des Bundes (nDSG) siehe Botschaft vom 25. September 2020 zum Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG), BBl 2020 7639.

[100] Gesetz vom 12. Februar 2007 über die Information und den Datenschutz des Kanton Zürich (Informations- und Datenschutzgesetz, IDG ZH; ON 170.4).

[101] BSK DSG-Urs Maurer-Lambrou/Simon Kunz, in: Urs Maurer-Lambrou/Gabor Blechta, Datenschutzgesetz – Öffentlichkeitsgesetz, Basler Kommentar, Basel 2014 (zit. BSK DSG-VerfasserIn), Art. 1 N 26; Rudin, PraKom IDG BS (FN 77), § 1 N 12; Bruno Baeriswyl, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zürich/Basel/Genf 2012 (zit. VerfasserIn, PraKom IDG ZH), § 1 N 10 f.; eher restriktiv interpretiert bei David Rosenthal, in: David Rosenthal/Yvonne Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich 2008 (zit. VerfasserIn, in: Handkommentar DSG), Art. 1 N 3; Vgl. auch die qualifizierte Form der gesetzlichen Verbindung von Datenschutz und Grundrechten in § 3 Abs. 4 Bst. a IDG BS, der die besonderen Personendaten definiert als «Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht»; zum neuen Datenschutzgesetz des Bundes (nDSG) siehe BBl 2020 7639.

[102] Zum Begriff *datafication* siehe Viktor Mayer-Schönberger/Kenneth Cukier, Big Data – The Essential Guide to Work, Life and Learning in the Age of Insight, üb. u. erw. A., London 2017, 78 ff.

[103] Mireille Hildebrandt, Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning, Theoretical Inquiries in Law, Vol. 20.1 83 (2019), 92 f.

Weitergabe und Löschung.[104] Die tatsächliche Verwirklichung eines datenbasierten grundrechtlichen Risikos fällt nach wie vor in den «traditionellen» Schutzbereich des betreffenden Grundrechts. Denn das Datenschutzrecht schützt nicht direkt vor Grundrechtsverletzungen, sondern vor Datenbearbeitungen, welche diese als Risiko oder Gefahr für die Betroffenen begünstigen. Es ist mithin ein mit den Grundrechten eng verknüpfter, diesen vorgelagerter, präventiver und vor allem *eigenständiger* Schutzmechanismus.[105]

Im Ergebnis setzt das Datenschutzrecht angesichts der neuen Herausforderungen durch vernetzte künstlich intelligente Systeme und Agenten weiterhin auf die Autonomie des Einzelnen und die rechtliche Absicherung der hierzu notwendigen Bedingungen. In dieser Betonung der Selbstbestimmung ist die Forderung zu erblicken, auch in einer von Automation durchdrungenen Gesellschaft ein autonomes Subjekt bleiben zu dürfen – zumindest in einem gewissen Umfang. Schlussendlich ist für die Betroffenen unerheblich, ob die Bedrohung für ihre persönliche Entwicklung von empirischen oder probabilistischen Daten ausgeht. Letztere sind indes schwieriger zu verifizieren und stellen damit in der Tendenz die komplexere Bedrohung dar.

III. KI und Personendaten

A. Die künstlich intelligente Bearbeitung von Personendaten

Künstlich intelligente Systeme werden datenschutzrelevant, wenn mit ihnen Personendaten bearbeitet werden. Viele KI-Systeme, wie etwa solche zur vorausschauenden Instandhaltung von Maschinen, bearbeiten nur Sachdaten. Die Ergebnisse von KI-Bearbeitungen können aber potenziell auf dieselbe Weise wie empirisch erhobene Sachdaten mit Personen verknüpft werden, wodurch sie den Status von Personendaten erlangen.

---

[104] Albers (FN 75), 17.

[105] Vgl. aus der Perspektive des Privatrechts Alfred Früh, Roboter und Privacy: Informationsrechtliche Herausforderungen datenbasierter Systeme, AJP 2017 141–151, 145; Gächter/Werder (FN 26), 91.

Auch hier gilt, dass unter der Bearbeitung jede Form des Umgangs mit Personendaten durch das Programm gemeint ist. Dies ist grundsätzlich während sämtlichen Phasen des Lebenszyklus von Daten innerhalb einer KI-Anwendung[106] möglich. Personendaten können zunächst als Trainings-, Test- (bzw. Validierungs-) oder Inputdaten verwendet werden. Auch kann ein System darauf ausgerichtet sein, im Rahmen seines Outputs neue Personendaten zu generieren.

Schlussendlich birgt jedes Stadium des Lebenszyklus eines KI-Systems, also die Entwicklung bzw. das Trainieren von Transformationsregeln, die Erzeugung von Outputs aus Inputs, sowie die Einbettung in Entscheidungsprozesse eigene Risiken. Aus Sicht des Datenschutzrechts ist dies von Bedeutung, da sämtliche dieser Phasen je eigenständige Formen der Datenbearbeitung darstellen, die durch Verknüpfung mit Personen in den Geltungsbereich der Datenschutzgesetze fallen können. Die nachfolgende skizzenhafte Darstellung bezieht sich vornehmlich auf den Geltungsbereich des IDG ZH, indes sind die darin enthaltenen Überlegungen auf andere Datenschutzgesetze übertragbar.

1. Bearbeitung von personenbezogenen Daten als Trainings- oder Validierungsdaten

KI-Systeme, die nützliche künstlich intelligente Funktionen bereitstellen, können deterministischen Vorgaben folgen oder trainiert werden. Die initiale Programmierung eines Lernalgorithmus bleibt insofern statisch, als zunächst eine Grundformel entwickelt werden muss, auf deren Basis das KI-System trainiert wird.

Für die Beurteilung des grundrechtlichen Risikos ist von besonderer Bedeutung, dass das Training einer künstlich intelligenten Funktion stets darauf abzielt, eine Transformationsregel zwischen Input- und Outputdaten zu bilden; Ziel ist die Bildung einer Regel als Resultat des Lernprozesses und nicht eine Einzelfallentscheidung; in diesem Lernvorgang liegt das Moment der künstlichen Intelligenz.[107] Das KI-System als Ergebnis des Trainings

[106] Zum Lebenszyklus von KI-Systemen vgl. OECD (FN 13), 26.

[107] Kaminski/C.W. Glass (FN 38), 130.

prägt dadurch die spätere Entscheidungsfindung in der Anwendung.[108] Auch wenn das Modell anhand von personenbezogenen Daten trainiert wird, bleibt das Training damit auf eine Kategorienbildung beschränkt. Die Outputdaten des Trainings dienen der Überprüfung der Transformationsregel und bilden weder eine Unterstützung im Hinblick auf die Entscheidung eines Einzelfalls, noch beziehen sie sich auf eine bestimmte oder bestimmbare Person.[109]

2. Bekanntgabe von Personendaten zu Trainingszwecken

Aufgrund dessen ist davon auszugehen, dass für die Nutzung von Personendaten als Trainingsdaten die Bestimmungen über die Nutzung von Personendaten zu nicht personenbezogenen Zwecken zur Anwendung gelangen. Für den Kanton Zürich bestimmt das Gesetz zunächst in § 9 Abs. 2 IDG ZH, dass öffentliche Organe Personendaten zu nicht personenbezogenen Zwecken bearbeiten dürfen, «wenn sie anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind». Sie dürfen überdies gemäss § 18 IDG ZH Personendaten zum Zweck der nicht personenbezogenen Bearbeitung an Dritte bekanntgeben, soweit diese nachweisen, «dass die Personendaten anonymisiert werden, aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind und die ursprünglichen Personendaten nach der Auswertung vernichtet werden».

Entscheidend erscheint hier, dass nur eine (relative) Unmöglichkeit von Rückschlüssen auf *betroffene* Personen nachzuweisen ist – also jene Personen, deren Daten zum Zweck des Trainings bekannt gegeben wurden. Erwiesen und damit bedenkenswert erscheint in diesem Zusammenhang, dass es unter Umständen möglich sein kann, durch *re-engineering* des Modells einzelne Trainingsdaten zu de-anonymisieren und der richtigen Person zuzuordnen.[110] In diesen Fällen bzw. wenn keine Prognose bezüglich der Anonymität des Mo-

[108] Martini (FN 29), 50.

[109] Siehe I.B.

[110] Lena Leffer/Maximilian Leicht, Datenschutzrechtliche Herausforderungen beim Einsatz von Trainingsdaten für KI-Systeme, in: Jusletter IT vom 24.02.2022, N 21, schliessen daraus, dass gewisse KI-Modelle wie pseudonymisierte Personendaten zu behandeln sind, d.h. nach wie vor dem Datenschutzrecht unterstehen.

dells möglich ist, müsste ein KI-Modell im Zweifelsfall als «nicht anonym» und damit als Personendatum eingestuft werden.[111]

Die Zulässigkeit, zu einem späteren Zeitpunkt durch Anwendung der trainierten KI-Funktion Schlüsse auf *weitere* Personen zu ziehen, stellt insofern eine separate Datenschutzfrage dar, die bei Einsatz des KI-Systems zu beantworten ist.

Soweit schliesslich ein Teil der verfügbaren Daten von den Trainingsdaten getrennt wird, um die Leistungsfähigkeit des KI-Systems testen bzw. dessen Funktion validieren zu können,[112] sind diese Validierungsdaten wohl gleich zu behandeln wie die Trainingsdaten.

3. Bearbeitung von personenbezogenen Daten als Inputdaten

Soweit nun personenbezogene Daten als Inputdaten für ein KI-System verwendet werden, das System also im Rahmen der Tätigkeit eines öffentlichen Organs eingesetzt wird, sind verschiedene Szenarien denkbar. Erstens können personenbezogene Daten als Personendaten verwendet werden, beispielsweise für eine Profilbildung einer bestimmten bzw. bestimmbaren Person bzw. Gruppe von Personen oder als Grundlage für eine automatisierte Einzelentscheidung, beispielsweise für eine Parkbusse. In diesem Fall gelten die üblichen Bestimmungen des IDG ZH. Zweitens können die personenbezogenen Daten von den jeweiligen Personen entkoppelt werden, indem man die Sachdaten von den identifizierenden Daten trennt. Je nachdem, wie endgültig die Entkoppelung eingeschätzt wird, gelten andere gesetzliche Regelungen. Soweit eine Wiederherstellung des Personenbezugs ausgeschlossen werden kann, spricht man von *anonymen* Personendaten. Für sie gelten die besonderen Grundsätze der Bearbeitung von Personendaten in Abschnitt 2 des IDG ZH grundsätzlich nicht. Dies ergibt sich im Umkehrschluss aus der in § 3 Abs. 3 IDG ZH enthaltenen Definition von Personendaten als auf eine bestimmte oder bestimmbare Person bezogene Angaben.

---

[111] Dies entspricht offenbar gängiger Praxis, vgl. dazu David Rosenthal, Datenschutz und KI: Worauf in der Praxis zu achten ist, in: Sandra Husi-Stämpfli (Hrsg.), Jusletter IT vom 26.04.2022, N 52 ohne weitere Hinweise.

[112] Siehe I.B.2.

4. Bearbeitung von Personendaten als Outputdaten

Die Transformationsregel einer KI gilt gemeinhin als triviale Maschine, da die Inputdaten stets ein Paar mit den korrespondierenden Outputdaten bilden, d.h. die Regel deterministisch und unveränderbar funktioniert. Für Lernmaschinen ist dies insofern nicht uneingeschränkt der Fall, da diese darauf ausgelegt sind, einzelne Variablen der angewendeten Regel zu verändern, um den zu einem Input korrespondierenden Output zu optimieren. Ihre triviale Natur gilt demnach nur insoweit, als die Transformationsregel nicht verändert wird. Im Rahmen des Lernprozesses gelten sie daher als *nicht-trivial*.[113]

Die Verbindung zwischen Input und Output kann indes derart komplex sein, dass sie von Experten kaum oder gar nicht mehr ermittelt bzw. erklärt werden kann.[114] Aus Sicht des Datenschutzrechts stellt die korrelative Natur von berechneten Personendaten in solchen Fällen die Richtigkeit der Daten[115] sowie die Transparenz der Datenbearbeitung in Frage.[116] Zudem können (probabilistische) Personendaten generiert werden, ohne dass dies den Betroffenen bewusst ist. In diesen Fällen ist auch die Erkennbarkeit der Erhebung von Personendaten nicht ohne Weiteres gegeben.

B. Einbettung in den Verwaltungsprozess: KI-Technologie als qualifizierendes Merkmal für Datenbearbeitungen

Neben den gewöhnlichen Personendaten qualifiziert das Datenschutzrecht gewisse Personendaten bzw. gewisse Bearbeitungszusammenhänge von Daten, als «besondere»[117] bzw. «besonders schützenswerte»[118] Personendaten. Als besondere Personendaten gelten gem. § 3 Abs. 4 Bst. a IDG ZH jegliche «Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht» sowie gem. § 3 Abs. 4 Bst. a

---

113 Kaminski/C.W. Glass (FN 38), 132.

114 OECD (FN 13), 82.

115 Zur Datenrichtigkeit IV.A.3.

116 Zur Transparenz bzw. Erkennbarkeit siehe IV.A.1.c u. d.

117 In manchen Kantonen, z.B. § 3 Abs. 4 IDG ZH.

118 Bund: Art. 3 Bst. c DSG (Art. 5 Bst. c nDSG).

Ziff. 1–4 IDG ZH Personendaten aus gewissen besonderen Lebensbereichen. Weiter fallen hierunter gemäss § 3 Abs. 4 Bst. b IDG ZH auch Persönlichkeitsprofile.

Der einfachste Fall einer qualifizierten Bearbeitung von Personendaten durch KI ist jener, dass Personendaten aus einem gesetzlich geschützten Lebensbereich von § 3 Abs. 4 IDG ZH im Rahmen eines KI-unterstützten Entscheidungsprozesses der Verwaltung bearbeitet werden. Hier stellt die KI-Funktion ein Werkzeug bereit, mit dessen Hilfe eine administrative Bearbeitung von Personendaten vorgenommen wird, die für sich bereits den Tatbestand der Bearbeitung von besonderen Personendaten erfüllt. Ein weiterer einfacher Fall ist jener, dass KI-Funktionen dazu genutzt werden, ein Profiling i.S.v. § 3 Abs. 4 Bst. c IDG ZH vorzunehmen. In anderen Fällen wird die Qualifikation der Daten nach den üblichen Gesichtspunkten beurteilt, namentlich anhand der Bestimmbarkeit von Personen aus den generierten Daten sowie des hierzu benötigten Aufwandes für die Datenbearbeiterin.[119]

IV. Rechtliche Regelungen im Kanton Zürich

A. Regelungsansätze im IDG ZH und die damit zusammenhängenden Fragen

Das IDG ZH enthält mit den Bestimmungen zu der automatisierten Auswertung von personenbezogenen Informationen bzw. Profiling[120] nur einen einzigen Normenkomplex, der ausdrücklich den Einsatz von KI-Technologie regelt. Indes sind die übrigen Bestimmungen selbstverständlich auf KI-Technologien anwendbar. Die folgende Aufstellung zeigt die wichtigsten Grundsätze und inwiefern deren Umsetzung im Rahmen der Anwendung von KI eine Herausforderung darstellen kann.

[119] Siehe dazu Braun Binder et al. (FN 8), 42.

[120] Siehe § 3 Abs. 4 lit. c IDG ZH.

1. Die klassischen Grundsätze der Datenbearbeitung

a. Gesetzmässigkeit

Bezüglich der Gesetzmässigkeit wird in der Lehre die Position vertreten, dass der Einsatz von KI-Technologien im Hinblick auf das Legalitätsprinzip «keine besondere Herausforderung» darstellt.[121] Dem ist insofern zuzustimmen, als die Gültigkeitsvoraussetzungen der genügenden Normstufe und Normdichte auch für den Einsatz von KI-Technologien gelten und grundsätzlich auf diese angewendet werden können.[122] Eine separate gesetzlich Befugnis für den Einsatz von KI-Systemen zur Bearbeitung von Personendaten ist erforderlich, soweit der Einsatz von KI als zusätzlicher Eingriff in die Rechte der Betroffenen, bzw. als eine Bearbeitung von besonderen Personendaten i.S.v. § 3 Abs. 4 IDG ZH zu werten ist.[123]

Sofern aber der Einsatz von KI zur Erfüllung einer gesetzlichen Aufgabe als denknotwendig erscheint, muss das Gesetz nicht die Erlaubnis regeln, sondern den Einsatz in berechtigten Ausnahmefällen gegebenenfalls einschränken. Der Grund liegt darin, dass bei einer genügend engen funktionalen Verknüpfung einer Bearbeitungsmethode mit einer ausdrücklich im Gesetz vorgesehenen Aufgabe erstere als mitgeregelt gilt, also eine implizite Grundlage für die betreffende Bearbeitung vorliegt. Dies gilt grundsätzlich auch für besondere Datenbearbeitungen, wenn auch die Anforderungen an die Rechtsicherheit sehr viel höher sind.[124]

b. Zweckbindung und Verhältnismässigkeit

Die Bearbeitung von Personendaten durch öffentliche Organe darf nur zweckgebunden erfolgen. Öffentliche Organe dürfen sich nicht ohne Weiteres für Private interessieren, sondern nur in Zusammenhang mit der Erfüllung einer ihnen zugewiesenen gesetzlichen Aufgabe. Der Bearbeitungszweck bindet somit die Datenbearbeitung über die staatlichen Aufgaben an das Recht und bildet somit einen Teilgehalt der Gesetzmässigkeit von Datenbearbeitungen.[125]

---

[121] Braun Binder et al. (FN 8), 35.

[122] Siehe dazu Braun Binder et al. (FN 8), 34.

[123] Baeriswyl, PraKom IDG ZH (FN 101), § 8 N 13 ff.

[124] Glass (FN 26), 225 f.

[125] Glass (FN 26), 191 f.

Mithin wird durch die Festlegung des Zwecks einer Datenbearbeitung deren gesetzliche Grundlage im Einzelfall vervollständigt und ist damit ein «unverzichtbarer Bestandteil der Gesetzmässigkeit».[126] Es handelt sich um einen genuin datenschutzrechtlichen Grundsatz, der zudem auch Parallelen zur Verhältnismässigkeit aufweist.[127] Das Zusammenspiel dieser drei Grundsätze (Gesetzmässigkeit, Zweckbindung und Verhältnismässigkeit) läuft darauf hinaus, dass die Erhebung und Speicherung von Daten ohne konkreten Bearbeitungszweck bzw. «auf Vorrat» unverhältnismässig und somit unzulässig ist.[128] Ausnahmen in Bundesgesetzen sind indes gemäss Art. 191 BV «massgeblich» und damit unabhängig von dieser Beurteilung anzuwenden.[129]

Für den Kanton Zürich definiert das Gesetz diese Zweckbindung in § 9 Abs. 1 IDG ZH dahingehend, dass die öffentlichen Organe Personendaten nur zu dem Zweck bearbeiten dürfen, zu dem sie erhoben wurden. Jede Erhebung von Daten wiederum setzt gemäss § 8 IDG ZH einen plausiblen Zusammenhang mit der Erfüllung einer öffentlichen Aufgabe voraus. Die Zweckbindung an den Erhebungsgrund der Daten gilt neben den im Gesetz genannten Arten – Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Vernichten – für sämtliche Bearbeitungsarten über den gesamten Lebenszyklus eines Personendatums.[130]

Nach dem Gesagten liegt der rechtmässige Zweck einer Datenbearbeitung stets in der Erfüllung einer gesetzlichen Aufgabe. Die beiden Voraussetzungen sind untrennbar miteinander verbunden. Somit muss stets klar sein, welche gesetzlich begründete Aufgabe durch die Datenbearbeitung befördert wird. Entsprechend muss der Bearbeitungszweck jeweils vor der Bearbeitung fest-

---

[126] Harb, PraKom IDG ZH (FN 101), § 9 N 1.

[127] Epiney (FN 26), Datenschutzrecht Grundlagen, 539.

[128] Florent Touvenin, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Volker Boehme-Nessler/Manfred Rehbinder (Hrsg.), Big Data: Ende des Datenschutzes? – Gedächtnisschrift für Martin Usteri, Bern 2017, 36 m.w.H.; Bruno Baeriswyl, in: Bruno Bäriswyl/Kurt Pärli (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 1. A. Bern 2015 (zit. SHK DSG-VerfasserIn), Art. 4 N 34; Rosenthal, in: Handkommentar DSG (FN 101), Art. 4 N 20; Gerrit Hornung, Erosion traditioneller Prinzipien des Datenschutzrechts durch Big Data, in: Wolfgang Hoffmann-Riem (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018, 85.

[129] So beispielsweise die Vorratsspeicherung auf Grundlage des BÜPF (SR 780.1).

[130] Rudin, PraKom IDG ZH (FN 101), § 3 N 32 ff.

gelegt[131] und auf eine rechtlich begründete Bearbeitungsbefugnis des Organs gestützt werden.[132] Bearbeitungen, die zu einem anderen Zweck erfolgen, sind demzufolge als separate Datenbearbeitungen zu betrachten und erfordern demnach grundsätzlich eine neue rechtliche Grundlage.

Für besondere Personendaten i.S.v. § 3 Abs. 4 IDG ZH müssen gemäss § 8 Abs. 2 IDG ZH nebst dem Zweck auch die Art und Weise der Bearbeitung selbst gesetzlich vorgesehen sein, wobei diese sich aus der Umschreibung der Aufgabe notwendigerweise ergeben kann.[133] Die Anforderungen sowohl an die Erlassstufe (Gesetz, Verordnung, interne Richtlinie etc.), als auch an die Bestimmtheit der rechtlichen Bearbeitungsgrundlage im Einzelfall, variieren dabei je nach Risiko für die Betroffenen.[134]

Eine Zweckänderung für bereits vorhandene Personendaten ist gemäss § 9 Abs. 1 IDG ZH nur möglich, wenn das Gesetz dies ausdrücklich ermöglicht oder die betroffene Person einwilligt. Zudem kann das öffentliche Organ die bei ihm vorhandenen Personendaten im Rahmen der rechtmässigen Bekanntgabe an Dritte einem weiteren Zweck zuführen. Ebenso ist eine Bearbeitung zu nicht personenbezogenen Zwecken möglich. Einer drohenden «Aushöhlung»[135] des Zweckbindungsprinzips kann über die Informationspflicht begegnet werden, indem von den Datenempfängern bzw. Umsetzungsbefugten des neuen Zwecks als Beschaffer der Daten eine erneute Information gemäss § 12 IDG ZH verlangt wird, in der die Betroffenen auf die Zweckänderung hingewiesen werden.

c. Transparenz, Erkennbarkeit sowie das Handeln nach Treu und Glauben

Die Transparenz des Handelns öffentlicher Organe bildet neben dem Schutz der Grundrechte den zweiten in § 1 Abs. 2 IDG ZH ausdrücklich genannten Zweck des Gesetzes. Sie birgt verschiedene Aspekte, namentlich eine «aktive» und eine «passive» Transparenz der Verwaltung gegenüber der Allgemeinheit,

---

131 Harb, PraKom IDG ZH (FN 101), § 9 N 1.

132 Glass (FN 26), 92.

133 Harb, PraKom IDG ZH (FN 101), § 9 N 3 f.

134 Baeriswyl, PraKom IDG ZH (FN 101), § 8 N 14.

135 Harb, PraKom IDG ZH (FN 101), § 9 N 12.

die in § 4 IDG ZH verankert ist,[136] sowie Transparenz gegenüber den von einer Datenbearbeitung betroffenen Personen.[137] Aus letzterer folgt der in § 12 IDG ZH konkretisierte Grundsatz der *Erkennbarkeit* der Datenbeschaffung, welche die Betroffenen in die Lage versetzen soll, die Rechtmässigkeit der Bearbeitung zu beurteilen und gegebenenfalls dagegen vorzugehen.[138] Es handelt sich mithin um eine Ausprägung des Grundsatzes von Treu und Glauben.[139]

Obwohl § 1 Abs. 2 Bst. a IDG ZH primär das in Art. 17 und 49 KV verankerte Öffentlichkeitsprinzip umschreibt,[140] gilt dieses als Ordnungsprinzip[141] der Verwaltung ebenso bei der Umsetzung des Datenschutzrechts. Dies zeigt sich am deutlichsten in den Zugangsrechten zu Informationen und «eigenen» Personendaten gemäss § 20 ff. IDG ZH[142] sowie in den Informationspflichten der öffentlichen Organe in Bezug auf die Bearbeitung von Personendaten gemäss § 12 IDG ZH und in der in § 12a IDG ZH statuierten Meldepflicht für gewisse Datenschutzverletzungen. Da diese Pflichten ebenfalls spezifisch datenrechtliche Ausprägungen des Grundsatzes von Treu und Glauben sind, gehen sie diesem vor, wobei letzterer ergänzend anzuwenden ist.[143]

Die Folgen von intransparenten Datenbearbeitungen sind im Gesetz angedeutet. Aus § 1 Abs. 1 IDG ZH kann die Vermutung oder auch Befürchtung des Gesetzgebers herausgelesen werden, dass dadurch die freie Meinungsbildung, die Wahrnehmung der demokratischen Rechte sowie die Kontrolle staatlichen Handelns beeinträchtigt werden können. Entsprechend ist das Transparenzprinzip auch kein Selbstzweck, sondern stets in Hinblick auf diese Vermutung

---

136 Baeriswyl, PraKom IDG ZH (FN 101), § 4 N 2.

137 Siehe den Hinweis bei Rudin, PraKom IDG BS (FN 77), § 2 N 17.

138 Harb, PraKom IDG ZH (FN 101), § 12 N 2.

139 Epiney (FN 26), Datenschutzrecht Grundlagen, 544 f.; BSK DSG-Maurer-Lambrou/Steiner (FN 101), Art. 4 DSG N. 16a f.; Rosenthal, in: Handkommentar DSG (FN 101), Art. 4 N 51.

140 Baeriswyl, PraKom IDG ZH (FN 101), § 1 N 4.

141 Baeriswyl, PraKom IDG ZH (FN 101), § 1 N 4.

142 Baeriswyl, PraKom IDG ZH (FN 101), § 1 N 7.

143 Epiney (FN 26), Datenschutzrecht Grundlagen, 545.

zu lesen.[144] Mit anderen Worten kann eine Datenbearbeitung in dem Masse intransparent erfolgen, als der Nachweis gelingt, die gesetzliche Vermutung in Bezug auf die genannten Gefahrenmomente sei unzutreffend.

d. Transparenz als Explainability von KI-Systemen

Die Transparenz von KI-Systemen kann sich sowohl auf den Output des Systems beziehen als auch auf dessen Wirkungsweise oder Hintergrund (Design, Entwicklung, Einbettung in Entscheidungsprozesse).[145] Die Transparenz einer KI-Instanz misst sich an der Möglichkeit, Entscheidungsprozesse sowie einzelne Entscheidungen zu interpretieren und erklären. Verlangt wird also eine Form von *actionable transparency*, welche die Opazität[146] von KI-Systemen sowie das jeweils damit einhergehende Informationsgefälle genügend auszugleichen vermag.[147]

Zusammengefasst wird dies alles unter dem Stichwort der *explainability*.[148] Dieses Konzept einer «nutzbaren Transparenz» umfasst die Interpretierbarkeit sowie die Erklärbarkeit, die sich als allgemein anerkannte Grundsätze der «ethischen» KI-Nutzung herausgebildet haben.[149] Sie kann grundsätzlich *by design* in jede KI als Funktion des Systems integriert werden.[150]

Aus rechtlicher Sicht entscheidend ist die Nachvollziehbarkeit des Outputs eines KI-Systems im Hinblick auf Nachvollziehbarkeit staatlichen Handelns

---

[144] Baeriswyl, PraKom IDG ZH (FN 101), § 1 N 5 ff.; Robert van den Hoven van Genderen, Transparancy Requirements for Algorithms and AI, Wishful Thinking?, in: Jusletter IT vom 27.05.2021, N 32.

[145] Siehe dazu Nicholas Diakopoulos, Transparency, in: Markus D. Dubber/Frank Pasquale/Sunit Das (Hrsg.), The Oxford Handbook of Ethics of AI, Oxford University Press 2020, 199 f.

[146] Zur Begriffsbildung Hoffmann-Riem (FN 5), 41.

[147] Emre Bayamlioglu, Contesting Automated Decisions, in: EDPL 4/2018, 438 f.; oder auch *usable transparency*, Diakopoulos (FN 145), 204.

[148] Ella Hafermalz/Marlen Huysman, Please Explain: Key Questions for Explainable AI Research from an Organizational Perspective, Morals + Machines 2/2021, 15.

[149] Bernahrd Waltl/Roland Vogl, Explainable Artificial Intelligence – the New Frontier in Legal Informatics, in: Erich Schweighofer/Franz Kummer/Ahti Saarenpää/Burkhard Schafer (Hrsg.), Datenschutz/Legal Tech, Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018, 117 f.

[150] Bryson (FN 61), 8.

sowie die Möglichkeit der Anfechtung der rechtlichen und sachlichen Begründung eines darauf gestützten Entscheids. Das Prinzip der Transparenz sowie die damit einhergehenden Erfordernisse der Interpretier- und Erklärbarkeit, sind somit eng mit der Begründungspflicht für rechtliche Entscheidungen verknüpft.[151]

Technisch betrachtet hängen Transparenz, Interpretier- und Erklärbarkeit von der Nachvollziehbarkeit der internen mathematischen Struktur des Algorithmus ab. Die technisch bedingte Veranlagung zu Intransparenz unterscheidet sich je nach Modell.[152] Lineare Modelle oder Entscheidungsbäume (*decision trees*) funktionieren beispielsweise nach zusammenhängenden Regeln und sind daher sowohl im Hinblick auf ihre Wirkungsweise als auch auf die Nachvollziehbarkeit einer Entscheidung im Einzelfall nachvollziehbar.[153]

Als zweites Problem entpuppt sich die Bandbreite an unterschiedlichen denkbaren Adressaten der Transparenz und deren Verständnishorizont, so etwa Laien, zur Entscheidung befugte Fachpersonen oder KI-Ingenieure.[154] Denn je komplexer die zugrundeliegenden mathematischen Formeln einer KI-Instanz sind, desto weniger ist diese für Laien nachvollziehbar und wird entsprechend für sie intransparent.[155] Soweit indes eine Überprüfung sowie eine darauf aufbauende nützliche Erklärung durch Fachpersonen möglich bleibt, kann die Transparenz grundsätzlich als gewahrt gelten. Bei steigender Komplexität wird indes möglicherweise ein Punkt erreicht, an dem Entscheidungen auch von Fachleuten nicht mehr in rechtsgenüglicher Weise nachvollzogen werden können. Hier ist die Rechtmässigkeit einer auf KI-Output basierten

---

[151] Zum Ganzen Paul Vogel, Künstliche Intelligenz und Datenschutz, – Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze, zugl. Diss. Univ. Würzburg 2021, Baden-Baden 2022, 199 f.

[152] Für eine Übersicht verschiedener Methoden siehe Waltl/Vogl (FN 149), 119, Tabelle 1.

[153] Waltl/Vogl (FN 149), 119; für automatisch generierte *trees* siehe Badr Hssina/Abdelkarim Merbouha/Hanane Ezzikouri/Mohammed Erritali, A comparative study of decision tree ID3 and C4.5, International Journal of Advanced Computer Science and Applications (IJACSA), Special Issue on Advances in Vehicular Ad Hoc Networking and Applications 2014, http://dx.doi.org/10.14569/SpecialIssue.2014.040203 (Abruf 01.06.2022), 13 ff.

[154] Rolf H. Weber, Künstliche Intelligenz: Regulatorische Überlegungen zum «Wie» und «Was», in: EuZ 1/2022, B12.

[155] van den Hoven van Genderen (FN 144), N 8 f.; Hafermalz/Huysman (FN 148), 17 ff.

Entscheidung wohl nur anzunehmen, wenn diese auf andere Weise plausibilisiert werden kann. Dies kann beispielsweise durch entsprechende statistische Studien erfolgen.[156] Je nach Qualität der behaupteten Rechtsverletzung ist es zudem denkbar, dass der Nachweis genügt, welches Gewicht im Rahmen der Entscheidung welchem Input zugemessen wurde bzw. welche Faktoren für das Ergebnis von Bedeutung waren.[157]

Soweit ein Modell eine konstruktionsbedingte Intransparenz aufweist, muss diese im Rahmen der Festlegung der Parameter eines geplanten KI-Modells berücksichtigt und im Hinblick auf die Vorgaben des Datenschutzes mit technischen Mitteln dahingehend umgeformt werden, dass die daraus generierten Erklärungen für die jeweiligen Adressaten nützlich sind, um ihre Rechte wahrzunehmen.

2. Von der Qualität zur Qualitätssicherung der Datenbearbeitung

Insgesamt ist den klassischen Grundsätzen der Datenbearbeitung anzumerken, dass sie aus einer Zeit stammen, in der künstliche Intelligenz eine Wissenschaftsdisziplin ohne merkliche Auswirkungen auf die Datenbearbeitungspraxis der Verwaltung war, und Datenbanken noch eher in der Form von Karteikästen als von Computerservern daherkamen. Erkennbar ist dies an dem Umstand, dass keiner der Grundsätze ausdrücklich auf die Minimierung der mit den spezifischen Eigenschaften von KI-Technologien verbundenen Risiken gerichtet ist. Dies erstaunt nicht, wenn man bedenkt, dass das weltweit erste Datenschutzgesetz aus dem Jahr 1970 stammt,[158] und in der Schweiz das Datenschutzgesetz des Bundes am 1. Juli 1993 in Kraft trat.[159] Seither entstanden neue Datenschutzgesetze in den Kantonen, von denen die meisten zwi-

---

156 Siehe I.C.

157 Siehe dazu Christen et al. (FN 10), 136.

158 Das Hessische Datenschutzgesetz von 1970; eine historische Kurzdarstellung findet man auf der Seite des Hessischen Beauftragten für Datenschutz und Informationsfreiheit unter https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes (Abruf 07.02.2022).

159 AS (1993) 1945, 1958.

schenzeitlich revidiert wurden.[160] Auch das DSG des Bundes wurde mehrfach revidiert, die neuste Version tritt voraussichtlich auf den 1. September 2023 in Kraft.[161] Die neuen Gesetzesbestimmungen tragen den KI-Technologien vermehrt Rechnung.

Gemeinsam ist den klassischen Bearbeitungsgrundsätzen, dass sie sich auf die Art und Weise bzw. auf die *Qualität der Datenbearbeitung* beziehen. Dies im Gegensatz zu den weiter unten thematisierten «neuen» Grundsätzen der Datenbearbeitung, die mit Einzug von Computern und nun auch der Möglichkeit des Einsatzes von KI-Systemen in die Datenschutzgesetze aufgenommen wurden. Diese betreffen nicht die Qualität der Datenbearbeitung als solche, sondern schreiben den öffentlichen Organen vielmehr gewisse Massnahmen des Risikomanagements vor,[162] mithin der *Qualitätssicherung der Datenbearbeitung*. Darunter fallen die Pflicht zur Durchführung von Datenschutzfolgeabschätzungen bzw. zur Einrichtung eines laufenden Risikomonitorings,[163] eine damit verbundene Pflicht der Vorlage zur Vorabkontrolle von riskanten Datenbearbeitungen an das Aufsichtsorgan sowie eine Meldepflicht in Bezug auf festgestellte Datenschutzverletzungen.

Ergänzt werden diese Massnahmen durch die Schutzziele der Informationssicherheit, die auch für Informationen aus Sachdaten gelten. Diesbezüglich enthält das Gesetz in § 7 Abs. 2 IDG ZH die Pflicht der öffentlichen Organe, Massnahmen zu ergreifen, welche gewisse Schutzziele im Hinblick auf die durch sie bearbeiteten Informationen sicherstellen. Als Schutzziele nennen § 7 Abs. 2 Bst. a-e IDG ZH die Verhinderung unrechtmässiger Kenntnisnahme, die Richtigkeit, Vollständigkeit und Verfügbarkeit der Information, die Zurechenbarkeit der Bearbeitung zu bestimmten Personen sowie die Erkennbarkeit und Nachvollziehbarkeit von Änderungen. Diese Pflichten gelten denknotwendig auch für die den Informationen zugrundeliegenden Daten, d.h. auch

---

[160] So auch das IDG des Kantons Zürich, dessen jüngste Teilrevision im Juni 2020 in Kraft trat.

[161] Hinweis auf https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzsta erkung.html (Abruf 06.09.2022).

[162] Vgl. Baeriswyl, PraKom IDG BS (FN 77), § 8 N 3 ff.

[163] Dazu Philip Glass, Gedanken zur Revision des DSG, datalaw.ch, 23.01.2018, https://www.datalaw.ch/gedanken-zur-revision-des-dsg/ (Abruf 01.06.2022) N 13.

für Personendaten. Entsprechend gelten die Schutzziele der Informationssicherheit als Bearbeitungsgrundsätze für Personendaten.[164]

3. Insbesondere Datenrichtigkeit

a. Richtigkeit als Voraussetzung der rechtmässigen Bearbeitung

Die Richtigkeit der von den öffentlichen Organen als Entscheidungsgrundlagen herangezogenen Daten ist in § 7 Abs. 2 Bst. b IDG ZH vorgeschrieben und bildet ein zentrales Schutzziel für den Umgang mit Informationen und Daten, insbesondere auch im Hinblick auf künftige KI-Anwendungen.[165] Die Bearbeitung von unrichtigen Daten im Sinne von § 7 Abs. 2 Bst. b IDG ZH bzw. die «unrichtige Datenbearbeitung» stellt eine Persönlichkeitsverletzung dar.[166]

Richtigkeit von Personendaten bedeutet zunächst, dass diese keine Falschaussagen über die Betroffenen enthalten, d.h. keine Informationen abbilden dürfen, die nicht den objektiv feststellbaren Tatsachen entsprechen. In dieser Hinsicht ist der gesetzliche Anspruch an die Richtigkeit der bearbeiteten Daten absolut. Dabei ist stets im konkreten Zusammenhang zu ermitteln, worauf sich der Anspruch der Richtigkeit bezieht, was in der Lehre als relative Richtigkeit bezeichnet wird.[167] So muss die Voraussetzung beispielsweise im Zeitpunkt der Bearbeitung erfüllt sein,[168] wovon sich das öffentliche Organ zu vergewissern hat[169] und die Daten gegebenenfalls nachführen muss.

Soweit Daten subjektiv festgestellte Tatsachen oder Werturteile enthalten, etwa in polizeilichen Protokollen, ist die Richtigkeit der subjektiven Bewertung der in den Daten abgebildeten Umstände nicht objektiv feststellbar. Auch ist dies nicht erwünscht, da sich der Richtigkeitsanspruch auf die Dokumentation der amtlichen Beobachtungen bezieht. Mit anderen Worten geht es nicht

---

[164] So auch Baeriswyl, PraKom IDG ZH (FN 101), § 7 N 2.

[165] Braun Binder et al. (FN 8), 46.

[166] SHK DSG-Baeriswyl/Blonski (FN 128), Art. 5 N 5.

[167] Rudin, PraKom IDG BS (FN 77), § 11 N 3; SHK DSG-Baeriswyl/Blonski (FN 128), Art. 5 N 5, welche die Richtigkeit der Daten insgesamt als relativen Begriff bezeichnen; ebenso Rosenthal/Jöhri, in: Handkommentar DSG (FN 101), Art. 5 N 2.

[168] Botschaft vom 23. März 1988 zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 413, 450.

[169] Sog. «Vergewisserungspflicht»; Waldmann/Oeschger (FN 26), Datenschutzrecht Grundlagen, 815 f. m.w.H.

um die Richtigkeit von objektiv feststellbaren Angaben zu den betroffenen Personen, sondern um die Authentizität des Protokolls. Ausschlaggebend ist, ob die vorhandenen Daten die subjektive Beobachtung der ermächtigten Person zum Zeitpunkt der Vornahme der Bewertung wiedergeben.[170]

Um zu vermeiden, dass rechtmässig bearbeitete «subjektive Personendaten» nachträglich geändert und so verfälscht werden, sieht das Gesetz im Rahmen der Rechtsbehelfe in § 21 IDG ZH vor, dass in diesen Fällen ein Bestreitungsvermerk angebracht und die Bearbeitung der Daten gegebenenfalls eingeschränkt wird.

b. Richtigkeit der Outputdaten

Aufgrund der Funktionsweise von KI-Technologien kann es Schwierigkeiten bereiten oder gar unmöglich sein, eine mangelhafte Qualität der Outputdaten im Einzelfall nachzuweisen. Dies betrifft insbesondere auch Personendaten, die durch elektronisches Profiling generiert werden. Ergebnisse von wahrscheinlichkeitsbasierten Algorithmen können unter Umständen ebenso wenig objektiv überprüft werden, wie subjektive Tatsachen und Werturteile. Das Problem besteht darin, dass nicht ohne Weiteres auf eine intrinsische kausale Begründung zugegriffen werden kann, durch welche das Ergebnis objektiv nachprüfbar würde. Insofern besteht auch hier eine gewisse «Subjektivität der Bearbeitungsperspektive».

Im Gegensatz zu subjektiven Tatsachen und Werturteilen von Menschen, basieren die Ergebnisse eines KI-Systems indes auf mathematischen Formeln; aufgrund der Ergebnisse der Validierung besteht zumindest die Möglichkeit, eine statistische Wahrscheinlichkeit dafür anzugeben, dass die im Ergebnis abgebildeten Zusammenhänge gültig auf gewisse Tatsachen schliessen lassen. Ab welchem Grad an Wahrscheinlichkeit ein Datum als «richtig» im Sinne des Gesetzes gilt, ist indes unklar.[171]

---

[170] Waldmann/Oeschger (FN 26), Datenschutzrecht Grundlagen, 814 f.; Rosenthal/Jöhri, in: Handkommentar DSG (FN 101), Art. 5 N 2.

[171] Vgl. dazu David Vasella, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter vom 16.11.2015, N 10, der im Hinblick auf das Ergebnis im Schlussbericht des EDÖB i.S. PostFinance darauf hinweist, dass «Wahrscheinlichkeitsaussagen wie beispielsweise ein Rating i.d.R. als Werturteil beurteilt [werden], das nicht falsch, sondern höchstens unvertretbar sein kann»; zur Validierung siehe I.B.2.

Da die Richtigkeit eine gesetzliche Voraussetzung für die Bearbeitung von Personendaten durch öffentliche Organe ist, muss die Frage der Rechtmässigkeit des durch die negative und positive Fehlerquote des KI-Systems begründeten Risikos jeweils für die betreffende Bearbeitung im Rahmen einer Folgenabschätzung geklärt werden.

c. Spezialfall: Richtigkeit der Trainingsdaten

Die Verwendung von künstlicher Intelligenz in der Form von trainierten Modellen setzt die Nutzung Trainingsdaten voraus, die ihrerseits Personendaten sein können. Obwohl diese Daten dem Zweck dienen, statistische Modelle zu berechnen – und daher nicht der Output von Personendaten bezweckt wird – spielt die Datenrichtigkeit dennoch eine wichtige Rolle im Hinblick auf die Schutzziele des Datenschutzrechts. Dies ist insbesondere der Fall, wenn falsche Erhebung oder falsche Auswahl der Trainingsdaten zu einem rechtlich relevanten Bias im trainierten Modell führen.[172]

4. Die neuen Grundsätze der Datenbearbeitung

a. Vorabkontrolle und Datenschutz-Folgenabschätzung

Das Datenschutzgesetz des Kantons Zürich enthält seit geraumer Zeit eine Pflicht der staatlichen Organe, gewisse Datenbearbeitungen der Datenschutzbeauftragten zur Vorabkontrolle vorzulegen. Mit Inkrafttreten einer Änderung des IDG ZH am 1. Juni 2020 kommt die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung hinzu.[173]

Die Datenschutz-Folgenabschätzung verpflichtet die öffentlichen Organe von Kanton und Gemeinden gemäss § 10 Abs. 1 IDG ZH dazu «bei einer beabsichtigten Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen [zu bewerten]». Dies bedeutet zunächst, dass öffentlichen Organe grundsätzlich bei der Bearbeitung von Personendaten die damit verbundenen Persönlichkeitsrisiken im Auge behalten müssen.

---

[172] Zur Bearbeitung von Personendaten als Trainingsdaten siehe III.A.1.; Zur Problematik von Bias siehe I.B.3.c.

[173] Gesetz über die Information und den Datenschutz (IDG) (Änderung) vom 25. November 2019 (OS 75, 263; ABl 2018-07-13).

Je nach Ergebnis, bzw. ermitteltem Risikoprofil einer Datenbearbeitung besteht sodann die Pflicht, die betreffende Datenbearbeitung der kantonalen Datenschutzbehörde zur Vorabkontrolle vorzulegen. Dies ist gemäss § 10 Abs. 2 IDG ZH zwingend vorgeschrieben, wenn eine beabsichtigte Datenbearbeitung «mit besonderen Risiken für die Grundrechte der betroffenen Personen» verbunden ist. Gemäss § 24 Abs. 1 Bst. a-e IDV ZH[174] erfüllt eine Datenbearbeitung diese Voraussetzung «insbesondere» dann, wenn sie ein Abrufverfahren vorsieht, die Sammlung einer Vielzahl besonderer Personendaten betrifft, mit dem Einsatz neuer Technologien verbunden ist, wenn sie vorsieht, dass mindestens drei verschiedene öffentliche Organe gemeinsam Personendaten bearbeiten, oder wenn sie eine grosse Anzahl von Personen betrifft. Als typische Fälle eines besonderen Risikos gelten zudem auch die automatisierte Einzelentscheidung, die systematische Überwachung von Personen, die Bearbeitung von besonderen Personendaten im Allgemeinen, die Bearbeitung von Personendaten in grossem Umfang (insb. hohe Anzahl an Betroffenen bzw. grosse Datenmengen), das Zusammenführen/Kombinieren von Personendaten aus unterschiedlichen Prozessen, der Einsatz neuer Technologien oder biometrischer Verfahren, sowie Scoring bzw. Profiling.[175]

Von diesen gesetzlich typisierten Fällen der besonderen Risiken basieren die automatisierte Einzelentscheidung sowie das automatisierte Profiling i.S.v. § 3 Abs. 4 Bst. c IDG ZH notwendigerweise auf Technologien der künstlichen Intelligenz, während in anderen Fällen die Nutzung solcher Technologien naheliegend oder zumindest denkbar erscheint. Sowohl die systematische Überwachung, die Bearbeitung von besonderen Personendaten, die Bearbeitung in grossem Umfang (durch Excel-Tabellen und klassische Datenbanken aber auch Big Data-Anwendungen), die Zusammenführung aus verschiedenen Bereichen (z.B. durch elektronische Zugriffsberechtigungen auf verschiedene Datenbanken) und die biometrischen Verfahren[176] (z.B. Auswertung von DNA-Spuren) müssen nicht notwendigerweise, können aber durch KI-Technologien unterstützt werden. Zudem wird die Verwendung von KI-Technologien auf

[174] Verordnung vom 28. Mai 2008) über die Information und den Datenschutz des Kanton Zürich (IDV ZH; ON 170.41)

[175] Datenschutzbeauftragte des Kantons Zürich, Merkblatt Datenschutz-Folgenabschätzung DSFA, V.1.1. November 2020, Abschnitt 2

[176] Siehe VII.A.2.

absehbare Zeit als «Einsatz neuer Technologien» i.S.v. § 24 Abs. 1 Bst. c IDV ZH zu qualifizieren sein.[177]

Hier stellt sich die Frage, ob und gegebenenfalls wann solche Technologien zu einem späteren Zeitpunkt nicht mehr als «neu» gelten, und ihre Verwendung somit nicht mehr einer automatischen Vorlagepflicht unterliegt. In diesem Zusammenhang gilt es zum einen, zu bestimmen, was «neu» bedeutetet. Zum anderen, worauf sich die Qualität des «neu-seins» bezieht.

b. Der Einsatz von «neuen Technologien» i.S.v. § 24 Abs. 1 Bst. c IDV ZH

Dem Wortlaut des Gesetzes nach bezieht sich die Qualität des neu-seins auf eine Technologie, also eine Art und Weise oder auch Methode, wie Personendaten bearbeitet werden. Die Neuheit tritt in gewissen Situationen als zusätzlicher, nicht durch die Technologie selbst erzeugter Risikofaktor hinzu. Aus diesem Blickwinkel bezieht sich die Qualifizierung als «neu» nicht darauf, ob die Technologie erst kürzlich entwickelt wurde, sondern ob der Kontext ihres Einsatzes zur Datenbearbeitung – und damit auch deren Risikoprofil – neu sind. Ein neuer Kontext der Bearbeitung ist in diesem Zusammenhang anzunehmen, wenn weder das einsetzende öffentliche Organ noch die zuständige Datenschutzbehörde Erfahrungen mit dieser Technologie haben, und daher auch nicht *prima vista* über das damit zusammenhängende Risiko befinden können. Mithin muss nicht die Technologie, sondern deren Risikoprofil im konkreten Datenbearbeitungskontext für die betreffenden Stellen «neu» sein, um eine Vorlagepflicht auszulösen.

Im Ergebnis ist somit – ähnlich wie im Falle von besonderen Personendaten – die Tatsache, dass eine Technologie neu ist, lediglich ein beispielhaftes Indiz für ein ebenso neues Risikoprofil. Dies bedeutet, dass bereits bekannte Technologien, die in einem neuen Kontext eingesetzt werden, und dort ein qualitativ neues Risiko für die Grundrechte der Betroffenen begründen, grundsätzlich als «neu» gelten und daher vorlagepflichtig werden können. Ausschlaggebend kann nur sein, dass weder die betreffende Behörde noch die zuständige Datenschutzstelle sich zuvor mit der neuen Risikokonstellation auseinandergesetzt

[177] Datenschutzbeauftragte des Kantons Zürich, In der Krise ist nicht alles anders – Tätigkeitsbericht 2020, 33.

haben. Handkehrum gilt eine Technologie nicht mehr als neu im Sinne der Vorlagepflicht, wenn für ihre Verwendung in einem spezifischen Kontext genügend Erfahrungswerte in Bezug auf das eigentliche Risikoprofil vorliegen, um einschätzen zu können, ob eine Vorlagepflicht besteht oder nicht.

Auf der anderen Seite kann dies in seltenen Fällen dazu führen, dass Datenbearbeitungen, die unter Verwendung einer allgemein als «neu» empfundenen Technologie vorgenommen werden, nicht notwendigerweise als «neu» i.S. von § 24 Abs. 1 Bst. c IDV ZH gelten. In Bezug auf KI-Technologien dürfte die Vorlagepflicht regelmässig trotzdem gegeben sein, da solche Technologien oftmals auch ohne «neu» zu sein eine der Voraussetzungen erfüllen dürften.[178]

c. Ähnliche Risikostruktur bei voll- und teilautomatisierten Einzelentscheidung

Die Frage, ob ein KI-unterstützter Prozess voll- oder teilautomatisiert erfolgen soll, ist zunächst eine Frage des *designs*[179] eines Mensch-Maschine-Entscheidungsprozesses. Die möglichen Herausforderungen und Risiken für öffentliche Organe ergeben sich somit aus der Natur von KI-Systemen einerseits, sowie andererseits aus den Eigenheiten der Menschen im Allgemeinen sowie der Verwaltung im Speziellen.[180] Zunächst erscheint die Unterscheidung einfach, da im ersten Fall der Output der KI die Entscheidung und im zweiten Fall einen Vorschlag für eine Entscheidung durch den zuständigen Menschen darstellt. Allerdings ist zu bedenken, dass auch vollautomatisierte Einzelfallentscheidungen in einen Verwaltungsprozess eingebunden sein müssen, nicht zuletzt, um die Wahrung der Rechte der Betroffenen sicherzustellen bzw. den Rechtsweg zu öffnen. Für den Verwaltungsprozess läuft die Entscheidung für Voll- oder Teilautomatisierung – neben der technischen Machbarkeit – auf die Frage hinaus, wer eine solche Entscheidung als erstes beurteilen wird: eine Fachperson, welche direkt für die fragliche Materie zuständig ist, oder eine Instanz des Rechtsmittelwegs.

Ungeachtet dessen, wer entscheidet, wird sich das Problem des *automation bias* stellen. Es handelt sich hierbei um eine mentale Verzerrung in der Kritik-

---

[178] Siehe IV.A.4.a.

[179] Zu den *by design*-Prinzipien siehe V.D.

[180] Braun Binder et al. (FN 8), 6.

fähigkeit von Menschen zugunsten von automatisierten Vorgängen, insbesondere von Computern und deren Output. Als Hauptursachen gelten die durch vermeintliche Neutralität und vermittelte Autorität von Computern sowie die Tatsache, dass es kognitiv einfacher ist, eine Aufgabe an die Automation zu delegieren.[181] Aufgrund der Beobachtung, dass auch Fachpersonen wie beispielsweise Piloten, Nuklearingenieure oder Fachpersonen in der Intensivpflege durchaus für solche Fehlurteile anfällig sind,[182] wird eine pauschale Aussage darüber, wer bei einer ersten Plausibilitätsprüfung durch den Menschen (Fachstelle oder Rechtsmittelinstanz) bessere Chancen hat, nicht einer solchen Voreingenommenheit zu erliegen, schwierig zu treffen sein. Aus allgemeinen verwaltungsrechtlichen Überlegungen erscheint es indes sinnvoll, für automatisierte Entscheidungen nicht devolutive Rechtsmittel vorzusehen, etwa durch Einsprachemöglichkeit an die verfügende Instanz oder durch Einwendungsverfahren.[183]

5. Die Meldepflicht gemäss § 12a IDG ZH

Das IDG ZH enthält seit Sommer 2020 eine Meldepflicht der öffentlichen Organe für qualifizierte Datenschutzverletzungen. Das Gesetz schreibt neu in § 12a IDG ZH vor, dass öffentliche Organe «unverzüglich die unbefugte Bearbeitung oder den Verlust von Personendaten» dem oder der Datenschutzbeauftragten melden, «wenn die Grundrechte der betroffenen Person gefährdet sind».[184] Dies dürfte der Fall sein, wenn Bearbeitungszusammenhänge betroffen sind, die besondere Personendaten i.S.v. § 3 Abs. 4 IDG ZH darstellen, da diese definitionsgemäss eine «besondere Gefahr einer Persönlichkeitsverletzung» bergen. Im Übrigen ist unklar, wie diese beiden gesetzlichen Massstäbe

---

[181] Kathleen L. Mosier/Linda J. Skitka, Human Decision Makers and Automated Decision Aids: Made for Each Other?, in: Raja Parasuraman/Mustapha Mouloua (Hrsg.), Automation and Human Performance: Theory and Applications. NJ: Erlbaum 1996/ CRC Press 2009, 201–220, 206; Siehe auch Matthias Van Der Haegen, Quantative Legal Prediction: the Future of Dispute Resolution, in: Jan De Bruyne/Cedric Vanleenhove (Hrsg.), Artificial Intelligence and the Law, Cambridge Antwerp Chicago 2021, 85 ff.

[182] Mosier/Skitka (FN 181), 201.

[183] Dazu allgemein Ulrich Häfelin/Georg Müller/Felix Uhlmann, Allgemeines Verwaltungsrecht, 8. Auflage, Zürich 2020, N 1194 ff.

[184] Eingefügt durch das Gesetz vom 25. November 2019 (OS 75, 263; ABl 2018-07-13). In Kraft seit 1. Juni 2020.

systematisch zueinanderstehen, da die Unterscheidung zwischen einer Gefährdung von Grundrechten und einer besonderen Gefahr für die Persönlichkeit in der Praxis kaum sinnvoll vorzunehmen sein wird.

Schliesslich ist daran zu erinnern, dass die Bearbeitung von Personendaten durch KI-Technologien auf absehbare Zeit *prima vista* als «neue Technologien» im Sinne des IDG ZH gelten und daher aufgrund eines immanenten besonderen Risikos für die Grundrechte zur Vorabkontrolle vorgelegt werden müssen.[185] Parallel dazu dürften der Verlust oder die unrechtmässige Bearbeitung von Personendaten im Rahmen der Nutzung von KI-Systemen regelmässig auch meldepflichtig i.S.v. § 12a IDG ZH sein.

B. Schweiz

Im schweizerischen Recht sind erst wenige Normen auszumachen, die ausdrücklich auf die Regulierung von KI-Technologien ausgerichtet sind.[186] Auch wenn noch eine gewisse Unklarheit darüber auszumachen ist, wie eine allfällige Regulierung angegangen werden soll, so wurden von verschiedenen Seiten bereits einige Prinzipien ausgearbeitet, welche die Erschaffung eines rechtlichen Rahmens anleiten sollen.[187]

Eine Ausnahme bildet das Datenschutzrecht. Mit der Revision des neuen DSG werden Bestimmungen in Kraft treten, welche den Einsatz von KI-Technologien betreffen, insbesondere den Einsatz von automatisierten Einzelentscheiden (Art. 21 nDSG) und von automatisiertem Profiling (Art. 5 Bst. f u. g nDSG). Letzterer Begriff wurde ausdrücklich aus dem europäischen Recht übernommen.[188] Eine weitere Angleichung besteht darin, dass neu der Begriff

---

[185] Siehe IV.A.4.b.

[186] Vgl. die Bestandsaufnahme in Braun Binder et al. (FN 68).

[187] Vgl. Herausforderungen der künstlichen Intelligenz – Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» an den Bundesrat, SBFI Forschung und Innovation, Dezember 2019, Kapitel 4, https://www.sbfi.admin.ch/dam/sbfi/de/dokumente/2019/12/bericht_idag_ki.pdf.download.pdf/bericht_idag_ki_d.pdf (Abruf wann Januar 2022); Thouvenin et al. (FN 20), 2 f.

[188] Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff. (zit. Botschaft E-DSG), 6971 u. 7021 f.

des automatisierten Profilings mit hohem Risiko geschaffen wurde. Der Tatbestand ist gemäss Art. 5 Bst. g nDSG erfüllt, wenn ein automatisiertes Profiling ein besonderes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt. In diesem Bereich geht das Gesetz somit ausdrücklich von einem risikobasierten Regelungsmodell aus.

C. Europa

Der Entwurf für eine Regulierung der künstlichen Intelligenz in der EU sieht primär einen risikobasierten Ansatz vor: Neben der Aufzählung der regulierten Klassen von Technologien schlägt die EU-Kommission vor, die Risiken von KI-Systemen nach Graden einzuteilen und Risikoklassenanalysen vorzuschreiben. Angedacht ist eine Klassifizierung nach minimalem, geringem oder auch begrenztem sowie hohem Risiko, wobei gewisse Praktiken aufgrund eines unzulässigen Risikos verboten wären.[189]

Interessant ist, dass die Kategorien, die als typische Bereiche mit hohem Risiko aufgeführt sind, zum Teil konkreter beschrieben sind als die gesetzlich geschützten Lebensbereiche des Datenschutzrechts. Als Beispiele werden aufgeführt: kritische Infrastrukturen, Schul- und Berufsbildung, Sicherheitskomponenten von Produkten, Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit, wichtige private und öffentliche Dienstleistungen, Strafverfolgung, Migration, Asyl und Grenzkontrolle, Rechtspflege und demokratische Prozesse.[190] Die Liste in Anhang III des Entwurfs ist nicht abschliessend und soll von der Kommission bei Bedarf ergänzt werden können.[191]

---

[189] Siehe die Zusammenfassung bei Angela Müller, Der Artificial Intelligence Act der EU: Ein risikobasierter Ansatz zur Regulierung von Künstlicher Intelligenz – mit Auswirkungen auf die Schweiz, EuZ 1/2022, A7 f.; spannend wird nun die parlamentarische Debatte, siehe dazu Luca Bertuzzi, AI regulation filled with thousands of amendments in the European Parliament, https://www.euractiv.com/section/digital/news/ai-regulation-filled-with-thousands-of-amendments-in-the-european-parliament/ (Abruf 15.06.2022).

[190] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über die künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 22. April 2021, COM(2021) 206 final, Anhang III.

[191] COM(2021) 206 final (FN 190), Art. 7.

Die vorgesehene Risikoklassifizierung für KI ist von besonderem Interesse für das Datenschutzrecht, weil sie dieselbe Funktion erfüllt, wie der Begriff der besonderen Personendaten im IDG ZH: den Schutz der Grundrechte der betroffenen Personen.[192] Aufgrund der mit der Risikoklasse verbundenen Annahme einer hohen Gefährdung von Grundrechten, sollte die Klassifizierung auch bei Risikoanalysen berücksichtigt werden, welche die öffentlichen Organe im Kanton Zürich gemäss § 10 Abs. 1 IDG ZH (Datenschutz-Folgeabschätzung) vornehmen müssen. Aufgrund der gemeinsamen europäischen Grundrechts- und Datenschutzkultur, wie sie insbesondere in der EMRK bzw. im Übereinkommen SEV NR. 108 des Europarates zum Ausdruck kommt, erscheint es naheliegend, dass aus datenschutzrechtlicher Sicht die künstlich-intelligente Bearbeitung von Personendaten mit hohem Risiko im Sinne des Verordnungsentwurfs der EU oftmals zugleich als Bearbeitung von besonderen Personendaten i.S.v. § 3 Abs. 4 IDG ZH zu qualifizieren sein wird.

Schliesslich sieht der Entwurf für KI-Systeme, deren Einsatz nur mit einem geringen oder minimalen Risiko verbunden ist, grundsätzlich keine besonderen Regeln vor. Hierunter werden nach Ansicht des Parlaments und des Rates die meisten KI-Anwendungen fallen, so beispielsweise Videospiele oder Spamfilter. Ausnahmsweise kann für solche Systeme eine Transparenzpflicht gelten, d.h. die Betroffenen müssen darüber informiert werden, dass ein KI-System im Einsatz ist. Gemäss Art. 52 des Entwurfs gilt dies grundsätzlich für alle Systeme, die auf Interaktion mit Nutzern ausgelegt sind, wie beispielsweise Chatbots.[193] Die Transparenzpflicht gilt überdies auch für Systeme, die «zur Erkennung von Emotionen oder zur Assoziierung (gesellschaftlicher) Kategorien anhand biometrischer Daten eingesetzt werden oder Inhalte erzeugen oder manipulieren («Deepfakes»)».[194]

---

[192] COM(2021) 206 final (FN 190), Begründung Ziff. 3.5.

[193] Vgl. die Pressemitteilung der Europäischen Kommission vom 21. April 2021, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/ip_21_1682.

[194] COM(2021) 206 final (FN 190), Begründung Ziff. 5.2.4 sowie Titel VI.

V. Herausbildung von «ethischen» Grundsätzen des Einsatzes von KI

A. Metaprinzipien für den Einsatz von KI-Technologien

In den letzten Jahren haben internationale Organisationen, Regierungen sowie private Organisationen verschiedentlich dazu Stellung genommen, wie mit dem Phänomen der künstlichen Intelligenz und insbesondere den hiervon ausgehenden Risiken umzugehen sei. Solche Erklärungen beziehen sich regelmässig auf «ethische Standards» für den Umgang mit KI.[195]

Die Vielzahl von Erklärungen zur KI-Ethik hat zu ersten Metastudien geführt, die Gemeinsamkeiten untersucht und gewisse Metaprinzipien ausgearbeitet haben – und sich in den Ergebnissen (nur) zum Teil überschneiden.[196] Beispielsweise identifizierte eine Studie der ETH Zürich gewisse Metaprinzipien, namentlich Autonomie, Freiheit, Nachhaltigkeit, Abwendung von Schaden, Privatheit, Transparenz, Verantwortung und Würde,[197] während eine spätere Studie der Universität Harvard die Metathemen von Privatheit, Sicherheit, Fairness und Nichtdiskriminierung, Erklärbarkeit und Transparenz, Verantwortung, menschliche Kontrolle, Professionalität und die Förderung von menschlichen Werten herausarbeitet.[198]

---

[195] Eine aktuelle Zusammenstellung findet sich im «AI Ethics Guidelines Global Inventory» von AlgorithmWatch, abrufbar unter https://inventory.algorithmwatch.org (Abruf 13.06.2022).

[196] Anna Jobin/Marcello Ienca/Effy Vayena, Artificial Intelligence: the global landscape of ethics guidelines, Nat. Mach. Intell. (2019); Vgl. auch die Hinweise bei Michal Cichocki, Guidelines für Künstliche Intelligenz (KI): Besteht aus rechtlicher Sicht Handlungsbedarf?, in: Jusletter IT vom 25.02.2021, N 3 f.

[197] Jobin et al. (FN 196), Tabelle 3.

[198] Jessica Fjeld/Nele Achten/Hannah Hilligoss/Adam Nagy/Madhulika Srikumar, Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, Berkman Klein Center for Internet & Society, 2020, open access, https://dash.harvard.edu/handle/1/42160420, 66 f. (Abruf 01.06.2022).

B. Einbindung in das Recht durch Verweise

Von Interesse ist an dieser Stelle, dass beide Metastudien die Themenkomplexe Privatheit, Transparenz und Verantwortung als überschneidende Prinzipien in den verschiedenen Erklärungen identifizieren. Hierbei handelt es sich um rechtlich gefestigte Prinzipien, die im Datenschutzrecht von Bedeutung sind. Der Umstand, dass sie Gegenstand eines grossen Teils der globalen Diskussion zu «KI-Ethik» zwischen privaten und staatlichen Akteuren sind, zeugt von einem hohen Stellenwert in der Gesellschaft. Den Ausgleich zwischen verschiedenen, gegenläufigen gesellschaftlichen Werten bzw. wertungsbedürftigen Interessen kann Ethik als Befragungsmethode der Moral indes kaum leisten, da die jeweiligen konkreten sozialen Moralvorstellungen der verschiedenen Kulturen subjektiv und oftmals bezüglich Inhalt sowie Verbindlichkeit bzw. Kompromissbereitschaft sehr unterschiedlich konzipiert sind.[199] Das Recht kann hier seine Funktion wahrnehmen, widerstrebende moralische Ansprüche voreinander zu schützen,[200] indem es entsprechende Wertungsgesichtspunkte in die Rechtsfindung einbindet.

Das Bundesgericht anerkennt beispielsweise die rechtliche Verbindlichkeit «ethischer Leitlinien» von Fachverbänden, wenn und soweit dies rechtlich vorgesehen ist, typischerweise in einer Verweisnorm durch Gesetz oder Verordnung.[201] Klassische Fälle sind überdies ausdrückliche Verweise auf Normenkomplexe sozial-moralischer Wertung, wie etwa in Art. 2 Abs. 1 ZGB (Treu und Glauben), in Art. 19 Abs. 2 OR, Art. 20 Abs. 1 OR und Art. 230 Abs. 1 OR (gute Sitten) oder die bereits erwähnten Schutzziele der Informationssicherheit (Stand der Technik),[202] aber auch implizite Verweise, etwa die

---

[199] Bernd Rüthers/Christian Fischer/Axel Birk, Rechtstheorie und Juristische Methodenlehre, 11. üb. Aufl. München 2020, N 401 ff.; Vgl. dazu auch Karen Hao, Should a self-driving car kill the baby or the grandma? Depends on where you're from, Technology Review 24.10.2018.

[200] Kurt Seelmann/Daniela Demko, Rechtsphilosophie, 7. Auflage München 2019, § 3 N 13; zu Staaten mit «Einheit von Recht und Moral» Bernd Rüthers/Christian Fischer/Axel Birk, Rechtstheorie und Juristische Methodenlehre, N 406.

[201] BGE 136 VI 97 E. 6.2.2, bezüglich ethisch-medizinischer Richtlinien der Schweizerischen Akademie der Medizinischen Wissenschaften SAMW.

[202] Siehe IV.A.2.

Kerngehaltsgarantie in Art. 36 Abs. 4 BV (Menschenwürde)[203]. Insgesamt gilt es zu beachten, dass für die öffentlichen Organe vorrangig die Wertungen des Rechts verbindlich sind; Das Recht gibt grundsätzlich den Rahmen und den Platz für die Anwendung von «ethischen» Wertungen vor. Vorbehalten bleiben nach allgemeinem Verständnis lediglich offensichtliche Fälle von untragbaren Verstössen gegen den «Kern der Gerechtigkeit».[204]

Für öffentliche Organe können demnach «ethische» Anleitungen eine rechtliche Verbindlichkeit erlangen, wenn sie beispielsweise die *best practice* in einer Fachdomäne im Umgang mit moralischen Dilemmata im Berufsalltag wiedergeben, und das Recht auf eine solche verweist. Allerdings erfüllen die eingangs erwähnten Erklärungen zur ethischen Nutzung von KI-Technologie diese Anforderungen regelmässig nicht, da sie zu abstrakt und generisch formuliert sind und kaum Anleitungen zur Auflösung praktischer Probleme enthalten.[205]

C. Indizien für öffentliche Interessen und Auslegungshilfen

Ein weiterer Aspekt der Thematik besteht darin, dass in den entsprechenden Erklärungen jeweils von «ethischen» Prinzipien für die Entwicklung und Nutzung von KI die Rede ist. Damit wird zunächst mitgeteilt, dass es sich um eine moralische Position handeln soll, beispielsweise zur Verwirklichung der Grund- und Menschenrechte in ihrer Funktion als moralische Werte im Recht. Zweitens wird signalisiert, dass es sich nicht um rechtliche Normen handelt, dass also keine rechtlich durchsetzbare Verbindlichkeit erwartet wird. Schliesslich ermöglicht die Berufung auf diese Erklärungen die Teilnahme an

---

[203] Markus Schefer, Die Kerngehalte von Grundrechten – Geltung, Dogmatik, inhaltliche Ausgestaltung, Bern 2001, 83 f. «Ziel grundrechtlicher Kerngehalte bleibt ein absoluter Schutz der Menschenwürde»; OFK BV-Biaggini (FN 49), Art. 36 N 24 ff.; SGK BV-Rainer Schweizer (FN 49), Art. 36 BV, N 44 m.w.H., Menschenwürde als «Auffangkerngehalt»; CR Cst.-Dubey (FN 49), Art. 36 N 126.

[204] Radbruch'sche Formel, vgl. Bernd Rüthers/Christian Fischer/Axel Birk, Rechtstheorie und Juristische Methodenlehre, N 970 f.; Kurt Seelmann/Daniela Demko, Rechtsphilosophie, § 2 N 27.

[205] Hoffmann-Riem (FN 5), 291; Bezüglich privater Compliance David Rosenthal, Datenethik – ein praktischer Zugang aus Sicht der Compliance, in: Recht relevant, Ausgabe 1/2022, 2–4, 3.

der entsprechenden (globalen) Debatte. Die tatsächliche Verbindlichkeit der «ethischen» KI-Prinzipien ist entsprechend unklar.[206] Es handelt sich mithin um eine laufende politische Diskussion,[207] die das Recht unter Umständen sinnvoll ergänzen kann.[208]

Im Anwendungsbereich des öffentlichen Rechts ist es zudem naheliegend, Erklärungen zur «ethischen KI» von Staaten und öffentlichen Organen i.S.v. § 3 IDG ZH als Absichtserklärungen in Bezug auf die Sicherung der Grundrechte und insofern als (mehr oder weniger deutliche) Indizien für den Bestand von entsprechenden öffentlichen Interessen bzw. Schutzpositionen für die Grundrechte Dritter i.S.v. Art. 36 Abs. 2 BV zu werten.

Gewisse «ethische» Grundsätze überschneiden sich denn auch mit den Grundsätzen der Datenbearbeitung, indem sie den Schutz derselben Güter oder Interessen bezwecken.[209] Diese Überschneidung der Schutzfunktion kann für die Beurteilung der betreffenden rechtlichen Grundsätze von Bedeutung sein, etwa in Bezug auf deren Auslegung.[210] Zudem kann die öffentliche Erklärung von «ethische Grundsätzen» als Indiz für das Vorhandensein eines entsprechenden öffentlichen Interesses gewertet werden, wodurch punktuell das öffentliche Interesse an der Durchsetzung der datenschutzrechtlichen Schutzpflichten öffentlicher Organe verstärkt und damit den jeweiligen grundrechtlichen Schutzpositionen ein höheres Gewicht verliehen würde. Aufgrund der bereits genannten subjektiven Qualität von Moral muss indes beachtet werden, dass auch jene Interessen zu berücksichtigen sind, die in den beigezogenen «ethischen» Prinzipien weniger zum Ausdruck kommen.

---

[206] Zum Ganzen Philip Glass, Eine Skizze zur rechtlichen Verbindlichkeit «ethischer» KI-Prinzipien, in: Jusletter IT vom 28.02.2020.; zur Verankerung im deutschen Recht durch das Bundesverfassungsgericht siehe Robert Alexy, Begriff und Geltung des Rechts, erw. Neuausgabe, Freiburg/München 2020, 52 f.

[207] Fjeld et al. (FN 198), 200 ff.

[208] Hoffmann-Riem (FN 5), 291; OECD (FN 13), 85.

[209] Glass (FN 206), N 18 ff.; vgl. auch die Gegenüberstellung (aus der Perspektive von privaten Akteuren) bei Cichocki (FN 196), N 5 ff.

[210] Hoffmann-Riem (FN 5), 291; Glass (FN 206), N 13 ff.; im Ergebnis auch Cichocki (FN 196), N 26.

D. Insbesondere die «Förderung menschlicher Werte»

Einen besonderen Platz nimmt das Prinzip der Förderung menschlicher Werte ein, da es einerseits auf das bereits angesprochene Problem des *value alignment* verweist,[211] und nicht auf klassische verfassungsrechtliche Schutzgüter wie im Falle des Verbots der Diskriminierung oder andere Verletzungen der Menschenwürde «beschränkt» ist. Andererseits entstammt es einer Denktradition und -methode aus den Ursprüngen der Computerwissenschaften, und bildet dort in der Form von *value sensitive design* eine zentrale Komponente guten Maschinendesigns. Wie jede Technologie ist auch KI immer ein Ergebnis von Design.[212] Computertechnologie bzw. computerbasierte Algorithmen als Ergebnis von Design transportieren immer Werte. Sie verleihen dadurch Macht und sind politisch.[213] Wertebezogene Designprinzipien, wie *value sensitive design* bzw. *design for values*[214] oder auch *X by design*[215], folgen der entsprechenden Erkenntnis, dass Computersysteme und andere technologische Artefakte auf die Beachtung von erwünschten moralischen Wertungsgesichtspunkten ausgerichtet werde müssen.[216] Hierzu ist es unabdingbar, im Vorfeld und während sämtlichen Phasen der Entwicklung diese Werte zu identifizieren und gegebenenfalls anzupassen.[217] Werteorientierte Designansätze fordern somit eine bewusste Technikgestaltung zur Beförderung von bestimmten Werten. Für lernende Algorithmen bedeutet dies die Identifikation von möglichen Fehlerquellen im Vorfeld und während der Entwicklung sowie

---

[211] Siehe II.A.

[212] Bryson (FN 61), 6.

[213] Woodrow Hartzog, Privacy's Blueprint – The Battle to Control the Design of New Technologies, Harvard University Press 2018, 51; Martini (FN 29), 48 f.

[214] Für einen Überblick siehe Janet Davis/Lisa P. Nathan, Value Sensitive Design: Applications, Adaptations, and Critiques, in: Jeroen van den Hoven/Pieter E. Vermaas/Ibo van de Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theories, Values and Application Domains, Dordrecht 2015, 11–35.

[215] AI High Level Expert Group, Draft Ethics Guidelines for Trustworthy AI, European Commission, April 2019, 21.

[216] Zur historischen Entwicklung Batya Friedman/David G. Hendry, Value Sensitive Design – Shaping Technology with Moral Imagination, The MIT Press, 2019, 11 f.

[217] Friedman/Hendry (FN 216), 29 f.; Lawrence Lessig, Code Version 2.0, New York 2006, 6.

des Einsatzes.[218] In dieser Hinsicht stellen *by design*-Methoden einen Aspekt des Qualitätsmanagements dar.

Das Datenschutzrecht kennt spezifische Formen von Vorgaben für *value sensitive design*, namentlich *privacy by design* sowie das spezifischere *privacy by default*, wobei letzteres als «Prinzip der datenschutzfreundlichen Voreinstellung»[219] für öffentliche Organe nur eine geringe Rolle spielt, da diese in der Regel aufgrund von gesetzlichen Ermächtigungen Daten bearbeiten und nicht aufgrund von Einwilligungen der Betroffenen.[220] Beide sind Ausprägungen des Prinzips der Rechtsdurchsetzung durch Technikgestaltung.[221]

Mit Inkrafttreten des neuen Datenschutzgesetzes des Bundes wird *privacy by design* unter dem Begriff «Datenschutz durch Technik» in Art. 6 Abs. 1 nDSG im schweizerischen Recht auf Bundesebene kodifiziert. Der Bundesrat verspricht sich hiervon eine Symbiose der gegenseitigen Ergänzung zwischen Recht und Technik sowie eine durch das Ethos der technischen Risikominimierung bedingte verringerte Notwendigkeit rechtlicher Technikregulierung; Die Bearbeitungsgrundsätze des Datenschutzes sollen so weit wie möglich auf technischem Weg verwirklicht werden.[222]

Das Informations- und Datenschutzgesetz des Kantons Zürich kennt bereits die eine oder andere ausdrückliche *by design*-Norm. So hält § 4 IDG ZH die

---

[218] Lucia M. Sommer, Personenbezogenes Predictive Policing – Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose, Diss. Univ. Göttingen, Baden-Baden 2020, 105 ff.; in der Praxis beispielsweise durch die Definition von *failure modes*; vgl. dazu eingehend Sophie Stalla-Bourdillon/Alfred Rossi/Gabriela Zanfir-Fortuna, Data Protection by Process – How to Operationalize Data Protection by Design for Machine Learning, Future of Privacy Forum, White Paper V. 1.0, Dezember 2019, abrufbar unter https://iapp.org/resources/article/fpf-how-to-operationalize-data-protection-by-design-for-machine-learning/ (Abruf 24.10.2022), 11 ff.

[219] Vgl. Art. 7 Abs. 3 nDSG, BBl 2020 7639, 7642 f.

[220] Botschaft E-DSG (FN 188), 7030; Glass (FN 26), 235 ff.; Thomas Gächter/Philipp Egli, Informationsaustausch im Umfeld der Sozialhilfe, in: Jusletter vom 06.09.2010, N 55.

[221] Walter Hötzendorfer, Zum Verhältnis von Recht und Technik: Rechtsdurchsetzung durch Technikgestaltung, in: Walter Hötzendorfer/Christof Tschohl/Franz Kummer, International Trends in Legal Informatics – Festschrift for Erich Schweighofer, Bern 2020, 424 f.

[222] Botschaft E-DSG (FN 188), 7029.

öffentlichen Organe an, ihre Informationsverwaltung auf die Ermöglichung von Transparenz und Erkennbarkeit auszurichten, während der mehr oder weniger analoge § 5 IDG ZH auf die Gewährleistung der Nachvollziehbarkeit ausgerichtet ist. Dadurch werden insbesondere das Akteneinsichtsrecht, die Informations- und Datenzugangsrechte sowie das Auskunftsrecht durch technische Zielvorgaben gesichert.[223] Auf ähnliche Weise wirken die Schutzziele der «Informationssicherheit» bzw. Datensicherheit in § 7 Abs. 2 IDG ZH als *design choices* für Informationssysteme förderlich für die Ziele des Datenschutzes.[224]

VI. Spezifische Datenschutzfragen

A. Geltungsbereich des Datenschutzrechts

Die Bestimmung des Geltungsbereichs des IDG ZH durch die Qualität des Personenbezugs der bearbeiteten Daten steht auch ohne den Einsatz von KI-Systemen in der Kritik.[225] Durch den Einsatz von KI-Systemen wird die Rechtslage noch etwas komplizierter.[226] Dies zeigte sich bereits in Zusammenhang mit Diskussionen um *big data*, eine Sammelbezeichnung für die Bearbeitung von sehr grossen Mengen von Daten mittels sehr leistungsfähiger Computersysteme, deren Funktionsweise auf KI-Technologie, genauer: *machine learning*, zurückzuführen ist. Insofern ist die datenschutzrechtliche Diskussion um KI schon seit einigen Jahren im Gange und kann auf die entsprechende Literatur verwiesen werden.[227] Nun aber beginnt sich die Diskussion vermehrt auf die Technologie hinter diesen Anwendungen zu verlagern.

---

[223] Baeriswyl, PraKom IDG ZH (FN 101), § 5 N 6.

[224] Zur Datensicherheit siehe IV.A.2

[225] Hoffmann-Riem (FN 5), 164; David Rosenthal, Personendaten ohne Identifizierbarkeit?, in: digma 2017, 199 f.

[226] Hoffmann-Riem (FN 5), 175.

[227] Eine aktualisierte Problemübersicht findet man bei Astrid Epiney, Big Data und Datenschutzrecht – Gibt es einen gesetzgeberischen Handlungsbedarf?, Jusletter vom 27.04.2020; siehe auch Michal Cichocki, Big Data und Datenschutz: Ausgewählte Aspekte, in: Jusletter IT vom 21.05.2015; René Huber, «Big Data», das kantonale Recht und der Datenschutz, in: Jusletter IT vom 21.05.2015; Rolf H. Weber, Big Data: Sprengkörper des Datenschutzrechts?, in: Jusletter IT vom 11.12.2013; Bruno Baeriswyl, «Big Data» ohne Datenschutz-Leitplanken, in: digma 2013, 14–17.

Im Vordergrund steht damit die Frage, ob Anonymisierung als Begrenzung des Geltungsbereichs des Datenschutzrechts nach wie vor sinnvoll ist.

In Zusammenhang mit Datenschutzfragen beruht die Wirkung von Anonymisierung primär auf der Tatsache, dass die verwendeten Daten personenbezogene Informationen einer grossen Zahl unbekannter Personen abbilden. Damit wird die Bestimmbarkeit erschwert oder gar verunmöglicht. Indes sind die Tatsachen über einzelne Personen nach wie vor als Muster in den Daten vorhanden. Es besteht somit grundsätzlich die Möglichkeit, durch künstlich intelligente Mustererkennung Gruppen von Personen zu bilden oder gar einzelne Personen zu *singularisieren*. Dadurch kann eine Re-identifikation möglich werden. [228] Aufgrund dessen ist eine erfolgreiche Anonymisierung nicht ohne Weiteres anzunehmen.[229]

Die aktuelle Lehre geht denn auch von einem relativen Anonymisierungsbegriff aus, der sich nach dem Grad der Bestimmbarkeit der betroffenen Person und dem hierzu benötigten Aufwand richtet – ähnlich wie im Falle der Qualifikation von Daten als Personendaten. Insofern können auch «anonyme» Personendaten als Personendaten im Sinne des Datenschutzrechts gelten.[230] Verfügt eine Behörde beispielsweise über einen Schlüssel zur Wiederherstellung des Personenbezugs oder kann sie mit vertretbarem Aufwand einen solchen beschaffen, gelten anonyme Datensätze lediglich als *pseudonymisiert* und damit als Personendaten.[231]

---

[228] Vgl. dazu David Vasella, DSB Österreich: Einsatz von Google Analytics untersagt; Standard bei der Drittstaatsprüfung; Singularisierung statt Identifizierung, https://www.datenrecht.ch 26.01.2022, https://datenrecht.ch/dsb-oesterreich-einsatz-von-google-analytics-untersagt-standard-bei-der-drittstaatspruefung-singularisierung-statt-identifizierung/ (Abruf 01.06.2022); Philip Glass, Singularisierung und Identifizierung, https://www.datalaw.ch, 24.02.2018, https://www.datalaw.ch/singularisierung-und-identifizierung/ (Abruf 01.06.2022), N 6 ff.; Rosenthal (FN 225), 198 ff.; Philippe Meier, Le défi de Big Data dans les relations entre privés, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Big Data und Datenschutzrecht, Zürich/Basel/Genf 2016, 56 ff.

[229] Früh (FN 105), AJP 2017, 144 m.w.H.; OECD (FN 13), 87.

[230] Epiney (FN 227), N 12.

[231] Früh (FN 105), AJP 2017, 144; Glass (FN 26), 114; vgl. Botschaft E-DSG (FN 188), 7076, wonach pseudonymisierte Personendaten bei fehlendem Schlüssel als «faktisch anonymisiert» bezeichnet werden.

In Zusammenhang mit KI-Technologien stellt sich neu die Frage, ob ein solcher Schlüssel vorbestehen muss oder ob es für die Annahme von Pseudonymisierung ausreichend ist, wenn ein Schlüssel durch maschinelles Lernen modelliert, also nachgebildet und auf diese Weise ermittelt werden kann. Aus der Perspektive des laufenden technologischen Fortschritts auf diesem Gebiet wird die Grenze zwischen anonym und pseudonym zunehmend unklar, und es stellt sich die weitergehende Frage, ob «anonyme» Personendaten nicht grundsätzlich im Geltungsbereich des Datenschutzrechts verbleiben sollten.[232]

Bedenkenswert ist hier der Einwand, dass in diesem Fall eine «Löschung durch Anonymisierung»[233] nicht mehr oder nur in einem sehr eingeschränkten Umfang möglich wäre. Dagegen lässt sich wiederum einwenden, dass die Aufnahme von anonymisierten Personendaten in den Geltungsbereich des Datenschutzrechts am Status von derart «gelöschten Personendaten» zunächst nichts ändern würde. Indes würde es bedeuten, dass die öffentlichen Organe für die weitere Bearbeitung der anonymen Daten weiterhin nach Datenschutzrecht verantwortlich wären.

Die Diskussion erscheint allerdings – zumindest in Bezug auf das IDG ZH – nicht dringlich, als bereits heute nach § 23 Abs. 1 IDG ZH von der Bekanntgabe von anonymen Personendaten – quasi als personenbezogenen Sachdaten – abgesehen werden müsste, wenn ein überwiegendes privates Interesse dagegen spricht. Abgesehen von den typischen Fällen der Gefährdung der Privatsphäre von Dritten gemäss § 23 Abs. 2 IDG ZH muss dies umso mehr dann gelten, wenn eine plausible Gefahr der De-Anonymisierung nachgewiesen werden kann.

B. Durchsetzung von Datenschutzrechten gegenüber KI-Bearbeitungen

Das Datenschutzrecht sieht gewisse Rechte vor, die den Betroffenen gegenüber Datenbearbeitern zustehen. Es handelt sich hierbei um Informationsrechte auf der einen und Rechte zur Beseitigung von Verletzungen auf der

---

[232] Meier (FN 228), 57; Roland Mathys, Big Data in der Rechtspraxis, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Big Data und Datenschutzrecht, Zürich/Basel/Genf 2016, 99; Hoffmann-Riem (FN 5), 164; Weber (FN 227), 457 f.

[233] Baeriswyl, PraKom IDG ZH (FN 101), § 11 N 12; dazu eingehend David Rosenthal, Löschen und doch nicht löschen, in: digma 2019/4, 190 ff.

anderen Seite. Die Informationsrechte beinhalten das Recht, über gewisse Datenbearbeitungen informiert zu werden sowie das Recht, beim öffentlichen Organ Einsicht in die «eigenen» Personendaten zu nehmen. Während die Informationspflicht im Hinblick auf die Bearbeitung von Personendaten mittels künstlicher Intelligenz nicht offensichtlich problematisch ist, kann die Einsichtnahme in KI-Personendaten gewisse Probleme bergen.

1. Recht auf Information über die Erhebung von Personendaten

Das Gesetz verlangt in § 12 Abs. 1 IDG ZH, dass öffentliche Organe jene Personen informieren, über die sie Personendaten erheben. Dieser Grundsatz wird in § 12 Abs. 3 IDG ZH relativiert, indem weitreichende Ausnahmen von dieser Informationspflicht vorgesehen sind, namentlich wenn die betroffene Person bereits genügend Kenntnis von der Datenerhebung hat, die Beschaffung der Personendaten gesetzlich vorgesehen ist, die Mitteilung nicht möglich ist oder einen unverhältnismässigen Aufwand erfordern würde sowie in den Ausnahmefällen von § 23 IDG ZH, in denen eine Datenbekanntgabe verweigert werden kann.

Grundsätzlich stellt die Erhebung von Personendaten zum Zweck der oder durch die Bearbeitung von KI keinen signifikanten Unterschied dar zur «empirischen» Erhebung von Personendaten. In beiden Fällen muss klar sein, welche Kategorien von Daten erhoben werden und wozu. Dass für Personendaten, die als Output einer KI generiert wurde, ein spezifisches Risiko besteht, dass die Daten falsch sind, stellt nicht ein Problem der Information über die Erhebung der Daten dar, sondern ein Problem der Richtigkeit der Daten bzw. der rechtmässigen Bearbeitung.

2. Recht auf Einsichtnahme in die vorhandenen Personendaten

Das Recht auf Zugang zu den «eigenen» Personendaten gemäss § 20 Abs. 2 IDG ZH gilt insoweit, als Daten bei einem öffentlichen Organ vorhanden und mit der betreffenden Person verknüpft sind oder zumindest ohne grossen Aufwand verknüpft werden können. Dies ist der Fall für Personendaten, die das öffentliche Organ im Rahmen seiner normalen Aufgabenerfüllung bearbeitet

bzw. auf die es zugreifen kann. Vorhanden sind die Daten demnach, wenn die Behörde diese ohne weiteres bearbeiten kann, insbesondere ohne Rückgriff auf eine amtshilfeweise Bekanntgabe oder die Erfüllung einer gesetzlichen Auskunftspflicht durch ein anderes öffentliches Organ.[234] Hinsichtlich des Bestands eines Einsichtsrechts ist nicht von Belang, auf welche Weise die Daten erhoben wurden, ob durch empirische Tatsachenfeststellung oder mathematische Berechnung mittels KI.

In Bezug auf KI-Systeme dürfte das Zugangsrecht insbesondere gegenüber Outputdaten wirksam werden, da diese in der Regel als Ergebnis einer Datenbearbeitung gespeichert und weiterbearbeitet werden. Inputdaten werden hingegen nicht notwendigerweise gespeichert, zumindest nicht durch das Organ, welches den Input veranlasst. Nutzt eine Mitarbeiterin eines öffentlichen Organs beispielsweise eine Such- oder Übersetzungsmaschine, werden die Suchbegriffe in der Regel nicht durch das öffentliche Organ gespeichert. Unter Umständen besteht aber dennoch eine aus der Begründungs- und Dokumentationspflicht fliessende Pflicht die Inputdaten zu speichern oder eine entsprechende Aktennotiz zu erstellen. Dies erscheint denkbar, wenn die KI-Funktion einen Output generieren soll, der als Begründung für eine rechtlich relevante Entscheidung dient, und dessen Erklärungszusammenhang sich allein aus der KI-Funktion ergibt. Soweit der für eine Begründung relevante Erklärungszusammenhang allein in der KI-Funktion abgebildet ist bzw. durch diese verborgen bleibt, ist davon auszugehen, dass die Inputdaten gespeichert werden müssen, damit im Rahmen einer rechtlichen Überprüfung des Entscheids gegebenenfalls die Funktionsweise der KI nachvollzogen werden kann.[235]

[234] Vgl. Rudin, PraKom IDG ZH (FN 101), § 20 N 13.

[235] Siehe zur Explainability IV.A.1.d

VII. Ausgewählte Use Cases

A. KI-Bearbeitungen in gesetzlich besonders geschützten Lebensbereichen

1. Klassisch sensitive Bereiche: Religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Gesundheit, Intimsphäre, ethnische Herkunft

Diese in § 3 Abs. 4 IDG ZH genannten Bereiche können aus zwei Gründen als «klassisch sensitiv» bezeichnet werden. Erstens stehen sie durch thematische Überschneidung in einem gewissen Zusammenhang mit den Diskriminierungsmerkmalen in Art. 8 Abs. 2 BV.[236] Zweitens unterscheiden sie sich von den nachfolgenden besonderen Bereichen durch die Art und Weise, in der das grundrechtliche Risiko der entsprechenden Datenbearbeitung wirkt. Sie bezeichnen Themen, die üblicherweise als «sensibel» bzw. «privat» angesehen werden und den klassischen «Schutzbereich» des Datenschutzrechts im Sinne einer erweiterten Privatsphäre mitumschreiben. Ihre Bearbeitung ist denn auch nicht notwendigerweise mit einer Bedrohung für die Grundrechte verbunden, diese ist vielmehr kontextabhängig.[237]

Die Bearbeitung von Daten aus diesen Bereichen ist rechtlich ambivalent. Zum einen können durch die daraus erkennbaren Informationen wesentliche Aspekte der Persönlichkeit rekonstruiert werden, was der Gesetzgeber grundsätzlich als eine Bedrohung für die Grundrechte der Betroffenen wertet. Zum anderen kann eine in der Gesellschaft vorhandene diskriminierende Benachteiligung durch den Verzicht auf die Bearbeitung von Diskriminierungsmerkmalen i.S.v. Art. 8 Abs. 2 BV aus diesen Bereichen nicht ausgeglichen werden. Es besteht vielmehr die Gefahr, dass bereits vorhandene Probleme verschlimmert bzw. die Identifikation von diskriminierenden Praktiken verhindert wird, indem korrelative Daten zu einem Diskriminierungsmerkmal dieses redundant in den Datensatz hinein codieren.[238]

---

[236] Dazu Glass (FN 26), 141.

[237] Rudin, PraKom IDG ZH (FN 101), § 3 N 25.

[238] Dazu ausführlich Christian (FN 19), 64 ff.

Den klassischen sensitiven Merkmalen ist schliesslich gemeinsam, dass sie persönliche Eigenschaften einer Person erfassen, und dass diese Eigenschaften für sich allein keine eineindeutige Identifikation der betroffenen Person ermöglichen, diese aber oftmals einer definierbaren Gruppe von Personen zuweisen. Demgegenüber handelt es sich bei den nachfolgend dargestellten gesetzlichen Kategorien von besonderen Personendaten einerseits um Fälle der eineindeutigen Identifikationsmöglichkeit (biometrische Daten), andererseits um Daten von Behörden, deren Verbindung zu einer Person eine Stigmatisierung bewirken können (Sozialhilfe, Verfolgung und Sanktionen). Auch hier sind unproblematische Bearbeitungskonstellationen grundsätzlich denkbar.[239]

2. Genetische und biometrische Daten

Das Datenschutzrecht betrachtet biometrische Daten aufgrund ihrer Universalität, Einzigartigkeit und Beständigkeit als besonders risikoreich für die Grundrechte der betreffenden Person. Unter den Begriff der biometrischen Daten fallen gemäss der Botschaft des Bundesrates zum neuen DSG Personendaten, «die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen», wobei ausdrücklich betont wird, dass ein technisches Verfahren beteiligt sein muss, welches «die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt».[240] Dies entspricht wohl zugleich der Qualifizierung von biometrischen Daten als Personendaten.

Die ausdrückliche Nennung der genetischen Daten im Gesetz – die sich unbestrittenermassen zur Verwendung als biometrische Daten eignen – weist darauf hin, dass diese grundsätzlich auch dann besonders geschützt sind, wenn

---

[239] Rudin, PraKom IDG ZH (FN 101), § 3 N 25.

[240] Botschaft E-DSG (FN 188), 7020; dazu eingehend Dominika Blonski, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, Diss. Univ. Bern 2015, 6 ff.; siehe auch EDÖB – Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Leitfaden zu biometrischen Erkennungssystemen, Version 1.0 2009, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/leitfaden-zu-biometrischen-erkennungssystemen.html (Abruf 01.06.2022); *privatim*, Leitfaden zur datenschutzrechtlichen Beurteilung von biometrischen Verfahren, Version 1.0 Oktober 2006, https://www.privatim.ch/wp-content/uploads/2017/06/privatim_Leitfaden_Biometrie_2006_d-1.pdf (Abruf 01.06.2022).

sie nicht zur eindeutigen Identifizierung oder Authentifizierung einer Person mittels eines technischen Verfahrens genutzt werden. Allerdings fallen nach wie vor nur genetische Personendaten in den Geltungsbereich des DSG,[241] d.h. genetische Daten, die geeignet sind, die betreffende Person mit einem zumutbaren Aufwand zu ermitteln.

Aufgrund der gesetzlichen Qualifikation von biometrischen Daten als besondere Personendaten müssen Bearbeitungen gemäss § 8 Abs. 2 IDG ZH in einer hinreichend bestimmten Regelung in einem formellen Gesetz geregelt sein, d.h. insbesondere Bestimmung des verantwortlichen Organs, Ziel und Zweck der Bearbeitung, Kategorien der bearbeiteten Daten sowie die Art und Weise der Bearbeitung.[242]

Das Gesetz muss somit die Befugnis erteilen, eine Identifikation oder Authentifizierung mittels biometrischer Daten vorzunehmen. Von einer genügenden Regelung gedeckt wären sämtliche begleitenden Datenbearbeitungen gedeckt, die zur Durchführung eines biometrischen Vergleichs notwendig sind, und die zugleich kein zusätzliches persönliches Risiko für die Betroffenen schaffen, insbesondere die Erhebung und Speicherung sowie der Vorgang des Vergleichens. Spezifisch geregelt werden müsste indes die Frage, was nach Abschluss eines Identifizierungs- bzw. Authentifizierungsvorgangs mit den biometrischen Profilen geschieht, die für den Vergleich benutzt wurden.[243] Dies gilt vor allem auch dann, wenn es sich um Identifizierungs- oder Authentifizierungsvorgänge handelt, die üblicherweise mehrmals durchgeführt werden. Da die Vorratsdatenspeicherung mangels Bearbeitungszweck grundsätzlich als unrechtmässig gilt,[244] muss die Bearbeitung in irgendeiner Dimension begrenzt werden, beispielsweise durch Ablauf des Arbeitsverhältnisses (zeitlich) bzw. die Ausübung der Funktion, welche für die betreffende Bearbeitung zuständig ist (sachlich/personell).

Schliesslich sind die weiteren Umstände der Datenbearbeitung in die Risikobewertung mitaufzunehmen. Zu unterscheiden wäre insbesondere zwischen

---

[241] David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter vom 16.11.2020, N 20, 22.

[242] Baeriswyl, PraKom IDG ZH (FN 101), § 8 N 14.

[243] Für das Beispiel der Gesichtserkennung siehe VII.A.3.

[244] Siehe IV.A.1.b.

offenen, von den Betroffenen steuerbaren Bearbeitungsvorgängen (etwa der Nutzung eines Fingerabdrucks zum Entsperren eines Arbeitscomputers) und verdeckten Bearbeitungen bzw. einer biometrischen Fernidentifizierung. Eine solche liegt beispielsweise vor, wenn Personen ohne ihr Wissen bzw. auf Distanz mittels Sensoren aufgrund ihres Gesichts, ihrer Gangart, Pulsrythmen und ähnlichen biometrischen Eigenheiten identifiziert werden. Dies erzeugt ein zusätzliches Risiko für die Grundrechte der Betroffenen und ist daher rechtlich separat zu bewerten.[245]

3. Insbesondere biometrische Gesichtserkennung

a. Automatisierte biometrische Erkennung

Biometrische Erkennung bedeutet die Erkennung einer Person anhand von biometrischen Merkmalen. Im Falle einer automatisierten Erkennung erfolgt diese über Sensoren, welche mit einem entsprechenden KI-System verbunden sind. Als Sensoren werden beispielsweise Kameras bzw. Scanner oder Mikrofone eingesetzt. Die Outputdaten der KI stellen eine maschinelle Erkennung dar, soweit sie die Identität einer Person bestätigen. Neben Finger- bzw. Handabdruck-, Iris- oder Venenmustern ist vor allem die Gesichtserkennung im Einsatz. Sie hat den Vorteil, dass sie auf Distanz bzw. anhand von alltäglichen Fotos bzw. Videoaufnahmen der Betroffenen vorgenommen werden kann.[246]

Die spezifischen Risiken von biometrischer Erkennung sind mittlerweile anerkannt und führen dazu, dass Datenschutzgesetze in der Schweiz die Bearbeitung biometrischer Daten als neue Kategorie von besonders schützenswerten bzw. besonderen Personendaten eingeführt haben oder einführen werden, so beispielsweise im Kanton Zürich.[247] Noch nicht in Kraft ist die entsprechende Anpassung im neuen Datenschutzgesetz des Bundes. Unter den Begriff der besonders schützenswerten Personendaten fallen künftig gemäss Art. 5 Bst. c

---

[245] EDÖB (FN 240), 3.

[246] Gerrit Hornung/Stefan Schindler, Datenschutz bei der biometrischen Gesichtserkennung – Künstliche Intelligenz und Mustererkennung als Herausforderung für das Recht, DuD 8/2021, 515–521, 515.

[247] In § 3 Abs. 4 lit. a Ziff. 2 IDG ZH mit der Änderung vom 25. November 2019, in Kraft seit dem 1. Juni 2020 (OS 75, 63).

Ziff. 4 nDSG ausdrücklich «biometrische Daten, welche eine Person eindeutig identifizieren».[248]

Derweil sieht ein Regulierungsentwurf der Europäischen Union vor, die biometrischen Fernidentifizierung in Echtzeit zu Strafverfolgungszwecken im öffentlichen Raum in der EU je nach dem damit verbundenen Risiko für die Betroffenen stark einzuschränken bzw. grundsätzlich zu verbieten.[249]

b. Gesichtserkennung als stellvertretendes Beispiel

Die biometrische Erkennung ist vermutlich eine der in der Öffentlichkeit bekanntesten KI-Technologien mit einer sehr grossen Bandbreite an möglichen Einsatzfeldern, wie beispielsweise der Authentifizierung von Telefon- und Computernutzern. Konzeptionell bedeutet automatisierte Gesichtserkennung, dass ein mit Personendaten verbundenes Gesichtsmuster durch die Auswertung von physiognomischen Eigenheiten einer Person zugeordnet wird. Ihre grundlegende Funktion ist demnach jene des biometrischen Erkennens von Personen. Durch sie kann beispielsweise eine Zugangsberechtigung bestätigt oder Bilder und Videomaterial in Bezug auf die darin erfassten Personen ausgewertet werden. Im ersten Fall spricht man von einem *one-to-one matching*: das Muster, das von der zu erkennenden Person erstellt wird, wird mit einem Muster in der Datenbank verglichen, um die betreffende Person zu verifizieren. Diese Person ist dem System also bekannt, muss aber ihre Identität beweisen. Im zweiten Fall spricht man von einem *one-to-many matching*: die erfassten Personen werden mit vielen Mustern in einer Datenbank verglichen, um sie zu identifizieren. Die sensorisch erfassten Personen sind dem System nicht bekannt und sollen zwecks Identifikation mit den in der Datenbank vorhandenen Personen verglichen werden. [250]

---

[248] BBl 2020 7639, 7641.

[249] Siehe den Vorschlag für ein Gesetz über die künstliche Intelligenz vom 22. April 2021, COM(2021) 206 final, Art. 5 Abs. 1 Bst. d des Entwurfs.

[250] Vgl. EDÖB (FN 240), 5; FRA – Agentur der Europäischen Union für Grundrechte, Gesichtserkennungstechnologien: grundrechtsrelevante Erwägungen im Rahmen der Strafverfolgung, Januar 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper_de.pdf (Abruf 01.06.2022), 4; Nadja Braun Binder/Eliane Kunz/Liliane Obrecht, Maschinelle Gesichtserkennung im öffentlichen Raum, in: sui generis 2022, N 7.

Die automatisierte Gesichtserkennung ist als allgemeines technologisches Konzept zu verstehen, dessen Hauptfunktion, die Erkennung, sowie die hierdurch ermöglichten Funktionen der Verifizierung und Identifizierung bzw. Suche in sämtlichen Lebensbereichen einsetzbar sind.[251] Das Konzept lässt sich in der Regel datenschutzkonform ausgestalten, indem die mit dem konkreten Einsatz von automatisierter Gesichtserkennung verbundenen Risiken identifiziert und durch geeignete Massnahmen gemindert werden. Diese Risiken ergeben sich einerseits aus der verwendeten Technologie und andererseits aus den Umständen ihrer Anwendung bzw. aus der Automatisierung von Verwaltungs- und Entscheidungsprozessen in der Gesellschaft.[252] Dabei betreffen die technologischen Risiken die Qualität der durch sie generierten Daten, die Risiken der Automatisierung und gesellschaftlichen Einbettung hingegen die Verwendung dieser Daten. Hierbei stellen sich je unterschiedliche Rechtsfragen.[253]

c. Grundlegende Risikostruktur

Im Gegensatz zu anderen eineindeutigen biometrischen Merkmalen, beispielsweise Fingerabdruck- oder DNA-Muster, verändern sich die Gesichter über Zeit merklich. Es handelt sich demnach um eine permanente, nicht ohne weiteres änderbare aber zugleich veränderliche Eigenschaft einer Person. Mit der zunehmenden Leistungsfähigkeit der Gesichtserkennungstechnologie, scheint diese Veränderung mittel- bis langfristig eine überwindbare Hürde darzustellen: Personen werden auch dann erkannt, wenn zwischen Bild und Gesicht (derselben Person) mehrere Jahre liegen, wobei die Fehlerrate leicht

---

[251] Zu den Begriffen der Verifizierung (oder auch Authentifizierung) und Identifizierung siehe Blonski (FN 240), 12 ff.; siehe auch die illustrativen Beispiele bei Ramona Keist, Gesichtserkennung im zivilrechtlichen Persönlichkeitsschutz, in: Jusletter vom 20.05.2019, N 7.

[252] Vgl. dazu I.A.3.

[253] Vgl. dazu IV.A.2. und IV.A.3.; Unklar hier Braun Binder et al. (FN 250), 53 ff., die betonen, dass die mit der automatisierten Gesichtserkennung zusammenhängenden Rechtsfragen sich «grundsätzlich unabhängig» von der eingesetzten Technologie stellen (N 7) und an anderer Stelle auf die Gefahr einer Diskriminierung durch *false positives* hinweisen (N 32) – letztere wird aber durch das Training des verwendeten Modells begründet und stellt ein intrinsisches Problem trainierter KI-Modelle dar; siehe dazu I.B.3.c.

zunimmt.[254] Theoretisch können alte Fotos (von genügender Qualität) und möglicherweise Bilder aus der Kindheit zur Erkennung von erwachsenen Gesichtern ausreichen.[255] Neuerdings soll das Gesicht gar aus der DNA einer Person berechnet werden können.[256]

Neben dem zeitlichen Faktor kann als weiterer Risikofaktor der Umstand genannt werden, dass Gesichter in der Regel für Dritte mit verhältnismässig wenig Aufwand zugänglich sind. Sie können per Foto- oder Videoaufnahme auf Distanz ermittelt werden. Dies kann in unmittelbarer Weise mittels Livebilder geschehen oder mittelbar[257] aufgrund von Fotos und Videos.

d. Risiken durch Datenbearbeitung

Neben den intrinsischen Risiken der Gesichtserkennung bestehen weitere, durch die Art und Weise sowie den Zweck der Datenbearbeitung begründete Risiken. Dabei ist zu unterscheiden zwischen Risiken, welche die Betroffenen einer Bearbeitung von Personendaten tragen sowie Risiken, die eine unbekannte Anzahl von Personen betreffen. Denn mit der vereinfachten Skalierbarkeit moderner KI- und Big-Data-Technologien weiten sich die hier besprochenen Risiken der automatisierten Gesichtserkennung auf die gesellschaftliche Ebene aus. Es wird befürchtet, dass ein unreflektierter Einsatz von Gesichtserkennungstechnologien die demokratische Meinungsbildung erschweren und einzelne Gruppen in diskriminierender Weise benachteiligen könnte.[258]

Betroffene einer Bearbeitung von Personendaten im Rahmen einer Gesichtserkennung sind zunächst jene Personen, deren biometrisches Gesichtsmuster

---

[254] Lacey Best-Rowden/Anil K. Jain, Longitudinal Study of Automatic Face Recognition, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 40/1 2018, 148.

[255] Alexis C. Madrigal, Computers See Your Face as a Child: Will They Recognize You as an Adult?, The Atlantic, 13.05.2014, legt die (damalige) untere Altersgrenze bei 7 Jahren fest.

[256] Tate Ryan-Mosley, This company says it's developing a system that can recognize your face from just your DNA, Technology Review 31.01.2022; unklar, ob dies tatsächlich realisierbar ist.

[257] Auch als »nachträgliche Gesichtserkennung« bezeichnet; vgl. Braun Binder et al. (FN 250), N 14.

[258] FRA (FN 250), 4; Braun Binder et al. (FN 250), N 32 m.w.H.

als Vergleichsmuster vom System für den Vergleichsvorgang herangezogen wird. Erstens werden biometrischen Personendaten verwendet und zweitens besteht der Zweck der Bearbeitung darin, diese Personen zu erkennen, also zu identifizieren. Dagegen gelten Personen, die sich beispielsweise im Sichtfeld einer Videokamera mit Gesichtserkennungsfunktion aufhalten, *datenschutzrechtlich* nicht als Betroffene der Gesichtserkennung, solange sie nicht einem bestimmten Gesichtsprofil zugeordnet wurden, da sie diesbezüglich weder bestimmt noch bestimmbar sind, bzw. nicht identifiziert wurden.[259] Soweit aber ein KI-System sie zum Zweck des Vergleichs sensorisch erfasst, sind sie – wie auch jene Personen, die tatsächlich identifiziert werden – von der Überwachung betroffen, die gegebenenfalls durch die Gesichtserkennung bewirkt werden soll. Eine solche Überwachung birgt eigene Grundrechtsrisiken, namentlich jenes des Einschüchterungseffekts oder auch *chilling effect*.[260]

Die Unterscheidung der beiden Gruppen von Betroffenen ist somit von Bedeutung, weil die Risikostruktur für die datenschutzrechtlich von der Gesichtserkennung betroffene Personen sich von jener der übrigen erfassten Personen unterscheidet. Indes sind die Übergänge fliessend, da für Personen, die an und für sich datenschutzrechtlich nicht von der Gesichtserkennung betroffen wären, die Möglichkeit besteht, dass sie fälschlicherweise das Lager wechseln, wenn die KI «einen Fehler macht»[261] und für sie ein *false positive* ausgibt, d.h. sie falsch, d.h. als eine andere Person identifiziert.[262] Durch den fehlerhaften Personenbezug entstehen unrichtige Personendaten,[263] die je nach Verwendungszusammenhang ein beträchtliches persönliches Risiko für die Betroffenen bedeuten, und die im Sinne der Datenrichtigkeit mittels geeigneter Qualitätskontrollen möglichst schnell zu berichtigen bzw. zu löschen sind.[264]

---

[259] Dazu Rosenthal (FN 225), 200; Glass (FN 228), N 5; hier zeigt sich erneut die Problematik, dass der Geltungsbereich der Datenschutzgesetze durch den relativen Begriff des Personendatums mitbestimmt wird.

[260] Glass (FN 26), 154; Braun Binder et al. (FN 250), N 30.

[261] Technisch handelt es sich nicht um einen Fehler, sondern um die Manifestation der statistischen Fehlerquote des Systems; vgl. FRA (FN 250), 9.

[262] FRA (FN 250), 9.; zur Terminologie zuletzt Braun Binder et al. (FN 250), N 31.

[263] Tina Krügel/Julia Pfeiffenbring, Datenschutzrechtliche Herausforderungen von KI, in: Martin Ebers /Christian Heinze/Tina Krügel/Björn Steinrötter (Hrsg.), Künstliche Intelligenz und Robotik – Rechtshandbuch, München 2020, § 11 N 26.

[264] Zur Datenrichtigkeit siehe IV.A.3.

e. Rechtliche Vorgaben

Im kantonalen Recht existieren soweit ersichtlich keine ausdrücklichen Vorgaben für den Einsatz von Gesichtserkennungstechnologie durch öffentliche Organe, wohingegen dies im Bundesrecht vereinzelt vorgesehen ist.[265] Dies ist insofern bemerkenswert, als die betreffenden Vergleichs- und Outputdaten aufgrund ihrer Eigenschaft als biometrische Daten als besondere Personendaten im Sinne von § 3 Abs. 4 Bst. a Ziff. 2 IDG ZH gelten. Der Einsatz von Gesichtserkennungstechnologien muss daher gemäss § 8 Abs. 2 IDG ZH in einem formellen Gesetz hinreichend geregelt sein.[266]

Was in diesem Zusammenhang eine hinreichende Regelung im Gesetz bedeutet, ist unklar. Je nach Einsatzzweck der Gesichtserkennung wird die betreffende gesetzliche Grundlage mehr oder weniger bestimmt ausfallen müssen. So erscheint es beispielsweise als naheliegend, dass die Verwendung von Laptops mit kamerabasiertem Login durch das Personal eines öffentlichen Organs auf Gesetzes- bzw. Verordnungsebene weniger klar vorgespurt sein muss – tatsächlich reicht hierzu wohl die Pflicht zur Sicherstellung der Datensicherheit aus – als beispielsweise der Einsatz zur Identifikation von Fahrzeuglenkern bei Geschwindigkeitskontrollen.

Für die Normdichte einer Befugnis zum Einsatz von Gesichtserkennungstechnologie gelten grundsätzlich die allgemeinen Kriterien für gesetzliche Bearbeitungsgrundlagen für besondere Personendaten. Zumindest müssen das verantwortliche Organ, Ziel und Zweck der damit verbundenen Datenbearbeitungen, die zulässigen Datenkategorien sowie die Art und Weise der Datenbearbeitungen geregelt werden.[267] Hierbei muss das Gesetz deutlich zum Ausdruck bringen, wie die Gesichtserkennungsfunktion in den betreffenden Arbeitsprozess eingebunden ist und welche Aufgabe durch sie in diesem Rahmen erfüllt werden soll. Weiter muss in den Materialien plausibel begründet werden, weshalb kein milderes Mittel das verfolgte Ziel ausreichend

---

[265] So etwa in Art. 103 Abs. 1 und 5 AIG, die es den zuständigen kantonalen Behörden ermöglichen, ankommende Flugpassagiere mittels elektronischer Erkennung zu identifizieren; dazu Braun Binder et al. (FN 250), N 29.

[266] Gesichtsdaten werden im Rahmen eines Trainings nicht personenbezogen bearbeitet und stellen insofern keine Personendaten dar; Siehe dazu III.A.1.

[267] Baeriswyl, PraKom IDG ZH (FN 101), § 8 N 14.

verwirklichen würde.[268] Hierbei muss die Risikobeurteilung für jede mit dem Einsatz der Gesichtserkennungstechnologie verbundene Bearbeitung von personenbezogenen Daten (inkl. Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Vernichten)[269] je separat sowie kumulativ vorgenommen und rechtlich bewertet werden.

4. Massnahmen der sozialen Hilfe

Die Sozialhilfe in der Schweiz wird seit Jahren von Debatten über die Verhinderung unrechtmässiger Leistungen geprägt, welche dazu geführt hat, dass verschiedene Kantone entsprechende Massnahmen zur Bekämpfung von unrechtmässig bezogenen Leistungen im Gesetz verankert haben. Im Kanton Zürich ist dies insbesondere die in § 48a SHG geregelte Observation, welche den Einsatz von Observationsspezialisten ermöglicht sowie die in § 48 SHG geregelten, weitreichenden Auskunftsbefugnisse von Behörden und Privatpersonen gegenüber der Sozialhilfe. Flankiert werden diese Massnahmen durch die in § 47b SHG[270] enthaltenen, umfassenden gesetzlichen Anzeigepflichten von Verwaltungsbehörden des Kantons, der Gemeinden sowie der mit der Erfüllung von öffentlichen Aufgaben betrauten Organisationen und Personen gegenüber der Sozialhilfe.

Die Sozialhilfebehörden verfügen auch inhaltlich über sehr weitreichende Befugnisse zur Bearbeitung von Personendaten ihrer Klientinnen und Klienten. Tatsächlich enthält § 18 SHG, der die zulässigen Datenkategorien bezeichnet, welche durch die Sozialhilfebehörde in Erledigung ihrer Aufgaben bearbeiten dürfen, keine nennenswerten Einschränkungen. Entsprechend sind die Behörden grundsätzlich berechtigt, vorbehalten der genügenden Plausibilisierung eines Zusammenhangs mit ihren weit gefassten Aufgaben, Personendaten aus beliebigen Lebensbereichen der Betroffenen zu bearbeiten. Aufgrund dieser weitreichenden Bearbeitungsbefugnisse zur Erfüllung ihrer Aufgaben, insbesondere die Bedürftigkeit von Gesuchstellerinnen zu beurteilen, über entsprechende Hilfe zu entscheiden und unrechtmässig bezogene Unterstützung zu

[268] Vgl. dazu Braun Binder et al. (FN 250), N 17.

[269] Siehe FN 130.

[270] Sozialhilfegesetz vom 14. Juni 1981 des Kantons Zürich (SHG; ON 851.1).

entdecken, verfügen Sozialhilfebehörden in der Regel über sehr detaillierte Daten zu den Lebensumständen ihrer Klientinnen und Klienten.

An und für sich wäre damit eine Fülle von Trainingsdaten für den Einsatz von KI-Technologien gegeben, mit deren Hilfe möglicherweise Fälle von unrechtmässiger Unterstützung oder gar Missbrauch identifiziert werden könnten. Systeme zur Aufdeckung von unrechtmässig ausbezahlten Sozialhilfeleistungen bzw. der diesbezüglichen Risikoanalyse sind denn auch vereinzelt bereits im Einsatz, so beispielsweise in Dänemark und den Niederlanden.[271] Solche Analysen sind funktional eng mit der personenbezogenen prädiktiven Polizeiarbeit verwandt. Aufgrund der noch jungen Technologie, die zum Einsatz kommt, sind Ergebnisse mit Vorbehalt zu nutzen bzw. nur zurückhaltend als Indizien für das Vorliegen eines tatsächlichen unrechtmässigen Bezugs zu werten. Auch ist die Transparenz der Bearbeitung stets zu wahren,[272] d.h. verdeckte Missbrauchsanalysen durch intelligente Mustererkennung in den Klientinnendaten müssten gesetzlich vorgesehen und geregelt sein und die Betroffenen in irgendeiner Form informiert werden.[273] Ersteres ergibt sich nicht zuletzt aus dem Umstand, dass Ergebnisse einer Mustererkennungsanalyse von Sozialhilfedaten einer Person in der Regel als eine «Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben» i.S.v. § 3 Abs. 4 Bst. b IDG ZH zu werten sein werden, und daher eine Bearbeitung von besonderen Personendaten i.S.v. § 8 Abs. 2 IDG ZH vorliegt.

---

[271] Braun Binder et al. (FN 8), 29 (Dänemark), 31 (Niederlande); sowie Hinweis bei OECD (FN 13), 70. m.w.H (GB); siehe auch Melissa Heikkilä, Dutch scandal serves as a warning for Europe over risks of using algorithms, Politico.eu, 29.03.2022.

[272] Zur Transparenz siehe IV.A.1.c.

[273] Zur Rechtsgrundlage für KI-Bearbeitungen siehe IV.A.1.a.

5. Administrative oder strafrechtliche Verfolgungen oder Sanktionen

Neben *predictive policing*[274] und künstlich intelligenten Onlinetools zur Bekämpfung komplexer krimineller Strukturen[275] sind hier insbesondere auch niederschwellige Verfolgungs- und Sanktionsmassnahmen der Massenverwaltung zu nennen, so beispielsweise automatische Geschwindigkeitskontrollen oder die Videoüberwachung und -analyse von Menschenmengen zwecks *crowd management, hotspot policing* oder die anlässlich von Sportveranstaltungen durchgeführte Erkennung von Personen, die im «Hooligan-Register» des Bundes[276] verzeichnet sind. Weiter fallen auch die im Rahmen der Darstellung von Bias genannten Systeme, wie COMPAS, in diese Kategorie.[277]

6. Insbesondere Predictive Policing

a. Breiter Abwehr- und Präventionsauftrag der Polizei

Polizeigesetze sind von offenen Normen geprägt, welche die Aufgaben und Mittel der Polizeien beschreiben. Ergänzt werden diese zunehmend durch verfassungskonkretisierende Grundsätze der Polizeiarbeit, welche zur verfassungskonformen Auslegung der Gesetze anmahnen. Abgesehen davon besteht für die Polizeien ein weiter gesetzlicher Spielraum mit nur wenigen Vorentscheidungen des Gesetzgebers in Bezug auf Einzelfälle. Eine Konkretisierung besteht insofern, als die zulässigen Massnahmen der Aufgabenerfüllung gewisse Konturen verleihen, indem sie die zulässigen Datenbearbeitungen genauer beschreiben.[278] Diese werden ihrerseits durch die Regelungen der zulässigen Datenbanken

---

[274] Zu *predictive policing* siehe sogleich VII.A.6.

[275] Beispielsweise das Projekt Memex der DARPA (Entdecken von Menschenhandel), https://www.defense.gov/News/News-Stories/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/ (Abruf 01.06.2022); Projekt zur Bekämpfung von Kinderpornografie des Bundeslandes NRW in Zusammenarbeit mit Microsoft Deutschland vgl. https://www.sueddeutsche.de/digital/software-maschinenlernen-ki-kuenstiche-intelligenz-kinderpornografie-polizei-nrw-1.4553870 (Abruf 01.06.2022).

[276] Zum Informationssystem Hoogan und den in den letzten Jahren erfassten Personengruppen und Straftaten siehe den Bericht des Fedpol vom 1. Juli 2021, https://www.fedpol.admin.ch/fedpol/de/home/sicherheit/hooliganismus/zahlen/hoogan.html (Abruf 01.06.2022).

[277] Siehe I.B.3.c.

[278] Glass (FN 26), 245 ff.

sowie den darin zu bearbeitenden Datenkategorien ergänzt, insbesondere auch bezüglich der Zugriffsrechte, woraus in der Regel die wichtigsten Eckdaten der polizeilichen Informationssysteme ersichtlich werden.[279]

Die hier beschriebene offene Normierung findet ihre Begründung in der Offenheit der Gefahrenabwehr als zentrale Aufgabe der Polizei, insbesondere in der Aufklärung und dem Vorbeugen von Straftaten.[280] Da die Gefahrenabwehr regelmässig im Schutzbereich der Grundrechte erfolgt, muss sie sich in besonderem Masse an den Bestimmungen über die Umsetzung der Grundrechte in Art. 35 BV orientieren. Dies gilt insbesondere auch für die Frage, welche Gefahren im Einzelfall prioritär bekämpft werden.[281]

b. Das Konzept der automatisierten polizeilichen Gefahrenprognose

In der Schweiz werden diverse polizeiliche Prognoseprogramme eingesetzt.[282] Diese Formen der Polizeiarbeit nutzen algorithmische Prognosen, um «lagebezogene Wahrscheinlichkeitsaussagen» in Bezug auf mögliche künftige Straftaten zu generieren.[283] Ziele sind die Verbesserung der Präventionsarbeit sowie die effizientere Nutzung von Ressourcen.[284] Es handelt sich um modellbasierte Vorfeldermittlung.[285]

Dabei wird versucht, die Aufgabe der präventiven Gefahrenabwehr durch künstlich intelligente Algorithmen anzugehen und automatisch voraussagen zu lassen, wo (raumbezogen) oder durch wen (personenbezogen) künftig die

---

[279] Siehe die Hinweise bei Belser/Noureddine (FN 26), Datenschutzrecht Grundlagen, 448.

[280] Belser/Noureddine (FN 26), Datenschutzrecht Grundlagen, 448.

[281] Glass (FN 26), 251.

[282] Monika Simmler/Simone Brunner, Die Kantone im Bann der Algorithmen?, in: Monika Simmler (Hrsg.), Smart Criminal Justice – Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege, Basel 2021, 15 f.; Braun Binder et al. (FN 8), 25.

[283] Johanna Sprenger, Verbrechensbekämpfung: Predictive Policing, in: Künstliche Intelligenz und Robotik – Rechtshandbuch, München 2020, § 31 N 5 f.; Sommer (FN 218), 36.

[284] Sprenger (FN 283), § 31 N 38.

[285] Glass (FN 26), 258 f.

Verwirklichung einer polizeilichen Gefahr droht.[286] Gewisse Systeme verbinden beide Formen, indem sie per Videoanalysen in Echtzeit Gefahren erkennen sollen. Dies geschieht anhand verschiedener biometrischer Merkmale, wie etwa Gesichtserkennung (bekannte Person) oder Erkennung von gefährlichen Bewegungsabläufen (unbekannte Personen).[287]

Raumbezogene Gefahrenprognosen können datenschutzrechtlich relevant werden, indem sie Personengruppen erzeugen, die unter einem Generalverdacht stehen, gefährlicher zu sein als die allgemeine Bevölkerung, indem sie deren Basisrate[288] im Risikoscore übertreffen. Weiter darf nicht vergessen gehen, dass die verwendeten Analyseparameter (beispielsweise Tatzeitraum, Tatort, Tatobjekt, *modus operandi* und Beute vergangener Delikte)[289] personenbezogene Daten sind, die (vorerst) nicht bestimmbare Personen betreffen. Ziel der Prognose ist es schlussendlich, jene Personen zu identifizieren und überführen, welche durch ihre Tätigkeit die Daten liefern. Schliesslich kann mit dem Gedanken gespielt werden, Erkenntnisse aus der raumbezogenen Gefahrenprognose Personen «aus der Gegend», für die ein Risikoscore berechnet wird, als erschwerenden Faktor zuzuweisen.

B. Profiling

Neu definiert Art. 5 Bst. f nDSG den Begriff des Profiling als «jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen». Der Begriff des Persönlichkeitsprofils wird aus dem Gesetz gestrichen, ausschlaggebend soll

---

[286] Jennifer Pullen/Patricia Schefer, Predictive Policing – Grundlagen, Funktionsweise und Wirkung, in: Monika Simmler (Hrsg.), Smart Criminal Justice – Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege, Basel 2021, 103–122, 105 f.; Christen et al. (FN 10), 211 f.; Sommer (FN 218), 36 f.

[287] Wischmeyer (FN 64), § 20 N 17.

[288] Zum Begriff Sommer (FN 218), 52.

[289] Vgl. die Darstellung zu PRECOBS bei Simmler/Brunner (FN 282), 17 ff.

neu der Vorgang sein und nicht mehr das Ergebnis.[290] Das nDSG unterscheidet zwischen einfachem Profiling und Profiling mit hohem Risiko. Letzteres wurde vom Ständerat vorgeschlagen und die endgültige Fassung erst auf Antrag der Einigungskonferenz in beiden Räten genehmigt.[291]

Ein hohes Risiko liegt gemäss Art. 5 Bst. g nDSG dann vor, wenn das Profiling «ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt». Hier klingt die Legaldefinition des Persönlichkeitsprofils von Art. 3 Bst. d DSG nach: eine solches besteht in einer «Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt». Ob und wie sich diese Unterscheidung in der Praxis bewähren wird, ist noch unklar. Es kann indes davon ausgegangen werden, dass Datenauswertungen mittels KI-Technologien, welche sich auf bestimmte oder bestimmbare Personen beziehen, zumindest als «einfaches» Profiling gelten werden.[292]

In jedem Fall soll gemäss Vorschlag des Bundesrates ein Profiling nur dann vorliegen, wenn die *Bewertung* einer Person *vollautomatisiert* vorgenommen wird. Hierunter fällt «jede Auswertung mit Hilfe von computergestützten Analysetechniken».[293] Damit wird die Betonung auf die Automatisierung der Auswertung gelegt und nicht auf den Grad der Automatisierung des gesamten Entscheidungsprozesses, in den eine Auswertung eingebettet ist. Die hieraus ersichtliche Relativierung der Unterscheidung zwischen voll- und teilautomatisierten Entscheiden ist zu begrüssen, da die Problemlage jeweils eine ähnliche ist.[294]

Unklar bleibt schliesslich, weshalb die Botschaft betont, dass die Definition des Profiling nicht bedeute, dass Algorithmen verwendet werden müssten,[295]

---

[290] Botschaft E-DSG (FN 188), 7021.

[291] Geschäft des Bundesrates 17.059, Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz, Beschlüsse gemäss Antrag der Einigungskonferenz des National-, bzw. des Ständerates vom 24.09.2020.

[292] Siehe auch den Hinweis bei Klaus (FN 36), 86.

[293] Botschaft E-DSG (FN 188), 7022.

[294] Siehe IV.A.4.c.

[295] Botschaft E-DSG (FN 188), 7022.

da *prima vista* nicht ersichtlich ist, wie eine vollautomatisierte computergestützte Auswertung ohne die Verwendung von Algorithmen stattfinden soll.

C. KI-Bearbeitungen in allgemeinen Verwaltungsprozessen

Unabhängig davon, ob Daten aus einem gesetzlich geschützten Bereich gemäss § 3 IDG ZH bearbeitet werden, ist absehbar, dass Verwaltungsprozesse künftig durch neue KI-Technologien unterstützt werden.[296] Man verspricht sich davon beispielsweise eine Entlastung der Arbeitsprozesse durch Steigerung der Effizienz, indem etwa Routinearbeit durch einen KI-Agenten erledigt wird, bessere statistische Prognosen für komplexe wirtschafts-, sozial-, umwelt-, oder sicherheitspolitische Zusammenhänge, besseren Service und mehr Kundennähe durch Chatbots und andere e-Government-Dienstleistungen mit KI-Funktionen, die Überprüfung und Vereinfachung von Prozessabläufen oder eine bessere Verwendung der bei der Verwaltung vorhandenen grossen Datenmengen.[297] Im Folgenden werden zwei aktuelle Anwendungen mit KI-Einschlag thematisiert: *chatbots* und online-Übersetzungen.

1. Chatbots

Verschiedene Verwaltungen in der Schweiz setzten für die Kommunikation mit ihren Kundinnen und Kunden Chatbots ein. Im Vordergrund steht zurzeit die Bereitstellung von interaktiv aufbereiteter Information in Dialogform, doch sollen künftig auch rechtswirksame Handlungen gegenüber öffentlichen Organen möglich werden (etwa die Einreichung von Gesuchen).[298] Als Chatbot werden Userinterfaces bezeichnet, die einen Text- oder auch Sprachdialog in Alltagssprache simulieren (to chat = plaudern). Es handelt sich demnach um eine «konversationsbasierte Schnittstelle»[299] zwischen Nutzerinnen und Nutzern und einem Informationssystem. Dagegen gelten Schnittstellen, die auf der Grundlage eines vorprogrammierten Frage-/Antwort-Systems (FAQs)

---

[296] Gewisse KI-Anwendungen sind schon länger in Betrieb. Es handelt sich um mittlerweile alltägliche, «niederschwellige» Anwendungen wie Rechtschreibeprüfungen, Spamfilter oder Antimalware.

[297] Zum Ganzen siehe Braun Binder et al. (FN 8), 15.

[298] Übersicht bei Braun Binder et al. (FN 8), 27.

[299] Braun Binder et al. (FN 8), 27.

aufgebaut sind, nicht als Chatbots – können aber durch erläuternde Chatbots ergänzt werden.[300]

Im Rahmen des Einsatzes als Auskunftssystem muss ein Bot zusätzlich auf entsprechende Inhalte zugreifen können, welche die Grundlage für eine korrekte Antwort bilden. Hierbei kommen verschiedene KI-Funktionen zusammen: das Programm muss zunächst die Eingabe der Nutzerinnen und Nutzern sprachlich korrekt interpretieren, diese erfolgreich mit den zur Verfügung stehenden Inhalten *vergleichen*, d.h. ein *intent matching* vornehmen, und eine sinnvolle und inhaltlich richtige Antwort formulieren. Während die Spracherkennung und -aufbereitung für den Dialog auf *machine learning* bzw. *natural language processing* (NLP) basiert, wird die Auswahl der Antwort typischerweise von einem Expertensystem übernommen.[301]

Die Bearbeitung von Personendaten durch Chatbot-Applikationen, welche durch ein öffentliches Organ bereitgestellt werden, stellt eine Bearbeitung von Personendaten i.S.v. § 3 Abs. 5 IDG ZH dar und unterliegt damit – innerhalb des Geltungsbereichs von § 2 IDG ZH – den Bestimmungen dieses Gesetzes. Als (vorerst) neue Technologie muss vor der Verwendung eines KI-basierten Chatbots, durch den Personendaten bearbeitet werden sollen, stets geprüft werden, ob die Applikation gemäss § 10 Abs. 2 IDG ZH bei der kantonalen Datenschutzbeauftragten zur Vorabkontrolle angemeldet werden muss.[302] In der Anwendung ergibt sich schliesslich aus dem Transparenzprinzip eine Pflicht, die KI-Funktionalität eines Chatbots gegenüber den Nutzerinnen und Nutzern auszuweisen.

Ob eine Bearbeitung von Personendaten durch den Chatbot stattfindet, ergibt sich aus dem Zweck sowie der angeschlossenen Systemarchitektur. Ein Chatbot, der anonym genutzt wird, bearbeitet keine Personendaten. Eine anonyme Nutzung liegt vermutungsweise vor, wenn kein Login in ein Onlineportal notwendig ist, um den Chatbot zu nutzen, und wenn im Rahmen des Chats keine Personendaten, wie etwa Kontaktdaten, erhoben werden.

---

[300] Für den Kanton Zürich vgl. Braun Binder et al. (FN 8), 27.

[301] Siehe zum Ganzen Michael Krähenbühl, Ein Chatbot als Rechtsberater – ein haftungsrechtlicher Albtraum für den Betreiber?, in: Jusletter IT vom 30.09.2021, N 10; dies scheint sich zu ändern, vgl. https://openai.com/blog/chatgpt/ (Aufruf 23.12.2022).

[302] Siehe IV.A.4.b.

Die Anonymität ist insofern relativ, als gewisse Randdaten der technischen Verbindung zwischen Nutzerin und Nutzer und Chatinterface durch den ISP gemäss Art. 2 BÜPF i.V.m. Art. 21 BÜPF während der gesetzlichen Frist von 6 Monaten gespeichert werden und insofern eine theoretische Möglichkeit der De-anonymisierung bzw. Identifikation der betreffenden Person über ihre IP-Adresse besteht.[303] Soweit aber der Chatbot sich in einem durch Login geschützten Bereich befindet, besteht zumindest gegenüber dem Portalsystem, in das er eingebettet ist, keine Anonymität. Konzeptionell könnten sämtliche im Portal vorhandenen Daten der betreffenden Person mit dem Chat verknüpft werden, wodurch diese grundsätzlich Personendaten darstellen. Eine solche Verknüpfung kann typischerweise dazu dienen, die Antworten für die betreffende Person zu verbessern.[304] In solchen Fällen ist der Chatbot als Teil des Portals zu sehen und sind die datenschutzrechtlichen Vorgaben für elektronische Portale[305] sinngemäss anzuwenden.

Schliesslich bearbeiten Chatbots die Personendaten der Nutzerinnen und Nutzern immer dann, wenn sich der Chat auf ein spezifisches, diese Person betreffendes Geschäft bezieht, etwa indem er das Stellen eines Gesuchs unterstützt oder eine medizinische Erstberatung anbietet. Inwiefern hier ein zusätzliches Risiko für die Persönlichkeit der Nutzerinnen und Nutzern besteht, hängt von der Architektur des Gesamtsystems ab, beispielsweise davon, ob die Chatinhalte gespeichert und anderen Applikationen zur Verfügung gehalten werden. Wäre dies der Fall, müssten solche Zugriffe die Voraussetzungen der Bekanntgabe gemäss § 16 bzw. 17 IDG ZH erfüllen.

---

[303] Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF; SR 780.1).

[304] Jörn von Lucke/Jan Etscheid, Wie Ansätze künstlicher Intelligenz die öffentliche Verwaltung und die Justiz verändern könnten, in: Walter Hötzendorfer/Christof Tschohl/Franz Kummer, International Trends in Legal Informatics – Festschrift für Erich Schweighofer, Bern 2020, 253 f.

[305] Vgl. dazu *privatim* – Konferenz der schweizerischen Datenschutzbeauftragten, Merkblatt für Online-Portale der öffentlichen Verwaltung, https://www.privatim.ch/wp-content/uploads/2018/10/031018_privatim_Merkblatt_Online-Portale.pdf (Abruf 28.01.2022).

2. Online-Übersetzung

Moderne Übersetzungsprogramme nutzen neuronale Netze, sog. *neural machine translation*, um anhand von Sprachmustern und deren Kontext die korrekte Übersetzung von einer Sprache in eine andere Sprache zu erstellen. Dazu werden sie mit Satzpaaren trainiert und anhand der Resultate optimiert.[306] Der Wechsel der grossen Anbieter wie Google oder Microsoft von regelbasierten Systemen auf Lernalgorithmen erfolgte soweit ersichtlich innerhalb der letzten fünf bis zehn Jahre.[307]

Wenn öffentliche Organe Dokumente, wie beispielsweise Verfügungen, amtliche Schreiben oder fremdsprachige Originaldokumente, die Personendaten enthalten, mit Hilfe von Übersetzern übersetzen lassen, so gilt dies je nach Inhalt des Textes als eine Bearbeitung von (besonderen) Personendaten. Wird die Onlineversion eines Übersetzungstools benutzt, gilt die Übermittlung des zu übersetzenden Originaltextes an den Server, der die KI-Funktion bereitstellt, als Bekanntgabe von (besonderen) Personendaten an Private und sind die Bestimmungen in § 16 Abs. 1 bzw. § 17 Abs. 1 IDG ZH anwendbar. Da es sich um eine Form von Cloud-Computing handelt, sind die entsprechenden Vorschriften zu beachten.[308]

---

[306] Zur Beschreibung der Funktionsweise von DeepL siehe Ruth Fulterer, Warum automatische Übersetzer so gut funktionieren, NZZ vom 29.01.2022.

[307] Barak Turovsky, Found in translation: More accurate, fluent sentences in Google Translate, Google Blog, 15.11.2016; Microsoft Translator, Microsoft brings AI-powered translation to end users and developers, whether you're online or offline, Microsoft Translator Blog, 18.04.2018.

[308] Vgl. dazu DSB Kanton Zürich, Merkblatt Cloud Computing, V 1.5/April 2021, https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf (Abruf 01.06.2022).

ISBN 978-3-03891-513-3