1/22

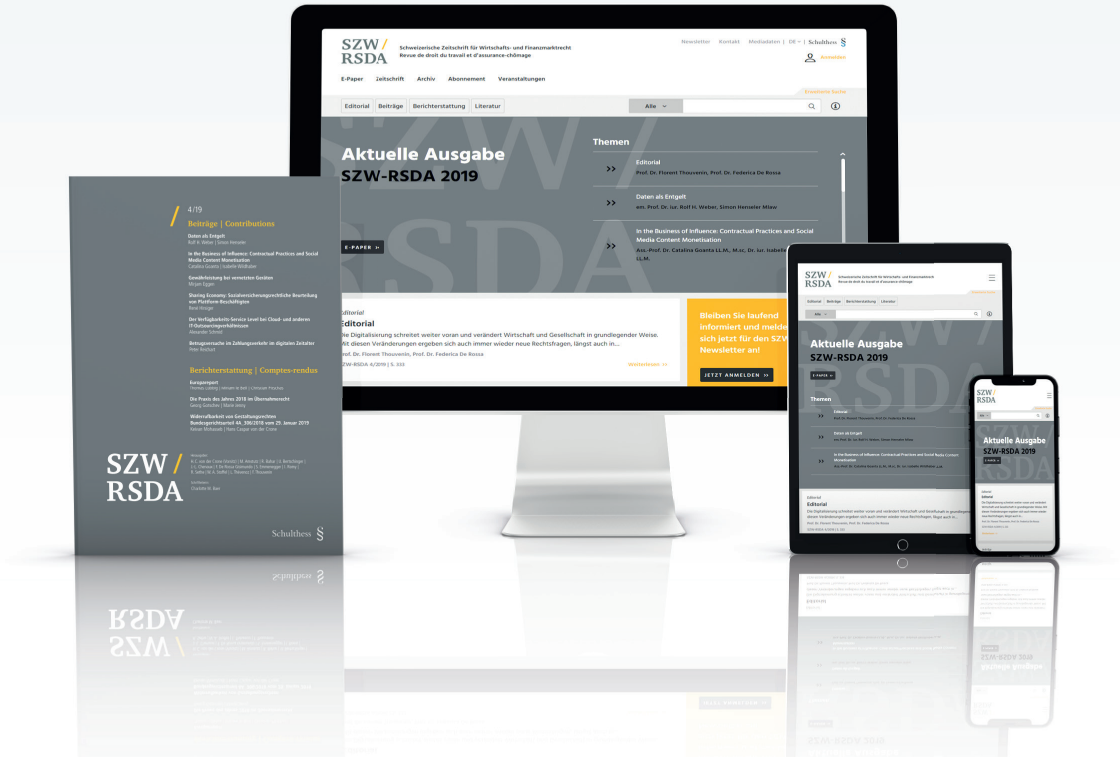
Beiträge | Contributions

Berichterstattung | Comptes-rendus

SZW / RSDA

Schulthess §

Lesen Sie die SZW neu auch online.



- SZW Printausgabe – weiterhin alle zwei Monaten im Briefkasten
- SZW E-Paper – bequem digital im Printlayout lesen NEU
- SZW E-Recherche – schnelles Finden im Online-Archiv NEU

www.szw.ch

Alle SZW-Abonnenten profitieren ab sofort vom neuen Online-Angebot der SZW
Sie erhalten Ihre persönlichen Zugangsdaten per E-Mail und können sich damit unter www.szw.ch einfach anmelden.

Sie möchten die neue SZW kennenlernen?
Testen Sie jetzt die SZW im kostenlosen Probeabonnement. Sie erhalten zwei Printausgaben sowie für 2 Monate einen Testzugang zu www.szw.ch.
Mehr Infos unter www.szw.ch/abonnement

Schulthess Juristische Medien AG · Zwingliplatz 2 · CH-8021 Zürich · Tel. +41 (0)44 200 29 29 · service@schulthess.com

Schulthess §

Inhalt | Table des matières

KI Sandboxen für die Schweiz?

Stephanie Volz*

A sandbox allows companies to test innovative products, services, and business models in a live market environment. Stemming originally from the FinTech sector, sandboxes have recently gained importance, especially in the context of artificial intelligence, where they are intended to serve to resolve the conflict between data protection and innovation by allowing innovation while ensuring that appropriate safeguards are in place. This paper provides an overview of the provisions of data protection law that inhibit innovation, then delves into the concept of the regulatory sandbox and finally explains how a sandbox program could be implemented in Switzerland.

Inhaltsübersicht

I. Einleitung

Die fortschreitende technologische Entwicklung führt zu zahlreichen innovativen Produkten und Dienstleistungen, die im Idealfall einen positiven Einfluss auf die Menschen und die Umwelt haben. Ein Grossteil dieser Innovationen beruht auf Technologien, die umgangssprachlich als Künstliche Intelligenz («KI») bezeichnet werden. Der Begriff der KI ist jedoch unscharf, es fehlt an einer allgemeinen Definition.[1] Gemeint sind damit in der Regel algorithmische (Entscheid-)Systeme, die ihren Entscheidprozess aufgrund von statistischen Zusammenhängen modifizieren (maschinelles Lernen bzw. Machine Learning).[2]

Ein Unternehmen, welches ein auf innovativen Technologien basierendes Produkt auf den Markt bringen will, sieht sich oft mit dem Problem konfrontiert, dass sich die Chancen und Risiken des Produkts nur schwer abschätzen lassen.[3] Gerade bei Technologien, die auf maschinellem Lernen basieren, lässt sich kaum voraussagen, wie sich die Technologie entwickelt.[4] Dies macht es schwierig, zu beurteilen, ob ein Produkt rechtskonform ist bzw. wie es zu gestal-

* Dr. iur., Geschäftsführerin des Center for Information Technology, Society, and Law (ITSL) Universität Zürich und Rechtsanwältin in Zürich.

1 Dazu der Bericht des Staatssekretariats für Bildung, Forschung und Innovation SBFI, Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» an den Bundesrat, 13. Dezember 2019, 7.

2 *Thouvenin Florent/Früh Alfred,* Automatisierte Entscheidungen, Grundfragen aus der Perspektive des Privatrechts, SZW 2020, 3 ff., 7 m.w.H., *Braun Binder Nadja,* Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ 2019, 467 ff., 473.

3 *Zech Herbert,* Einführung in das Technikrecht, Berlin 2021, 44.

4 *Zech* (Fn. 3), 46.

ten wäre, damit es dem geltenden Recht entspricht.[5] Mit diesem Problem sind auch Behörden konfrontiert, die mit der Überwachung der Rechtmässigkeit der Tätigkeit betraut sind und deren Wissen über die Technologie in der Regel noch geringer sein wird als dasjenige des Unternehmens.[6]

Besonderes Konfliktpotenzial besteht dabei zwischen datengetriebener Innovation und datenschutzrechtlichen Vorgaben, welche der Verwendung von (Personen-)Daten Restriktionen auferlegen. Verschiedene Bestimmungen des Datenschutzrechts erweisen sich in der Praxis als Hindernis für die Entwicklung und Implementierung von innovativen Technologien, Produkten und Geschäftsmodellen (dazu II).

Um die mit einer starken Regulierung verbundenen Innovationshindernisse zu überwinden, wurde im FinTech-Bereich mit sog. Sandboxen eine Möglichkeit für Unternehmen geschaffen, innovative Vorhaben in einer sicheren Umgebung zu testen.[7] Sandboxen gibt es mittlerweile auch in anderen Bereichen. Der Begriff der Sandbox wird jedoch uneinheitlich und für eine breite Palette von Konzepten verwendet. Während an einigen Stellen bereits eine partielle Ausnahme von der Bewilligungspflicht als Sandbox bezeichnet wird, gibt es andernorts ausdifferenzierte Sandbox Programme, bei denen das Testen einer Anwendung in der Sandbox nur ein Teil eines umfassenden Programms ist. Teil III dieses Aufsatzes erläutert den Begriff der Sandbox, zeigt deren charakteristischen Merkmale und gibt einen Überblick über weitere innovationsfördernde Instrumente (dazu III).

Das derzeitige datenschutzrechtliche Regime in der Schweiz lässt die temporäre Modifikation von gesetzlichen Vorgaben nicht zu. Die Einführung einer Sandbox müsste sich deshalb auf die Ausnutzung von gesetzlichen Spielräumen konzentrieren; die einzelfallweise Anpassung von gesetzlichen Vorschriften bedürfte der Einführung einer Experimentierklausel. In Kapitel IV wird der Versuch unternommen, eine mögliche Ausgestaltung einer Sandbox zu skizzieren, wobei darauf hinzuweisen ist, dass bezüglich der optimalen Lösung noch Forschungsbedarf besteht.

II. (Datenschutz-)Rechtliche Hürden für Innovation

1. Grundproblem

Die meisten algorithmischen Systeme bedürfen Daten in irgendeiner Form: sei es als Trainingsdaten oder sei es, weil ein Geschäftsmodell auf der Bearbeitung von Daten beruht. Ob und inwieweit Daten bearbeitet werden dürfen, beurteilt sich in erster Linie nach den Massstäben des Datenschutzrechts.[8] Weil Datenschutzgesetze darauf ausgerichtet sind, die Persönlichkeit der von der Datenbearbeitung betroffenen Person zu schützen und die Datenbearbeitung entsprechend eher eindämmen, wirken sie sich regelmässig hemmend auf die Entwicklung und Verbreitung von datenbasierten Technologien aus.

2. Die Frage nach dem anwendbaren Recht

2.1 Personendaten vs. Nicht-Personendaten

Zu Beginn jeden Vorhabens, das in irgendeiner Form mit Daten zu tun hat, stellt sich die Frage nach der Anwendbarkeit der Datenschutzgesetze. Deren Anwendung knüpft an das Vorliegen von Personendaten an. Dabei handelt es sich um Daten, die sich auf eine bestimmte oder eine bestimmbare Person beziehen (Art. 3 lit. a DSG, Art. 5 lit. a revDSG). Bestimmt oder bestimmbar ist eine Person, wenn sich ihre Identität aus den Daten selbst, aus dem Kontext oder durch eine Kombination mit weiteren Daten ergibt, sofern die Feststellung der Identität ohne unverhältnismässigen Aufwand möglich ist.[9] Als unverhältnismässig gilt der Aufwand, wenn nach der allgemeinen Lebenserfahrung nicht damit zu rechnen ist, dass ein

5 *Krönke Christoph,* Sandkastenspiele – «Regulatory Sandboxes» aus der Perspektive des Allgemeinen Verwaltungsrechts, JZ 2021, 434 ff., 436.

6 *Krönke* (Fn. 5), 436.

7 FCA, Regulatory sandbox lessons learned report, 2017, Ziff. 2.1, abrufbar unter <*https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf*> zuletzt besucht 12.12.2021.

8 In der Schweiz sind dies das eidgenössische Datenschutzgesetz (DSG) und die kantonalen Gesetze, in Europa ist es die Datenschutzgrundverordnung (DSGVO).

9 SHK-DSG-*Rudin,* Art. 3 N 10, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG), Stämpflis Handkommentar, Bern 2015, (zit. SHK-DSG-*Verfasser*).

Interessent diesen auf sich nehmen wird.[10] Zur Beurteilung des Aufwandes sind sowohl der Stand der Technik wie auch die Entwicklungsmöglichkeiten zu berücksichtigen.[11] Von Bedeutung ist auch das Interesse, das die bearbeitende Person an der Identifizierung hat.[12] Die Bestimmbarkeit ist dabei relativ, d.h., sie kann für eine Person vorliegen, für eine andere nicht.[13]

Wird der Personenbezug irreversibel aufgehoben, liegen anonyme Daten vor, deren Bearbeitung nicht mehr den Datenschutzgesetzen unterliegt. Die Anonymisierung selbst ist aber eine Datenbearbeitung, welche dem Datenschutzgesetz unterliegt. Algorithmische Systeme arbeiten oft mit anonymisierten oder pseudonymisierten Daten. Im Zusammenhang mit der technischen Entwicklung wird jedoch immer wieder darauf hingewiesen, dass Irreversibilität aufgrund der heute verfügbaren technischen Möglichkeiten praktisch nicht mehr möglich sei.[14] Je grösser die Datenmenge, desto wahrscheinlicher ist die De-Anonymisierung der Daten.[15]

Aus technischer Sicht ist dem sicherlich zuzustimmen, jedoch kommt bei dieser Beurteilung das genannte Interesse an der Identifizierung zu kurz. Im Rahmen von Forschung und Innovation fallen personenbezogene Daten oft als Nebenprodukte an, oder sie werden zum Trainieren eines Algorithmus benötigt. Die bearbeitenden Personen haben in diesen Fällen kein Interesse daran, die Daten zu re-identifizieren. Deshalb könnte man sich durchaus auf den Standpunkt stellen, dass in diesen Fällen selten Personendaten vorliegen und innovative Projekte damit auch kaum durch die Vorgaben des Datenschutzrechts behindert werden. Die breite Auslegung des Begriffs der Personendaten durch die Behörden und die Angst vor datenschutzrechtlichen Konsequenzen kann aber dazu führen, dass gerade das Gegenteil der Fall ist: Unternehmen gehen im Zweifelsfall von der Anwendung der Datenschutzgesetze aus, was dazu führt, dass gewisse innovative Vorhaben gar nicht erst angegangen werden.

2.2 Kantonales vs. Bundesrecht

Schwierigkeiten kann auch das Auffinden des anwendbaren Datenschutzrechts bereiten. Die Quellen des Datenschutzrechts sind nicht nur im eidgenössischen, sondern auch im kantonalen Recht zu finden.

Das eidgenössische Datenschutzgesetz (DSG) gilt für die Bearbeitung von Personendaten durch Bundesorgane und Privatpersonen (Art. 2 Abs. 1 DSG, Art. 2 Abs. 1 revDSG), wobei für die Bearbeitung durch Privatpersonen und für öffentliche Organe[16] teilweise unterschiedliche Regeln vorgesehen sind. Für kantonale sowie kommunale Behörden gilt das jeweilige kantonale Datenschutzgesetz, im Kanton Zürich das Gesetz über die Information und den Datenschutz (IDG).[17]

Obwohl sich die Vorschriften von Bund und Kantonen an die Datenbearbeitung inhaltlich oftmals entsprechen, gibt es auch relevante Unterschiede, nicht zuletzt bei der aufsichtsrechtlichen Zuständigkeit.[18] Abgrenzungsschwierigkeiten ergeben sich so-

[10] Botschaft zum Bundesgesetz über den Datenschutz, BBl 1988 II 413 ff., 445 (nachfolgend: Botschaft DSG 1988); BSK-DSG-*Blechta,* Art. 3 N 11, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz (DSG)/Öffentlichkeitsgesetz (BGÖ), 3. Aufl., Basel 2014 (zit. BSK-DSG-*Verfasser*); SHK-DSG-*Rudin,* Art. 3 N 10. Daran ändert auch im neuen Recht nichts, vgl. *Rosenthal David,* Das neue Datenschutzgesetz, Jusletter vom 16. November 2020, N 19 f.

[11] BSK-DSG-*Blechta,* Art. 3 N 11; SHK-DSG-*Rudin,* Art. 3 N 10.

[12] SHK-DSG-*Rudin,* Art. 3 N 11; BGE 136 II 508, Erw. 3.2; *Rosenthal David/Jöhri Yvonne,* Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 N 26.

[13] *Rosenthal/Jöhri* (Fn. 12), Art. 3 N 25; BGE 136 II 508, Erw. 3.4.

[14] BSK-DSG-*Blechta,* Art. 3 N 13; SHK-DSG-*Rudin,* Art. 3 N 15; *Weber Rolf H.,* Big Data: Rechtliche Perspektive, in: Weber Rolf H./Thouvenin Florent, Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 20; *Thouvenin Florent,* Forschung im Spannungsfeld von Big Data und Datenschutz: Eine Problemskizze, in: Boehme-Nessler Volker/Rehbinder Manfred, Big Data: Ende des Datenschutzes, Bern 2017, 33; *Weber Rolf H./Oertly Dominic,* Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics, Jusletter IT vom 21. Mai 2015; *Baeriswyl Bruno,* Die Einwilligung hilft (nicht) weiter, digma 2020, 49.

[15] *Weber* (Fn. 14), 20.

[16] Der Begriff der Bundesorgane umfasst nach Art. 3 lit. h DSG (Art. 5 lit. i revDSG) sämtliche Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind.

[17] Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007, ZH LS 170.4.

[18] Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ist zuständig bei Datenbearbeitungen durch Bundesorgane. Datenbearbeitungen durch kantonale und kommunale Organe fallen unter kantonales Recht; die Aufsicht darüber obliegt den kantonalen und

mit einerseits zwischen staatlichen und nicht-staatlichen Datenbearbeitenden sowie andererseits zwischen Datenbearbeitenden des Bundes und der Kantone bzw. der Gemeinden.

Probleme bezüglich der anwendbaren Grundlage akzentuieren sich insbesondere bei kooperativen Projekten zwischen Privaten und öffentlichen Institutionen wie kantonalen oder eidgenössischen Hochschulen, in denen die verschiedenen Gesetze parallel zur Anwendung kommen. Ein Projekt unter Einbindung der Universität Zürich, der ETH Zürich und von privaten Akteuren führt dazu, dass sowohl das DSG mit den allgemeinen Bestimmungen für die Privaten und den besonderen Bestimmungen für Bundesbehörden (ETH) wie auch das IDG zur Anwendung kommen.

3. Rechtmässigkeit der Datenbearbeitung und Ausnahme für Pilotprojekte

Erstes Gebot der Datenbearbeitung ist der Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 DSG, Art. 6 Abs. 1 revDSG). Für private Datenbearbeitende spielt dieser Grundsatz allerdings eine untergeordnete Rolle.[19] Im öffentlich-rechtlichen Bereich bringt der Grundsatz zum Ausdruck, dass für die Datenbearbeitung eine gesetzliche Grundlage erforderlich ist (Art. 17 Abs. 1 DSG, Art. 34 Abs. 1 revDSG), denn öffentliches Handeln unterliegt stets dem Legalitätsprinzip.[20] Für die Bearbeitung von besonders schützenswerten Personendaten ist zudem ein Gesetz im formellen Sinn erforderlich, wobei gewisse Ausnahmen möglich sind (Art. 17 Abs. 2 DSG, Art. 34 Abs. 2 revDSG).[21]

Die Bekanntgabe von Personendaten durch Bundesorgane an Dritte ist ein Unterfall der Datenbearbeitung und einer gesonderten Regelung unterworfen (Art. 19 DSG, Art. 36 revDSG).[22] Die Bestimmung verlangt eine gesetzliche Grundlage, die sich explizit auf die Bekanntgabe beziehen muss.[23] Diese Vorschrift wirkt sich dann negativ auf innovative Projekte aus, wenn diese in Zusammenarbeit mit einem öffentlichen Organ stattfinden oder wenn für ein Projekt Daten verwendet werden sollen, die bei einer öffentlichen Stelle vorhanden sind. Denn für solche Weitergaben fehlt es oft an einer gesetzlichen Grundlage, gerade wenn es sich um Daten handelt, an deren Weiterverwendung bislang kein Interesse bestand.

kommunalen Datenschutzbeauftragten, im Kanton Zürich der Datenschutzbeauftragen des Kantons Zürich.

19 Verlangt wird, dass die Datenbearbeitung nicht gegen eine in der Schweiz geltende Norm verstösst, SHK-DSG-*Baeriswyl,* Art. 4 N 4; *Sprecher Franziska,* Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 2018, 482 ff.; 510, *Epiney Astrid/Civitella Tamara/Zbinden Patricia,* Datenschutzrecht in der Schweiz, Freiburg 2009, N 8. Strittig ist, ob es sich dabei um eine Norm handeln muss, die direkt oder indirekt den Schutz der Persönlichkeit bezweckt, ablehnend SHK-DSG-*Baeriswyl,* Art. 4 N 5; BK-DSG-*Maurer-Lambrou/Steiner,* Art. 3 N 6; a.A. *Rosenthal* (Fn. 10), Art. 3 N 14 mit Verweis auf BVGE, A-3548/2018, Erw. 5.4.4.

20 *Häfelin Ulrich/Müller Georg/Uhlmann Felix,* Allgemeines Verwaltungsrecht, 8. Aufl., Zürich/St. Gallen 2020, N 368 ff. Das Legalitätsprinzip verlangt, dass jegliche staatliche Tätigkeit auf einer gesetzlichen Grundlage basieren muss.

21 Dasselbe gilt im Kanton Zürich (§ 8 IDG). Gemäss IDG muss die Datenbearbeitung zur Erfüllung ihrer gesetzlich umschriebenen Aufgaben geeignet und erforderlich sein (§ 8 Abs. 1 IDG); die Bearbeitung von besonders schützenswerten Personendaten verlangt ausnahmslos eine formellgesetzliche Grundlage (§ 8 Abs. 2 IDG). Als besonders schützenswerte Daten gelten gemäss Art. 3 lit. c DSG Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen einer Person. Im revidierten Recht werden neu auch genetische Daten und biometrische Daten, die eine natürliche Person eindeutig identifizieren, als besonders schützenswert bezeichnet (Art. 5 Abs. 1 lit. c revDSG).

22 *Krönke* (Fn. 5), 46. Der Anwendungsbereich der Bestimmung erstreckt sich auf die Weitergabe an Bundesorgane, an kantonale sowie an kommunale Organe, an ausländische Behörden aber auch an Privatpersonen.

23 *Epiney/Civitella/Zbinden* (Fn. 19), 47; SHK-DSG-*Mund,* Art. 19 N 9; Botschaft DSG 1988 (Fn. 10), 469. Auf die eigenständige Rechtsgrundlage kann verzichtet werden, wenn die Daten für den Empfänger im Einzelfall unentbehrlich sind oder wenn im Einzelfall eine Einwilligung vorliegt (Art. 19 Abs. 1 lit. a und b DSG/Art. 36 Abs. 2 lit. a und b revDSG). Das revidierte DSG erlaubt eine Bekanntgabe zudem, wenn diese notwendig ist, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es nicht möglich ist, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen (Art. 36 Abs. 2 lit. c revDSG). Eine zusätzliche Ausnahme besteht, wenn die betroffene Person ihre Daten allgemein zugänglich gemacht und die Bekanntgabe nicht ausdrücklich untersagt hat (Art. 19 Abs. 2 lit. c DSG/Art. 36 Abs. 2 lit. d revDSG).

Der Gesetzgeber hat zumindest erkannt, dass es im Bereich neuer Technologien nicht immer einfach ist, rechtzeitig eine adäquate gesetzliche Grundlage zu schaffen. Aus diesem Grund wurde Art. 17*a* DSG (Art. 35 revDSG) ins Gesetz aufgenommen, wonach der Bundesrat für eine zeitlich beschränkte Versuchsphase (Pilotprojekt) die automatisierte Datenbearbeitung von besonders schützenswerten Personendaten und anderen sensiblen Datenbearbeitungen bewilligen kann[24] bzw. befugt ist, diese auf Verordnungsstufe zu regeln. Auf diese Weise soll es möglich sein, dass vor dem Erlass eines Gesetzes genügend Erfahrungswerte aus der Praxis vorhanden sind, um die Gesetzesnorm entsprechend ausgestalten zu können.[25] Der Anwendungsbereich der Norm ist zwar begrenzt, doch vermag sie durchaus als Vorbild für eine allfällige Experimentierklausel zu dienen.[26]

4. Zweckbindung, Erkennbarkeit und Informationspflicht

Das Zweckbindungsgebot (Art. 4 Abs. 3 DSG, Art. 6 Abs. 3 revDSG) besagt, dass Daten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Primärzweck). Eine Weiterverwendung von Daten zu einem anderen Zweck (Sekundärzweck) ist nur in Einzelfällen möglich.[27]

Innovative Projekte sind regelmässig auf Daten angewiesen, die bereits vorhanden bzw. von einer anderen Stelle erhoben worden sind, da die Innovatoren weder über die personellen noch über die finanziellen Kapazitäten verfügen, um umfangreiche Datenerhebungen vorzunehmen. Mitunter können sie sich für ihr Vorhaben auch Daten zu Nutzen machen, für die bislang keine Verwendung bestand.[28]

Immerhin wird das Zweckbindungsgebot auf nationaler Ebene mit dem revidierten Datenschutzgesetz insofern etwas gelockert, als auch Datenbearbeitungen zulässig sein sollen, deren Zweck mit dem bei der Beschaffung angegebenen Zweck vereinbar ist (Art. 6 Abs. 3 revDSG). Damit werden auch Sekundärzwecke erlaubt sein, die bei der Beschaffung der Daten zwar nicht erkennbar waren, aber doch vernünftigerweise mit dem Ursprungszweck vereinbar sind.[29]

Der Grundsatz der Zweckbindung wird ergänzt durch den Grundsatz der Erkennbarkeit, wonach die Datenbeschaffung wie auch der Zweck bei der Beschaffung erkennbar sein müssen (Art. 4 Abs. 4

[24] Nach heutigem Recht fallen darunter neben den besonders schützenswerten Daten auch Persönlichkeitsprofile; das neue Recht dehnt den Anwendungsbereich aus, indem neben Profiling auch Datenbearbeitungen erfasst werden, bei denen der Bearbeitungszweck oder die Art und Weise der Datenbearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Personen führen können (Art. 35 Abs. 1 i.V.m. Art. 34 Abs. 2 lit. b und c revDSG).

[25] *Epiney/Civitella/Zbinden* (Fn. 19), 42. Die Anwendung von Art. 17*a* DSG ist an drei Voraussetzungen gebunden: so muss die Aufgabe, die die Bearbeitung der besonders schützenswerten Personendaten bzw. der Persönlichkeitsprofile erforderlich macht, in einem Gesetz im formellen Sinn vorgesehen sein, es müssen Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden, und die praktische Umsetzung der Aufgabe bedarf zwingend einer Testphase vor Inkrafttreten des Gesetzes. Der neue Art. 35 revDSG nimmt gewisse Präzisierungen vor, indem z.B. darauf hingewiesen wird, dass das Gesetz, welches die Aufgabe definiert, welche die Bearbeitung erforderlich macht, in einem bereits bestehenden Gesetz vorgesehen ist. Ausserdem wird lit. c dahingehend erweitert, dass eine Testphase «insbesondere aus technischen Gründen» erforderlich ist. Dies war vorher im aufzuhebenden Abs. 2 von Art. 17*a* DSG enthalten (vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, 7081 [nachfolgend: Botschaft DSG 2017]).

[26] Vgl. dazu hinten IV.2.

[27] SHK-DSG-*Baeriswyl,* Art. 4 N 34, 38 f.; *Thouvenin Florent,* Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: *Weber Rolf H./Thouvenin Florent,* Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 61 ff., 75; *Sprecher* (Fn. 19), 25. Die Möglichkeit «gesetzlich vorgesehen» bezieht sich insbesondere auf öffentliche Institutionen, denn für sie gilt auch hier das Legalitätsprinzip, d.h., eine Abweichung vom ursprünglichen Zweck ist nur möglich, wenn wiederum eine gesetzliche Grundlage dies vorsieht; vgl. SHK-DSG-*Baeriswyl,* Art. 4 N 41, Botschaft DSG 1988 (Fn. 10), 451. Für kantonale und kommunale Organe im Kanton Zürich gilt diesbezüglich § 9 Abs. 1 IDG.

[28] *Klaus Samuel,* KI trifft Datenschutz: Risiken und Lösungsansätze, in: Epiney Astrid/Rovelli Sophia (Hrsg.), Künstliche Intelligenz und Datenschutz, Zürich 2021, 81 ff., 86.

[29] *Rosenthal David,* Die rechtlichen und gefühlten Grenzen der Sekundärnutzung von Personendaten, sic! 2021, 168 ff., 172.

DSG).[30] Zur Gewährleistung der Erkennbarkeit sind zumindest für private Datenbearbeitende Informationspflichten vorgesehen, die im revidierten Recht noch ausgebaut werden.[31] Eine Person, die Daten bearbeitet, muss die davon betroffene Person mindestens über die Identität des Verantwortlichen und über den Bearbeitungszweck informieren.[32] Die Informationspflicht gilt auch bei der indirekten Datenbearbeitung. In diesen Fällen sind die Betroffenen sofort, jedoch spätestens innert eines Monats zu informieren (Art. 19 Abs. 4 revDSG). Ausnahmen von der Informationspflicht sind in diesem Fall nur möglich, wenn die Information nicht möglich ist oder einen unverhältnismässigen Aufwand erfordert (Art. 20 Abs. 2 revDSG).

Noch bestehen gewisse Unsicherheiten, wie ausführlich und in welcher Form der Informationspflicht im Zusammenhang mit der Datennutzung bei algorithmischen Systemen korrekt nachzukommen ist. Das Problem wird dadurch verstärkt, dass sich eine Verletzung der Informationspflicht nicht rechtfertigen lässt und direkt sanktioniert werden kann.[33]

5. Grundsatz der Verhältnismässigkeit

Weiter ist der Grundsatz der Verhältnismässigkeit zu beachten (Art. 4 Abs. 2 DSG, Art. 6 Abs. 2 revDSG). Die Bearbeitung von Personendaten darf nur soweit gehen, wie dies für einen bestimmten Zweck objektiv geeignet und erforderlich ist, und der Zweck der Datenbearbeitung muss in einem vernünftigen Verhältnis zum Eingriff in die Grundrechte des Betroffenen stehen.[34] Daraus ergibt sich der Grundsatz der Datenminimierung, wonach nur diejenigen Daten beschafft und bearbeitet werden dürfen, die für einen Zweck auch tatsächlich benötigt werden.[35] Dies gilt auch in zeitlicher Hinsicht; Daten dürfen nur solange aufbewahrt werden, wie dies zur Erreichung des Zwecks geeignet und erforderlich ist (Speicherbegrenzung).[36]

Diese Vorschrift steht den Interessen einer datengetriebenen Innovation entgegen, da diese oft darauf beruhen, dass Daten für eine längere Dauer zur Verfügung stehen und für Zwecke genutzt werden können, die zum Zeitpunkt der Beschaffung noch nicht bekannt sind. Je nachdem, wie ein System aufgebaut ist und inwiefern eine Korrelation der Daten im Vordergrund steht, ist für ein Projekt jedes einzelne Datum wichtig.[37]

6. Unklare Reichweite des Forschungsprivilegs

Weil an Forschung ein öffentliches Interesse besteht und die Bearbeitung von Daten zu Forschungszwecken in der Regel unbedenklich erscheint, wurde für den Bereich der nicht personenbezogenen Datenbearbeitung (Forschung, Planung und Statistik), eine Sonderregelung geschaffen.[38] Bei Privaten kann der fehlende Personenbezug eine Verletzung der Datenbearbeitungsgrundsätze rechtfertigen (Art. 13 Abs. 2 lit. e DSG; Art. 31 Abs. 2 lit. e revDSG). Der Rechtfertigungsgrund lässt sich auf alle Datenbearbeitungen anwenden, auch auf den Austausch oder die Weiter-

30 Im revidierten Recht wird der Grundsatz der Erkennbarkeit in die Zweckbindung von Art. 6 Abs. 3 revDSG integriert. Im Kanton Zürich findet sich der Grundsatz in § 12 IDG.

31 Bei den Bundesorganen entfällt die Informationspflicht in der Regel, weil regelmässig auf einer gesetzlich vorgesehenen Datenbearbeitung beruht (Art. 20 Abs. 1 lit. b revDSG).

32 Wenn die Daten Dritten bekannt gegeben werden, sind zudem die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern bekannt zu geben (Art. 19 Abs. 2 lit. c revDSG). Bei einer Bekanntgabe ins Ausland sind zudem der Staat oder die Organisation sowie gegebenenfalls Garantien zur Gewährleistung des angemessenen Datenschutzes bekannt zu geben (Art. 19 Abs. 4 revDSG).

33 *Rosenthal* (Fn. 10), N 92.

34 SHK-DSG-*Baeriswyl,* Art. 4 N 21; BSK-DSG-*Maurer-Lambrou/Steiner,* Art. 4 N 9; *Rosenthal/Jöhri* (Fn. 12), Art. 9 N 20; *Thouvenin* (Fn. 14), 34. Im Kanton Zürich sind die Voraussetzungen der Erforderlichkeit und der Eignung ausdrücklich im Gesetz vorgesehen (§ 8 Abs. 1 IDG). Zusätzlich gilt gemäss § 11 IDG der Grundsatz der Vermeidung des Personenbezugs.

35 BSK-DSG-*Maurer-Lambrou/Steiner,* Art. 4 N 11; *Rosenthal/Jöhri* (Fn. 12), Art. 4 N 20.

36 DSG-SHK-*Baeriswyl,* Art. 4 N 23; *Thouvenin* (Fn. 14), 35. Im neuen Gesetz so ausdrücklich vorgesehen, Art. 5 Abs. 4 revDSG.

37 *Sprecher* (Fn. 19), 508; *Baeriswyl Bruno,* Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 45 ff., 46.

38 Botschaft DSG 1988 (Fn. 10), 473. Unter «nicht personenbezogene Zwecke fallen Bearbeitungen, bei welchen nicht das einzelne Individuum, sondern die Eigenschaften der untersuchten Gesamtheit interessieren oder andererseits Forschung, bei welcher zwar die Eigenschaften von einzelnen Individuen von Bedeutung sind, nicht aber deren Identität (BSK-DSG-*Rampini,* Art. 13 N 43).

gabe von Daten zwischen Forschenden.[39] Jedoch ist in jedem Fall eine Abwägung zwischen den Interessen des Bearbeitenden und der betroffenen Personen vorzunehmen.

Auch Bundesorgane dürfen Personendaten für nicht personenbezogene Zwecke verwenden, wenn die Daten frühzeitig anonymisiert werden.[40] In diesem Fall entfällt das Gebot der Zweckbindung wie auch das Erfordernis einer gesetzlichen Grundlage (Art. 22 Abs. 2 DSG, Art. 39 revDSG). Dies gilt auch für die Bekanntgabe von Personendaten, die Daten dürfen also zu nicht zu personenbezogenen Zwecken an Dritte weitergegeben werden.[41] Jedoch ist Art. 22 DSG bzw. Art. 39 revDSG keine gesetzliche Grundlage, um Daten für die Forschung zu erheben. Für die Datenbeschaffung zu Forschungszwecken ist eine separate Gesetzesgrundlage notwendig.[42]

Die Aufzählung der nicht personenbezogenen Anwendungen ist nicht abschliessend. Die Bestimmung liesse sich auch auf weitere, nicht personenbezogene Datenbearbeitungen im Zusammenhang mit algorithmischen Systemen anwenden, wenn sich diese nicht sowieso unter den Begriff der Forschung subsumieren lassen sollten. Inwieweit das Forschungsprivileg jedoch auf die Verwendung neuer Technologien und Geschäftsmodelle Anwendung findet, ist im Einzelfall zu klären. Während es in der Entwicklungsphase wohl noch greift, wird dies bei der Markteinführung nicht mehr der Fall sein.

7. Privacy by Design und Datenschutz-Folgenabschätzung

Im revidierten Datenschutzgesetz wird der Grundsatz des «Privacy by Design» oder des «Datenschutz durch Technik» gesetzlich verankert (Art. 7 revDSG). Der Grundsatz verlangt, dass eine Datenbearbeitung von Anfang an technisch und organisatorisch so auszugestalten ist, dass die Datenschutzvorschriften eingehalten werden.[43] Projekte sind von Beginn an auf ihre Datenschutzkonformität zu überprüfen.

Wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, muss zudem eine Risikoabwägung (Datenschutz-Folgenabschätzung) durchgeführt werden (Art. 22 revDSG). Zeigt sich, dass die Datenbearbeitung ein besonders hohes Risiko mit sich bringt, ist zusätzlich eine Stellungnahme des EDÖB einzuholen (Art. 23 revDSG).

Gerade selbstlernenden Systemen ist eine gewisse Unsicherheit bezüglich ihrer Entwicklung immanent, was die Einhaltung des Grundsatzes des Privacy by Design und die Durchführung einer Datenschutz-Folgenabschätzung mitunter schwierig macht, insbesondere wenn unklar ist, ob es sich bei den verwendeten Daten überhaupt um Personendaten handelt. Selbst wenn ein Unternehmen gewillt ist, den datenschutzrechtlichen Anforderungen bestmöglich nachzukommen, stellt sich die Frage, wie dies im konkreten Einzelfall gewährleistet werden kann.

8. Spezialregeln für automatisierte Einzelfallentscheidung und Profiling

Für gewisse Anwendungsfälle von algorithmischen Systemen hat der Gesetzgeber im revidierten Datenschutzgesetz spezifische Vorkehrungen getroffen, so wurden Vorgaben für automatisierte Einzelfallentscheidungen und für das sog. Profiling ins Gesetz aufgenommen.[44]

Automatisierte Einzelfallentscheide sind grundsätzlich zulässig.[45] Die betroffenen Personen sind aber in der Regel darüber zu informieren, wenn ein Entscheid ausschliesslich auf einer automatisierten Entscheidung beruht und für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt. In diesem Fall besteht ein Recht

[39] BSK-DSG-*Rampini,* Art. 13 N 43. Im revidierten Recht wird die Bestimmung damit ergänzt, dass die Personendaten so schnell als möglich anonymisiert werden oder, wo das einen unverhältnismässigen Aufwand erfordert, angemessene Massnahmen getroffen werden, um die Bestimmbarkeit der betroffenen Personen zu verhindern (Art. 31 Abs. 2 lit. e revDSG).

[40] Dieses Erfordernis wird mit dem revidierten DSG auch für Privatpersonen gelten (Art. 30 Abs. 2 lit. e revDSG).

[41] BSK-DSG-*Maurer-Lambrou/Kunz,* Art. 22 N 34.

[42] BSK-DSG-*Maurer-Lambrou/Kunz,* Art. 22 N 4; SHK-DSG-*Baeriswyl,* Art. 22 N 3.

[43] Botschaft DSG 2017 (Fn. 25), 7029.

[44] Zum Profiling *Roth Simon,* Profiling im neuen Datenschutzrecht, SZW 2021, 34 ff., *Stengel Cornelia/Wirthensohn Gino/Stäuble Luca,* Regulierung von künstlicher Intelligenz für FinTech-Anwendungen – Stand der Diskussion in der Schweiz und im Ausland, SZW 2021, 395 ff., 407.

[45] Es ist unklar, ob gemäss der DSGVO automatisierte Einzelfallentscheide unter gewissen Voraussetzungen verboten sind oder nur einen Anspruch auf menschliche Überprüfung begründen, *Thouvenin/Früh* (Fn. 2), 11 ff. m.w.H., *Rosenthal* (Fn. 10), N 111.

auf menschliche Überprüfung.[46] Ergänzend gilt ein erweitertes Auskunftsrecht: es besteht ein Anspruch auf Information über die Logik, auf welcher die automatisierte Einzelfallentscheidung beruht (Art. 25 Abs. 2 lit. f revDSG).

Bezüglich der Tragweite der Bestimmung bestehen derzeit noch Unklarheiten; dies betrifft insbesondere einzelne Ermessensbegriffe wie z.B. die «erhebliche Beeinträchtigung». Auch wird sich weisen müssen, wie der Auskunftspflicht bezüglich der Logik am besten nachzukommen ist.

Das Profiling ist eine besondere Form der automatisierten Einzelfallentscheidung. Darunter versteht der Gesetzgeber jede Art der automatisierten Bearbeitung von Personendaten, wenn Daten verwendet werden, um bestimmte persönliche Aspekte einer natürlichen Person zu bewerten (Art. 5 lit. f revDSG). Profiling mit hohem Risiko liegt dann vor, wenn das Profiling ein hohes Risiko für die Persönlichkeit oder die Grundrechte mit sich bringt, indem es zu einer Verknüpfung von Daten führt, welche die Beurteilung wesentlicher Aspekte der Persönlichkeit erlaubt (Art. 5 lit. g revDSG). Profiling ist zulässig, jedoch unter gewissen Voraussetzungen mit Rechtsfolgen verknüpft; namentlich muss eine Einwilligung, sofern sie erforderlich ist, stets ausdrücklich erfolgen.

Soweit ein algorithmisches System auf personenbezogenen Daten beruht, wird überwiegend ein Profiling vorliegen.[47] Bei Vorliegen eines hohen Risikos stellt sich die Frage, wie das Einholen einer gültigen ausdrücklichen Einwilligung in einer adäquaten Form am besten gewährleistet werden kann.

III. Ausweg aus dem Dilemma – Sandboxen

1. Grundidee

Sandboxen sind ein vergleichsweise junges Phänomen, sie stammen aus dem Bereich der Finanztechnologie (FinTech). Die erste Sandbox startete in England Ende 2015 und ermöglichte es Unternehmen, ein Produkt auf die Marktfähigkeit zu testen, ohne eine definitive Marktzulassung zu erhalten. Sandboxen finden sich heute überwiegend in stark regulierten Bereichen, welche aufgrund ihres hohen Digitalisierungsgrades innovationsintensiv sind. Solche Märkte sind oftmals geprägt vom fehlenden Verständnis zwischen den Unternehmen, die ihre innovativen Produkte, Dienstleistungen oder Geschäftsmodelle den regulatorischen Anforderungen anpassen müssen, und den Behörden, die zwar über das regulatorische Fachwissen verfügen, aber nicht über ein vertieftes Verständnis der verwendeten Technologien.

Sandboxen sollen dieses Dilemma entschärfen: erstens sollen sie das Bewusstsein der Unternehmen für den bestehenden Rechtsrahmen erweitern, zweitens sollen die Behörden Innovation und die damit verbundenen Risiken und Chancen besser abschätzen können und drittens sollen sie ganz allgemein Innovation fördern.[48] Diese Förderung wird oft schon dadurch bewirkt, dass die Etablierung von Sandboxen als positives, innovationsfreundliches Signal wahrgenommen wird.[49]

Wie vorstehend aufgezeigt, bestehen im Zusammenhang mit Innovationen, die auf algorithmischen Systemen beruhen, insbesondere Konflikte mit den datenschutzrechtlichen Vorgaben. Aus diesem Grund konzentrieren sich die nachfolgenden Ausführungen im Wesentlichen auf eine Sandbox im Bereich des Datenschutzes.

[46] *Thouvenin/Früh* (Fn. 2), 13 f. Informationspflicht und Recht auf Überprüfung durch eine natürliche Person gelten nicht, wenn die Entscheidung in unmittelbarem Zusammenhang mit Abschluss oder Abwicklung eines Vertrags zwischen Verantwortlichem und betroffener Person steht und ihrem Begehren stattgegeben wird oder die betroffene Person ausdrücklich in die Entscheidung eingewilligt hat.

[47] *Klaus* (Fn. 28), 86.

[48] Joint ESA Report on Regulatory Sandboxes and Innovation Hubs, JC 2018 74, 19, 38, <*https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf*> zuletzt besucht am 23.12.21.

[49] *Buckley Ross P./Arner Douglas/Veidt Robin/Zetzsche Dirk,* Building Fintech Ecosystems: Regulatory Sandboxes, Innovation Hubs and Beyond, European Banking Institute Working Paper Series 2019 – no. 53, 55 ff., 58; *Allan Hilary J.,* Regulatory Sandboxes, George Washington Law Review, Vol. 87, 2019, 592.

2. Begriffliches

Obschon das Konzept der Sandboxen inzwischen weit verbreitet ist, fehlt es bislang an einem gemeinsamen Begriffsverständnis.[50] Was unter einer Sandbox verstanden wird, wie sie im Detail ausgestaltet ist und welche Möglichkeiten sie bietet, variiert von Land zu Land und von Branche zu Branche.[51]

Der Begriff «Sandbox» bezeichnet streng genommen nur den Test- oder Experimentierraum bzw. die geschützte Umgebung, in welcher ein Produkt oder eine Anwendung erprobt wird. Dieser Raum ist dabei weit zu verstehen und umfasst beispielsweise auch gesetzlich gewährte Ausnahmen von einer Bewilligungspflicht, etwa wenn sich ein Vorhaben unterhalb eines Schwellenwertes bewegt.

Häufig ist eine Sandbox Teil eines – meist von den Behörden – ins Leben gerufenen Sandbox Programms. In dessen Rahmen werden die zur Verfügung gestellten Mittel, der genaue Ablauf und die Anzahl der Teilnehmenden definiert. Die Vorgaben umfassen das Zulassungsverfahren mit den Kriterien sowie die verschiedenen Stufen inklusive des Abschlussberichts. Ein solches Programm ist meist zeitlich begrenzt; es endet, wenn die beschlossene Anzahl Projekte abgewickelt worden ist. Es können auch mehrere Programme nacheinander stattfinden, beispielsweise zu verschiedenen Themen. Das gesamte Sandbox Programm oder Teile davon werden oft auch als Sandbox bezeichnet.

Mit dem Begriff «Sandbox Projekt» wird sodann das Vorhaben bezeichnet, das in der Sandbox getestet wird. Im Rahmen eines Sandbox Programms können folglich verschiedene Sandbox Projekte parallel oder gestaffelt ablaufen.

3. Optionen zur Verwirklichung einer Sandbox

Sandboxen können sich innerhalb des gesetzlichen Rahmens bewegen und vorhandenen gesetzlichen Spielraum ausnützen oder eine Modifikation des gesetzlichen Rahmens ermöglichen. Im zweiten Fall spricht man von einer Regulatory Sandbox. Grundlage für die temporäre Aufhebung oder Modifikation von gesetzlichen Anforderungen kann eine Experimentierklausel oder ein Innovation Waiver sein.[52]

Die Experimentierklausel ermöglicht den für die Umsetzung oder Durchsetzung eines Gesetzes(komplexes) zuständigen Behörden bei der Erprobung innovativer Technologien, Produkte, Dienstleistungen oder Geschäftsmodelle, von Fall zu Fall unter zeitlicher, geografischer oder thematischer Begrenzung ein gewisses Mass an Flexibilität walten zu lassen. Solche Klauseln können unterschiedliche Formen annehmen, denkbar sind die Einräumung von Auslegungs- und Ermessensspielräumen, mögliche Ausnahmen von (Verbots-)Vorschriften oder von einer Genehmigungspflicht, wie dies insbesondere im Fintech-Bereich oft der Fall ist. Denkbar ist auch, der zuständigen Behörde ein Ermessen darüber zu gewähren, welche Vorschriften für ein Vorhaben konkret angepasst werden.[53]

In eine ähnliche Richtung geht ein sog. Innovation Waiver. Beim Innovation Waiver wird den Behörden jedoch kein Spielraum eingeräumt; vielmehr sieht die gesetzliche Bestimmung selbst einen Verzicht auf bestimmte rechtliche Vorgaben vor.[54] Es handelt sich damit um eine Ausnahmebestimmung, welche eine gewisse Technologie fördern soll. Im Stromrecht gibt es eine datenschutzrechtliche Erleichterung für Netzbetreiber, wenn diese Daten im Rahmen von intelligenten Mess-, Steuer- und Regelsystemen *(Smart Meter/Smart Grids)* bearbeiten. So ist für bestimmte Datenverarbeitungsvorgänge keine Einwilligung der betroffenen Person notwendig (Art. 8 StromVV).[55]

4. Merkmale einer Sandbox

Obschon die bislang verwendeten Sandbox Konzepte unterschiedlich ausgestaltet sind, lassen sich doch gewisse Charakteristika herausarbeiten, welche für das Vorliegen einer Sandbox typisch sind. Diese werden nachfolgend genauer beleuchtet.

50 *Allan* (Fn. 49), 587; *Allan Hilary J.,* Sandbox Boundaries, American University, WCL Research Paper No. 2019-18, 300.

51 *Allan* (Fn. 49), 592; ESA Joint Report (Fn. 48), 16 ff.

52 *Krönke* (Fn. 5), 443.

53 *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 69.

54 Vgl. *Errass Christoph,* Innovationsfördernde Regulierung als Aufgabe des öffentlichen Rechts, ZBl 2010, 203 ff., 215.

55 Dazu *Schreiber Markus,* Rechtliche Innovationssteuerung am Beispiel der Power-to-Gas-Stromspeichertechnologie, Zürich 2019, N 419 m.w.H.

4.1 Geschützter Raum

Meist handelt es sich bei der Sandbox um einen geschützten Raum, in dem ein Produkt, eine Dienstleistung oder ein neues Geschäftsmodell getestet wird. Die Besonderheit der Sandbox liegt darin, dass die Erprobung unter realen (Markt-)Bedingungen, aber nicht auf dem freien Markt erfolgt.

Dieser Test erlaubt den Unternehmen im Allgemeinen eine Abschätzung, ob sich das Vorhaben in einem realen Marktumfeld überhaupt verwirklichen liesse, und gibt Aufschluss über Verbesserungspotenzial. Der Raum schützt aber nicht nur die Unternehmen, auch weitere beteiligte Marktteilnehmer können durch die Begrenzung besser geschützt werden. Bei einem allfälligen späteren Markteintritt lassen sich die erkannten Risiken für alle Beteiligten minimieren.

4.2 Zeitliche, sachliche, örtliche Begrenzung

Sandboxen sind immer einer zeitlichen Beschränkung – der Testphase – unterworfen.[56] Diese kann von wenigen Wochen bis zu mehreren Monaten dauern;[57] sie variiert im Allgemeinen zwischen sechs Monaten und rund zwei Jahren.[58] Die Dauer kann entweder von vornherein festgelegt sein oder zwischen den Behörden und den teilnehmenden Unternehmen im Einzelfall ausgehandelt werden.[59] In der Regel sind Verlängerungen möglich.[60]

Je kürzer die Dauer eines Projekts, desto schneller können die gewonnenen Erkenntnisse in eine möglicherweise neue Regulierung umgesetzt werden;[61] kürzere Projekte sind auch mit weniger Kosten- und Ressourcenaufwand verbunden.[62] Demgegenüber können bei einer längeren Dauer umfangreichere Projekte getestet werden, die auch mit einem grösseren volkswirtschaftlichen Nutzen verbunden sein können.[63]

Die Sandbox unterliegt bisweilen auch sachlichen und/oder örtlichen Begrenzungen, so beispielsweise bezüglich der Anzahl der Teilnehmenden, des örtlichen Marktes, des Testvolumens oder im Hinblick auf bestimmte Personengruppen.[64]

4.3 Aufhebung oder Änderung bestehender gesetzlicher Anforderungen

Ein häufiges Merkmal von Sandboxen ist die Aufhebung oder die Modifikation bestehender Regeln für die Dauer der Testphase.[65] Wenn sich der bestehende gesetzliche Rahmen aufgrund seiner Dichte oder Komplexität innovationshindernd auswirkt, kann durch temporäres Aufheben von Vorschriften die Erprobung einer Technologie oder eines Geschäftsmodells erlaubt werden, die bzw. das sonst nicht genutzt bzw. umgesetzt werden könnte. Auch eröffnet das temporäre Aufheben von Vorschriften Behörden und Gesetzgebern die Möglichkeit, einen modifizierten Lösungsansatz in einem geschützten Umfeld zu testen.[66] Die Modifikation oder Änderung der gesetzlichen Vorgaben basiert auf einer gesetzlichen Grundlage, welche in Form einer Experimentierklausel oder eines Innovation Waiver vorliegen kann.

Um allfällige negative Konsequenzen des abgemilderten Rechtsrahmens abzufedern, sind in der Regel spezifische Schutzmassnahmen zu ergreifen. Diese können aus Massnahmen bestehen, welche allgemein für Sandbox Projekte vorgesehen sind; es sind aber auch zusätzliche individuelle Sicherheitsmassnahmen für ein bestimmtes Vorhaben möglich.[67]

Die Aufhebung bzw. Modifikation bestehender gesetzlicher Anforderungen wird aber nicht überall als zwingend für eine Sandbox verstanden.[68] Bei Sandboxen, welche sich im Bereich von übergeordne-

56 *Ranchordas Sofia,* Experimental Regulations for AI: Sandboxes for Morals and Mores, Morals and Machines, University of Groningen Faculty of Law Research Paper Series, No. 7/2021, 9; *Krönke* (Fn. 5), 435.

57 *Krimphove Dieter/Rohwetter Kerstin,* Regulatory Sandbox – Sandkastenspiele auch für Deutschland, BKR 2018, 494 ff., 495; ESA Joint Report (Fn. 48), 27.

58 *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 63.

59 ESA Joint Report (Fn. 48), 27; *Allan* (Fn. 49), 638; *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 63.

60 *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 63.

61 UVEK, Regulatory Sandboxes – Best Practices für die Schweiz, Bericht vom 28. Februar 2020, 50.

62 *Allan* (Fn. 49), 638.

63 Bericht UVEK (Fn. 61), 50.

64 BIAC (Business at OECD), Regulatory Sandboxes for Privacy Analytical Report, November 2020, 6.

65 *Ranchordas* (Fn. 56), 12; *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 58; *Krimphove/Rohwetter* (Fn. 57), 495.

66 *Krönke* (Fn. 5), 486; BIAC Report (Fn. 64), 13.

67 *Hagen Julia,* Regulatory Sandboxes – Ein Instrument für digitale Innovationen im Gesundheitssektor, in: Pfannstiel Marco A./Kassel Kristin/Rasche Christoph (Hrsg.), Innovationen und Innovationsmanagement im Gesundheitswesen, Wiesbaden 2020, 164 ff., 170.

68 *Krönke* (Fn. 5), 435.

tem – beispielsweise gesamteuropäischem – Recht bewegen, besteht wenig oder gar kein Spielraum für gesetzliche Modifikationen.[69]

4.4 Kooperation mit Behörden

Ein wichtiges Merkmal von Sandboxen ist die behördliche Begleitung bzw. die Kooperation von Behörden und teilnehmenden Unternehmen.[70] Der Austausch findet über die gesamte Laufzeit eines Projektes statt.

Von Seiten der Behörden werden den Unternehmen über das gesamte Verfahren hinweg spezifische Interpretationshilfen zur Verfügung gestellt, wie sie ein Vorhaben rechtlich beurteilen. Gegebenenfalls bieten sie auch Lösungsvorschläge für aufkommende Probleme.[71] Damit diese enge Begleitung möglich ist, müssen die Unternehmen gewissen Informations- und Berichterstattungspflichten nachkommen.[72]

Doch nicht nur die Unternehmen, auch die Behörden profitieren von der Zusammenarbeit. Durch den regelmässigen Austausch sind sie in der Lage, eine allfällige Aufsichtsfunktion besser wahrzunehmen. Sie erhalten vertiefte Einblicke in die praktische Anwendung des Rechts auf einen spezifischen Fall und sind entsprechend in der Lage, potenzielle Gefahren im Vorfeld zu erkennen und darauf zu reagieren, ohne dass durch ihr Handeln ein Gesetzesverstoss und damit verbunden allenfalls auch ein Schaden für den Einzelnen oder die Allgemeinheit entstanden ist.[73] Durch den Austausch entsteht ein Erkenntnisgewinn für ähnlich gelagerte Anwendungsfälle oder für eine Anpassung der Gesetzgebung.[74]

5. Ablauf eines Sandbox Projekts

5.1 Zulassungsverfahren und -kriterien

Die Durchführung eines Sandbox Programms ist mit beträchtlichem personellem und sachlichem Aufwand seitens der Behörden verbunden. Deshalb kann die Sandbox nur für eine beschränkte Anzahl interessierter Unternehmen offenstehen. Nur so kann auch gewährleistet werden, dass für ein Projekt genügend Ressourcen zur Verfügung stehen.[75] Auch sind nicht alle Innovationsprojekte für eine Sandbox geeignet.

Aus diesem Grund muss ein interessiertes Unternehmen gewisse Zulassungskriterien für die Teilnahme erfüllen.[76] Die Kriterien sind im Vorfeld zu veröffentlichen, nicht zuletzt, um dadurch das öffentliche Vertrauen zu fördern.[77] Wichtig ist, dass die Kriterien sachlich gerechtfertigt sind. Neben den Kriterien sind auch eine allfällige maximale Anzahl Teilnehmende und ein allfälliger Auswahlmechanismus im Vorfeld bekannt zu geben. Denn nur so lässt sich die Ungleichbehandlung bzw. die Schlechterstellung derjenigen Marktakteure rechtfertigen, die nicht an der Sandbox teilnehmen können.[78]

Obschon die Zulassungskriterien in der Praxis unterschiedlich sind, lassen sich doch gewisse Gemeinsamkeiten erkennen. Als erste Voraussetzung müssen die Vorhaben, die in der Sandbox getestet werden sollen, regelmässig innovativ sein. Die Umschreibung des Begriffs ist schwierig; meist wird er mit «neu» verbunden, so müssen neues Wissen und damit verbunden neue Produkte oder Dienstleistungen geschaffen werden.[79] Bei der Beurteilung besteht

69 ESA Joint Report (Fn. 48), 38. Dies ist insbesondere im Datenschutzrecht der Fall, wo mit der DSGVO ein verbindlicher Rahmen besteht. KI Sandboxen, wie sie bereits in England oder Dänemark existieren, müssen sich folglich darauf beschränken, die europäischen datenschutzrechtlichen Vorgaben optimal zu implementieren (Privacy by Design). Vgl. dazu hinten II.5.1.

70 *Ranchordas* (Fn. 56), 9; Bericht UVEK (Fn. 61), 17; *Krimphove/Rohwetter* (Fn. 57), 495.

71 Sog. Individual Guidance; *Krönke* (Fn. 5), 436.

72 *Krönke* (Fn. 5), 440.

73 BIAC Report (Fn. 64), 13; *Krönke* (Fn. 5), 441.

74 *Krönke* (Fn. 5), 486.

75 *Krimphove/Rohwetter* (Fn. 57), 496; FCA Lessons learned report (Fn. 7), 3.

76 *Krönke* (Fn. 5), 436; *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 58; ESA Joint Report (Fn. 48), 22.

77 BIAC Report (Fn. 64), 19.

78 *Ranchordas* (Fn. 56) 10, 15; *Hummel Konrad,* Recht der behördlichen Regulierungselemente, Berlin, 2003, 121; *Krönke* (Fn. 5), 436. *Krimphove/Rohwetter* (Fn. 57), 486.

79 Gemäss der Definition der ICO muss «neues Wissen auf die Produktion von Waren und Dienstleistungen angewendet werden und zu einer verbesserten Produktqualität oder zu effizienteren Prozessen führen», vgl. *<https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/how-will-the-ico-assess-applications-for-the-sandbox/>;* gemäss der norwegischen Digital Agency ist bei Innovation etwas neu zu aktualisieren oder neu zu schaffen, um einen Mehrwert für Organisationen, die Gesellschaft oder die Allgemeinheit zu schaffen. Innovation ist experimenteller Natur, und die Lösungen sind nicht im

ein grosser Ermessensspielraum der Behörden. Mitunter wird kritisiert, dass diese überhaupt nicht beurteilen können, ob ein Produkt innovativ ist.[80]

Weil sie staatliche Ressourcen binden, müssen Sandbox Projekte im öffentlichen Interesse liegen bzw. für die Gesellschaft, Konsumenten oder die beteiligten Personen einen Nutzen generieren.[81] Der verlangte gesellschaftliche Mehrwert ist oft bereits im Innovationsbegriff enthalten.[82] Der Nutzen kann sich beispielsweise in geringeren Kosten, effizienteren Verfahren oder auch im Zugang zu neuen Produkten oder Dienstleistungen manifestieren.[83]

Häufig wird auch verlangt, dass die Sandbox Projekte von den durch die Behörden bereitgestellten Dienstleistungen, bspw. die detaillierte Beratung, überhaupt profitieren können.[84] So müssen sich etwa gewisse Schwierigkeiten bei der rechtlichen Beurteilung ergeben. Wo in der Sandbox gewisse Modifikationen der gesetzlichen Anforderungen möglich sind, haben die Unternehmen darzulegen, weshalb ein Projekt nicht im gesetzlich vorgegebenen Rahmen realisiert werden kann.[85]

Eine weitere Voraussetzung ist, dass die Unternehmen und die von ihnen vorgeschlagenen Produkte oder Dienstleistungen für die Sandbox bereit sind (sog. Testreife).[86] Das Projekt muss folglich weit genug fortgeschritten sein, um in die Testphase zu gehen, und das Unternehmen muss in der Lage sein, ausreichend Ressourcen für das Projekt zur Verfügung zu stellen.[87]

Formal haben die interessierten Unternehmen eine Bewerbung an die zuständige Behörde zu richten, in welcher sie darlegen, inwiefern das von ihnen eingereichte Projekt die Zulassungskriterien erfüllt.[88] Oft gibt es feste Zeitfenster, um sich zu bewerben (Ausschreibung), weil diese den Behörden eine effiziente und gleichmässige Nutzung der vorhandenen Ressourcen ermöglichen.[89] Es gibt aber auch Sandboxen, an denen man jederzeit teilnehmen kann.[90]

5.2 Vorbereitung und Testphase

Wenn das Projekt die Zulassungsvoraussetzungen erfüllt und in das Sandbox Programm aufgenommen wird, beginnt die Vorbereitungsphase, in der das Unternehmen und die Behörden die Parameter des durchzuführenden Testverfahrens festlegen, Massnahmen zum Schutz von betroffenen Personen entwickeln und allfällige Exitstrategien definieren. Auch Regeln zur Beurteilung von Erfolg oder Misserfolg des Tests sind zu vereinbaren.[91] In dieser Phase wird dem Unternehmen meist ein bestimmter Mitarbeitender (Case Manager) zugeteilt, der sich vertieft mit der Materie befasst.

Sobald die Eckpunkte festgelegt worden sind, beginnt die zeitlich festgelegte Testphase in der Sandbox.[92] Während der Testphase sind die Unternehmen und die Behörden in einem engen Dialog; das Unternehmen berichtet den Behörden laufend über die Einhaltung der vereinbarten Vorgaben, Massnahmen und Kriterien.[93] Wenn wichtige Vorgaben nicht mehr eingehalten werden können, hat die zuständige Behörde jederzeit die Möglichkeit, das Projekt zu been-

Voraus bekannt. In diesem Zusammenhang umfasst Innovation auch technologische Innovationen oder innovative neue Arten von Dienstleistungen oder Produkten. Gerade im Bereich von KI Sandboxen sind darunter auch innovative Lösungen für den Schutz der Privatsphäre zu verstehen, vgl. dazu <*https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/framework-for-the-regulatory-sandboxgeneral-participation-criteria/*>, zuletzt besucht 13.12.2021.

80 *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 58; *Allan* (Fn. 49), 616.

81 BIAC Report (Fn. 64), 6; ESA Joint Report (Fn. 48), 23; vgl. Information Commissioner's Office (ico.), Sandbox assessment criteria indicators, abrufbar unter <*https://ico.org.uk/media/for-organisations/documents/2618128/sandbox-criteria-indicators.pdf*> auch <*https://www.cnil.fr/fr/bac-a-sable-2021*> zuletzt besucht am 10.12.2021.

82 Vgl. dazu die Definitionen des ICO oder des Datatilsynet in Fn 79.

83 *Allan* (Fn. 49), 627.

84 ESA Joint Report (Fn. 48), 24.

85 ESA Joint Report (Fn. 48), 24.

86 ESA Joint Report (Fn. 48), 22; *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 58; *Krönke* (Fn. 5), 442.

87 *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 63; Vgl. z.B. <*https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/framework-for-the-regulatory-sandbox/*> zuletzt besucht 12.12.2021.

88 *Krimphove/Rohwetter* (Fn. 57), 495; ESA Joint Report (Fn. 48), 23; *Allan* (Fn. 49), 626. Bei den Kriterien gilt insbesondere die Innovationskraft als kritisch und wird auch verschieden beurteilt. Oft ist es für die Behörden schwierig zu erkennen, was innovativ ist und was nicht, vgl. auch *Allan* (Fn. 49), 626.

89 Bericht UVEK (Fn. 61), 58.

90 ESA Joint Report (Fn. 48), 22.

91 *Krimphove/Rohwetter* (Fn. 57), 495; ESA Joint Report (Fn. 48), 25.

92 Vgl. dazu oben III.2.1.

93 *Krimphove/Rohwetter* (Fn. 57), 496.

den und Massnahmen gegen das Unternehmen zu ergreifen.[94]

5.3 Abschluss

Am Ende des Projekts haben die Unternehmen einen Abschlussbericht einzureichen, worin sie die wesentlichen Erkenntnisse aus dem Sandbox Projekt zusammenfassen. Der Bericht soll Rechenschaft darüber ablegen, was in der Sandbox ablief, um das Vertrauen in das Verfahren zu erhöhen. Die Berichte werden deshalb in geeigneter Form auch der Öffentlichkeit zur Verfügung gestellt.[95]

Das Ende des Projekts ist nicht notwendigerweise das Ende der Zusammenarbeit. Im Idealfall dient die Sandbox als Vorbereitung für den Marktzutritt, welcher nach dem Programm unter Einhaltung aller regulatorischen Vorgaben erfolgen kann.[96] Auch während dieser Transition kann eine Zusammenarbeit von Behörden und Unternehmen sinnvoll sein.

6. Begleitende Instrumente

6.1 Allgemeines

Sandboxen sind nur eine von verschiedenen Möglichkeiten zur Gestaltung eines innovationsfreundlichen Umfeldes. In der Praxis haben sich weitere Instrumente herausgebildet, die auch bei Sandbox Programmen Anwendung finden können.

6.2 Behördliche Rechtsberatung und Innovation Hub

Die Inanspruchnahme einer behördlichen Rechtsberatung ist in zahlreichen Rechtsgebieten möglich. Am bekanntesten ist die Rechtsberatung im Steuerrecht, in welchem mit dem Steuerruling sogar eine verbindliche Auskunft eingeholt werden kann.[97] Ferner gibt es für Unternehmen im Kartellrecht die Möglichkeit einer (unverbindlichen) Beratung des Sekretariats der Wettbewerbskommission.[98] Auch im eidgenössischen Datenschutzrecht ist eine Beratung vorgesehen (Art. 28 DSG, Art. 58 Abs. 1 lit. a revDSG). Diese Beratungen haben sich in jüngerer Zeit verändert, und der EDÖB ist dazu übergegangen, auf Wunsch von Privaten umfassende Projekte, welche mit der Bearbeitung grosser Datenmengen verbunden sind, beratend zu begleiten.[99]

Ein Innovation Hub geht über normale Beratung hinaus. Es handelt sich dabei um einen strukturierten Beratungsprozess. Die Innovatoren erhalten fundierte (nicht bindende) Einschätzungen zur rechtlichen Beurteilung ihrer Produkte oder Dienstleistungen von spezialisiertem Personal mit der entsprechenden technischen Expertise.[100] Sie sind einer Sandbox oft vorgelagert und können Aufschluss darüber geben, ob die Teilnahme am Sandbox Programm überhaupt notwendig ist.

Der Innovation Hub beschränkt sich jedoch auf den technischen und rechtlichen Beratungsprozess; weder werden Unternehmen über einen längeren Zeitraum begleitet, noch können die gesetzlichen Rahmenbedingungen angepasst werden.[101] Umgekehrt bedarf die Schaffung eines Innovation Hub nicht zwingend einer gesetzlichen Grundlage, die allgemeinen gesetzlich definierten Aufgaben von Behörden lassen sich als Legitimation heranziehen.[102]

6.3 No Action Letter

Auch No Action Letters (auch: No Enforcement Letters) sind ein Instrument, welches Sandboxen oft begleitet. Dabei handelt es sich um Zusagen von Behörden, keine aufsichtsrechtlichen Massnahmen zu ergreifen, solange sich die Unternehmen an die getroffenen Vereinbarungen bzw. an die von den Behörden vorgegebenen Interpretationshilfen der anwendbaren Gesetze halten.[103] Dies gibt den Betroffenen Rechts-

94 ESA Joint Report (Fn. 48), 27.

95 ESA Joint Report (Fn. 48), 29 f., BIAC Report (Fn. 64), 8; z.B. die Exit Reports der ICO Regulatory Sandbox, abrufbar unter <*https://ico.org.uk/for-organisations/regulatory-sandbox/previous-participants/*> zuletzt besucht 10.12.2021.

96 *Allan* (Fn. 49), 639.

97 Vgl. dazu § 132 des Steuergesetzes des Kantons Zürich (LS 631.1).

98 Vgl. Art. 23 des schweizerischen Kartellgesetzes (SR 251).

99 Vgl. dazu Nr. 24, Tätigkeitsbericht 2016/2017 des EDÖB, abrufbar unter <*https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/24--taetigkeitsbericht-2016-2017/aktuelle-herausforderungen-und-schwerpunkte.html*> zuletzt besucht am 12.12.2021.

100 Bericht UVEK (Fn. 61), 8; ESA Joint Report (Fn. 48), 7. *Buckley/Arner/Veidt/Zetzsche* (Fn. 49), 58; Bericht UVEK (Fn. 61), 17; ESA Joint Report (Fn. 48), 8.

101 Bericht UVEK (Fn. 61), 17.

102 ESA Joint Report (Fn. 48), 8.

103 *Krimphove/Rohwetter* (Fn. 57), 496; *Hagen* (Fn. 67), 169.

und Planungssicherheit, insbesondere in den Fällen, in denen unsicher ist, wie ein Geschäftsmodell rechtlich zu behandeln ist. Durch den No Action Letter erhalten die Unternehmen die Bestätigung, dass während der Erprobung in der Sandbox von einer Rechtsdurchsetzung abgesehen wird.[104]

No Action Letters kommen sowohl bei klassischen Sandboxen, bei welchen gesetzliche Vorgaben angepasst werden, als auch bei Sandboxen, die sich innerhalb der rechtlichen Vorgaben bewegen, vor. In diesem Fall gibt die Behörde eine Zusicherung ab, dass sie das geplante Vorhaben als rechtmässig beurteilt.

7. Bisherige Erfahrungen und Entwicklung

7.1 Beispiele aus Europa

Inzwischen haben zahlreiche Länder Sandboxen oder ähnliche Programme ins Leben gerufen, einige werden hier beispielhaft kurz erläutert. England gilt als Vorreiter für die Entwicklung von Sandboxen. Bereits 2015 wurde im Finanzsektor das Sandbox Programm der Financial Conduct Authority (FCA), der britischen Finanzmarktaufsichtsbehörden, eingeführt. Im Rahmen der Sandbox erhalten die beteiligten Unternehmen Unterstützung bei der Interpretation der bestehenden Regeln und deren Anwendung (Individual Guidance).[105] Während der Dauer des Experiments erhalten sie einen No Action Letter, in welchem die FCA zusichert, dass keine Massnahmen der Rechtsdurchsetzung, wie z.B. Sanktionen, ergriffen werden, wenn sich die Teilnehmenden an die Vorgaben der Individual Guidance halten. Die FCA hat zudem die Möglichkeit, punktuell und temporär bestimmte Vorschriften aufzuheben oder anzupassen.[106]

Aufgrund der guten Erfahrungen mit der Sandbox initiierte das Information Commissioner's Office (ICO), die britische Datenschutzaufsichtsbehörde, 2019 eine Sandbox Initiative für KI-Anwendungen, welche die Einhaltung der Vorgaben des Datenschutzes garantieren und Innovation unterstützten soll.[107] Die teilnehmenden Unternehmen haben die Möglichkeit, mit dem Sandbox Team des ICO zu interagieren und so von Anfang an «Data protection by Design» zu ermöglichen.[108] Auch in Norwegen und Frankreich sind Initiativen zur Umsetzung von Sandboxen im KI-Bereich lanciert worden. Das Ziel der norwegischen Sandbox ist es, bei den Anwendungen das Gebot von Privacy by Design zu verwirklichen, indem Lösungen gefunden werden, welche den datenschutzrechtlichen Anforderungen genügen; weitergehende Möglichkeiten gibt es nicht, weil die DSGVO keinen Spielraum für Anpassungen oder Aufhebungen von grundlegenden Vorschriften gibt.[109] Zwar enthält die DSGVO gewisse Öffnungsklauseln, die in bestimmten Bereichen eine nationale Regelung zulassen, wie z.B. Art. 89 Abs. 2 DSGVO; dieser Spielraum wurde von den Mitgliedstaaten jedoch noch wenig genutzt. Immerhin ermöglicht das norwegische Modell, während der Entwicklungsphase auf Vollstreckungsmassnahmen zu verzichten.[110] Eine ähnliche Lösung besteht in Frankreich, auch diese Lösung ist darauf ausgerichtet, dem Prinzip des Privacy by Design von Anfang an zu genügen.[111] Den verschiedenen KI Sandboxen ist gemein, dass keine Aufhebung oder Modifikation bestehender Vorschriften vorgesehen ist.

7.2 Sandboxen in der Schweiz

In der Schweiz gibt es eine Sandbox bzw. einen Innovationsraum im FinTech-Bereich. Damit Fin-Tech-Start-ups weniger schnell einer Bewilligungspflicht gemäss Bankengesetz unterliegen, wurde eine Ausnahme von der Gewerbsmässigkeit vorgenommen.[112]

104 *Hagen* (Fn. 67), 170; *Krimphove/Rohwetter* (Fn. 57), 496; *Krönke* (Fn. 5), 437.

105 FCA Lessons learned report (Fn. 7), 1.1; *Hagen* (Fn. 67), 169.

106 FCA Lessons learned report (Fn. 7), 1.1; *Krönke* (Fn. 5), 436; *Hagen* (Fn. 67), 169.

107 *Krönke* (Fn. 5), 436; vgl. Informationen zur ICO Sandbox *<https://ico.org.uk/for-organisations/regulatory-sandbox/>* zuletzt besucht 12.12.21.

108 ICO Sandbox, *<https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/>*.

109 ESA Joint Report (Fn. 48), 5; vgl. dazu auch *<https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/framework-for-the-regulatory-sandbox/what-are-the-relevant-regulations/>* zuletzt besucht am 12.12.21.

110 Vgl. Framework of the Sandbox *<https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/framework-for-the-regulatory-sandbox/>* zuletzt besucht am 12.12.21.

111 Vgl. dazu *<https://www.cnil.fr/fr/bac-a-sable-2021>* zuletzt besucht am 12.12.21.

112 Vgl. dazu *Mauchle Yves,* Die regulatorische Antwort auf FinTech: Evolution oder Revolution? Eine Verortung aktueller Entwicklungen, SZW 2017, 810 ff., 819; vgl. auch *Reiser Nina,* Ist der Bankbegriff im Lichte aktueller techno-

Werden gesamthaft Publikumseinlagen von höchstens CHF 1 Mio. zur Weiterleitung entgegengenommen, liegt keine Bewilligungspflicht vor, weil die Tätigkeit nicht als gewerbsmässig gilt (Art. 6 Abs. 2 lit. a BankV). Derzeit läuft in der Schweiz die Revision des Stromversorgungsgesetzes, in dessen Rahmen die Einführung einer Sandbox geplant ist.[113]

7.3 Sandboxen in der KI-VO

Auch die Europäische Kommission hat die Vorteile von Sandboxen erkannt und Vorschriften zur Errichtung von Sandboxen in den Vorschlag zur Regulierung von künstlicher Intelligenz **(E-KI-VO)**[114] aufgenommen. Die E-KI-VO enthält verschiedene Durchbrechungen und Abmilderungen der strengen Vorgaben der DSGVO, beispielsweise hinsichtlich des Zweckbindungsgrundsatzes. So können zu anderen Zwecken erhobene Daten in der Sandbox als Trainingsdaten genutzt werden, solange das zu entwickelnde System öffentlichen Interessen dient (Art. 54 E-KI-VO)[115]. Für diese Zwecke können selbst besonders schützenswerte Personendaten wie Gesundheitsdaten herangezogen werden.[116] Voraussetzung ist jedoch, dass die angestrebten Ziele nicht mit synthetischen oder anonymisierten Daten erreicht werden können.

Als Sicherheitsmassnahmen werden verschiedene Massnahmen statuiert, welche die Risiken für den Datenschutz minimieren sollen. Vorgesehen ist auch ein strenges Haftungsregime.[117] Die Regelung der konkreten Details ist indessen den Mitgliedstaaten überlassen. Um eine mögliche Fragmentierung der Sandbox Regulierung zu verhindern, sieht der Entwurf Kooperations- und Koordinationsmassnahmen für Staaten vor, welche Sandboxen einführen (Art. 53 Abs. 5 E-KI-VO).

IV. Sandboxen in der Schweiz

1. Derzeitige Rechtslage

Wie die vorstehenden Ausführungen gezeigt haben, gibt es in der Schweiz zwar durchaus innovationsfördernde Gesetzgebung; zumindest im Bereich des Datenschutzes existiert derzeit aber noch keine Sandbox. Weder die datenschutzrechtlichen Aufsichtsbehörden noch andere Behörden des Bundes oder der Kantone haben die Möglichkeit, gesetzliche Anforderungen zu modifizieren. Auch eine verbindliche Auskunft bzw. ein vorgängiger Verfolgungs- und Sanktionsverzicht sind nicht vorgesehen.

Immerhin besteht die Möglichkeit einer Beratung durch den Datenschutzbeauftragten (Art. 29 DSG, Art. 58 Abs. 1 lit. a revDSG). Gemäss neuem Recht können auch Bundesorgane die Beratung in Anspruch nehmen; bis jetzt steht eine solche nur privaten Personen zu.[118] Die Beratung ist aber unverbindlich, auch für den Datenschutzbeauftragten selbst; er kann in einem allfälligen Aufsichtsverfahren eine von der Beratung abweichende Rechtsauffassung vertreten.[119]

2. *De lege lata:* Ausnutzung rechtlicher Spielräume

Obschon sich die gesetzlichen Anforderungen nicht immer ohne Weiteres auf innovative Technologien anwenden lassen, gibt es auch im Rahmen des geltenden Rechts gewisse Spielräume, die man sich bei der Erprobung von neuen Produkten, Dienstleistungen oder Geschäftsmodellen zu Nutze machen kann.

logischer Entwicklungen noch zeitgemäss, AJP 2018, 818 ff., 818.

113 Vgl. dazu <*https://www.bfe.admin.ch/bfe/de/home/versorgung/stromversorgung/stromversorgungsgesetz-stromvg.html*> zuletzt besucht 12.12.21.

114 Abrufbar unter <*https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206*> zuletzt besucht 13.12.2021.

115 Als öffentliche Interessen werden beispielsweise die Strafverfolgung, die Verbrechensbekämpfung, die Gewährleistung der öffentlichen Sicherheit und Gesundheit, insbesondere die Bekämpfung von Krankheiten, oder auch die Verbesserung des Umweltschutzes genannt.

116 Art. 10 Abs. 5 E-VO-KI sieht vor, dass für das Training von KI im Gesundheitsbereich über den «European Health Data Space» Zugang zu relevanten Gesundheitsdaten eröffnet werden soll, dies allerdings unter institutioneller Aufsicht und unter Einhaltung spezifischer Sicherheitsbestimmungen. – Einschränkung des generellen Verarbeitungsverbots von Art. 9 DSGVO. Vor der Verarbeitung muss explizit keine Anonymisierung vorgenommen werden, wenn dies den verfolgten Zweck erheblich beeinträchtigen würde (Art. 10 Abs. 5 KI-VO).

117 Vgl. Art. 54 lit. c–h E-KI-VO; *Gerald Spindler,* Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung von künstlicher Intelligenz (KI-VO-E), CR 2021, 361 ff.

118 SHK-DSG-*Baeriswyl,* Art. 28 N 4.

119 SHK-DSG-*Baeriswyl,* Art. 28 N 13.

2.1 Vermeidung der Anwendung des Datenschutzrechts

Datenschutzrechtliche Bestimmungen finden nur Anwendung, wenn Personendaten, d.h. Daten mit Personenbezug, vorliegen. Oft lassen es innovative Geschäftsmodelle zu, dass man mit anonymen oder pseudonymisierten Daten arbeitet. Die Anonymisierung kann eine Möglichkeit sein, wenn die verwendete Technologie selbst nicht auf personenbezogenen Daten beruht, diese aber als Nebenprodukt anfallen, z.B. eine Kamera, die auch mit Sensoren arbeiten kann. Wenn die Verwendung anonymer Daten nicht möglich ist, kann bisweilen auch mit synthetischen Daten gearbeitet werden, die in der Regel die fast gleiche Datenqualität aufweisen wie personenbezogene Daten.[120] Es ist jedoch zu beachten, dass die Umwandlung eines Datensatzes mittels Algorithmus eine Datenbearbeitung darstellt, welche dem Datenschutzgesetz unterliegt.

Die Entfernung des Personenbezugs ist aber insbesondere mit zwei Problemen behaftet: Erstens sind gewisse Anonymisierungstechniken, wie die Aggregierung, mit einem Verlust an Datenqualität verbunden. Zweitens besteht auch die jederzeitige Gefahr der De-Anonymisierung.[121]

2.2 Rechtfertigung einer Verletzung von Datenbearbeitungsgrundsätzen

Die Widerrechtlichkeit, die sich bei der Verletzung eines Datenbearbeitungsgrundsatzes ergibt, lässt sich beim Vorliegen eines Rechtfertigungsgrundes zumindest für Private heilen (Art. 13 DSG, Art. 31 revDSG). Das Gesetz sieht drei Rechtfertigungsgründe vor, es sind dies die Einwilligung des Verletzten, das überwiegende private oder öffentliche Interesse oder eine gesetzliche Vorgabe.

Wenn nicht mit anonymisierten Daten gearbeitet werden kann, setzen Unternehmen in der Praxis für die Datenbearbeitung oft auf die Einwilligung der betroffenen Person; Bundesorgane hingegen dürfen Personendaten nur im Zweifelsfall gestützt auf die Einwilligung bearbeiten (Art. 17 Abs. 2 lit. c DSG).[122] Dabei sind die Voraussetzungen einer gültigen Einwilligung zu beachten; diese muss namentlich bestimmt sein, d.h. für eine spezifische Datenbearbeitung erteilt werden (Art. 4 Abs. 5 DSG, Art. 6 Abs. 6 revDSG). Für welche spezifische Bearbeitung Daten später genutzt werden, ist aber nicht immer im Vornherein bekannt. Gerade bei der Sekundärnutzung sollen Daten für Zwecke genutzt werden, die bei der Beschaffung noch nicht bekannt waren.[123]

Ein weiterer Rechtfertigungsgrund ist das Vorliegen überwiegender privater oder öffentlicher Interessen, worunter gemäss Art. 13 Abs. 2 lit. a DSG (Art. 31 revDSG) beispielsweise die Bearbeitung zum Abschluss und zur Abwicklung eines Vertrages zählt; dabei muss zwischen der Datenbearbeitung und dem Vertrag jedoch ein unmittelbarer Zusammenhang bestehen.[124] Wie bereits erwähnt, kommt bei Privaten auch die Datenbearbeitung zu Forschungszwecken als Rechtfertigungsgrund in Betracht.[125]

Neben den in den Gesetzen genannten Fällen gibt es weitere Beispiele von überwiegendem Interesse, wobei in diesen Fällen eine Abwägung zwischen den Interessen des Datenbearbeiters und der betroffenen Person vorzunehmen ist.[126] Die Abwägung der Interessen erfolgt jeweils konkret für den Einzelfall.[127] Es lassen sich keine pauschalen Aussagen darüber machen, wann die Interessenabwägung zugunsten der bearbeitenden Unternehmen ausfällt, sie tun aber gut daran, insbesondere dem Problem der Verhältnismässigkeit Rechnung zu tragen und die Daten nur soweit zu bearbeiten wie notwendig. Zudem sind, wann immer möglich, zusätzliche Vorkehrungen zum Schutz der Persönlichkeit der betroffenen Personen zu ergreifen, z.B. durch besondere Sicherheitsmassnahmen.

2.3 Problem: Keine Rechtssicherheit

Das Ausnützen rechtlicher Spielräume ist in der Praxis nicht unproblematisch. Insbesondere wenn es um die Interessenabwägung im Rahmen der Rechtfertigungsgründe geht, verfügen die beurteilenden Be-

120 Vgl. dazu BITKOM, Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens, abrufbar unter <*https://www.bitkom.org/sites/default/files/2020-10/201002_lf_anonymisierung-und-pseudonymisierung-von-daten.pdf*> zuletzt besucht 3.1.2022.

121 Vgl. dazu vorne II.2.1.

122 Grund dafür ist, dass die staatliche Datenbearbeitung immer einen Eingriff in die Grundrechte bedeutet; sie soll auch nicht freiwillig erfolgen (vgl. *Baeriswyl* [Fn. 14], 63).

123 Vgl. dazu vorne II.4.

124 SHK-DSG-*Wermelinger,* Art. 13 N 20.

125 Vgl. dazu vorne II.2.6.

126 SHK-DSG-*Wermelinger,* Art. 13 N 8.

127 BK-DSG-*Rampini,* Art. 13 N 24.

hörden über viel Ermessensspielraum. Für die Unternehmen verbleibt grosse Rechtsunsicherheit.

3. *De lege ferenda:* Mögliche Ausgestaltung

3.1 Schaffung einer Experimentierklausel

Eine Sandbox bietet dann einen Mehrwert, wenn sie die temporäre Abweichung von Normen erlaubt, welche die Realisierung eines innovativen Vorhabens behindern. Dafür ist eine rechtliche Grundlage in Form einer Experimentierklausel oder eines Innovation Waiver zu schaffen. Aufgrund der grösseren Flexibilität ist dabei die Form einer Experimentierklausel zu wählen. Diese ist im nationalen Datenschutzgesetz zu verankern. Damit liesse sich zumindest Innovation für private Personen und für Bundesbehörden erleichtern. Um eine Modifikation von gesetzlichen Vorgaben auch für Datenbearbeitungen von kantonalen oder kommunalen Behörden zu ermöglichen, wäre zusätzlich eine Verankerung in den kantonalen Gesetzen notwendig.

Bei der inhaltlichen Gestaltung ist abzuwägen, ob bereits in der Experimentierklausel selbst diejenigen gesetzlichen Bestimmungen aufzuführen sind, welche im Einzelfall aufgehoben oder modifiziert werden können oder ob die Auswahl der zu modifizierenden Bestimmungen den zuständigen Behörden zu überlassen ist. Während der erste Fall eher das Vertrauen der Bevölkerung fördert, gewährt der zweite Fall mehr Flexibilität. Aufgrund der Vielzahl der vorstehend genannten innovationshindernden Vorschriften ist der zweiten Variante der Vorzug zu geben.

Neben der gesetzlichen Ermächtigung in Form einer Experimentierklausel bedarf es auch der Festlegung eines flankierenden Sandbox Programms, welches unter anderem die Modalitäten der Zulassung, den Ablauf des Versuchs und die Ergebnisdokumentation regelt. Dies muss aber nicht auf Gesetzesstufe geschehen. Die wichtigsten Eckpunkte des Programms sollten aber auf jeden Fall öffentlich zugänglich sein.

3.2 Pflicht zur Kooperation von Behörden

Wenn für einen Sachverhalt mehrere (Aufsichts-)Behörden zuständig sind, hat nicht eine einzelne Behörde die Kompetenz, über allfällige Modifikationen von gesetzlichen Vorgaben zu bestimmen. Vielmehr müsste in solchen Fällen eine federführende Behörde bestimmt werden, welche sich bei Bedarf mit sämtlichen betroffenen Aufsichtsbehörden koordiniert.

Idealerweise geschieht diese Koordination nicht nur bereichsintern zwischen Datenschutzbehörden, sondern sektorübergreifend mit anderen im Einzelfall zuständigen Behörden, wie etwa Ethikkommissionen etc. Eine solche Koordination befähigt und verpflichtet die zuständigen Stellen, eine gemeinsame Lösung zu finden.

3.3 Offene Zulassungskriterien

Bei der Formulierung der Zulassungskriterien darf der Anwendungsbereich für Sandbox Projekte nicht zu eng gefasst werden. Insbesondere ist weder das Kriterium der «Innovation» noch jenes der «Verwendung von Künstlicher Intelligenz» vorzuschreiben. Im Zweifelsfall sollten Projekte und Vorhaben ohne inhaltliche oder technische Einschränkungen Teil einer Sandbox werden können.

Mehr Gewicht ist auf die Voraussetzung des gesellschaftlichen Mehrwerts bzw. Nutzens zu legen. Als Ergänzung ist sicherzustellen, dass die Persönlichkeit der betroffenen Personen soweit als möglich geschützt wird, beispielsweise durch spezifische Schutzmassnahmen für die Gewährleistung einer umfassenden Datensicherheit.

3.4 Zeitliche Begrenzung?

Man kann sich die Frage stellen, ob die Experimentierklausel als solche oder das Sandbox Programm von Anfang an einer zeitlichen Begrenzung zu unterwerfen sind. Wie bereits erwähnt, sind die einzelnen Sandbox Projekte in jedem Fall auf eine bestimmte Testphase zu begrenzen.

Versteht man die Sandbox als Möglichkeit für die Behörden und den Gesetzgeber, bestehende Gesetze zu überdenken und allenfalls neue Regelungen zu erproben, muss das Ziel sein, dass die Gesetze nach Durchführung entsprechender Versuche an die Gegebenheiten angepasst werden. In diesem Sinne sollte das Sandbox Programm eine Möglichkeit sein, um allfällige Anpassungen des Datenschutzrechts in einem geschützten Umfeld zu erproben, welche hernach ins Gesetz überführt werden. Wenn das Sandbox Programm zeitlich nicht befristet ist, könnte dies den Gesetzgeber dazu verleiten, eine solche Gesetzesänderung aufzuschieben und nur auserlesene Projekte einzelfallweise über die Sandbox zu lösen. Dies ist

im Ergebnis aber unbefriedigend, weil sich die Gesetzgebung weiterhin hemmend auf zahlreiche andere Vorhaben auswirkt.

Eine Befristung des Programms macht auch deshalb Sinn, weil man so die Möglichkeit hat, nach dem Abschluss von mehreren Sandbox Projekten Bilanz zu ziehen. Die Behörden könnten so evaluieren, ob die Sandbox zu den gewünschten Ergebnissen geführt hat, und es könnten im Hinblick auf künftige Programme Verbesserungen vorgenommen werden.

Abzulehnen ist eine Befristung der Experimentierklausel. Eine solche hätte zur Folge, dass nach Ablauf der Frist keine Grundlage mehr für zukünftige Sandbox Programme bestehen würde. Ergäbe sich in Zukunft erneut Handlungsbedarf, müsste eine neue gesetzliche Grundlage geschaffen werden. Eine beständige Experimentierklausel ist jedoch notwendig, um auch in Zukunft auf Veränderungen reagieren zu können und Innovation zu unterstützen.

4. Zusammenfassung und Fazit

Zusammenfassend lässt sich festhalten, dass die geltenden Datenschutzgesetze Innovation oft behindern. Für Bereiche, in denen sich Regulierung negativ auf Innovation auswirkt, wurden in jüngerer Zeit sogenannte Sandboxen geschaffen, welche es – teilweise in Verbindung mit einer temporären Modifikation gesetzlicher Vorgaben – Unternehmen ermöglichen, neue Lösungsansätze unter Realbedingungen in einem geschützten Umfeld zu testen. Doch auch Behörden und Gesetzgeber können von Sandboxen profitieren, weil auch sie potenzielle neue Regulierungsansätze in der Sandbox testen und Schlüsse für allfällige Praxis- oder auch Gesetzesänderungen ziehen können.

Das schweizerische Datenschutzrecht erlaubt derzeit keine Abweichung von gesetzlichen Vorgaben. Möglich ist nur eine Beratung des EDÖB hinsichtlich der rechtlichen Zulässigkeit eines Vorhabens. Eine solche Auskunft ist jedoch nicht bindend.

Um Innovation zu ermöglichen, sollte in den Datenschutzgesetzen der Schweiz eine Experimentierklausel verankert werden. Darauf aufbauende Sandbox Programme müssten grosszügige technologieunabhängige Zulassungskriterien vorsehen, die den Schwerpunkt auf die Generierung eines gesellschaftlichen Nutzens legen. Auch eine Kooperationspflicht der zuständigen Datenschutz- und anderen Behörden wäre vorzusehen. Es ist jedoch festzuhalten, dass bezüglich der optimalen Ausgestaltung einer KI Sandbox in der Schweiz noch gewisser Forschungsbedarf besteht.