GUTACHTEN

Umsetzung der BMWi-Strategie „Reallabore als Testräume für Innovation und Regulierung“: Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen (Projekt Nr. 113/19-FL1-2/03)

für das

Bundesministerium für Wirtschaft und Energie

erstellt durch

Rechtsanwalt Dr. Daniel Rücker
Rechtsanwalt Sebastian Dienst
Rechtsanwalt Alexander Brandt

Noerr

Im

Februar 2021

Noerr
Partnerschaftsgesellschaft mbB
Rechtsanwälte Steuerberater
Wirtschaftsprüfer
Brienner Str. 28
80333 München
Deutschland

T +49 89 286280
F +49 89 280110
www.noerr.com

Alicante
Berlin
Bratislava
Brüssel
Budapest
Bukarest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moskau
München
New York
Prag
Warschau

Inhaltsverzeichnis

A. Executive Summary

Dem europäischen Datenschutzrecht, namentlich der Datenschutz-Grundverordnung (DS-GVO), eilt gemeinhin der Ruf voraus, hohe Hürden für die Entwicklung, Erprobung und Anwendung innovativer digitaler Geschäftsmodelle aufzustellen. Nicht selten sieht sich die DS-GVO dem Vorwurf ausgesetzt, sie stünde digitaler Innovation kaum praxisgerecht und rechtskonform überwindbar im Wege. Nicht zuletzt mag der signifikante Bußgeldrahmen der DS-GVO durch seine abschreckende Wirkung diese Wahrnehmung in der Praxis verstärken.

In der Tat hat der europäische Gesetzgeber mit der seit 2018 in allen Mitgliedstaaten der EU, so auch in Deutschland, unmittelbar anwendbaren DS-GVO die schon mit der europäischen Datenschutz-Richtlinie (DS-RL) 1995 etablierten Anforderungen an die Verarbeitung personenbezogener Daten noch einmal deutlich erhöht und zugleich die nationalen Regelungsspielräume im Datenschutzrecht signifikant reduziert. Neben den schon bis dahin geltenden elementaren Datenschutzgrundsätzen, allen voran dem sog. „Verbot mit Erlaubnisvorbehalt“, setzt die DS-GVO nicht zuletzt mit nochmals gesteigerten Transparenzanforderungen und umfassenden Rechenschafts- und Dokumentationspflichten weitere mittelbare und unmittelbare Hürden nicht nur für die langfristige Anwendung, sondern auch die Erprobung digitaler Innovationen.

Wenngleich die im vorliegenden Gutachten skizzierten Hürden des Datenschutzrechts (**Abschnitt C**) die Entwicklung, Erprobung und Anwendung innovativer Technologien auf den ersten Blick vor große Herausforderungen stellen, lassen die datenschutzrechtlichen Regelungen doch bei näherer Betrachtung an vielen Stellen Gestaltungsspielräume, die sich gerade auch für die Erprobung digitaler Innovationen nutzbar machen lassen (**Abschnitt D**). Das Datenschutzrecht gibt dem Rechtsanwender eine Reihe vergleichsweise flexibler Instrumente an die Hand, die eine rechtskonforme Gestaltung digitaler Innovationen durchaus zulassen. Nicht selten unterschätzt wird in der Praxis der Gestaltungsspielraum durch Vermeidung personenbezogener Daten, insbesondere durch Verwendung gleichwertiger anonymer oder synthetischer Informationen (dazu **Abschnitt D.I.**). Insbesondere eröffnen Einwilligungs- und Vertragslösungen die Möglichkeit freiwilliger, gegebenenfalls incentivierter Teilhabe an innovativen Experimentierräumen (dazu **Abschnitt D.II**). Weitreichende Gestaltungsspielräume eröffnet vor allem auch das flexible Instrument der Interessenabwägung (dazu **Abschnitt D.III**).

Auch wenn die in diesem Gutachten aufgezeigten Gestaltungsspielräume (**Abschnitt D**) durchaus geeignet sind, viele als Hürden wahrgenommene Anforderungen des Datenschutzrechts bei der Entwicklung und Anwendung innovativer Technologien zu meistern, bleiben für die Erprobung digitaler Innovationen ohne Frage

eine Reihe datenschutzrechtlicher Hindernisse, die sich letzten Endes nur durch Anpassung des anwendbaren Rechtsrahmens aus dem Weg räumen ließen (**Abschnitt E**), insbesondere auf EU-Ebene. In Frage kommt hier insbesondere die Ergänzung der wenigen, derzeit in der DS-GVO vorgesehenen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten um ein „**Erprobungsprivileg**“ und um eine allgemeine, auch außerhalb des Reallabore-Kontext einsetzbare forschungsfreundliche Rechtsgrundlage zur Verarbeitung personenbezogener Daten in Forschungsvorhaben (dazu **Abschnitt E.I**). Selbst ohne Anpassung des europäischen oder deutschen Datenschutzrechts hat der deutsche Gesetzgeber auch bei Reallaboren die Möglichkeit, durch gezielte Gestaltung fachrechtlicher Anforderungen an in Reallaboren zu erprobende Technologien etwaige Hürden abzubauen und bei der Überwindung verbleibender Hürden zu unterstützen (dazu **Abschnitt E.II.1**). Auch darüber hinaus verbleiben dem deutschen Gesetzgeber, wenn auch nur punktuell, datenschutzrechtliche Regelungsspielräume, die in bestimmten Bereichen die Gestaltung von Experimentierräumen zulassen könnten (**Abschnitt E.II.2**).

Verglichen mit Jurisdiktionen außerhalb der EU, die kein der EU vergleichbares Datenschutzniveau bieten, konkret zum als sehr als innovationsfreundlich wahrgenommenen US-Bundesstaat Kalifornien (**Abschnitt F.I.1**), stellen sich die Hürden des deutschen/europäischen Datenschutzrechts vor allem auch mit Blick auf die Erprobung digitaler Innovationen als relativ hoch dar. Allerdings ist im internationalen Vergleich auch festzustellen, dass Jurisdiktionen mit einem der EU vergleichbaren Datenschutzniveau, konkret Japan (**Abschnitt F.I.2**), ähnlich hohe Hürden, teilweise sogar zusätzliche Hürden aufstellen. In Japan gibt es zwar rechtliche Rahmen für „regulatorische Sandkästen“ für Erprobungen, die allerdings zumindest bislang nicht zur Überwindung datenschutzrechtlicher Hürden zur Anwendung kamen.

Der europäische Vergleich, konkret mit Frankreich (**Abschnitt F.II.1**) und Ungarn (**Abschnitt F.II.2**) zeigt, dass in anderen EU-Mitgliedsstaaten die in diesem Gutachten aufgezeigten, vergleichsweise kleinen nationalen Regelungsspielräume der DS-GVO bereits punktuell genutzt werden, um die Erprobung von Innovationen zu erleichtern. In Frankreich befasst sich die Datenschutzaufsichtsbehörde aktiv mit dem Thema „regulatorische Sandkästen“ für den Bereich des Datenschutzrechts, allerdings nicht im Sinne von Ausnahmen von den Anforderungen der DS-GVO als vielmehr bezogen auf die „experimentellere“ Herangehensweise der Behörde bei der Umsetzung dieser Anforderungen.

B. Fragestellung

Die Reallabore-Strategie des BMWi verfolgt das Ziel, Testräume für eine Vielzahl von Wirtschafts- und Technologiebereichen zu eröffnen.

In Zeiten der digitalen Transformation und neuer Technologien nimmt dabei die Bedeutung des Datenschutzes zu.

Vor diesem Hintergrund wurden wir gebeten, zu prüfen,

- welche Hürden das deutsche/europäische Datenschutzrecht für die Erprobung/Umsetzung digitaler Technologien und Geschäftsmodelle aufstellt (dazu **Abschnitt C**),

- ob, und wenn ja, welche Gestaltungsspielräume im deutschen/europäischen Datenschutzrecht zur Erprobung neuartiger Technologien oder Geschäftsmodelle bestehen (dazu **Abschnitt D**) und

- welche Anpassungen im Datenschutzrecht auf deutscher/europäischer Ebene denkbar wären, um (mehr) Flexibilität zur Erprobung innovativer Geschäftsmodelle zu bieten (dazu **Abschnitt E**).

C. Hürden des deutschen/europäischen Datenschutzrechts

Es liegt geradezu in der Natur des europäischen Datenschutzrechts, die Verarbeitung[1] personenbezogener Daten[2] (unmittelbar) einzuschränken, um betroffene Individuen zu schützen, insbesondere auch vor etwaigen besonders hohen Risiken neuer Technologien[3]. Daneben enthält das Datenschutzrecht jedoch auch eine Reihe weiterer Anforderungen, die zwar nicht unmittelbar auf eine Einschränkung der Datenverarbeitung abzielen, aber aufgrund des mit ihrer Umsetzung verbundenen Aufwands durchaus geeignet sind, den Umgang mit personenbezogenen Daten in der Praxis denkbar unattraktiv zu machen und so zumindest mittelbar einzuschränken. Dazu zählen etwa umfassende Rechenschafts- und Dokumentationspflichten im Zusammenhang mit der Datenverarbeitung.

Zwar betont die Datenschutz-Grundverordnung (DS-GVO) ausdrücklich den Stellenwert des wirtschaftlichen und sozialen Fortschritts und der unternehmerischen Freiheit. So soll Datenschutz auch kein uneingeschränktes Recht sein, sondern ist gegen andere Grundrechte und Grundfreiheiten abzuwägen. Mit Blick auf eine rasche technologische Entwicklung und die Globalisierung bekräftigt der Verordnungsgeber sogar, dass er mit der DS-GVO eine Vertrauensbasis schaffen möchte, die die digitale Wirtschaft dringend benötige, um im Binnenmarkt weiter wachsen zu können.[4]

---

[1] „**Verarbeitung**" meint *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung*" (Art. 4 (2) DS-GVO).

[2] „**Personenbezogene Daten**" sind *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „**betroffene Person**") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind*" (Art. 4 (1) DS-GVO).

[3] Vgl. EG 90 DS-GVO.

[4] Vgl. EG 2, 4, 6 und 7 DS-GVO.

Dennoch sehen wir in unserer Beratungspraxis, dass gerade Unternehmen mit innovativen, datengetriebenen und globalen Geschäftsmodellen den Datenschutz insgesamt als (nicht selten nur mit großen Anstrengungen oder bisweilen gar nicht überwindbare[5]) Hürde wahrnehmen.[6] Der signifikante Bußgeldrahmen der DS-GVO und die davon ausgehende abschreckende Wirkung mag diese Wahrnehmung in der Praxis noch weiter verstärken.[7]

Folgende Herausforderungen des Datenschutzrechts werden nach unserer Erfahrung in der Praxis oft als besonders hohe Hürden wahrgenommen. Hierbei differenziert das Datenschutzrecht an sich bislang nicht zwischen der Erprobung neuer Technologien in Reallaboren und der eigentlichen Anwendung solcher Technologien nach der Erprobung, sondern stellt gleichermaßen hohe Anforderungen an die Verarbeitung personenbezogener Daten sowohl im Erprobungs- als auch im Anwendungskontext:

I. Generelles „Verarbeitungsverbot mit Erlaubnisvorbehalt“

Das zentrale Wesensmerkmal des deutschen und europäischen Datenschutzrechts ist der sog. Grundsatz der „Rechtmäßigkeit“, in der Praxis zum Teil auch als „Verbotsprinzip“ oder „Verbot mit Erlaubnisvorbehalt“ umschrieben. Eine Verarbeitung personenbezogener Daten ist danach nur dann zulässig, wenn für den konkreten Verarbeitungsvorgang eine ausreichende Rechtsgrundlage besteht. Eine solche Rechtsgrundlage kann sich etwa aus einer Einwilligung[8] der betroffenen Person ergeben. Daneben existiert ein eng begrenzter Kanon sog. gesetzlicher Rechtsgrundlagen, etwa für Verarbeitungen, die zur Erfüllung eines Vertrages mit der betroffenen Person oder zur Erfüllung gesetzlicher Pflichten erforderlich sind.[9]

Die DS-GVO schränkt damit nicht nur besonders riskante Verarbeitungstätigkeiten ein, sondern zwingt den Rechtsanwender ganz allgemein dazu, jeglichen Umgang mit personenbezogenen Daten – ob beabsichtigt oder unbeabsichtigt – vorab kri-

---

[5] Einige amerikanische Unternehmen haben anlässlich der DS-GVO zum 25.05.2018 EU-Nutzer von ihren Websites sogar völlig „ausgesperrt“ (siehe etwa http://www.backcountry.com; auch zahlreiche Websites amerikanischer Zeitungen waren zumindest zeitweise nicht mehr aus der EU erreichbar: https://www.sueddeutsche.de/digital/dsgvo-europaeer-muessen-draussen-bleiben-1.3992207).

[6] Diese Erkenntnis deckt sich auch mit einer im Auftrag der Bitkom durchgeführten Studie, wonach anscheinend *„drei von vier Unternehmen (74 Prozent) Datenschutzanforderungen als die größte Hürde beim Einsatz neuer Technologien“* sehen, https://www.bitkom.org/Presse/Presseinformation/Bitkom-zieht-gemischte-Jahresbilanz-zur-DS-GVO (abgerufen am 17.4.2020); zu ähnlichen Ergebnissen kommt auch eine Umfrage des Leibniz-Zentrums für Europäische Wirtschaftsforschung (ZEW) im März 2020, https://www.zew.de/de/presse/pressearchiv/viele-unternehmen-stellen-dsgvo-schlechtes-zeugnis-aus/?cHash=4fda5fb3c5661939e5016b405c2c406d (abgerufen am 7.5.2020).

[7] Für Verstöße sieht die DS-GVO einen Bußgeldrahmen von bis zu 4 % des weltweiten Jahresumsatzes oder € 20 Millionen vor, wobei der höhere der beiden Beträge maßgeblich ist (vgl. Art. 83 (4), (5) DS-GVO).

[8] „**Einwilligung**“ ist *„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“* (Art. 4 (11) DS-GVO).

[9] Vgl. allgemein Art. 5 (1) (a), 6 (1) DS-GVO; die genannten Rechtsgrundlagen sind in Art. 6 (1) (a), (b) und (c) DS-GVO geregelt.

tisch dahingehend zu hinterfragen, ob eine ausreichende Rechtsgrundlage einschlägig ist.

Praxisbeispiel:	**Unbeabsichtigte Verarbeitung personenbezogener Daten als „Nebenprodukt“ bei der Erprobung autonomer Fahrzeuge**
Beispielszenario:	Der Entwickler eines autonomen Fahrzeugs hat in einem Prototypen eine hochauflösende Videokamera installiert, die dauerhaft die Umgebung des Fahrzeugs aufzeichnet und die entsprechenden Bilder an ihn sendet. Damit möchte er die Sicherheitseinrichtungen des Fahrzeugs überprüfen und feststellen, ob das Fahrzeug sich im Verkehr und insbesondere im Umgang mit besonderen Verkehrssituationen und Hindernissen so verhält wie geplant. Es lässt sich nicht ausschließen, dass die Kamera auch Gesichter von Passanten und Kennzeichen anderer Fahrzeuge erfasst, die auf den Bildaufzeichnungen erkennbar sein könnten.
Hürde:[10, 11]	Auch für diese eigentlich **unbeabsichtigte Verarbeitung personenbezogener Daten ist eine Rechtsgrundlage erforderlich**.

II. Spezielles Verarbeitungsverbot für „besondere Kategorien personenbezogener Daten“ – Numerus clausus spezifischer Rechtfertigungstatbestände

Für sog. „besondere Kategorien personenbezogener Daten“ sieht die DS-GVO einen erhöhten Schutz vor. Hierunter fallen etwa Gesundheitsdaten oder biometrische Daten.[12] Die Verarbeitung solcher Daten erfordert nicht nur eine Rechtsgrundlage (siehe oben C.I.), sondern darüber hinaus einen besonderen Ausnahmetatbestand, der gerade die Verarbeitung besonderer Kategorien personenbezogener Daten gestattet[13].

Solche Ausnahmetatbestände zielen jeweils auf vergleichsweise konkrete Verarbeitungssituationen ab, beispielsweise die Verarbeitung personenbezogener Daten durch Fachpersonal für Zwecke der Gesundheitsvorsorge[14]. Dadurch kann sich die Verarbeitung besonderer Kategorien personenbezogener Daten nur in sehr starren Grenzen bewegen. Insbesondere ist die Verarbeitung solcher Daten nicht bereits dann zulässig, wenn sie für die Durchführung eines Vertragsverhältnisses mit der

[10] Die Praxisbeispiele dienen dazu, jeweils bestimmte Hürden zu veranschaulichen. Neben der jeweils angesprochenen Hürde bestehen häufig auch weitere Hürden, die es zu überwinden gilt.
[11] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.I.1, D.III.2 und E.II.1.
[12] Art. 9 (1) DS-GVO.
[13] Vgl. Art. 9 (2) DS-GVO.
[14] Art. 9 (2) (h), 3 DS-GVO, § 22 Abs. 1 Nr. 1 lit. b BDSG.

betroffenen Person erforderlich[15] ist oder wenn eine Interessenabwägung[16] ergeben würde, dass die Interessen des Verantwortlichen[17] an der Verarbeitung überwiegen.

In der Praxis führt dies für Organisationen, die zum Betrieb und zur Entwicklung ihrer digitalen Innovationen auf die Verarbeitung und Auswertung solcher besonderen Kategorien von Daten angewiesen sind, zu mitunter sehr schwer nachvollziehbaren Situationen:

Praxisbeispiel:	**Einwilligungserfordernis für innovative Gesundheits-Apps**
Beispielszenario:[18]	Ein Unternehmen möchte eine cloud-basierte App betreiben, die es registrierten Nutzen ermöglicht, ihre Ernährung, ihre sportlichen Aktivitäten sowie Informationen aus Fitness-Trackern (z. B. Puls und Bewegungsdaten) zu dokumentieren. Auf dieser Grundlage liefert die App den Nutzern Einschätzungen und Tipps zu deren Gesundheit.
Hürde:[19]	Ginge es hier nicht um Gesundheitsdaten, sondern um „normale“ Daten, ließe sich die Verarbeitung zur Erfüllung des mit dem Anwender bestehenden Nutzungsvertrages grundsätzlich gesetzlich auch ohne Einwilligung rechtfertigen. Die App verarbeitet jedoch auch **Gesundheitsdaten** (insbesondere etwa die Einschätzungen zur Gesundheit des Nutzers), weshalb hier das besondere Verarbeitungsverbot für solche Daten zu überwinden ist. Wird die App nicht von einem Arzt betrieben, sondern von einem „normalen“ Unternehmen, ist kein gesetzlicher Ausnahmetatbestand ersichtlich. Deshalb kann nur eine **ausdrückliche (und jederzeit frei widerrufliche) Einwilligung** des Nutzers die zur Erfüllung des Nutzungsvertrages zwingend erforderliche Verarbeitung personenbezogener Daten legitimieren.[20]

[15] Art. 6 (1) (b) DS-GVO.
[16] Art. 6 (1) (f) DS-GVO.
[17] „**Verantwortlicher**“ ist „*die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden*“ (Art. 4 (7) DS-GVO).
[18] Siehe Ergänzungen zu diesem Praxisbeispiel in den Praxisbeispielen **„Big-Data-Analysen und explorative Statistiken“** (→ C.III) und **„Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts“** (→ C.IX).
[19] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitt D.II.2.
[20] Art. 9 (2) (a) DS-GVO.

In der Praxis häufig anzutreffende „Einwilligungen“, bei denen ein Nutzer sich bei der Registrierung für einen Onlinedienst ganz pauschal „mit der Datenschutzerklärung einverstanden erklärt“, sind unwirksam. Eine wirksame Einwilligung wäre **deutlich konkreter/bestimmter zu formulieren**.

Praxisbeispiel: **Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte**

Beispielszenario:[21] Ein Arzt nutzt eine innovative Software as a Service (SaaS)-Lösung[22] zur Künstliche Intelligenz (KI)[23]-gestützten Auswertung von CT-Aufnahmen und Kooperation mit anderen Ärzten, um seine Patienten bestmöglich zu behandeln. Das Unternehmen, das die SaaS-Lösung anbietet, benötigt zur Weiterentwicklung der darin enthaltenen künstlichen Intelligenz fortlaufend Daten aus konkreten Behandlungen/Anwendungsfällen. Hierzu möchte das Unternehmen solche Informationen in vollständig anonymer Form von den jeweiligen Ärzten direkt über die SaaS-Lösung erhalten.

Hürde:[24] Blickt man isoliert auf die Rechtsgrundlage der Anonymisierung, ließe sich die Anonymisierung im Regelfall auf eine Interessenabwägung[25] stützen. Die anonymen Daten würden dann nicht mehr dem Anwendungsbereich des Datenschutzrechts unterfallen, wären also weitgehend uneingeschränkt verwendbar.

---

[21] Siehe Ergänzungen zu diesem Praxisbeispiel in den Praxisbeispielen **„Abgrenzung Anonymisierung und Pseudonymisierung“** und „**Forschung und Statistik zur Verbesserung von Produkten und Dienstleistungen**“ (→ C.VII) sowie „**Nutzung von Cloud-Diensten durch Krankenhäuser**“ (→ C.VIII).

[22] „***Software as a Service (SaaS)*** *ist ein Teilbereich des Cloud Computings. Das SaaS-Modell basiert auf dem Grundsatz, dass die Software und die IT-Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Dienstleistung genutzt werden. Für die Nutzung von Online-Diensten wird ein internetfähiger Computer sowie die Internetanbindung an den externen IT-Dienstleister benötigt. Der Zugriff auf die Software wird meist über einen Webbrowser realisiert*“ (vgl. https://de.wikipedia.org/wiki/Software_as_a_Service).

[23] „*Im Allgemeinen bezeichnet* ***künstliche Intelligenz*** *den Versuch, bestimmte Entscheidungsstrukturen des Menschen nachzubilden, indem z. B. ein Computer so gebaut und programmiert wird, dass er relativ eigenständig Probleme bearbeiten kann. Oftmals wird damit aber auch eine nachgeahmte Intelligenz bezeichnet, wobei durch meist einfache Algorithmen ein „intelligentes Verhalten“ simuliert werden soll, etwa bei Computergegnern in Computerspielen*“ (vgl. https://de.wikipedia.org/wiki/K%C3%BCnstliche_Intelligenz).

[24] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.I.2, D.II.3 und D.V.

[25] Art. 6 (1) (f) i. V. m. Art. 6 (4) DS-GVO.

Da es sich bei den Ausgangsdaten allerdings um **Gesundheitsdaten** handelt, wäre der datenschutzrechtlich nur wenig invasive, ja sogar datenschutzfreundliche Anonymisierungsvorgang jedoch wegen des besonderen Verarbeitungsverbots für Gesundheitsdaten wohl[26] nur mit einer **ausdrücklichen (und jederzeit frei widerruflichen) Einwilligung** der jeweiligen Patienten zulässig.[27]

III. Strenge Zweckbindung, Datenminimierung und Speicherbegrenzung

Mit den Grundsätzen der Zweckbindung, Datenminimierung und Speicherbegrenzung gestattet die DS-GVO die Verarbeitung personenbezogener Daten nur in einem sehr begrenzten, auf den jeweiligen Verarbeitungszweck fokussierten Umfang.[28] Für die Rechtfertigung der Verarbeitung personenbezogener Daten genügt es also nicht, festzustellen, dass eine Rechtsgrundlage grundsätzlich besteht (z. B. kann die Verarbeitung personenbezogener Daten zum Zwecke der Vertragserfüllung *grundsätzlich* zulässig sein[29]). Es ist vielmehr für *jedes konkrete Einzeldatum* zu hinterfragen, ob, und wenn ja, für *welche konkreten Einzelzwecke* und für *wie lange* die Verarbeitung zulässig ist:

- Der Zweckbindungsgrundsatz besagt, dass personenbezogene Daten *„für festgelegte, eindeutige und legitime Zwecke erhoben werden [müssen] und […] nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“*[30] dürfen.

  Bereits bei der Planung einer Verarbeitungstätigkeit sind daher alle angestrebten Zwecke zu ermitteln und zu berücksichtigen. Schon bei herkömmlichen, nicht besonders innovativen Verarbeitungsaktivitäten kann die konkrete Zweckbestimmung und die Identifizierung verschiedener Einzelzwecke in der Praxis oft eine Herausforderung darstellen.

[26] Auch wenn hier Rechtsunsicherheit verbleibt, erscheint es zumindest denkbar, die Datenverarbeitung anstelle einer Einwilligung auf gesetzliche Ausnahmetatbestände zu stützen; hierzu Abschnitt D.V unten.
[27] Vgl. Art. 9 (1) und (2) (a) DS-GVO.
[28] Vgl. Art. 5 (1) (b), (c) und (e) DS-GVO.
[29] Vgl. Art. 6 (1) (b) DS-GVO.
[30] Art. 5 (1) (b) DS-GVO.

Die in einem Onlineshop erhobenen Bestelldaten dienen meist nicht ausschließlich dem Versand der Ware, sondern können etwa auch folgenden **weiteren Zwecken dienen, die dann bereits vor der Verarbeitung zu definieren wären**: (1) Auswertung zur Betrugsprävention, (2) Anonymisierung zur statistischen Auswertung, (3) Speicherung zu Beweiszwecken, (4) Aufbewahrung zur Erfüllung gesetzlicher Aufbewahrungspflichten etc.

- Nach dem Grundsatz der Datenminimierung dürfen personenbezogene Daten, vereinfacht ausgedrückt, nur erhoben/verarbeiten werden, soweit das für den im Voraus festgelegten Zweck auch tatsächlich erforderlich ist.

Die Erhebung des Geburtsdatums wäre zur Abwicklung einer Online-Bestellung grundsätzlich **nicht erforderlich**.

Möchte der Onlineshop-Betreiber das Geburtsdatum dagegen nutzen, um dem Kunden an dessen Geburtstag einen Gutschein zuzusenden, wäre das (1) ein **weiterer Verarbeitungszweck, der im Voraus zu definieren** wäre, und (2) wäre es wegen des Datenminimierungsgrundsatzes **zu hinterfragen, ob zur Erreichung dieses Zwecks nicht die Angabe des Geburtstages und -monats genügen würde** (also nicht auch des Geburtsjahres).

- Nach dem Grundsatz der Speicherbegrenzung müssen personenbezogene Daten *„in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“*[31].

Werden personenbezogene Daten nur zur Abwicklung einer Online-Bestellung verarbeitet, wären diese **nach Versand der Ware und Erhalt der Zahlung zu löschen (oder zu anonymisieren)**.

Für eine Speicherung der Daten über diesen Zeitpunkt hinaus mag es verschiedene Gründe geben, beispielsweise (i) die Erfüllung gesetzlicher Aufbewahrungspflichten, (ii) die Aufbewahrung zur Prüfung etwaiger Gewährleistungsansprüche der Kunden oder (iii) die Nutzung dieser Daten zu Marketingzwecken. Dies wären jeweils **weitere, im Voraus zu definierende Zwecke, bei denen der Verantwortliche jeweils im Detail prüfen müsste, welche konkreten Daten er für diese Zwecke in welchem Umfang verarbeiten darf und wann welche Daten zu löschen sind**.

[31] Art. 5 (1) (e) DS-GVO.

Wie die obigen Beispiele zeigen, ist die Einhaltung der Datenschutzgrundsätze also schon bei herkömmlichen, nicht besonders innovativen Verarbeitungsaktivitäten wie dem Betrieb eines Onlineshops relativ komplex. Umso herausfordernder kann die Umsetzung dieser Grundsätze bei innovativen, datengetriebenen Technologien sein:

Praxisbeispiel:	**Big-Data-Analysen und explorative Statistiken**
Beispielszenario:[32]	Ein Unternehmen im Gesundheitssektor verfügt über umfangreiche Datensätze zu Kunden seiner verschiedenen Geschäftsbereiche, unter anderem aus dem Betrieb einer Gesundheits-App (dazu auch das Praxisbeispiel **„Einwilligungserfordernis für innovative Gesundheits-Apps“** (→ C.II.)). Die bestehenden Datensätze sowie zusätzliche, aus zahlreichen Online-Quellen (z. B. soziale Medien) gewonnene Daten möchte das Unternehmen auswerten, um Abhängigkeiten und Muster zwischen den Datensätzen erkennen zu können. Das Unternehmen erhofft sich dadurch Erkenntnisgewinne zu verschiedensten gesundheitsbezogenen Themen, aber auch zu weiteren, vor der Auswertung noch nicht absehbaren Themen. Hiermit möchte das Unternehmen stetig neue, jeweils an den aktuellen Bedürfnissen orientierte Produkte entwickeln und künftig noch individueller auf einzelne Kunden eingehen können.
Hürde:[33]	Die Datensätze dienten ursprünglich der Abwicklung der Geschäftsbeziehungen in den verschiedenen Geschäftsbereichen des Unternehmens. Mit der geplanten Big-Data-Auswertung kommt ein weiterer Zweck hinzu. Zunächst ist also im Einzelnen zu klären, **ob der geänderte Zweck überhaupt mit dem bisherigen Zweck vereinbar ist**.[34]

[32] Siehe Ergänzungen zu diesem Praxisbeispiel im Praxisbeispiel „**Forschung und Statistik zur Verbesserung von Produkten und Dienstleistungen**“ (→ C.VII).
[33] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.I.3, D.II.1, D.II.3, D.III.2, D.V, D.VII.1 und D.VIII.
[34] Vgl. Art. 6 (4) DS-GVO.

Für die geplante Auswertung ist ebenfalls ein konkreter Verarbeitungszweck festzulegen.[35] Bisher hat das Unternehmen jedoch nur vage Vorstellungen, wie die Auswertung erfolgen soll und welche konkreten Erkenntnisse sich aus den vorhandenen Datensätzen ermitteln lassen könnten. Ein **klar abgrenzbarer Verarbeitungszweck ist daher nicht ohne Weiteres formulierbar**. Eine Verarbeitung zu nicht definierten Zwecken ist jedoch unzulässig.

Eine Verarbeitung personenbezogener Daten ohne klar definierten Zweck widerspräche auch den **Grundsätzen der Datenminimierung und Speicherbegrenzung**.

Praxisbeispiel:	**Blockchain-basierte Zahlungstechnologie**
Beispielszenario:	Der Betreiber einer elektronischen Geldbörse möchte Transaktionen mittels blockchain-gestützter Technologien protokollieren. Wesensmerkmal der Blockchain-Technologie ist die Unveränderlichkeit in der Blockchain abgelegter Informationen.
Hürde:[36]	Die dauerhafte und nicht reversible Speicherung personenbezogener Daten in der Blockchain steht in **Konflikt mit dem Grundsatz der Speicherbegrenzung**.

IV. Grundsätzliches Verbot „automatisierter Entscheidungen“

Technische Innovationen erlauben mehr und mehr die Verlagerung menschlicher Tätigkeiten und Entscheidungen auf Maschinen, gerade wenn diese Maschinen mittels künstlicher Intelligenz auch in der Lage sind, zunehmend komplexere Problemstellungen zu lösen. Die betroffene Person hat allerdings *„das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“*[37]. Insbesondere bei Implementierung künstlicher Intelligenz ist dieses Verbot automatisierter Entscheidungen besonders zu berücksichtigen:

---

[35] Art. 5 (1) (b) DS-GVO.
[36] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitt D.I.1.
[37] Art. 22 (1) DS-GVO.

Praxisbeispiel:	**KI-gestützte Automatisierung der Kundenkommunikation**
Beispielszenario:	Ein Unternehmen möchte die Kundenkommunikation automatisieren und hierzu auf seiner Website einen Chatbot einsetzen, der mittels künstlicher Intelligenz selbstständig und vergleichbar mit einem menschlichen Kundenberater die Anliegen der Kunden bearbeiten soll. Dabei soll das System sich anhand der von ihm bearbeiteten Kundenanfragen sowie anhand früherer, noch durch menschliches Personal bearbeiteter Kundenanfragen selbständig weiterentwickeln.
Hürde:[38]	Bei diesem System wäre zunächst im Detail zu prüfen, **ob es „automatisierte Entscheidungen“ im Sinne der DS-GVO fällt**.[39] In diesem Fall wäre nicht nur die Datenverarbeitung durch das System an sich zu rechtfertigen.[40] Zusätzlich wäre zu prüfen, ob für das grundsätzliche **Verbot automatisierter Entscheidungen** ein Ausnahmetatbestand eingreift.

Praxisbeispiel:	**Vollautomatisiertes Depotmanagement über Robo-Advisor**
Beispielszenario:	Ein FinTech-Startup möchte einen Robo-Advisor entwickeln, der ein vollautomatisches Depotmanagement für die Verwaltung von Bitcoin-Investments ermöglicht. Das System soll umfassende Informationen zur finanziellen Situation des Kunden, zu von ihm bereits genutzten Finanzprodukten sowie zu dessen Wünschen und Ängsten im Zusammenhang mit Kapitalanlagen erhalten. Auf dieser Grundlage trifft das System eigenständig Investmententscheidungen und führt diese direkt im Namen des Kunden aus.
Hürde:[41]	Beim Betrieb des Robo-Advisor **greift das grundsätzliche Verbot automatisierter Entscheidungsfindungen**, das es zu überwinden gilt.

[38] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.II.3 und D.III.2.
[39] Vgl. Art. 22 (1) DS-GVO.
[40] Art. 6 DS-GVO.
[41] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.II.2, D.VII.1 und E.II.1.

> Darüber hinaus muss das Unternehmen seinen Kunden *„**aussagekräftige Informationen über die involvierten Logik** sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“*[42] zur Verfügung stellen.

V. Hohe Transparenzanforderungen und weitreichende Betroffenenrechte

Der datenschutzrechtliche Transparenzgrundsatz verlangt, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.[43] Darüber hinaus gibt die DS-GVO betroffenen Personen umfassende individuelle Rechte an die Hand:

1. Umfang und Komplexität von Datenschutzerklärungen

Die DS-GVO sieht umfangreiche Informationspflichten vor.[44] Insbesondere muss ein Verantwortlicher betroffene Personen im Detail darüber informieren, zu welchen konkreten Zwecken er welche Daten verarbeitet, auf welcher Rechtsgrundlage dies geschieht und wie lange er die Daten speichert.

Diese Fülle an Informationen muss der Verantwortliche den betroffenen Personen in einer transparenten und für sie nachvollziehbaren Art und Weise mitteilen. Gerade bei umfangreichen Verarbeitungsaktivitäten führt das in der Praxis zwangsläufig zu einem nur sehr schwer auflösbaren Konflikt zwischen umfassender Erfüllung der Informationspflichten und, ob des daraus resultierenden Umfangs von Datenschutzinformationen, gleichzeitiger Wahrung der erforderlichen Transparenz. Selbst bei einem mittelständischen Unternehmen oder einem kleinen, aber datengetriebenen Start-up können Datenschutzinformationen für Beschäftigte oder Kunden leicht mehrere hundert Seiten umfassen. Die gewissenhafte Erfüllung der Informationspflichten ist in der Praxis zudem häufig mit einem hohen zeitlichen und finanziellen Aufwand verbunden.

---

[42] Art. 13 (2) (f) DS-GVO.
[43] Vgl. EG 7 und 11 DS-GVO und Art. 5 (1) (a) DS-GVO.
[44] Art. 13 und 14 DS-GVO.

Praxisbeispiel:	**Datenschutzinformationen für ein smartes Hausautomatisierungssystem**
Beispielszenario:	Ein Unternehmen hat ein smartes Hausautomatisierungssystem entwickelt, das über zahlreiche Sensoren und Schaltelemente (Mikrophone, Videokameras, Temperaturmesser, Rollladen- und Heizungssteuerung etc.) eine per KI automatisierte sowie zusätzlich per App steuerbare Verwaltung sämtlicher Geräte im Haushalt ermöglicht (Temperaturregelung, Licht, Musik, Küchengeräte, Alarmanlage etc.). Über die anfallenden Daten entwickelt sich das System selbständig weiter mit dem Ziel, jeden Wunsch der Hausbewohner zu erkennen und automatisch zu erledigen. Die gesamte Konfiguration und Nutzung des Systems erfolgt über die zugehörige App.
Hürde:[45]	Der Nutzer (Hausbewohner) sowie sämtliche andere betroffenen Personen (z. B. Besucher) sind über die zahlreichen Verarbeitungsvorgänge im Detail zu informieren. Insbesondere steht das Unternehmen vor der Herausforderung, die Informationen **so zu gestalten, dass sie ggf. auch auf Smartphone-Bildschirmen lesbar sind**. Auch über etwaige von der KI neu oder weiter entwickelte **Verarbeitungsvorgänge wären die Nutzer zu unterrichten**.

2. Anforderungen an die Beantwortung von Auskunftsersuchen und sonstigen Betroffenenanfragen

Die DS-GVO gewährt betroffenen Personen eine ganze Reihe an individuellen Datenschutzrechten, wie etwa das Auskunftsrecht, das Recht auf Löschung oder das Recht auf Datenübertragbarkeit.[46] Anfragen zur Geltendmachung dieser Rechte sind unverzüglich, grundsätzlich jedenfalls aber innerhalb eines Monats, vom Verantwortlichen zu beantworten.

Um eine realistische Chance zu haben, diese Zeitvorgabe in der Praxis einzuhalten, müssen Verantwortliche bereits vorab robuste Prozesse etablieren, die die Wahrung der betroffenen Rechte sicherstellen. Hier sind nicht nur rechtliche Fragen anhand der Spezifika der jeweiligen Organisation zu beantworten, etwa wie weit und unter welchen Beschränkungen die jeweiligen Be-

[45] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.VI und D.VIII.
[46] Vgl. Art. 15, 17, 20 DS-GVO.

troffenenrechte gelten.[47] Vielmehr muss der Verantwortliche auch operative Strukturen und Prozesse schaffen, um beispielsweise die für die Beantwortung eines Auskunftsersuchens erforderlichen personenbezogenen Daten und zugehörigen Metainformationen (Verarbeitungszwecke etc.) innerhalb der Organisation rasch aufzufinden und diese dem Betroffenen fristgerecht zur Verfügung zu stellen.

Schwierig ist das Herausfiltern aller Daten schon in „herkömmlichen" komplexen Verarbeitungssituationen. Etwa im Beschäftigungskontext sind personenbezogene Daten einer konkreten Person häufig in **zahlreichen speziellen IT-Systemen** (Personalverwaltungssystem, CRM-System, Backup-System etc.), **in allgemeinen IT-Systemen** (E-Mail-System, Netzlaufwerke etc.) **sowie auch in Papierakten** (Personalakte etc.) vorhanden.

Bei **innovativen, datengetriebenen Geschäftsmodellen** (z. B. Daten aus vernetzten Autos; dazu auch **Praxisbeispiel** „**Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars**" (→ C.VII)) ist dieser Prozess typischerweise noch weitaus komplexer. Zwar sind die relevanten Daten ggf. nur in wenigen Systemen vorhanden. Allerdings erfordert die schiere Masse der Daten häufig einen **signifikanten operativen Aufwand, um der betroffenen Person eine komplette Kopie aller Daten auszuhändigen und transparent die jeweiligen Einsatzzwecke und weitere Informationen mitzuteilen**. Gerade bei KI-gestützten Datenverarbeitungsprozessen mag es auch sein, dass der datenschutzrechtlich Verantwortliche nicht einmal alle Daten und von der KI entwickelten konkreten weiteren Verarbeitungszwecke im Einzelnen kennt, geschweige denn diese beauskunften könnte.

VI. Accountability: Umfassende Dokumentations- und Nachweispflichten

1. Verarbeitungsverzeichnis und weitere allgemeine Dokumentationspflichten

Die DS-GVO sieht umfangreiche Dokumentations- und Nachweispflichten vor. Der Grundsatz der Rechenschaftspflicht[48] verlangt, dass der Verantwortliche die Datenschutzgrundsätze nicht nur einhalten, sondern deren Einhaltung auch nachweisen können muss.

---

[47] Zu den hier bestehenden Abgrenzungsschwierigkeiten auch **Praxisbeispiel „Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars"** (→ C.VII).

[48] Art. 5 (2), 24 (1) DS-GVO.

Eine besondere Ausprägung dieses Grundsatzes der Rechenschaftspflicht ist etwa die Pflicht, ein Verarbeitungsverzeichnis zu führen.[49] Das Verarbeitungsverzeichnis muss, ähnlich wie Datenschutzinformationen[50], unter anderem Informationen über die konkreten Verarbeitungszwecke und die jeweils verarbeiteten Kategorien personenbezogener Daten enthalten. Hierfür sind alle Geschäftsprozesse im Detail zu inventarisieren und daraufhin zu überprüfen, ob und welche personenbezogenen Daten für welche Zwecke verarbeitet werden.

Das Verarbeitungsverzeichnis ist dabei nur der Ausgangspunkt der erforderlichen Dokumentation und kann für sich alleine genommen nicht als Nachweis einer datenschutzkonformen Verarbeitung personenbezogener Daten dienen. In größeren Organisationen dauert die vollständige Dokumentation und Bearbeitung der sich daraus ergebenden Folgethemen meist mehrere Monate.

So ist etwa bei Verarbeitungstätigkeiten, die auf Grundlage einer Interessenabwägung[51] erfolgen sollen, eine **umfassende Dokumentation dieser Interessenabwägung** erforderlich.

Für Verarbeitungstätigkeiten, die auf Grundlage einer Einwilligung erfolgen sollen, muss der Verantwortliche in der Lage sein, nachzuweisen, **dass und wie konkret die Einholung der Einwilligung jeweils erfolgt ist**. Das erfordert ein umfangreiches internes **Einwilligungsmanagement**.

Für Verarbeitungstätigkeiten, an denen mehrere Stellen beteiligt sind, sind ggf. **Datenschutzverträge** erforderlich, etwa Verträge zur Auftragsverarbeitung[52] oder zur gemeinsamen Verantwortung[53].

Um einen Überblick über die komplette Datenverarbeitung zu behalten und in der Lage zu sein, die umfangreichen Dokumentations- und Nachweispflichten zu erfüllen, ist jedenfalls bei größeren Organisationen ein robustes Datenschutz-Management-System (DSMS) unerlässlich. Insbesondere muss sichergestellt sein, dass jegliche neue Verarbeitungsaktivität vorab datenschutzrechtlich geprüft wird, das Verarbeitungsverzeichnis aktualisiert wird und betroffene Personen vorab informiert werden. Erst wenn diese formellen Anforderungen erfüllt sind, darf die neue Verarbeitungstätigkeit operativ starten. Das führt nicht nur zu einem hohen administrativen Aufwand, sondern kann

[49] Vgl. Art. 30 DS-GVO.
[50] Dazu oben Abschnitt C.V.1.
[51] Art. 6 (1) (f) DS-GVO.
[52] Art. 28 DS-GVO.
[53] Art. 26 DS-GVO.

auch die Erprobung, Einführung und ggf. Anpassung neuer Geschäftsmodelle verlangsamen. Gerade in typischerweise agilen Erprobungsphasen, die oft zahlreiche, schnell durchzuführende operative und technische Änderungen mit sich bringen, bestehen wegen dieser Schnelllebigkeit Schwierigkeiten, die datenschutzrechtliche Dokumentation aktuell zu halten.

2. Datenschutz-Folgenabschätzungen bei datengetriebenen Technologien

Haben Verarbeitungstätigkeiten voraussichtlich ein hohes Risiko „für die Rechte und Freiheiten natürlicher Personen“ zur Folge, ist eine Datenschutz-Folgenabschätzung durchzuführen.[54] Ziel dieser Maßnahme ist es, die konkreten Risiken zu definieren und durch geeignete Abhilfemaßnahmen zu reduzieren. Gerade bei neuen, datengetriebenen Technologien (z. B. autonome Fahrzeuge, die eine große Masse an Daten über ihre Insassen sowie andere Verkehrsteilnehmer hervorbringen) wird häufig eine Datenschutz-Folgenabschätzung erforderlich sein.

Die Durchführung einer Datenschutz-Folgenabschätzung ist typischerweise ein umfangreiches Projekt und erfordert eine intensive Auseinandersetzung mit allen datenschutzrechtlich relevanten Themen und Risiken der geplanten Verarbeitungstätigkeit.

Wie ausführlich eine solche Dokumentation zu erfolgen hat, verdeutlichen die vom *Bayerischen Landesamt für Datenschutzaufsicht* und vom *Unabhängigen Landeszentrum für Datenschutz Schleswig Holstein* in einem Planspiel zu einem **„Pay-as-you-drive“-Versicherungstarif** durchgeführten Datenschutz-Folgenabschätzungen.[55] Beide Aufsichtsbehörden zeigen, dass eine detaillierte und kleinteilige Auseinandersetzung mit allen erdenklichen Risiken erforderlich ist. Wie das *Bayerischen Landesamt für Datenschutzaufsicht* verdeutlicht, wären in der Realität jedoch noch deutlich umfangreichere Systembeschreibungen erforderlich, als es in dem Planspiel der Fall war.

VII. Verbleibende Rechtsunsicherheit

Bei der Auslegung vieler datenschutzrechtlicher Anforderungen verbleibt im Detail wegen abstrakter Regelungen, unklarer Begriffe und bislang nur punktueller gerichtlicher Klärung noch ein vergleichsweise hohes Maß an Rechtsunsicherheit. Gerade für die Erprobung innovativer, datengetriebener Geschäftsmodelle führt diese Rechtsunsicherheit zu beträchtlichen zusätzlichen praktischen Hürden, zumal es

[54] Vgl. Art. 35 (1) DS-GVO.
[55] Links zu sämtlichen Dokumenten sind unter https://www.lda.bayern.de/de/thema_dsfa.html abrufbar.

hier typischerweise um neuartige Fragestellungen geht, zu denen sich bis dahin häufig weder durch Rechtsprechung oder Behördenstellungnahmen noch in der rechtlichen Literatur robuste Leitlinien für die konkrete Anwendung und Auslegung des Datenschutzrechts herausgebildet haben:

Praxisbeispiel:	**Abgrenzung Anonymisierung und Pseudonymisierung**
Beispielszenario:	Der Anbieter einer SaaS-Lösung für Ärzte (**Praxisbeispiel** „**Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“** (→ C.II)) verarbeitet im Auftrag von Ärzten Patientendaten zur Unterstützung der Behandlung. Dabei handelt es sich um allgemeine Angaben zum Patienten (Patienten-ID, Alter, Größe, Gewicht etc.), Diagnosen sowie um CT- und Röntgenbilder. In anonymer Form möchte das Unternehmen diese Angaben zur Weiterentwicklung seiner SaaS-Lösung nutzen.
Hürde:[56]	Beim Thema Anonymisierung und Pseudonymisierung[57] stehen Unternehmen vor zahlreichen ungelösten Rechtsfragen, die ganz erhebliche Auswirkungen haben können. Klar ist nur, dass die Verarbeitung anonymer Informationen nicht dem Datenschutzrecht unterfällt und dass die Verwendung von Pseudonymen sich zumindest positiv auf die Risiken der Verarbeitung und damit auch auf die Rechtfertigung auswirkt.[58] Umstritten ist jedoch, **unter welchen Voraussetzungen Informationen tatsächlich im Sinne der DS-GVO „anonym“ bzw. „pseudonym“** sind und ob und wie der **Anonymisierungsvorgang datenschutzrechtlich zu rechtfertigen** ist.[59]

[56] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.I.2 und D.III.2.

[57] „**Pseudonymisierung**“ ist „*die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden*“ (Art. 4 (5) DS-GVO).

[58] Vgl. EG 26, 28 DS-GVO.

[59] Das hat beispielsweise auch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit dazu veranlasst, zu diesem Thema ein Konsultationsverfahren durchzuführen: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/03_Konsultationsverfahren.html.

Speichert der SaaS-Anbieter neben der mit dem Ziel einer Anonymisierung bearbeiteten Kopie des Originaldatensatzes weiterhin für den Arzt auch den Originaldatensatz, ist bei Beibehaltung der gleichen Datenqualität **eine Anonymisierung kaum möglich, da über einen Abgleich mit dem für den Arzt gespeicherten Originaldatensatz** (z. B. über den Vergleich der CT-Bilder) eine Reidentifizierung der Patienten möglich wäre. Hohe Rechtsunsicherheit besteht auch dann, wenn der Originaldatensatz **nur bei einem Dritten** lagert (z. B. wenn der SaaS-Anbieter den Originaldatensatz löscht, dieser aber beim Arzt verbleibt), da in diesen Fällen höchst umstritten ist, inwieweit die Kenntnis des Originaldatensatzes beim Dritten auch dem SaaS-Anbieter zuzurechnen ist.

Ist der beim SaaS-Anbieter verbleibende Datensatz nicht anonym, stellt sich die Frage, ob dieser **zumindest pseudonym** ist. Auch hier ist höchst umstritten, wann von einer hinreichenden und damit „echten" Pseudonymisierung auszugehen ist. Enthalten etwa die CT-Bilder biometrische Besonderheiten, die theoretisch eine Identifikation einer konkreten natürlichen Person ermöglichen, ist zweifelhaft, ob der Datensatz tatsächlich pseudonym sein kann, auch wenn ansonsten jeder direkte Bezug zum Patienten entfernt wurde.

Praxisbeispiel: **Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars**

Beispielszenario: Ein Automobilhersteller setzt bei seinen Fahrzeugen zunehmend auf Digitalisierung. Zahlreiche Funktionen des Fahrzeugs lassen sich „on demand" vom Fahrer hinzubuchen/abbestellen, es sind zahlreiche Assistenzfunktionen enthalten, und die Fahrzeugentwickler nutzen unzählige Sensordaten aus dem Realbetrieb der Fahrzeuge, um diese stetig zu verbessern und an die Nutzerbedürfnisse anzupassen. Mit jeder Bewegung des Fahrzeugs entstehen jede Millisekunde weitere Datensätze (zum Bremsen, Beschleunigen, Lenken, Türe öffnen/schließen, zu Bewegungen auf den Sitzen, zur Kolbenstellung und Temperatur des Motors etc.).

Hürde:[60]	Stellt ein Fahrzeugeigentümer einen Auskunftsanspruch und verlangt eine Kopie seiner Daten vom Hersteller, stellt sich zunächst die Frage, wie weit dieser Anspruch überhaupt reicht. Einerseits ist unklar, **welche Fahrzeugdaten überhaupt personenbezogene Daten sind** und bei welchen es sich um reine Maschinendaten handelt (z. B. Kolbenstellungen, Verhalten von Einspritzdüsen etc.). Um Risiken dieser Rechtsunsicherheit zu minimieren, müsste der Hersteller über sämtliche einem Fahrzeug zugeordnete Daten Auskunft erteilen, was bei der **Masse der Daten in einer transparenten Form allenfalls mit exorbitantem Aufwand möglich** ist.[61] Außerdem lässt sich für den Hersteller kaum ermitteln, um **wessen personenbezogene Daten** es sich handelt – schließlich könnte der Fahrzeugeigentümer sein Fahrzeug auch verliehen haben, und die entstandenen Daten wären dem eigentlichen Fahrer zuzuordnen und **dürften dem Eigentümer grundsätzlich nicht offengelegt werden**. Weitgehend unklar ist auch, inwieweit der Fahrzeughersteller beispielsweise wegen des mit der Auskunftserteilung verbundenen immensen Aufwands oder in den Daten ggf. enthaltener Geschäftsgeheimnisse eine **Auskunft verweigern darf**.

Praxisbeispiel:	**Forschung und Statistik zur Verbesserung von Produkten und Dienstleistungen**
Beispielszenario:	Der Anbieter einer SaaS-Lösung für Ärzte möchte Daten aus den jeweiligen Behandlungen in seiner Forschungs- und Entwicklungsabteilung zur Weiterentwicklung der in der SaaS-Lösung enthaltenen künstlichen Intelligenz nutzen (dazu auch **Praxisbeispiel „Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“** (→ C.II)).

[60] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.III.2 und D.VIII.
[61] Dazu schon Abschnitt C.V.2 oben.

Der Anbieter einer innovativen Gesundheits-App möchte Daten aus der App sowie sonstigen Quellen nutzen, um daraus insbesondere Erkenntnisgewinne zu verschiedensten gesundheitlichen Themen zu erlangen. Anhand dessen möchte er neue, an aktuellen Bedürfnissen orientierte Produkte entwickeln und außerdem künftig noch individueller auf einzelne Kunden eingehen (dazu auch **Praxisbeispiel „Big-Data-Analysen und explorative Statistiken“** (→ C.III)).

Beide Anbieter stellen sich die Frage, ob die datenschutzrechtlichen Privilegien[62] für wissenschaftliche Forschung und statistische Zwecke für diese Vorhaben gelten.

Hürde:[63]

Es ist unklar, wie weit die Begriffe der „wissenschaftlichen Forschung“ und der „statistischen Zwecke“ zu verstehen sind. Insbesondere ist die **Abgrenzung zwischen der rein kommerziellen (Weiter-)Entwicklung von Produkten zur privilegierten wissenschaftlichen Forschung** umstritten. Gerade bei der Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. **Gesundheitsdaten**) hat diese Unterscheidung einen erheblichen Einfluss auf die Rechtfertigung der Verarbeitung.

VIII. Keine Vollharmonisierung: Zersplitterte Anforderungen im nationalen Recht der EU-Mitgliedstaaten

Eine weitere praktische Hürde besteht darin, dass in der EU trotz weitreichender Harmonisierung durch die DS-GVO nach wie vor sehr viele unterschiedliche Regelungen zum Datenschutz existieren.

Die DS-GVO verfolgt als EU-weit unmittelbar anwendbare Verordnung[64] das Ziel, eine unionsweit gleichmäßige und einheitliche Anwendung des Datenschutzrechts sicherzustellen, um Hemmnisse für den Verkehr personenbezogener Daten in der Union und eine unionsweite Ausübung von Wirtschaftstätigkeiten zu beseitigen.[65]

Tatsächlich hat die DS-GVO auch in weiten Bereichen zu einer Harmonisierung des Datenschutzrechts geführt. In bestimmten Bereichen gibt es jedoch signifikante Un-

---

62 Vgl. EG 33 DS-GVO, Art. 5 (1) (b), (e), Art. 9 (2) (j), Art. 14 (5) (b), Art. 17 (3) (d) DS-GVO, § 27 (1), (2) BDSG
63 Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.V und D.VIII.
64 Vgl. Art. 288 (2) AEUV.
65 EG 9 ff. DS-GVO.

terschiede nicht nur zwischen den EU-Mitgliedstaaten, sondern auch innerhalb der Mitgliedstaaten, in Deutschland etwa zwischen den einzelnen Bundesländern.

Durch die in der DS-GVO vorgesehenen Spezifizierungsklauseln ist es in einigen Situationen denkbar, dass zumindest für bestimmte Details abweichendes nationales oder sogar Landesrecht besteht. Trotz der an sich vollharmonisierenden Wirkung der DS-GVO ist der Rechtsanwender daher gezwungen, nationales Recht, Landesrecht und bereichsspezifisches Recht zu prüfen, um tatsächlich alle datenschutzrechtlichen Rahmenbedingen ermitteln zu können. So erreichen uns in der Praxis häufig auch Anfragen europäischer Kanzleien zu bestimmten datenschutzrechtlichen Fragestellungen, die sich zwar letztlich weitestgehend auf Grundlage der EU-weit anwendbaren DS-GVO beantworten lassen, also ohne größere nationale Besonderheiten. Im Vorfeld ist das aber natürlich aus Perspektive der europäischen Kanzleien bzw. von deren Mandanten nicht ohne Weiteres ersichtlich.

Räumlich eng umrissene Reallabore mögen hier zwar kurzfristig gewisse Vorteile haben, da neben dem EU-Recht „nur“ Gesetze des jeweilig betroffenen Mitgliedstaats und ggf. Bundeslandes relevant sind. Doch auch bei einer solchen räumlich begrenzten Erprobung neuer Technologien dürfte in der Praxis – nicht zuletzt auf Seiten beteiligter Investoren – oft der Wunsch bestehen, schon in der Entwicklungsphase einschätzen zu können, ob der spätere Betrieb auch über ein räumlich begrenztes Reallabor hinaus Deutschland- oder EU-weit zulässig wäre.

Praxisbeispiel:	**Biometrische Zutrittssysteme für Arbeitnehmer**
Beispielszenario:	Ein Software-Anbieter hat ein biometrisches Zutrittssystem entwickelt. Unternehmen sollen dieses System nutzen können, um ihren Arbeitnehmern Zutritt zu den Räumlichkeiten zu gewähren bzw., je nach Berechtigungsstufe, zu verweigern. Außerdem lässt sich damit die Anwesenheits- und Zeiterfassung automatisieren („digitales Ein- und Ausstempeln“).
Hürde:	Die DS-GVO gewährt den Mitgliedstaaten die Möglichkeit, spezifischere Vorschriften zur Datenverarbeitung im Beschäftigungskontext zu erlassen. Daher können hier in jedem Mitgliedstaat unterschiedliche Anforderungen an solche Zutrittssysteme existieren.[66] Das Produkt ist daher nicht ohne eine Detailprüfung der jeweiligen nationalen Rechtsordnungen EU-weit ausrollbar.

[66] Vgl. Art. 88 DS-GVO. Deutschland hat in § 26 BDSG hiervon Gebrauch gemacht.

Praxisbeispiel:	**Nutzung von Cloud-Diensten durch Krankenhäuser**
Beispielszenario:	Ein Träger von Krankenhäusern möchte die im **Praxisbeispiel „Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“** (→ C.II) vorgestellte SaaS-Lösung bei der Behandlung seiner Patienten nutzen.
Hürde:[67]	Vereinzelte deutsche Landesgesetze **lassen den Einsatz von Auftragsverarbeitern**[68] **außerhalb von Krankenhäusern zumindest ihrem Wortlaut nach nicht zu**.[69] Diese Regelungen gestatten zwar beispielsweise Auftragsverarbeiter zur Mikroverfilmung von Patientenakten innerhalb des Krankenhauses, nicht aber cloud-basierte Lösungen. Der Cloud-Dienstleister muss daher nicht nur die DS-GVO, das deutsche Bundesdatenschutzgesetz (BDSG) und die Vorgaben des Strafgesetzbuches (StGB) einhalten, sondern muss auch **alle einschlägigen landesrechtlichen und berufsrechtlichen Regelungen im Blick haben**. Nur so kann er beurteilen, ob und unter welchen Voraussetzungen sein Produkt überhaupt an das Zielpublikum vermarktbar ist und **welche Lösungen er seinen Kunden zum rechtskonformen Einsatz des Produkts an die Hand geben kann**.

IX. Unabdingbarkeit des Datenschutzrechts

Nicht zuletzt ist auch die Unabdingbarkeit des Datenschutzrechts eine signifikante Hürde. Zwar ist das Datenschutzrecht maßgeblich vom Grundsatz der informationellen Selbstbestimmung und der Teilhabe des Einzelnen geprägt. Dennoch können betroffene Personen gegenüber den ihre Daten verarbeitenden Stellen nicht einfach auf den Schutz ihrer Daten verzichten.

Das gilt nicht etwa nur für interne Anforderungen, wie etwa die Pflicht zur Führung von Verarbeitungsverzeichnissen oder die Durchführung von Datenschutz-

---

[67] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.II.1, D.VIII und E.II.

[68] „**Auftragsverarbeiter**“ ist „*eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*“ (Art. 4 (8) DS-GVO). „*Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf **Weisung des Verantwortlichen** verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind*“ (Art. 29 DS-GVO). Es ist ein Auftragsverarbeitungsvertrag nach Art. 28 (3) DS-GVO erforderlich.

[69] Vgl. etwa § 24 (7) des Berliner Landeskrankenhausgesetzes oder Art. 27 (4) des Bayerischen Krankenhausgesetzes.

Folgenabschätzungen. Nach überwiegender Meinung ist beispielsweise auch ein freiwilliger Verzicht betroffener Personen auf die Erfüllung von Informationspflichten und Datensicherheitsanforderungen nicht möglich.

Praxisbeispiel:	**Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts**
Beispielszenario:	Um seine Gesundheits-App in einer **Betaphase unter Realbedingungen** testen zu können, hat der App-Betreiber aus dem **Praxisbeispiel „Einwilligungserfordernis für innovative Gesundheits-Apps“** (→ C.II) einige wenige Testpersonen gefunden, die die App nutzen und ihm Feedback geben wollen. Dabei handelt es sich um innovationsoffene Tester, die von dieser Technologie begeistert sind und denen Datenschutz hierbei nicht wichtig ist. Ähnliche Daten, die auch die Gesundheits-App verarbeitet (Angaben zur Ernährung, Krankheiten, Laufstrecken, Tagesabläufen etc.) veröffentlichen die Tester ohnehin gerne freiwillig in sozialen Medien, um ihre Erlebnisse mit ihren Followern zu teilen. Um Kosten zu sparen und damit mehr finanzielle Mittel in die eigentliche App-Entwicklung zu stecken, möchte der Betreiber möglichst wenig Datenschutzanforderungen erfüllen müssen, insbesondere kann er auf seinen Testsystemen noch kein State-of-the-Art-Sicherheitsniveau gewährleisten.
Hürde:[70]	Insbesondere beseitigt die Einwilligung nicht die Notwendigkeit der **ausführlichen Information**, die Pflichten zur **Dokumentation in Verarbeitungsverzeichnissen** oder zur **Durchführung einer Datenschutz-Folgenabschätzung** sowie die **Anforderungen an Datensicherheit**.[71]

[70] Zu Gestaltungsspielräumen für dieses Praxisbeispiel unten Abschnitte D.II.3, D.III.3.a) und D.IV.
[71] Vgl. Art. 13, 14, 30, 32, 35 DS-GVO.

D. Praxisempfehlung: Spielräume bei der Erprobung digitaler Innovationen nutzen

Wenngleich die vorstehend skizzierten Hürden des Datenschutzrechts die Entwicklung und Anwendung innovativer Technologien auf den ersten Blick vor große Herausforderungen stellen, lassen die datenschutzrechtlichen Regelungen doch bei näherer Betrachtung an vielen Stellen Gestaltungsspielräume, die sich gerade auch für die Erprobung digitaler Innovationen nutzbar machen lassen.

Im Folgenden geben wir einen Überblick über die nach unserer Wahrnehmung in der Praxis bedeutsamsten Gestaltungsinstrumente im bestehenden Rechtsrahmen. Dabei greifen wir zur Veranschaulichung auch die im vorgehenden Abschnitt herangezogenen Praxisbeispiele auf.

I. Personenbezogene Daten vermeiden: Nutzung anonymer Informationen und synthetischer Daten bei der Erprobung neuer Technologien

Das Datenschutzrecht ist nur auf die Verarbeitung „personenbezogene Daten“ anwendbar, nicht aber auf die Nutzung anonymer Informationen. Ein in der Praxis nicht selten übersehenes, aber durchaus sehr wirkungsvolles Gestaltungsinstrument ist, soweit es das jeweilige Geschäftsmodell zulässt, die Vermeidung personenbezogener Datenverarbeitung.

Was zunächst banal klingen mag, entpuppt sich in der Praxis als häufig unterschätzte Lösung. In der Beratungspraxis beobachten wir nicht selten, dass innovative Technologien bei näherer Betrachtung tatsächlich ebenso gut oder mit nur geringen Einschränkungen auch ohne Verarbeitung personenbezogener Daten realisierbar sind. Schon eine gezielte Reduzierung des Umfangs personenbezogener Datenverarbeitung auf ein absolutes Minimum reduziert den Aufwand für die Einhaltung datenschutzrechtlicher Anforderungen dabei oft signifikant.

1. Personenbezogene Daten als „Nebenprodukt“ vermeiden

Die gezielte Vermeidung der Verarbeitung personenbezogener Daten ist ein effektives Gestaltungsinstrument, um dem Datenschutzrecht (insoweit) zu entgehen.

Eine (Um-)Gestaltung der jeweiligen Prozesse und Produkte dahin, dass sie keine personenbezogenen Daten verarbeiten, ist insbesondere dann denkbar, wenn es bei der jeweiligen Technologie im Kern überhaupt nicht auf einen Personenbezug der verarbeiteten Daten ankommt, sondern personenbezogene Daten unbeabsichtigt, gewissermaßen „als Nebenprodukt“ anfallen.

So mag sich die Erprobung von Sicherheitseinrichtungen des Prototypen eines neuen autonomen Fahrzeugs etwa technisch so gestalten lassen, dass eine **Videokamera dauerhaft Aufzeichnungen der Umgebung** macht, die im cloud-basierten Backend ausgewertet werden. In diesem Fall wäre von der Verarbeitung personenbezogener Daten auszugehen, da etwa Passanten auf den Bildaufzeichnungen erkennbar sein könnten (dazu **Praxisbeispiel** „**Unbeabsichtigte Verarbeitung personenbezogener Daten als „Nebenprodukt" bei der Erprobung autonomer Fahrzeuge**" (→ C.I)).

Um die Verarbeitung personenbezogener Daten zu vermeiden, **mag es technisch machbar sein, anstelle der Videokamera spezielle Sensoren an Bord des Fahrzeuges zu nutzen, die keine Bildaufzeichnung erfordern**.

Bei der blockchain-basierten Speicherung von Transaktionsdaten zu einer elektronischen Geldbörse (dazu **Praxisbeispiel** **„Blockchain-basierte Zahlungstechnologie"** (→ C.III)) erscheint es denkbar, in der Blockchain anstelle personenbezogener Transaktionsdaten zum Nachweis dafür, dass die Daten nicht verändert wurden, **nur nicht direkt personenbezogene Hashes/ Quersummen** zu speichern. Die personenbezogenen Transaktionsdaten würden dann nur in einem **separaten System außerhalb der Blockchain gespeichert, das auch eine spätere Löschung dieser Daten zulässt**.

2. Anonymisierte Informationen nutzen

Auch die Auswertung anonymisierter Informationen ist ein Gestaltungsmittel, um die Verarbeitung personenbezogener Daten für das jeweilige Vorhaben zu vermeiden.

Die Anonymisierung bearbeitet personenbezogene Daten so, dass die betroffene Person auf Grundlage der bearbeiteten Daten danach nicht mehr identifiziert werden kann.[72] Abhängig vom konkreten Informationsgehalt des jeweiligen Originaldatensatzes ist eine Anonymisierung anhand verschiedener Methoden denkbar. Manche Daten lassen sich beispielsweise schon durch Löschung bestimmter Identifikatoren aus dem Originaldatensatz anonymisieren (Löschung von Namen, Patienten-IDs etc.). Gerade umfangreiche Datensätze enthalten allerdings häufig weitere Informationen, anhand derer sich die dahinterstehenden Personen identifizieren lassen (z. B. sehr seltene Merkmale,

[72] Vgl. EG 26 DS-GVO.

über die sich anhand einer Internetrecherche die dahinterstehende Person herausfinden ließe). Auch solche weiteren Informationen wären zu löschen oder so zu aggregieren, dass eine Identifikation nicht mehr möglich ist.

Es ist denkbar, dass ein Anbieter einer SaaS-Lösung für Ärzte die in der Cloud anfallenden Daten anonymisiert und **in anonymer Form für die Weiterentwicklung seines Produkts** verwendet (dazu **Praxisbeispiele** **„Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“** (→ C.II) und **„Abgrenzung Anonymisierung und Pseudonymisierung“** (→ C.VII)). Für eine rechtssichere Anonymisierung wären die in einer Kopie des Originaldatensatzes enthaltenen Informationen so zu **aggregieren**, dass auch zusammen mit einem weiterhin vorhandenen Originaldatensatz keine Identifikation konkreter Patienten mehr möglich ist. Insbesondere könnten hier, abhängig vom konkreten Einzelfall, wohl etwa Bilder (z. B. CT-Bilder) und seltene Diagnosen nicht aus dem Originaldatensatz in den anonymen Datensatz übernommen werden, da anhand solcher Bilder in der Regel eine Zuordnung/Identifikation möglich sein dürfte.

Zwar bedarf hier der Vorgang der Anonymisierung einer Rechtsgrundlage. Für die spätere Auswertung der anonymisierten Datensätze gilt das Datenschutzrecht dann allerdings nicht mehr.

Je mehr Datenelemente in einem für zunächst anonym befundenen Datensatz enthalten sind, desto eher besteht das Risiko, dass zumindest im Zuge des weiteren technischen Fortschritts zu einem späteren Zeitpunkt eine „Deanonymisierung“ möglich werden könnte und die für anonym befundenen Daten dann nicht (mehr) im datenschutzrechtlichen Sinne anonym sind. Insbesondere bei einer längerfristigen Verarbeitung anonymisierter Daten wäre die Anonymisierung daher auch fortlaufend zu verifizieren.

3. Erprobung digitaler Innovationen anhand synthetischer Daten

Synthetische Daten sind ein weiteres Gestaltungsmittel, um die Verarbeitung personenbezogener Daten zu vermeiden. Dabei werden die Nachteile der „einfachen“ Anonymisierung vermieden.

Wie oben beschrieben, ist eine einfache Anonymisierung oft nur mit einer Verringerung der Datenqualität zu erreichen. Synthetische Daten sollen dieses Problem lösen, indem man völlig neue, nicht-personenbezogene Daten generiert, die jedoch die (fast) gleiche Datenqualität aufweisen wie die ursprünglichen personenbezogenen Daten. Für die Erprobung neuer Technologien er-

scheint die Nutzung solcher nahezu realen Daten als eine attraktive und erwägenswerte Alternative.[73]

> Im **Praxisbeispiel** **„Big-Data-Analysen und explorative Statistiken“** (→ C.III) könnte der Anbieter der Gesundheits-App beispielsweise eine künstliche Intelligenz einsetzen, die die im Originaldatensatz der Gesundheits-App bestehenden statistischen Verteilungen, Strukturen und Korrelationen erkennt. Auf dieser Grundlage generiert die künstliche Intelligenz neue Daten, die in ihrer Gesamtheit den Originaldatensatz widerspiegeln, ohne jedoch Rückschlüsse auf konkrete natürliche Personen zuzulassen, auf die sich der Originaldatensatz bezieht.
>
> Zwar bedarf ein solcher Prozess zur Erstellung synthetischer Daten einer Rechtsgrundlage, für die spätere Auswertung der synthetischen, nichtpersonenbezogenen Daten gilt das Datenschutzrecht allerdings nicht mehr.

II. Anreize für betroffene Personen setzen und betroffene Personen aktiv an Reallaboren teilhaben lassen

Das Datenschutzrecht gewährt natürlichen Personen ein hohes Maß an Selbstbestimmung. Das führt auch dazu, dass grundsätzlich jede Verarbeitung personenbezogener Daten zulässig ist, wenn die betroffene Person in Kenntnis der Sachlage mit der Verarbeitung einverstanden ist oder die Verarbeitung zur Erfüllung eines Vertrages mit der betroffenen Person erforderlich ist.

Gerade der innovative und für viele Adressaten sicherlich sehr interessante Charakter von Reallaboren dürfte es erleichtern, Einwilligungen der jeweiligen Teilnehmer zu erhalten. Transparenz und eine aktive Teilhabe der betroffenen Personen an einer Testphase können die Akzeptanz fördern und wirken sich positiv auf die datenschutzrechtliche Rechtfertigung aus.

1. „Einwilligung“ als Gestaltungsinstrument

Mit der Rechtsgrundlage der „Einwilligung“[74] ermöglicht die DS-GVO einen erheblichen Gestaltungsspielraum für die Rechtfertigung der Verarbeitung personenbezogener Daten. Mit ihrer Einwilligung kann die betroffene Person

[73] Siehe etwa auch das auf der österreichischen Innovationsplattform angebotene Projekt zu synthetischen Daten: https://www.ioeb-innovationsplattform.at/marktplatz-innovation/detail/synthetische-daten-von-mostly-ai/.

[74] Vgl. Art. 6 (1) (a) DS-GVO.

grundsätzlich die Verarbeitung jedweder[75] Art ihrer personenbezogenen Daten zu jedem beliebigen Zweck zulassen.

Die Einwilligung muss zwar stets „bestimmt" sein, sich also auf konkrete Verarbeitungszwecke beziehen, über die der Einwilligende im Detail zu informieren ist. Das Datenschutzrecht enthält allerdings keine Aussage dazu, wie konkret ein Zweck bestimmt sein muss, sodass hier bei der Gestaltung der Einwilligung ein gewisser Argumentationsspielraum verbleibt.

Dass ein Verarbeitungszweck nicht zwingend absolut konkret bestimmt sein muss, zeigen schon die Erwägungsgründe der DS-GVO, die im Rahmen wissenschaftlicher Forschung das oft angewandte Konzept des sog. „broad consent" aufgreifen: Kann der Zweck der Verarbeitung personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung „*nicht vollständig angegeben werden*", soll eine breiter gefasste Einwilligung möglich sein, die auf „*bestimmte Bereiche wissenschaftlicher Forschung*" gerichtet ist.[76] Dieser Gedanke lässt sich durchaus auch auf andere Gebiete übertragen, etwa Big-Data-Analysen.

Auch bei sehr datenintensiven und aus datenschutzrechtlicher Sicht invasiven Geschäftsmodellen ist es denkbar, diese auf eine Einwilligung zu stützen. Das gilt etwa für die im **Praxisbeispiel** „**Big-Data-Analysen und explorative Statistiken**" (→ C.III) beschriebenen Auswertungen großer Mengen an (Gesundheits-)Daten aus verschiedensten Quellen zu verschiedensten, noch nicht im Detail vordefinierten Zwecken.

Dabei ist die Einwilligung trotz der noch nicht absolut klaren Zwecke der Verarbeitung dennoch so bestimmt und konkret wie möglich zu gestalten. Es erscheint denkbar, den Verarbeitungszweck und die Einwilligung für diese Big-Data-Auswertungen gerade **anhand ihres experimentellen, ergebnisoffenen Charakters entsprechend weit zu definieren** und dabei nur so konkret zu bleiben, wie es das konkrete Vorhaben eben ermöglicht.

[75] Selbst das spezielle Verarbeitungsverbot für die Verarbeitung besonderer Kategorien personenbezogener Daten lässt sich mit einer (ausdrücklichen) Einwilligung umgehen (vgl. Art. 9 (2) (a) DS-GVO).

[76] EG 33 DS-GVO; siehe hierzu etwa auch die von der Datenschutzkonferenz mit Beschluss vom 15.04.2020 akzeptierten Einwilligungsdokumente der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung (abrufbar unter https://datenschutz.hessen.de/pressemitteilungen/datenschutzbehörden-des-bundes-und-der-länder-akzeptieren-die).

Entscheidend ist dabei eine **faire und transparente** Gestaltung. Den betroffenen Personen muss also bewusst sein, dass es hier um sehr weit gefasste Verarbeitungszwecke geht und welche Risiken damit verbunden sind. Auch hier **dürfte gerade der inhaltlich und zeitlich begrenze Experimentierraum von Reallaboren es häufig erleichtern**, die Rahmenbedingung der Verarbeitungstätigkeit abzugrenzen, konkret zu definieren und somit für die Einholung einer Einwilligung möglichst klar und transparent zu beschreiben.

Bei der Gestaltung der jeweiligen Geschäftsmodelle ist zu berücksichtigen, dass die Einwilligung freiwillig und jederzeit widerruflich ist. Die betroffene Person muss also grundsätzlich eine freie Wahl haben und in der Lage sein, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Bei der Nutzung externer Cloud-Dienste durch Krankenhäuser lässt sich trotz teilweise sehr restriktiver landesrechtlicher Regelungen zumindest argumentieren, **dass die Krankenhäuser Auftragsverarbeiter auf Grundlage einer Einwilligung ihrer Patienten einsetzen dürfen** (dazu **Praxisbeispiel** **„Nutzung von Cloud-Diensten durch Krankenhäuser“** (→ C.VIII)).

Hierbei ist jedoch zu beachten, dass es für den Patienten echte Alternativen zur Erteilung der Einwilligung geben muss. **Der experimentelle Charakter von Reallaboren erscheint hierfür prädestiniert**. Wenn das Krankenhaus die neue cloud-basierte Technologie zur Erprobung einsetzt und zumindest übergangsweise auch noch eine alternative herkömmliche Lösung bereithält, kann der Patient frei wählen, ob er mit Einwilligung am Reallabor teilhaben möchte oder ohne Einwilligung auf die herkömmliche Lösung zurückgreift.

Nicht durch eine Einwilligung überwindbar sind allerdings andere Anforderungen des Datenschutzrechts, wie etwa Informations- und Rechenschaftspflichten oder Datensicherheitsanforderungen.

2. „Vertragserfüllung“ als Gestaltungsinstrument

Der Rechtsanwender hat auch über die Gestaltung der Kundenverträge und des Geschäftsmodells erhebliche Spielräume für die Rechtfertigung der Verarbeitung personenbezogener Daten. Nach der Rechtsgrundlage „Vertragserfüllung“[77] ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn

[77] Vgl. Art. 6 (1) (b) DS-GVO.

sie für die Erfüllung eines Vertrages mit der betroffenen Person oder sie betreffende vorvertragliche Maßnahmen erforderlich ist.

Auch sehr komplexe und dateninvasive Prozesse können sich so rechtfertigen lassen. Die KI-gestützte Verarbeitung personenbezogener Daten zum automatisierten Treffen und Durchführen von Anlageentscheidungen im **Praxisbeispiel** „**Vollautomatisiertes Depotmanagement über Robo-Advisor**“ (→C.IV) wäre bei entsprechender Vertragsgestaltung absoluter **Kern des Depotmanagementvertrages** und damit grundsätzlich zur „Vertragserfüllung“ zulässig. In diesem Fall kann auch die damit verbundene **automatisierte Entscheidungsfindung zulässig**[78] sein.

Dabei ist zu beachten, dass die „Vertragserfüllung“ und die damit einhergehende Gestaltung von Vertragsinhalten kein Allheilmittel ist, weil die jeweilige Datenverarbeitung den Kern des Vertrages betreffen muss; dateninvasive Themen nur im Kleingedruckten zu „verstecken“ würde typischerweise nicht ausreichen.

Nicht alleine durch die „Vertragserfüllung“ überwindbar ist das spezielle Verarbeitungsverbot für besondere Kategorien personenbezogener Daten. Aber auch ist der Umstand der Vertragserfüllung ein argumentativer Ansatzpunkt für die Schaffung einer datenschutzrechtlichen Rechtsgrundlage.

Betreibt im **Praxisbeispiel** **„Einwilligungserfordernis für innovative Gesundheits-Apps“** (→ C.II) nicht ein „normales“ Unternehmen die Gesundheits-App, sondern ein Arzt, könnte dieser sich als Arzt – ohne Einwilligungserfordernis – für die vertragserforderliche Verarbeitung auf einen auf Ärzte zugeschnittenen Ausnahmetatbestand[79] berufen, um das spezielle Verarbeitungsverbot zu überwinden.

[78] Vgl. Art. 22 (2) (a), (3) DS-GVO.
[79] Vgl. Art. 9 (2) (h) DS-GVO.

Für „normale“ Unternehmen greift meist keiner der gesetzlichen Ausnahmetatbestände, sodass selbst die vertragserforderliche Verarbeitung von Gesundheitsdaten einer **ausdrücklichen Einwilligung der Nutzer** bedarf[80]. Obwohl eine Einwilligung freiwillig zu erfolgen hat, wäre in diesem Fall **eine Koppelung der Einwilligung an den Abschluss und die Erfüllung des App-Nutzungsvertrages grundsätzlich zulässig**. Denn die **Einwilligung wäre zur Vertragserfüllung erforderlich**[81].

Hingegen sind etwa Anforderungen an Datensicherheit und Dokumentationspflichten nicht durch die „Vertragserfüllung“ überwindbar.

3. Setzen von Anreizen für die Teilhabe an Reallaboren

Um möglichst viele betroffenen Personen dafür zu gewinnen, an einem Reallabor durch Abschluss entsprechender Verträge und Erklärung von Einwilligungen teilzunehmen, bietet es sich an, ihnen hierfür Vorteile zu gewähren.

In der Praxis ist es beispielsweise bei vielen Onlineshops üblich, dass Kunden einen Gutschein erhalten, wenn sie einen Newsletter abonnieren. Denkbar wäre es etwa auch, unter denjenigen, die eine Einwilligung erteilt haben, eine Verlosung durchzuführen oder für vertragliche Leistungen in der Erprobungsphase besonders attraktive Konditionen vorzusehen.

Solche am Beispiel von Newsletter-Einwilligungen illustrierten Incentivierungen sind auch bei Einwilligungen im Zusammenhang mit digitalen Innovationen denkbar:

- Der Anbieter einer Gesundheits-App könnte für Betatester oder diejenigen, die umfangreichen Big-Data-Analyasen zur Entwicklung neuer Produkte zustimmen, als Anreiz etwa **Pizzagutscheine** ausgeben (hierzu **Praxisbeispiele** „**Big-Data-Analysen und explorative Statistiken**“ (→ C.III) und **„Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts“** (→ C.IX)).

[80] Vgl. Art. 9 (2) (a) DS-GVO.
[81] Art. 7 (4) DS-GVO.

- Die Entwickler KI-gestützter Medizinprodukte oder KI-gestützter Chatbots zur Kundenkommunikation könnten unter den Einwilligenden etwa ein **Smartphone verlosen** (hierzu Praxisbeispiele **„Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“** (→ C.II), „**KI-gestützte Automatisierung der Kundenkommunikation**“ (→ C.IV)).

III. Interessenabwägung in der Praxis nutzen und positiv beeinflussen: Begrenzter Umfang von Reallaboren als Kriterium für die Interessenabwägung

Als zentrale Abwägungsklausel bietet der Rechtfertigungstatbestand der „Interessenabwägung“[82] einen erheblichen Gestaltungsspielraum.

1. Gestaltungsspielraum der Interessenabwägung

Der Rechtfertigungstatbestand der „Interessenabwägung“ gestattet die Verarbeitung personenbezogener Daten, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Diese offene Formulierung führt zwar einerseits zu einer vergleichsweise hohen Rechtsunsicherheit, eröffnet aber andererseits in der Praxis einen ganz erheblichen Anwendungs- und Argumentationsspielraum und ein sehr hohes Maß an Flexibilität. Insbesondere sieht die Regelung keine konkreten Abwägungskriterien vor, ist nicht auf konkrete Verarbeitungssituationen beschränkt und erfordert auch keine Mitwirkung der betroffenen Person (Vertragsschluss oder Einwilligung).

Gerade der Tatbestand der Interessenabwägung zeigt, dass das Datenschutzrecht innovations- und technikoffenen ist. Verantwortliche sind nicht auf starre Rechtfertigungstatbestände angewiesen, die nur ganz bestimmte, gesetzlich vordefinierte Verarbeitungssituationen gestatten. Stattdessen haben sie über die Interessenabwägung die Flexibilität, grundsätzlich jede beliebige „interessengerecht gestaltete“ Verarbeitung vorzunehmen (mit Ausnahme solcher Verarbeitungstätigkeiten, die unter das spezielle Verarbeitungsverbot für „besondere Kategorien personenbezogener Daten“ fallen; hierzu sogleich Abschnitt D.III.3.a)).

[82] Vgl. Art. 6 (1) (f) DS-GVO.

Zwar ist die Verarbeitung auf Grundlage einer Interessenabwägung nur insoweit zulässig, als sie auch tatsächlich für die Wahrung der Interessen des Verantwortlichen oder eines Dritten „erforderlich" ist. Diese Erforderlichkeit lässt sich jedoch zumindest in einem gewissen Umfang auch durch die Gestaltung der jeweiligen Verarbeitungsschritte und der Zweckdefinition beeinflussen. Auf die Beachtung des Erforderlichkeitsgrundsatzes ist in der Praxis besonderes Augenmerk zu legen. Denn in der Praxis fehlt es, vermeidbarerweise, in vielen Verarbeitungssituationen schon an der „Erforderlichkeit" der Verarbeitung für die jeweiligen konkreten Zwecke, sodass es auf die Interessenabwägung im engeren Sinne oft gar nicht mehr ankommt. Das zeigen auch viele der von den Aufsichtsbehörden geschilderten Beispiele, in denen die Behörden eine Unzulässigkeit der Verarbeitung alleine auf Grundlage mangelnder Erforderlichkeit begründen.

2. Interessenabwägung positiv beeinflussen

Unter welchen Voraussetzungen eine Interessenabwägung in einem Reallabor (oder sonstigen Szenarien) zu Gunsten des Verantwortlichen ausfällt, lässt sich nicht pauschal beantworten, sondern bedarf einer detaillierten Einzelfallprüfung.

Die nachfolgenden Punkte zeigen einige in der Praxis sehr relevante Maßnahmen, um die Interessenabwägung positiv zu beeinflussen:

- Mit einer Pseudonymisierung lässt sich das Risiko für die betroffenen Personen senken[83] und damit die Interessenabwägung zu Gunsten des Verantwortlichen positiv beeinflussen.

  Verstärken lässt sich der Effekt der Pseudonymisierung etwa, indem die Informationen zur Zuordnung der pseudonymen Daten zu einer spezifischen betroffenen Person (z. B. Zuordnungstabellen) nicht beim Verantwortlichen selbst lagern, sondern durch einen unabhängigen Datentreuhänder geschützt werden.

[83] Vgl. EG 28 DS-GVO.

Wie im **Praxisbeispiel** **„Abgrenzung Anonymisierung und Pseudonymisierung“** (→ C.VII) ausgeführt, sind zu Unrecht für anonym befundene personenbezogene Daten tatsächlich häufig nur pseudonym oder sogar direkt personenbezogen. Reduziert man den Personenbezug jedoch, soweit dies im jeweiligen Verarbeitungskontext möglich ist, **wirkt sich auch das typischerweise positiv auf die Interessenabwägung aus**.

In der Praxis kommen **Datentreuhändermodelle** beispielsweise in der Forschung zum Einsatz. Hier verarbeiten Forschungsinstitute etwa pseudonymisierte Daten zu Studienteilnehmern, die aus sich heraus nicht unmittelbar personenbezogen sind, während ein unabhängiger Datentreuhänder eine Zuordnungsliste dieser Daten zu den jeweiligen Probanden führt und damit als **externe Kontrollinstanz bei einer etwaig erforderlichen Aufhebung der Pseudonymisierung** dient. Nur unter im Vorfeld konkret festgelegten Bedingungen würde das Forschungsinstitut dann die Kontaktdaten der jeweiligen Probanden erhalten, beispielsweise zur Klärung von Rückfragen mit einzelnen Studienteilnehmern. Vergleichbare Modelle erscheinen beispielsweise bei **Reallaboren im Bereich der wissenschaftlichen Forschung** erwägenswert.

- Gewährt ein Verantwortlicher der betroffenen Person in transparenter Weise ein überobligatorisches[84], bedingungsloses und leicht auszuübendes Widerspruchsrecht, wiegen die schutzwürdigen Belange der betroffenen Person geringer, da sie es selbst in der Hand hat, die Verarbeitung durch ihren Widerspruch jederzeit zu unterbinden. Dieser Effekt verstärkt sich, wenn der Verantwortliche die Verarbeitung erst dann beginnt, wenn die betroffene Person genügend Zeit hatte, vor Beginn der Verarbeitung über die Ausübung des Widerspruchs zu entscheiden.

[84] *Hintergrund:* Die DS-GVO gewährt betroffenen Personen nur für die Datenverarbeitung für Direktwerbung ein bedingungsloses Widerspruchsrecht, bei dem die Verarbeitung nach einem erfolgten Widerspruch nicht mehr erfolgen darf. Ansonsten haben betroffene Personen gegen eine auf eine Interessenabwägung gestützte Verarbeitung nur aus *„Gründen, die sich aus ihrer besonderen Situation ergeben“*, ein Widerspruchsrecht. Im Fall eines solchen Widerspruchs bleibt die Verarbeitung aber zulässig, wenn *„zwingende schutzwürdige Gründe“* die Interessen der betroffenen Person überwiegen (vgl. Art. 21 (1), (2) DS-GVO).

In den **Praxisbeispielen** **„Big-Data-Analysen und explorative Statistiken“** (→ C.III) sowie **„KI-gestützte Automatisierung der Kundenkommunikation“** (→ C.IV) erscheint es etwa denkbar, die jeweiligen Daten erst dann auszuwerten, wenn die betroffenen Personen transparent und rechtzeitig über ihr Widerspruchsrecht informiert wurden und der Verarbeitung nicht widersprochen haben.

- Bei der Interessenabwägung sind die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen.[85] Je eher eine betroffene Person nach objektiven Kriterien mit der Verarbeitung ihrer Daten rechnen muss, desto besser lässt sich diese Verarbeitung auf Grundlage einer Interessenabwägung rechtfertigen.

Zumindest in einem gewissen Rahmen lässt sich die für die Interessenabwägung relevante Erwartungshaltung der Betroffenen auch durch die **transparente Gestaltung der konkreten Verarbeitungssituation** beeinflussen (z. B. Informationen im direkten Kundengespräch oder gut sichtbar platzierte Informationen im Frontend einer Website, anstatt nur in den Datenschutzinformationen).

- Auch Maßnahmen, die eine besonders faire und diskriminierungsfreie Verarbeitung sicherstellen oder die Interessen der betroffenen Personen sonst auf besondere Weise schützen, wirken sich positiv auf die Interessenlage aus.

Denkbar erscheint hier etwa die **Einbeziehung unabhängiger Kontrollinstanzen**, die die Verarbeitung und ihre Auswirkungen auf die betroffenen Personen überwachen (wie z. B. der Ethikkommissionen bei medizinischer Forschung).

- Auch eine sehr enge Zweckbindung und eine sehr kurze Verarbeitungsdauer lassen sich bei der Interessenabwägung als Argument zu Gunsten des Verantwortlichen heranziehen.

[85] Vgl. EG 47 DS-GVO.

Wie im Praxisbeispiel „**Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars**“ (→ C.VII) gezeigt, fallen beim Hersteller von Connected Cars unüberschaubar viele Daten zur Fahrzeugnutzung an (z. B. zur Verbesserung und Weiterentwicklung dieser Fahrzeuge). Hier steht beispielsweise das Risiko im Raum, dass diese Daten auch zu Lasten der Fahrzeughalter/Fahrer verwendet werden könnten. Denkbar wäre hier etwa, dass Ermittlungsbehörden diese Daten herausverlangen könnten, um Verkehrsverstöße aufzudecken. Es erscheint denkbar, solche Risiken etwa dadurch zu reduzieren, dass der Hersteller eine **schnellstmögliche Anonymisierung der Daten auf seinen Systemen sowie die Löschung** der im Fahrzeug gespeicherten Daten gewährleistet.

Erfolgen bei **Testfahrten des Prototypen eines autonomen Fahrzeugs Videoaufzeichnungen**, um feststellen, ob das Fahrzeug sich im Verkehr und insbesondere im Umgang mit besonderen Verkehrssituationen und Hindernissen so verhält wie geplant, ist es denkbar, die Interessenabwägung hier dadurch positiv zu beeinflussen, dass Kennzeichen und Aufzeichnungen von Passanten **schnellstmöglich automatisch schon in den Rohdaten gelöscht werden** (hierzu Praxisbeispiel **„Unbeabsichtigte Verarbeitung personenbezogener Daten als „Nebenprodukt“ bei der Erprobung autonomer Fahrzeuge“** (→ C.I)).

3. Durch Interessenabwägung nicht gestaltbare Aspekte

a) Keine Überwindung spezieller Verarbeitungsverbote durch einfache Interessenabwägung

Die Interessenabwägung lässt sich zwar in den meisten Verarbeitungssituationen nutzen. Dort, wo es spezielle Verarbeitungsverbote gibt, ist eine Verarbeitung allerdings nicht alleine auf Grundlage einer einfachen Interessenabwägung möglich, sondern es ist ein zusätzlicher Ausnahmetatbestand erforderlich (z. B. bei automatisierter Entscheidungsfindung oder bei der Verarbeitung von Gesundheitsdaten).

Greifen Tatbestände, die Ausnahmen von dem speziellen Verarbeitungsverbot für Gesundheitsdaten vorsehen, so kann ausnahmsweise auch die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten im Wege einer Interessenabwägung zu legitimieren sein. Das gilt etwa dann, wenn der App-Anbieter für die Erprobung und Entwicklung seiner Gesundheits-App Gesundheitsdaten seiner Testpersonen verarbeitet, die er aus sozialen Medien abgegriffen hat (hierzu **Praxisbeispiel „Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts“** (→ C.IX)). In diesem Fall gilt das spezielle Verarbeitungsverbot für besondere Kategorien personenbezogener Daten nicht, soweit es um Daten geht, *„die die betroffene Person offensichtlich öffentlich gemacht hat“*.[86]

b) Interessenabwägung nur sehr eingeschränkt für behördliche Verarbeitungen anwendbar

Die DS-GVO gestattet Behörden, die in Erfüllung ihrer Aufgaben handeln, insoweit nicht die Nutzung der „Interessenabwägung“ als Rechtsgrundlage.[87] Zwar ist bislang ist noch nicht abschließend geklärt, wie weit diese Einschränkung im Einzelnen tatsächlich reicht. Zumindest im Bereich der Eingriffs- und Leistungsverwaltung ist die Interessenabwägung jedoch nicht anwendbar.

c) Dokumentationspflichten

Die Durchführung einer Interessenabwägung macht die Dokumentation der Verarbeitungsaktivitäten nicht entbehrlich. Im Gegenteil: Die Interessenabwägung zieht sogar gesteigerte Dokumentationspflichten nach sich. Für die Erfüllung der datenschutzrechtlichen Rechenschaftspflicht ist nicht nur eine Dokumentation der eigentlichen Verarbeitungsaktivität erforderlich, sondern auch eine detaillierte Dokumentation der Interessenabwägung, also der in die Waagschale gelegten Interessen des Verantwortlichen, Dritter und der betroffenen Personen sowie die konkrete Abwägung dieser Interessen.

Zwar ist dies in der Praxis vergleichsweise aufwändig. Jedoch kann der Verantwortliche durch die Dokumentation der konkret durchgeführten Interessenabwägung diesen sehr offen gehaltenen Rechtfertigungstatbestand in konkrete Bahnen lenken und damit greifbarer sowie besser

[86] Vgl. Art. 9 (2) (e) DS-GVO.
[87] Art. 6 (1) Satz 2 DS-GVO.

handhabbar machen, was letztlich zur Rechtssicherheit beiträgt. Selbst wenn eine Aufsichtsbehörde im Ergebnis zu der Bewertung gelangen sollte, dass die Interessenabwägung anders ausfällt und die jeweilige Verarbeitung nicht zulässig ist, wäre eine ordnungsgemäß durchgeführte, objektiv nachvollziehbare und dokumentierte Interessenabwägung für den Verantwortlichen positiv. Denn zumindest bei der Entscheidung über ein etwaiges Bußgeld und dessen Höhe sind alle Umstände des Einzelfalls zu berücksichtigen[88].

IV. Erforderliche Datenschutzmaßnahmen durch Reduzierung der Risiken der Verarbeitung minimieren

Durch gezielte Maßnahmen zur Reduzierung des mit der Verarbeitung einhergehenden Risikos für die betroffenen Personen lassen sich in der Folge auch die datenschutzrechtlich erforderlichen (Schutz-)Maßnahmen minimieren.

Das mit der Verarbeitung einhergehende Risiko ist ein zentraler Richtwert für die Bewertung, welche datenschutzrechtlichen (Schutz-)Maßnahmen im Einzelfall tatsächlich erforderlich sind. Das Risiko ist beispielsweise bei den folgenden Themen zu berücksichtigen:

- Art der Maßnahmen zur Umsetzung der Datenschutzgrundsätze,[89]
- Gestaltung der Sicherheitsmaßnahmen,[90]
- Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.[91]

Je geringer das Risiko für die betroffenen Personen ist, desto geringere Pflichten treffen den Verantwortlichen in Zusammenhang mit der jeweiligen Verarbeitungstätigkeit (z. B. verlangt die Verarbeitung hochsensibler Daten ein höheres Sicherheitsniveau als die Verarbeitung weniger sensibler Daten).

Auch hier können Reallabore dank ihrer räumlichen und zeitlichen Begrenzungen naturgemäß Vorteile haben. Denn auch die Anzahl der betroffenen Personen und Datensätze wirkt sich auf die Höhe des Risikos aus.[92] Beides dürfte in einem Reallabor typischerweise niedriger ausfallen als etwa in einem vollständigen nationalen oder internationalen Rollout eines Geschäftsmodells.

---

88 Art. 83 (2) DS-GVO.
89 Art. 25 (1) DS-GVO.
90 Art. 32 (1) DS-GVO.
91 Art. 35 (1) DS-GVO.
92 In diese Richtung auch Erwägungsgründe 75 und 91 DS-GVO.

Der App-Betreiber im **Praxisbeispiel** **„Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts“** (→ C.IX) ist zwar auch dann an die Anforderungen zur Datensicherheit gebunden, wenn seinen Kunden die Datensicherheit egal sein sollte. Die Verarbeitung betrifft aber zunächst nur einige wenige Testpersonen. Daher ist wohl das **erforderliche Schutzniveau im Testzeitraum zumindest etwas niedriger** als bei einem voll ausgerollten Geschäftsmodell mit Millionen Kunden(daten).

V. Privilegien für Forschung und Statistik nutzen

Die DS-GVO sieht für die wissenschaftliche Forschung und statistische Zwecke zahlreiche Privilegien vor, so etwa für folgende Aspekte:[93]

- Weite Zweckdefinition und „*broad consent*“ für wissenschaftliche Forschung,[94]
- Erleichterungen bei der Zweckbindung und Speicherbegrenzung,
- Ausnahme vom speziellen Verarbeitungsverbot für besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten),
- Bestimmte Ausnahmen von den Informationspflichten und vom Recht auf Löschung.

Eine konkrete und abschließende Definition der Begriffe „wissenschaftliche Forschung“ und „statistische Zwecke“ enthält die DS-GVO jedoch nicht. Die Erwägungsgründe der DS-GVO sprechen durchaus für eine eher weite Auslegung: „*Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken […] sollte weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. […]Die wissenschaftlichen Forschungszwecke sollten auch Studien umfassen, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden.*“[95] Dennoch muss es sich nach Auffassung der Datenschutz-Aufsichtsbehörden um Forschungsprojekte handeln, die mit den einschlägigen sektorspezifischen methodischen und ethischen Standards sowie mit bewährten Verfahren (Good Practice) in Einklang stehen.[96] Unter dem Begriff „statistische Zwecke“ verstehen die Erwägungsgründe der DS-GVO

[93] Vgl. EG 33 DS-GVO, Art. 5 (1) (b), (e), Art. 9 (2) (j), Art. 14 (5) (b), Art. 17 (3) (d) DS-GVO, § 27 (1), (2) BDSG
[94] Dazu schon oben Abschnitt D.II.1.
[95] EG 159 DS-GVO.
[96] Vgl. etwa Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, Working Paper 259.rev01, S. 33 f., abrufbar unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

jeden *„für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche[n] Vorgang der Erhebung und Verarbeitung personenbezogener Daten“*[97]. Auch hier dürfte jedoch grundsätzlich ein wissenschaftlich abgesichertes, auf anerkannten statistischen Methoden basierendes Vorgehen erforderlich sein.

Bei der konkreten Definition dieser vergleichsweise offenen und im Detail umstrittenen Begriffe und somit auch bei der Reichweite der Privilegien für Forschung und Statistik verbleibt derzeit noch Rechtsunsicherheit, damit aber auch ein gewisser Argumentations- und Gestaltungsspielraum. Gerade bei innovativen Reallaboren, die nicht nur „einfach“ neue Produkte entwickeln, sondern tatsächlich einen erheblichen Beitrag zur technologischen Entwicklung[98] und Innovation betragen, ist es abhängig vom konkreten Verarbeitungskontext durchaus denkbar, zu argumentieren, dass diese Privilegien greifen. Insbesondere im Kontext der Verarbeitung besonderer Kategorien personenbezogener Daten kann die Verfolgung wissenschaftlicher Forschungszwecke oder statistischer Zwecke eine ansonsten erforderliche Einwilligung entbehrlich machen.

Im **Praxisbeispiel** **„Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“** (→ C.II) lässt sich der Verarbeitungsvorgang der Anonymisierung der Behandlungsdaten zur Weiterentwicklung der SaaS-Lösung auch bei positiver Interessenabwägung nicht ohne Weiteres rechtfertigen, da diese das spezielle Verarbeitungsverbot alleine nicht überwinden kann.

Allerdings erscheint es hier zumindest denkbar, anstelle der Einwilligung gesetzliche **Ausnahmetatbestände** zu nutzen, die die Verarbeitung von Gesundheitsdaten zulassen. So könnte man hier argumentieren, dass die Verarbeitung aus Gründen des öffentlichen Interesses **zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei Medizinprodukten** oder für **wissenschaftliche Forschungszwecke** erforderlich ist. Für beides sieht das Datenschutzrecht Ausnahmen vom besonderen Verarbeitungsverbot für Gesundheitsdaten vor (siehe auch das **Praxisbeispiel** **„Forschung und Statistik zur Verbesserung von Produkten und Dienstleistungen“** (→ C.VII)).[99]

[97] Vgl. EG 162 DS-GVO.
[98] Vgl. EG 159 DS-GVO.
[99] Vgl. Art. 9 (2) (i), (j) DS-GVO i. V. m. § 22 Abs. 1 lit. c, § 27 Abs. 1 BDSG; für eine weite Auslegung dieser Begriffe auch EG 159 DS-GVO.

Eine ähnliche Argumentation ist auch im Praxisbeispiel **„Big-Data-Analysen und explorative Statistiken“** (→ C.III) denkbar, insbesondere wenn der App-Betreiber seine Auswertungen auf Grundlage wissenschaftlich anerkannter Standards durchführt und hieraus etwa auch Erkenntnisgewinne für die Allgemeinheit resultieren sollen.

Zur Erhöhung der Rechtssicherheit ist es jeweils denkbar, diese **Entwicklungstätigkeiten in gesonderte, unabhängige Forschungsgesellschaften auszulagern**, um so eine klarere Trennung zwischen rein kommerziellen Tätigkeiten und wissenschaftlicher Forschung und Entwicklung herbeizuführen.

VI. Bildsymbole für die Gestaltung von Datenschutzinformationen verwenden

Als Gestaltungsmittel für die transparente Information über die Datenverarbeitung sieht die DS-GVO die Nutzung standardisierter Bildsymbole vor.[100] Diese Bildsymbole sollen nicht die nach der DS-GVO erforderlichen Detailinformationen[101] ersetzen, sondern in Kombination mit diesen Detailinformationen eingesetzt werden.

Gerade bei datenintensiven Verarbeitungstätigkeiten, wie etwa einem smarten Hausautomatisierungssystem, in dem zahlreiche Daten aus verschiedenen Endgeräten zu unterschiedlichsten Zwecken verarbeitet werden, erscheint es denkbar, aussagekräftige Bildsymbole zu verwenden, um den Nutzern auch am kleinen Smartphone-Display zumindest einen guten Überblick über die Verarbeitung zu schaffen (hierzu Praxisbeispiel **„Datenschutzinformationen für ein smartes Hausautomatisierungssystem“** (→ C.V.1)).

Da es für solche innovativen Verarbeitungstätigkeiten noch keine standardisierten Bildsymbole gibt, wäre hier aktuell in erster Linie die Kreativität der Anbieter gefragt, um solche Bildsymbole zu erstellen.

Die DS-GVO sieht in diesem Zusammenhang auch eine zentrale Möglichkeit vor, wie die Exekutive an der Standardisierung und Entwicklung von Bildsymbolen mitwirken und so zur Rechtssicherheit beitragen kann. So ist die Europäische Kommission befugt, delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole darzustellen sind, und der Verfahren für die Bereitstellung solcher standardisierter Bildsymbole zu erlassen.[102] Hier wäre es erforderlich, bei der Europäischen Kommission darauf hinzuwirken, dass sie entsprechend tätig wird.

---

[100] Vgl. Art. 12 (7) DS-GVO.
[101] Vgl. Art. 13, 14 DS-GVO.
[102] Vgl. Art. 12 (8) DS-GVO.

VII. Genehmigte Verhaltensregeln und Zertifizierungen nutzen

Ein weiteres Gestaltungsinstrument zur Steigerung der Rechtssicherheit ist die Nutzung von genehmigten Verhaltensregeln und Zertifizierungen. Diese Selbstregulierungsmechanismen dienen der Präzisierung der Anforderungen der DS-GVO und zum Nachweis für die Einhaltung der DS-GVO.[103]

„*Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten*“,[104] können der zuständigen Aufsichtsbehörde einen Entwurf von Verhaltensregeln vorlegen, den diese genehmigt, wenn sie der Auffassung ist, dass die Verhaltensregeln mit der DS-GVO vereinbar sind und ausreichende geeignete Garantien für den Datenschutz bieten.

Verantwortliche oder Auftragsverarbeiter können von ihnen durchgeführte Verarbeitungen durch die zuständige Aufsichtsbehörde oder eine akkreditierte Zertifizierungsstelle zertifizieren lassen (hierzu sogleich Abschnitt D.VII.2.a)).

1. Höhere Rechtssicherheit durch Verhaltensregeln und Zertifizierungen

Wie oben dargestellt, besteht durchaus Gestaltungs- und Argumentationsspielraum für den datenschutzkonformen Betrieb innovativer Geschäftsmodelle, wobei wegen der abstrakten und technikoffenen Gestaltung der DS-GVO stets eine gewisse Rechtsunsicherheit verbleibt. Mit genehmigten Verhaltensregeln oder einer Zertifizierung im Sinne der DS-GVO lässt sich diese Rechtsunsicherheit erheblich reduzieren (z. B. durch Präzisierungen und Konkretisierungen der Kriterien für die Interessenabwägung oder der Transparenzpflichten).

Gerade für die Erprobung und den Betrieb innovativer, datengetriebener Geschäftsmodelle bietet es sich an, diese Selbstregulierungsmechanismen zu nutzen, da es hier, verglichen mit etablierten, nicht-datengetriebenen Geschäftsmodellen, weitaus mehr Unsicherheitsfaktoren gibt, etwa bei der konkreten Zweckbestimmung einer Big-Data-Analyse (so etwa im **Praxisbeispiel „Big-Data-Analysen und explorative Statistiken“** (→ C.III)). Auch etwa bei der Frage, in welchem Umfang betroffene Personen über die Logik einer automatisierten Entscheidung im Rahmen des Depotmanagements zu informieren sind, erscheint die Nutzung dieser Selbstregulierungsinstrumente denkbar (hierzu **Praxisbeispiel „Vollautomatisiertes Depotmanagement über Robo-Advisor“** (→ C.IV)).

[103] Vgl. Art. 40, 42 DS-GVO.
[104] Art. 40 (2) DS-GVO.

Die konkrete Rechtswirkung von Verhaltensregeln und Zertifizierungen ist zwar umstritten.[105] Allerdings sieht die DS-GVO etwa bei folgenden Aspekten zumindest eine Berücksichtigung genehmigter Verhaltensregeln und genehmigter Zertifizierungsverfahren vor:

- Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.[106]

- Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der Anforderungen an technische und organisatorische Sicherheitsmaßnahmen nachzuweisen.[107]

- Die Einhaltung von genehmigten Verhaltensregeln oder genehmigten Zertifizierungsverfahren ist bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag gebührend zu berücksichtigen.[108]

Restlos ausräumen lässt sich die Rechtsunsicherheit also auch mit diesen Selbstregulierungsmechanismen zwar nicht, doch tragen sie erheblich zur Rechtssicherheit bei, da neben dem Verantwortlichen jeweils eine neutrale Kontrollinstanz involviert ist.

2. Grenzen dieser Selbstregulierungsmechanismen

a) Noch kaum Beachtung in der Praxis

Diese Selbstregulierungsmechanismen wirken natürlich nur dann, wenn sie in der Praxis auch eingesetzt werden. Bislang haben sie sich allerdings in der Praxis noch nicht durchgesetzt.

- Soweit ersichtlich, gibt es bislang in Deutschland nur eine einzige genehmigte Verhaltensregel (die „*Verhaltensregeln für die Prüf-*

[105] Unklar ist bislang, inwieweit Verhaltensregeln und Zertifizierungen eine Bindungswirkung herstellen, also ob eine Verarbeitungstätigkeit tatsächlich stets als rechtskonform zu bewerten ist, wenn sie den Verhaltensregelungen/der Zertifizierung entspricht. Für von der EU-Kommission für allgemeingültig erklärte Verhaltensregeln (Art. 40 (9) DS-GVO) spricht vieles dafür, dass diese normative Wirkung haben. Ansonsten dürften diese Instrumente höchstens zu einer (zumindest faktischen) Selbstbindung der Verwaltung führen.

[106] Art. 24 (3) DS-GVO.

[107] Art. 32 (3) DS-GVO.

[108] Art. 83 (2) (j) DS-GVO.

und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien“[109]).

- Zertifizierungen nach der DS-GVO wurden, soweit ersichtlich, bislang noch überhaupt nicht erteilt. Bislang gibt es auch noch keine akkreditierten Zertifizierungsstellen. Zwar könnten auch Aufsichtsbehörden selbst Zertifizierungen erteilen, allerdings ist auch das bislang wohl noch nicht erfolgt.[110]

Es liegt daher (auch) an den EU-Mitgliedstaaten, die Etablierung dieser Instrumente in der Praxis zu fördern.[111] Uns ist bekannt, dass das BMWi solche Projekte bereits fördert, etwa die Entwicklung eines DSGVO-konformen Zertifizierungsverfahrens für Cloud-Anbieter im Forschungsprojekt „AUDITOR“[112] oder den „*Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung*“.[113]

Auch speziell auf **Reallabore** zugeschnittene Fördermaßnahmen erscheinen denkbar, etwa die Entwicklung von Verhaltensregeln für die Verarbeitung personenbezogener Daten bei der **Erprobung autonomer Fahrzeuge** oder Verhaltensregeln zur Wahrung der berechtigten Interessen betroffener Personen bei **Big-Data-Analysen** durch die jeweiligen Branchenverbände.

b) Nur Präzisierung, aber keine Schaffung neuer Rechtfertigungstatbestände

Verhaltensregeln/Zertifizierungen präzisieren nur die Anforderungen der DS-GVO, können allerdings keine neuen Rechtfertigungstatbestände oder sonst Abweichungen von der DS-GVO schaffen (z. B. wären über Verhaltensregeln keine neuen Abweichungen vom speziellen Verarbeitungsverbot für Gesundheitsdaten möglich).

---

[109] Siehe https://www.datenschutzkonferenz-online.de/media/vr/20180525_vr_pruef_loesch_fristen_genehmigung.pdf und https://www.datenschutzkonferenz-online.de/media/vr/20180525_vr_pruef_loesch_fristen.pdf.

[110] Das Bayerische Landesamt für Datenschutzaufsicht führt auf seiner Website sogar aus, dass es mangels personeller Ressourcen überhaupt keine Zertifizierungen durchführen wird, sondern hierzu ausschließlich auf die noch zu schaffenden akkreditierten Zertifizierungsstellen setzt: https://www.lda.bayern.de/de/thema_zertifizierung.html.

[111] So verlangen es Art. 40 (1), 42 (1) DS-GVO.

[112] Vgl. https://www.auditor-cert.de/zielsetzung/.

[113] Vgl. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p9-code-of-conduct.pdf.

VIII. Aufsichtsbehörden konsultieren

Auch außerhalb des Genehmigungsverfahrens für Verhaltensregeln und Zertifizierungen ist eine Konsultation der zuständigen Aufsichtsbehörde denkbar, in der Betreiber von Reallaboren oder etwa Branchenverbände Stellungnahmen der Aufsichtsbehörde zu bestimmten Themengebieten einholen, um die Rechtsunsicherheit zu reduzieren.

Gesetzlich geregelt und zwingend erforderlich ist eine solche Konsultation nur dann, wenn eine Datenschutz-Folgenabschätzung ergeben hat, dass die Verarbeitung ein hohes Risiko zur Folge hätte.[114] Die praktische Erfahrung zeigt jedoch, dass die Aufsichtsbehörden auch außerhalb dieses gesetzlichen Rahmens auf informeller Grundlage unterstützen. So hat die deutsche Datenschutzkonferenz[115] (DSK) beispielsweise bei der Schaffung von Mustertexten für eine Einwilligung von Patienten in die Nutzung ihrer personenbezogenen Daten für die medizinische Forschung einschließlich einer Patienteninformation unterstützt und die durch die „Medizininformatik-Initiative“ erstellten Dokumente schließlich als datenschutzkonform „akzeptiert“.[116]

Für **Reallabore** erscheint eine solche Abstimmung mit den Aufsichtsbehörden beispielsweise in folgenden Formen denkbar:

[114] Vgl. Art. 36 DS-GVO.

[115] *„Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.“* (siehe https://www.datenschutzkonferenz-online.de/dsk.html).

[116] Vgl. Datenschutzkonferenz, Beschluss vom 15.04.2020 (abrufbar unter https://datenschutz.hessen.de/pressemitteilungen/datenschutzbehörden-des-bundes-und-der-länder-akzeptieren-die); als ein weiteres Beispiel scheinen die Aufsichtsbehörden den „Code of Conduct der Versicherungswirtschaft“ bereits informell anzuerkennen, auch solange dieser noch nicht förmlich als Verhaltensregel im Sinne der DS-GVO anerkannt werden kann, vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Tätigkeitsbericht 2019, S. 88 f.

- Als **generelle Unterstützungsmaßnahme zur Förderung von Reallaboren** zu konkret umrissenen Anwendungsszenarien könnten Branchenverbände oder sonstige Einrichtungen beispielsweise mit Aufsichtsbehörden abgestimmte „Reallabor-Pakete" entwickeln, die standardisierte Muster, etwa für Verarbeitungsverzeichnisse, Datenschutzinformationen und Einwilligungserklärungen, enthalten und die den **Reallaboren als Rahmenwerk dienen und für den Einzelfall nur noch minimal anzupassen wären**. So lässt sich für die einzelnen Reallabore der Dokumentationsaufwand und die Rechtsunsicherheit in diesem Bereich erheblich reduzieren (siehe hierzu etwa das **Praxisbeispiel** **„Datenschutzinformationen für ein smartes Hausautomatisierungssystem"** (→ C.V.1) und die Ausführungen zum Verarbeitungsverzeichnis und weiteren allgemeinen Dokumentationspflichten (→ C.VI.1)).

- Auch zu ganz **konkreten Einzelfragen** erscheint eine Abstimmung mit den Aufsichtsbehörden denkbar, etwa zu den in den **Praxisbeispielen** **„Big-Data-Analysen und explorative Statistiken"** (→ C.III), **„Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars"** (→ C.VII), **„Forschung und Statistik zur Verbesserung von Produkten und Dienstleistungen"** (→ C.VII) und „**Nutzung von Cloud-Diensten durch Krankenhäuser**" (→ C.VIII) beschriebenen Herausforderungen des Datenschutzrechts.

Selbstverständlich hat eine solche informelle Abstimmung keinerlei normative Wirkung, sondern bewirkt nur eine gewisse Selbstbindung der beteiligten Aufsichtsbehörden. Dadurch lässt sich die Rechtunsicherheit in der Praxis jedoch bereits erheblich verringern.

Eine **Liste der Datenschutz-Aufsichtsbehörden** in Deutschland und der EU ist auf der Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit abrufbar.[117]

[117] Siehe https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html.

E. Denkbare Anpassungen im deutschen/europäischen Recht zur Erleichterung der Erprobung digitaler Innovationen

Wenngleich die vorstehend skizzierten Gestaltungsspielräume durchaus geeignet sind, viele als Hürden wahrgenommene Anforderungen des Datenschutzrechts bei der Entwicklung und Anwendung innovativer Technologien zu meistern, bleiben für die Erprobung digitaler Innovationen ohne Frage eine Reihe datenschutzrechtlicher Hindernisse.

Verglichen mit anderen, für viele Reallabore relevanten Rechtsgebiete (z. B. Straßenverkehrsrecht), sind viele dieser Hindernisse durch die beteiligten Organisationen gut überwindbar, sodass eine Anpassung des Datenschutzrechts als solches für den Betrieb von Reallaboren häufig nicht zwingend erforderlich erscheint. Während beispielsweise ein Reallabor für den Betrieb autonomer, bislang noch nicht straßenverkehrsrechtlich freigegebener Fahrzeuge im Straßenverkehr auf gesetzgeberische oder zumindest behördliche Gestaltung angewiesen sein dürfte, lassen sich zentrale datenschutzrechtliche Weichenstellungen etwa über Vertragsgestaltung, Einholung von Einwilligungen und/oder „interessengerechte“ Gestaltung durch das Reallabor vornehmen.

Wollte man diese verbleibenden Hindernisse dennoch aus dem Weg zu räumen, bliebe im Ergebnis nur eine Anpassung des anwendbares Rechtsrahmens, allen voran der DS-GVO (dazu sogleich I.). Im Rahmen der dem nationalen Gesetzgeber verbleibenden datenschutzrechtlichen Regelungsspielräume wären auch punktuelle Anpassungen im deutschen Datenschutzrecht denkbar (dazu II.).

I. Anpassungen im europäischen Datenschutzrecht

Eine pauschale Absenkung des Datenschutzstandards im Sinne einer umfassenden Ausnahme von der DS-GVO für die Erprobung digitaler Innovationen in Reallaboren dürfte mit dem Grundrecht auf Schutz personenbezogener Daten[118] kaum vereinbar sein.

Zumindest denkbar erscheinen hingegen punktuelle Anpassungen speziell für zeitlich und räumlich limitierte und klar spezifizierte Erprobungsszenarien mit einer begrenzten Zahl betroffener Personen, etwa auf Grundlage von spezifizierenden Rechtsvorschriften der EU oder der EU-Mitgliedstaaten, die das jeweilige regulatorische Erprobungsszenario klar umreißen und flankierende Maßnahmen zur Wahrung des Datenschutzes vorsehen, beispielsweise eine strenge und engmaschige Beauf-

[118] Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (Charta), Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV); vgl. auch EG 1 DS-GVO.

sichtigung durch die zuständigen Datenschutzbehörden. Anwendungsfelder für solche punktuellen Anpassungen könnten beispielsweise folgende Aspekte sein, wobei hier ggf. die räumliche und zeitliche Beschränkung von Reallaboren – und damit auch die beschränkte Anzahl verarbeiteter Daten – als Argument für ein reduziertes Risiko und damit für eine ausnahmsweise Abmilderung der datenschutzrechtlichen Anforderungen im Gesetzgebungsverfahren dienen könnte:

- Schaffung einer besonderen gesetzlichen Rechtsgrundlage für die Verarbeitung personenbezogener Daten für Erprobungsszenarien:

  Vergleichbar zu den Forschungsprivilegien der DS-GVO (dazu oben Abschnitt D.V) wäre es denkbar, bestimmte „**Erprobungsprivilegien**" zu schaffen. Denkbar wäre beispielsweise, spezifische Rechtsgrundlagen für Erprobungsszenarien in Art. 6(1) DS-GVO aufzunehmen, die die Verarbeitung personenbezogener Daten in räumlich und zeitlich beschränkten Reallaboren gestatten.

  Denkbar erscheint etwa die Schaffung eines gesonderten Rechtfertigungstatbestandes, der die Verarbeitung personenbezogener Daten zulässt, soweit sie für die Durchführung eines behördlich begleiteten Reallabors erforderlich ist. Die schutzwürdigen Interessen der betroffenen Personen könnten in diesem Fall durch die mit der Sache befasste Behörde als externe Kontrollinstanz gewahrt werden. Ein solches Erprobungsprivileg könnte etwa vorsehen, dass die jeweilige Behörde die Datenverarbeitung zu prüfen hat und weitere individuelle Maßnahmen verlangen kann, soweit das zur Wahrung der Interessen der betroffenen Personen erforderlich ist, etwa ein bedingungsloses Widerspruchsrecht der Teilnehmer (ähnlich Art. 21(2) DS-GVO).

- Erweiterung von Forschungsprivilegien, nicht nur aber auch für Erprobungsszenarien:

  Nicht nur für Reallabore, sondern auch außerhalb des Reallabore-Kontext, erscheint es außerdem denkbar, die in der DS-GVO bereits angelegten Forschungsprivilegien durch einen gesonderten Rechtfertigungstatbestand zu erweitern, der keine Umsetzung in mitgliedstaatliches Recht erfordert und der die Verarbeitung personenbezogener Daten unter gewissen forschungsfreundlichen Voraussetzungen gestattet, soweit das für das jeweilige Forschungsvorhaben erforderlich ist.

Auch hier wären Maßnahmen zum Schutz der Interessen der betroffenen Personen zu treffen, etwa eine besondere Zweckbindung, die eine forschungsfremde Weiterverarbeitung unterbindet.

- Schaffung von besonderen Ausnahmetatbeständen zur Verarbeitung besonderer Kategorien personenbezogener Daten in Erprobungsszenarien, etwa zur Erfüllung von Verträgen mit den betroffenen Personen:

  Hierzu müsste der Katalog der Ausnahmetatbestände in Art. 9 (2) DS-GVO um spezifische Erprobungsausnahmen ergänzt werden. Auch hier erscheint die Schaffung einer Art „**Erprobungsprivileg**" denkbar.

- Lockerungen im Bereich der Betroffenenrechte in Erprobungsszenarien, insbesondere im Bereich der Informationspflichten, etwa durch freiwillige Abdingbarkeit individueller Rechte durch betroffene Personen:

  Es erschiene etwa denkbar, in Art. 12 DS-GVO zu regeln, dass Betroffene in behördlich streng kontrollierten Erprobungsszenarien beispielsweise freiwillig für einen bestimmten Zeitraum auf die Geltendmachung ihrer Betroffenenrechte, insbesondere Auskunftsrechte, verzichten können.

- Erleichterungen bei Datensicherheitspflichten in Erprobungsszenarien, beispielsweise durch freiwillige Abdingbarkeit von Sicherheitsstandards durch betroffene Personen:

  Hier käme eine Anpassung des Art. 32 DS-GVO in Betracht, nach der in Erprobungsszenarien von bestimmten Sicherheitsanforderungen mit Zustimmung der betroffenen Personen ausnahmsweise abgewichen werden kann.

- Erleichterungen bei Dokumentationspflichten in Erprobungsszenarien, etwa bei der Pflicht zur Führung eines Verarbeitungsverzeichnisses oder der Durchführung von Datenschutz-Folgeabschätzungen:

  Für eine effektive Absenkung der Dokumentationspflichten in Erprobungsszenarien wären insbesondere Anpassungen der Art. 5 (2), 24, 30 (1) und 34 DS-GVO erforderlich.

Auch die deutschen Datenschutzbehörden haben bereits punktuelle Anpassungen der DS-GVO vorgeschlagen, die in der Praxis auch für die Erprobung von innovativen Geschäftsmodellen zu einer gewissen Erleichterung führen könnten.[119]

Dabei ist jedoch zu beachten, dass für etwaige Anpassungen der DS-GVO auch im Einzelnen zu prüfen wäre, ob der europäische Gesetzgeber hierfür auch die erforderlichen Kompetenzen hat. Beispielsweise im Arbeits- und Sozialrecht oder in der Gesundheitsvorsorge und der Medizin mag es an erforderlichen Kompetenzen zur Regelung auf EU-Ebene fehlen.

Vor allem erfordert aber jedwede Anpassung eine sorgfältige Abwägung der widerstreitenden Grundrechte und Grundfreiheiten unter Wahrung des Verhältnismäßigkeitsprinzips, insbesondere der Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, des Schutzes personenbezogener Daten, der Gedanken-, Gewissens- und Religionsfreiheit, der Freiheit der Meinungsäußerung und Informationsfreiheit sowie der unternehmerischen Freiheit.[120] Auf Seiten der Reallabore ließe sich bei dieser Abwägung für eine partielle Absenkung des Datenschutzniveaus ggf. auch der teils faktisch prohibitive Charakter bestimmter datenschutzrechtlicher Hürden ins Feld führen. Die Kosten für die Erfüllung aller Dokumentationspflichten lassen sich bei einem etablierten, breit ausgerollten Geschäftsmodell etwa typischerweise leichter amortisieren, während sie demgegenüber für ein Reallabor in Form eines „Start-Ups“ bereits eine unüberwindbare Hürde darstellen könnten.

Eine Änderung des europäischen Rechtsrahmens, namentlich der DS-GVO, dürfte allerdings allenfalls als mittel- bis langfristige Lösung in Betracht kommen. Der Gesetzgebungsprozess für die DS-GVO hat alles in allem mehr als 7 Jahre in Anspruch genommen. Während des Gesetzgebungsprozesses wurden auch bereits zumindest manche der obigen Anpassungsvorschläge diskutiert und letztendlich verworfen[121]. Auch das Gesetzgebungsverfahren zur E-Privacy-VO dauert nunmehr schon seit mehr als 3 Jahren an. Eine kurzfristige Änderung des europäischen Rechtsrahmens erscheint vor diesem Hintergrund nicht realistisch.

---

[119] DSK; Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/12/20191209_Erfahrungsbericht-zur-Anwendung-der-DS-GVO.pdf, zuletzt abgerufen am 14.05.2020.

[120] Dazu auch EG 4 DS-GVO.

[121] So enthielt der Kommissionsentwurf der DS-GVO etwa noch den Vorschlag, dass die Kommission den Rechtfertigungstatbestand der Interessenabwägung durch delegierte Rechtsakte näher regeln kann. Auch andere Forderungen, den Rechtfertigungstatbestand der Interessenabwägung näher zu präzisieren oder etwa Regelbeispiele im Text der DS-GVO vorzusehen, wurden letztendlich nicht in der DS-GVO umgesetzt.

II. Anpassungen im deutschen Recht

Die DS-GVO lässt dem nationalen Gesetzgeber durch vereinzelte Spezifizierungsklauseln gewisse Regelungsspielräume.

1. Gestaltung fachrechtlicher Anforderungen, denen ein Reallabor unterfällt (z. B. Straßenverkehrsrecht)

Durch die Gestaltung fachrechtlicher Anforderungen an die Betreiber von Reallaboren lassen sich datenschutzrechtliche Rechtfertigungstatbestände schaffen und Dokumentationspflichten und Rechtsunsicherheiten reduzieren.

Das Datenschutzrecht gestattet grundsätzlich die Verarbeitung personenbezogener Daten, soweit das erforderlich ist, um eine rechtliche Verpflichtung zu erfüllen, der der Verantwortliche unterliegt.[122] Für den Verantwortlichen schaffen solche rechtlichen Verpflichtungen, die von ihm eine bestimmte Verarbeitung verlangen, Rechtssicherheit. Denn der Verantwortliche muss dann nicht selbst etwa eine Interessenabwägung durchführen und verantworten, sondern der Gesetzgeber hat für ihn bereits eine Abwägungsentscheidung getroffen.

Selbstverständlich kann sich eine Organisation nicht selbst solche rechtlichen Verpflichtungen auferlegen, um damit jegliche Verarbeitung zu rechtfertigen. Gerade bei solchen Reallaboren, die ohnehin aus anderen regulatorischen Gründen Gesetzesänderungen erfordern, beispielsweise in Form von Experimentierklauseln, erscheint es jedoch denkbar, hier zumindest auch bestimmte Datenverarbeitungen gesetzlich zu regeln und so Rechtssicherheit zu schaffen:

[122] Vgl. Art. 6 (1) (c) DS-GVO sowie für die Zweckänderung Art. 6 (4) DS-GVO und für eine Ausnahme vom Verarbeitungsverbot für besondere Kategorien personenbezogener Daten Art. 9 (2) (g) DS-GVO.

Bei der **Erprobung autonomer Fahrzeuge** ist in besonderem Maße der **Schutz anderer Verkehrsteilnehmer** zu gewährleisten. Hier wäre es aus datenschutzrechtlicher Perspektive etwa denkbar, die Unternehmen, die autonome Fahrzeuge testen, im Wege einer begleitenden Pflicht gesetzlich zu verpflichten, **Videoaufzeichnungen** zum Zweck des Schutzes anderer Verkehrsteilnehmer und zum Zweck der Prüfung der im Fahrzeug enthaltenen Sicherheitssysteme vorzunehmen (hierzu **Praxisbeispiel „Unbeabsichtigte Verarbeitung personenbezogener Daten als „Nebenprodukt" bei der Erprobung autonomer Fahrzeuge"** (→ C.I)). Ein solches Gesetz müsste angemessene Datenschutzvorkehrungen vorsehen und insbesondere auch den Grundsatz der Verhältnismäßigkeit wahren, etwa durch Regelung von Schutzmechanismen für die betroffenen Passanten (z. B. Verpixelung; hierzu auch sogleich).

Auch im **Praxisbeispiel „Vollautomatisiertes Depotmanagement über Robo-Advisor"** (→ C.IV) erscheint es aus datenschutzrechtlicher Perspektive denkbar, im Wertpapierhandelsrecht konkret festzulegen, welche personenbezogenen Daten ein Robo-Advisor bei seinen Entscheidungen berücksichtigen muss. Dadurch ließe sich etwa Rechtsunsicherheit über die Frage umgehen, welche Verarbeitung tatsächlich „erforderlich" für die Vertragserfüllung ist.

An mitgliedstaatliche Regelungen, die eine Verarbeitung personenbezogener Daten erfordern, stellt die DS-GVO gewisse Mindestanforderungen und erlaubt solchen Verpflichtungen darüber hinaus, weitere datenschutzrechtliche Aspekte konkret zu regeln:

- Als Mindestvoraussetzung muss die mitgliedstaatliche Rechtsgrundlage, die einen Verantwortlichen zu einer bestimmten Verarbeitung personenbezogener Daten verpflichtet,
    - den „*Zweck der Verarbeitung*" festlegen,
    - „*ein im öffentliches Interesse liegendes Ziel verfolgen*" und
    - „*in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen*".[123]
- Die mitgliedsstaatliche Rechtsgrundlage kann außerdem weitere spezifische Bestimmungen enthalten, unter anderem zu folgenden Themenbereichen:[124]

[123] Art. 6 (3) Satz 2 und 4 DS-GVO.

- Allgemeine Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen
- Arten von Daten, die verarbeitet werden sollen
- Welche Personen betroffen sein sollen
- An welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen
- Welcher Zweckbindung die Daten unterliegen
- Welche Speicherdauer einzuhalten ist
- Welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen
- Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung

Je konkreter diese mitgliedstaatliche Rechtsgrundlage vorgibt, welche Daten wie zu verarbeiten sind, desto mehr Rechtssicherheit entsteht hierdurch für die jeweilige Organisation, die zur Verarbeitung verpflichtet sein soll. Denn durch eine möglichst konkrete Regelung reduzieren sich Auslegungsschwierigkeiten bei der Frage vermeiden, welches Maß an Datenverarbeitung konkret zur Erfüllung der jeweiligen Rechtspflicht tatsächlich „erforderlich“[125] ist.

Im Gesetzgebungsprozess haben die Mitgliedstaaten auch die Möglichkeit, eine allgemeine Datenschutz-Folgenabschätzung durchzuführen und die Rechtsanwender von der Pflicht zur Durchführung einer individuellen Datenschutz-Folgenabschätzung zu befreien.[126]

2. Anpassungen im deutschen Datenschutzrecht

Auch darüber hinaus erscheinen in dem relativ engen Regelungsspielraum, den die DS-GVO dem nationalen Gesetzgeber lässt, zumindest punktuelle Anpassungen speziell für eng umrissene Erprobungsszenarien denkbar, etwa in folgenden Anwendungsfeldern:

---

[124] Vgl. Art. 6 (3) Satz 3 DS-GVO.
[125] Vgl. die Anforderung an die „Erforderlichkeit“ der Datenverarbeitung etwa in Art. 6 (1) (c) DS-GVO.
[126] Vgl. Art. 35 (10).

- besondere Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zur Erprobung neuer Technologien, die im öffentliches Interesse liegen,[127]

- Schaffung von besonderen Rechtsgrundlagen für Zweckänderungen zur Erprobung neuer Technologien,[128]

- Spezifizierungen für die Verarbeitung personenbezogener Daten zur Erprobung neuer Technologien im Arbeitnehmerkontext.[129]

Nicht nur für Reallabore zielführend könnte auch eine bundesweite Harmonisierung der datenschutzrechtlichen Regelungen in den Landesgesetzen der Bundesländer sein. Beispielsweise wäre denkbar, über die Anforderungen der DS-GVO hinausgehende Restriktionen im Krankenhausbereich auf Landesebene zu beseitigen und länderübergreifend anzugleichen (hierzu **Praxisbeispiel „Nutzung von Cloud-Diensten durch Krankenhäuser“** (→ C.VIII)).

Im Gegensatz zu einer Änderung des europäischen Rechtsrahmens (dazu oben) erscheint eine Anpassung nationaler Regelungen auch kurz- bis mittelfristig realistisch, wenngleich der Regelungsspielraum hier stark begrenzt ist.

Etwaige nationale Regelungen wären im Einzelnen dahingehend zu prüfen, ob die Spezifizierungsklauseln der DS-GVO tatsächlich ausreichenden Regelungsspielraum für den nationalen Gesetzgeber belassen. Darüber hinaus bedarf auch im nationalen Recht jedwede Anpassung ebenfalls einer sorgfältigen Abwägung der widerstreitenden Grundrechte und Grundfreiheiten unter Wahrung des Verhältnismäßigkeitsprinzips (dazu schon oben).

[127] Vgl. Art. 6 (1) (e), (3) DS-GVO.
[128] Vgl. Art. 6 (4) DS-GVO.
[129] Vgl. Art. 88 DS-GVO.

F. Europäischer und internationaler Vergleich

Um die Attraktivität Deutschlands als Innovationsstandort im europäischen und internationalen Vergleich der datenschutzrechtlichen Rahmenbedingungen einordnen zu können, wurden wir gebeten, auf Basis der in diesem Gutachten gewonnenen Erkenntnisse in weiteren, gesonderten Schritten jeweils anhand von zwei ausgewählten Beispiel-Jurisdiktionen in der EU und außerhalb der EU

- eine Einschätzung vorzunehmen, wie sich das deutsche/europäische Datenschutzrecht mit Blick auf die Erprobung/Umsetzung digitaler Innovationen im **internationalen Maßstab** darstellt, sowie

- den **europäischen Vergleich** in den Blick zu nehmen und zu prüfen, ob andere EU-Mitgliedstaaten zu den in Abschnitt E.II skizzierten Ansätzen vergleichbare Lösungen bereits eingeführt haben, um in datenschutzrechtlicher Hinsicht (mehr) Flexibilität zur Erprobung innovativer Geschäftsmodelle zu bieten.

Für den **internationalen Vergleich** wurden wir gebeten, als Beispiel-Jurisdiktion zum einen den als sehr als innovationsfreundlich wahrgenommene US-Bundesstaat **Kalifornien** (dazu **Abschnitt F.I.1**) zu betrachten. Außerdem sollten wir **Japan** (dazu **Abschnitt F.I.2**) in den Blick nehmen, dem die Europäische Kommission ein der EU vergleichbares Datenschutzniveau bescheinigt hat.

Für den **europäischen Vergleich** wurden wir gebeten, als Beispiel-Jurisdiktionen **Frankreich** (dazu **Abschnitt F.II.1**) und **Ungarn** (dazu **Abschnitt F.II.2**) zu betrachten.

I. Internationaler Vergleich

1. Kalifornien

a) Überblick über Datenschutzrecht in Kalifornien

Am 1. Januar 2020 trat in Kalifornien ein neues Verbraucherdatenschutzgesetz in Kraft, der „California Consumer Privacy Act" (***„CCPA"***)[130]. Vom kalifornischen Generalstaatsanwalt erlassene Durchführungsbestimmungen zum CCPA (***„CCPA Regulations"***)[131] legen detaillierte zusätzliche Anforderungen an Mittel und Methoden zur Einhaltung des Gesetzes fest.

Der CCPA gilt für „**persönliche Informationen**". Die vergleichsweise weite Definition des Begriffs ist der Definition der „personenbezogenen Daten" im deutschen/europäischen Datenschutzrecht ähnlich. Allerdings gilt der CCPA im Unterschied zum deutschen/europäischen Datenschutzrecht nicht für personenbezogene Daten aller natürlichen Personen, sondern nur für persönliche Informationen von „**Verbrauchern**". Jedoch schließt die relativ weite Definition des für den CCPA maßgeblichen Verbraucherbegriffs neben typischen Verbrauchern von Waren und Dienstleistungen auch Beschäftigte ein.

Im Unterschied zum deutschen/europäischen Datenschutzrecht sieht der CCPA einen **schwellwertbasierten Anwendungsbereich** vor, der insbesondere kleinere Unternehmen mit vergleichsweise geringem Umfang von Datenverarbeitungstätigkeiten pauschal ausnimmt:

Der CCPA gilt für **gewinnorientierte Unternehmen**, die in Kalifornien geschäftlich tätig sind, persönliche Informationen über kalifornische Verbraucher verarbeiten, die Zwecke und Mittel der Verarbeitung dieser Informationen festlegen und **eines oder mehrere der folgenden Kriterien** erfüllen:

- Das Unternehmen erzielt **Einnahmen von mehr als 25 Millionen** USD jährlich,
- das Unternehmen hat **mehr als 50.000 kalifornische Nutzer**, und/oder

[130] https://oag.ca.gov/privacy/ccpa.
[131] https://oag.ca.gov/privacy/ccpa/regs.

- das Unternehmen erzielt **mehr als 50 % der Einnahmen aus dem „Verkauf" persönlicher Informationen**.

Der CCPA gilt auch für jedes Unternehmen, das ein Unternehmen kontrolliert oder von einem Unternehmen kontrolliert wird, das die obigen Kriterien erfüllt, vorausgesetzt, dass die Unternehmen zu einem gemeinsamen Branding gehören.

Gemeinnützige und staatliche Einrichtungen unterliegen dem CCPA **nicht**. Darüber hinaus unterliegen auch Daten, die unter Gesundheitsgesetze fallen, wie Daten von Gesundheitseinrichtungen und -anbietern sowie Daten, die Teil der formellen Gesundheitsforschung sind, nicht dem CCPA.

Erst kürzlich wurde außerdem der „California Privacy Rights Act" (***„CPRA"***)[132] verabschiedet, der am 1. Januar 2023 in Kraft treten soll. Der CPRA ergänzt und verschärft den CCPA. Der CPRA führt beispielsweise eine neue Kategorie sensibler persönlicher Informationen mit besonderen Anforderungen an Transparenz und Opt-In/Opt-Out für deren Erhebung ein. Der CPRA ergänzt außerdem weitere Verbraucherrechte. Zudem führt der CPRA die Grundsätze der Datenminimierung, der Speicherbegrenzung und der Zweckbindung ein. Der CPRA erhöht allerdings auch die Schwelle für die Anwendung des CCPA und des CPRA für Unternehmen, die persönliche Informationen kaufen, erhalten, verkaufen oder teilen (vgl. oben), von jährlich 50.000 auf 100.000 Nutzer.

Neben CCPA und CPRA finden in Kalifornien einige weitere Gesetze mit Bezug zu Daten und Datenschutz Anwendung. Größtenteils handelt es sich dabei um „sektorspezifische" Regelungen, die sich auf bestimmte (typischerweise regulierte) Industrien beziehen, beispielsweise das Gesundheitswesen oder Finanzinstitute.[133]

Für Kalifornien existiert derzeit kein Angemessenheitsbeschluss der Europäischen Kommission.[134] Den Angemessenheitsbeschluss der Europäischen Kommission für unter dem EU/US Datenschutzschild zertifizierte Unternehmen in Kalifornien hat der Europäische Gerichtshof (EuGH) für

---

[132] https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

[133] Einen Überblick über die einzelnen in Kalifornien anwendbaren Datenschutzgesetze gibt die Website des Generalstaatsanwalts von Kalifornien: https://oag.ca.gov/privacy/privacy-laws.

[134] Vgl. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

ungültig erklärt.[135] In seinem Urteil stellte der EuGH ausdrücklich fest, dass in den USA derzeit kein angemessenes Datenschutzniveau bestehe.

b) Hürden für die Erprobung digitaler Innovationen im kalifornischen Datenschutzrecht im Vergleich zum deutschen/europäischen Datenschutzrecht

Zusammengefasst gibt der CCPA im Wesentlichen folgenden datenschutzrechtlichen Rahmen vor, der zumindest punktuell auch Aspekte des deutschen/europäischen Datenschutzrechts aufgreift:

- Transparenz: Unternehmen müssen Verbrauchern bestimmte Informationen über ihre Datenschutzpraktiken bereitstellen.

- Verbraucherrechte: Verbraucher haben bestimmte Rechte in Bezug auf ihre persönlichen Informationen, insbesondere Rechte auf Information, Auskunft und Löschung.

- Verbotene Geschäftspraktiken: Bestimmte Geschäftspraktiken mit persönlichen Informationen sind verboten. Insbesondere ist der „Verkauf" persönlicher Informationen verboten, es sei denn, ein Unternehmen hat darüber informiert und Erwachsenen ein Widerspruchsrecht (Opt-Out) eingeräumt oder von Kindern eine Einwilligung (Opt-In) eingeholt.

- Operative Anforderungen: Unternehmen müssen Personal, das mit persönlichen Informationen umgeht, hinsichtlich der Anforderungen des CCPA schulen. Insbesondere zur Beantwortung von Anfragen von Verbrauchern müssen Unternehmen eine angemessene Dokumentation vorhalten. Für Verträge mit Dienstleistern sind bestimmte Regelungen zum Datenschutz erforderlich.

Im Vergleich zu den im deutschen/europäischen Datenschutzrecht identifizierten Hürden für die Erprobung digitaler Innovationen (vgl. Abschnitt C.) lässt sich Folgendes feststellen:

- Der CCPA kennt **kein generelles „Verarbeitungsverbot mit Erlaubnisvorbehalt"** (vgl. Abschnitt C.I.), sondern lediglich gezielte Verbote besonderer Geschäftspraktiken.

[135] EuGH - Urteil vom 16.07.2020 - Rechtssache C-311/18 - Data Protection Commissioner gegen Facebook Ireland Ltd („Schrems II"),, http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677.

- Der CCPA kennt **kein spezielles Verarbeitungsverbot für „besondere Kategorien personenbezogener Daten“** (vgl. Abschnitt C.II.). Erst der CPRA führt das Konzept der sensiblen persönlichen Informationen ein, für die besondere Anforderungen gelten. Allerdings erfordert der Umgang mit sensiblen Daten auch auf Grundlage anderer Gesetze typischerweise einen höheren Sorgfaltsmaßstab.

- Der CCPA kennt (noch) **keine Zweckbindung, Datenminimierung und Speicherbegrenzung** (vgl. Abschnitt C.III.). Erst der CPRA führt diese Grundsätze ein.

- Auch das **grundsätzliche Verbot „automatisierter Entscheidungen“** (vgl. Abschnitt C.IV.) ist im CCPA **nicht** vorgesehen. Der CPRA wird jedoch Opt-Out-Anforderungen für bestimmte Formen automatisierter Entscheidungen einführen.

- Der CCPA sieht **umfassende Transparenzanforderungen und weitreichende Betroffenenrechte** (vgl. Abschnitt C.V.) vor, die im Einzelnen sogar deutlich umfangreicher sind, als die Vorgaben im deutschen/europäischen Recht.

- Der CCPA sieht **keine derart umfassende Dokumentations- und Nachweispflichten** (vgl. Abschnitt C.VI.) vor wie das deutsche/europäische Datenschutzrecht. Jedoch müssten auch Unternehmen, die dem Anwendungsbereich des CCPA unterfallen, angemessene Dokumentation vorhalten, um Anfragen von Verbrauchern zur Geltendmachung ihrer Rechte beantworten zu können.

- Auch unter dem CCPA verbleibt **erhebliche Rechtsunsicherheit** (vgl. Abschnitt C.VII.), zumal es sich bei dem Gesetz im Gegensatz zu deutschen/europäischen Datenschutzrecht um eine vergleichsweise junge Gesetzgebung handelt, bei der viele Rechtsfragen im Detail noch ungeklärt sind.

- Ebenso wie die **zersplitterten Anforderungen im nationalen Recht** der EU-Mitgliedstaaten (vgl. Abschnitt C.VIII.) stellen die verschiedenen nationalen datenschutzrechtlichen Regelungen der US-Bundesstaaten Unternehmen, die in mehreren Staaten tätig sind, vor große Herausforderungen.

- Zwar gilt auch unter dem CCPA grundsätzlich eine **Unabdingbarkeit des Datenschutzrechts** (vgl. Abschnitt C.IX.), Verbraucher

können also auf die Einhaltung der datenschutzrechtlichen Anforderungen ebenfalls nicht einfach verzichten. In der Praxis stellt diese Unabdingbarkeit allerdings eine deutliche niedrigere Hürde auf, da die Anforderungen des CCPA im Vergleich zum deutschen/europäischen Datenschutzrecht insgesamt betrachtet deutlich weniger umfangreich ausfallen.

Im Ergebnis lässt sich also festhalten, dass der CCPA im Vergleich zum deutschen/europäischen Datenschutzrecht in weiten Teilen deutlich weniger bzw. niedrigere Hürden aufstellt. Allerdings stellt der CCPA punktuell sogar höhere Hürden auf, etwa im Bereich der Transparenzanforderungen.

c) Spielräume bei der Erprobung digitaler Innovationen in Kalifornien

Da es sich beim CCPA und dem verabschiedeten, aber noch nicht in Kraft getretenen CCRA um vergleichsweise junge Gesetzgebungen handelt, lässt sich derzeit noch nicht prognostizieren, wie Unternehmen in der Praxis die rechtlichen Hürden bei der Erprobung digitaler Innovationen angehen werden.

Übergreifend lässt sich allerdings festhalten, dass der CCPA im Vergleich zum deutschen/europäischen Datenschutzrecht gerade für die Erprobung digitaler Innovationen deutlich größere Spielräume belässt, da sein schwellwertbasierter Anwendungsbereich (vgl. oben) kleinere Unternehmen mit vergleichsweise geringem Umfang von Datenverarbeitungstätigkeiten ausnimmt. Das begünstigt insbesondere die Erprobung digitaler Innovationen durch Startups in frühen Stadien. Zudem findet der CCPA keine Anwendung auf gemeinnützige und staatliche Einrichtungen, so dass er auch in diesen Bereichen keine Hürden für die Erprobung digitaler Innovationen aufstellt.

Darüber hinaus eröffnet das im kalifornischen Datenschutzrecht vergleichsweise stark ausgeprägte Instrument der Einwilligung relativ großen Gestaltungsspielraum, da Geschäftspraktiken im Umgang mit personenbezogenen Daten in größerem Umfang durch Einwilligung legitimiert werden können. Auch dieser Aspekt lässt einige (wenngleich nicht alle) datenschutzrechtlichen Hürden für die Erprobung digitaler Innovationen deutlich niedriger erscheinen.

Aufgrund der unterschiedlichen regulatorischen Herangehensweise lassen sich die für das deutsche/europäische Datenschutzrecht (dazu oben Abschnitt D) identifizierten Spielräume für die Erprobung digitaler Inno-

vationen im Übrigen nicht unmittelbar auf die Hürden des kalifornischen Datenschutzrechts anwenden. Folgende Spielräume dürften sich aber entsprechend auch im kalifornischen Datenschutzrecht für die Erprobung digitaler Innovationen nutzbar machen lassen:

- Personenbezogene Daten vermeiden (vgl. Abschnitt D.I.)
- „Einwilligung" als Gestaltungsinstrument (vgl. Abschnitt D.II.1.) und Setzen von Anreizen für die Teilhabe an Reallaboren (vgl. Abschnitt D.II.3.)

d) „Regulatorische Sandkästen" / „Reallabore" in Kalifornien

Gegenwärtig gibt es in Kalifornien soweit ersichtlich keine Bestrebungen, „regulatorische Sandkästen" oder „Reallabore" zu schaffen, um datenschutzrechtliche Hürden für die Erprobung digitaler Innovationen abzusenken oder zu beseitigen.

Der Grund hierfür liegt wohl vor allem darin, dass der Anwendungsbereich des kalifornische Datenschutzrechts an sich schon vergleichsweise großen Spielraum für die Erprobung digitaler Innovationen durch kleinere Startups, gemeinnützige und staatliche Einrichtungen lässt und dass zudem das vergleichsweise stark ausgeprägte Instrument der Einwilligung ebenfalls relativ großen Gestaltungsspielraum eröffnet (dazu oben F.I.1.c)).

2. Japan

a) Überblick über Datenschutzrecht in Japan

Der japanische „Act on the Protection of Personal Information" („***APPI"***)[136] regelt als Querschnittsgesetz die Verarbeitung persönlicher Informationen im nicht-öffentlichen Sektor. Die Durchsetzung des APPI obliegt der „Personal Information Protection Commission" (***„PPC"***)[137].

Der „Act on the Protection of Personal Information Held by Administrative Organisations" (***"APPI for AO"***) regelt die Verarbeitung persönlicher Informationen durch die nationale Regierung. Der „Act on Personal Information Held by Independent Administrative Institutions" (***„APPI for IAI"***) gilt für quasi-staatliche Organisationen.

---

[136] https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf.
[137] https://www.ppc.go.jp/en/index.html.

Außerdem gibt es eine beträchtliche Anzahl lokaler Gemeindeverordnungen bezüglich persönlicher Informationen, die für die lokalen Regierungen und in einigen Fällen sogar für private Einrichtungen mit Sitz in einem solchen lokalen Gebiet gelten.

Bestimmte Organisationen sind aus dem Anwendungsbereich des APPI ausgenommen, beispielsweise **akademische Einrichtungen**, die persönliche Informationen für Zwecke akademischer Tätigkeiten verarbeiten.

Die vergleichsweise weite Definition der für den Anwendungsbereich des APPI maßgeblichen „**persönlichen Information**“ ist der Definition der „personenbezogenen Daten“ im deutschen/europäischen Datenschutzrecht ähnlich.

Die Europäische Kommission hat Japan ein angemessenes Datenschutzniveau bescheinigt.[138] Die Angemessenheitsfeststellung der Europäischen Kommission bedeutet zwar nicht eine Eins-zu-eins-Übereinstimmung mit den Vorschriften der EU. Die Feststellung geht aber davon aus, dass das japanische System insgesamt aufgrund des Wesensgehalts der Rechte auf Privatsphäre sowie ihrer wirksamen Anwendung, Überwachung und Durchsetzung das erforderliche Maß an Schutz bietet, das mit dem Schutzniveau in der EU im Wesentlichen vergleichbar ist.

b) Hürden für die Erprobung digitaler Innovationen im japanischen Datenschutzrecht im Vergleich zum deutschen/europäischen Datenschutzrecht

Zusammengefasst gibt der APPI im Wesentlichen folgenden datenschutzrechtlichen Rahmen vor, der in einigen zentralen Aspekten den deutschen/europäischen Vorgaben ähnlich ist:

- Erhebung: Persönliche Informationen dürfen grundsätzlich nicht durch Täuschung oder andere unzulässige Mittel erlangt werden. Die Erhebung als besonders sensibler definierter Information bedarf außerdem einer Einwilligung.

- Einwilligung: Bestimmte Verarbeitungstätigkeiten bedürfen einer Einwilligung. Dazu gehören insbesondere die Erhebung als beson-

[138] 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, http://data.europa.eu/eli/dec_impl/2019/419/oj.

ders sensibler definierter Information (vgl. oben) sowie grundsätzlich mit wenigen Ausnahmen auch die Übermittlung und grenzüberschreitende Übermittlung persönlicher Informationen (dazu noch unten). Das japanische Datenschutzrecht erlaubt umfassende Einwilligungen in die Verarbeitung persönlicher Informationen. Betroffene Personen können erteilte Einwilligungen (im Unterschied zum deutschen/europäischen Datenschutzrecht) nicht ohne Weiteres widerrufen.

- Zweckbindung: Der Zweck für die Verarbeitung persönlicher Informationen muss festgelegt und die betroffenen Personen müssen über die festgelegten Zwecke informiert werden. Eine Verarbeitung zu anderen als den festgelegten Zwecken darf nur erfolgen, wenn ein angemessener Zusammenhang zum ursprünglichen Zweck besteht und der neue Zweck den betroffenen Personen mitgeteilt oder veröffentlicht wurde.

- Übermittlung: Persönliche Informationen dürfen grundsätzlich nur mit Einwilligung der betroffenen Personen an Dritte übermittelt werden. Ausnahmsweise kann eine Übermittlung für bestimmte Fälle auf Grundlage eines Opt-Out zulässig sein. Wenige Ausnahmen gestatten die Übermittlung ohne Einwilligungen, beispielsweise bei Unternehmensverkäufen oder Umstrukturierungen.

- Grenzüberschreitende Übermittlung: Für die Übermittlung persönlicher Informationen ins Ausland ist grundsätzlich eine separate Einwilligung der betroffenen Personen erforderlich. Ausnahmsweise ist keine Einwilligung erforderlich, wenn das jeweilige Land auf einer „Weißen Liste“ steht (derzeit nur Länder in der EU und UK) oder der Empfänger Schutzvorkehrungen getroffen hat, die dem Niveau des APPI entsprechen.

- Sicherheit: Es sind erforderliche und angemessene Sicherheitsmaßnahmen zum Schutz persönlicher Informationen zu treffen, beispielsweise organisatorische, personelle, physische und technische Maßnahmen.

- Datenschutzverletzungen: Nach aktueller Gesetzeslage *soll* der Betroffene beste Anstrengungen unternehmen, um die betroffenen Personen und das PPC im Fall einer Datenschutzverletzung informieren. Zukünftig soll eine gesetzliche Pflicht eingeführt werden, der zu Folge der Betroffene informieren *muss*, sofern die Daten-

schutzverletzung wahrscheinlich Interessen der betroffenen Personen verletzt.

- Betroffenenrechte: Betroffene Personen haben bestimmte Rechte in Bezug auf ihre persönlichen Informationen, insbesondere auf Auskunft, Berichtigung, Einschränkung und Löschung.

- Anonymisierte Informationen: Die Verarbeitung anonymisierter Informationen unterfällt leichteren regulatorischen Anforderungen. Im Wesentlichen dürfen anonymisierte Informationen auch ohne Einwilligung verarbeitet und übermittelt werden. Es gelten allerdings besondere Transparenzanforderungen.

Im Vergleich zu den im deutschen/europäischen Datenschutzrecht identifizierten Hürden für die Erprobung digitaler Innovationen (vgl. Abschnitt C) lässt sich Folgendes feststellen:

- Der APPI kennt **kein generelles „Verarbeitungsverbot mit Erlaubnisvorbehalt“** (vgl. Abschnitt C.I.).

  Allerdings ist für bestimmte Verarbeitungstätigkeiten grundsätzlich eine Einwilligung erforderlich, beispielsweise für die Erhebung als besonders sensibler definierter Information oder für die Übermittlung persönlicher Informationen.

  Insoweit stellt der APPI sogar punktuell **höhere Hürden** auf als das deutsche/europäische Datenschutzrecht, das für die Erhebung als besonderer Kategorien personenbezogener Daten oder für die Übermittlung personenbezogener Daten auch eine Reihe gesetzlicher Erlaubnistatbestände vorsieht, wonach eine Einwilligung also nicht zwingend erforderlich ist.

  Allerdings erlaubt das japanische Datenschutzrecht inhaltlich vergleichsweise weit reichende Einwilligungen in die Verarbeitung persönlicher Informationen. Betroffene Personen können erteilte Einwilligungen außerdem nicht ohne Weiteres widerrufen.

- Der APPI kennt **kein spezielles Verarbeitungsverbot für „besondere Kategorien personenbezogener Daten“** (vgl. Abschnitt C.II.)

  Allerdings sieht der APPI ein im Ergebnis vergleichbares **grundsätzliches Einwilligungsbedürfnis** für als besonders sensibel definierte persönliche Informationen vor.

Auch insoweit stellt der APPI punktuell **höhere Hürden** auf als das deutsche/europäische Datenschutzrecht, das für die Erhebung besonderer Kategorien personenbezogener Daten eine Reihe gesetzlicher Erlaubnistatbestände vorsieht, wonach eine Einwilligung also nicht zwingend erforderlich ist.

- Der APPI sieht eine **Zweckbindung** und **Datenminimierung** (vgl. Abschnitt C.III.) vor. Im Unterschied zum deutschen/europäischen Datenschutzrecht sieht der APPI allerdings **keine strenge Speicherbegrenzung** (vgl. Abschnitt C.III.) vor, sondern lediglich eine Verpflichtung, sich um die Löschung personenbezogener Daten zu bemühen, wenn eine weitere Speicherung für die Verarbeitungszwecke nicht mehr erforderlich ist.

- Der APPI sieht **kein grundsätzliches Verbot „automatisierter Entscheidungen“** (vgl. Abschnitt C.IV.) oder andere Regelungen zur automatisierten Entscheidungsfindung einschließlich Profiling vor.

- Der APPI sieht ebenfalls die Verpflichtung zur Bereitstellung bestimmter Informationen über die Datenverarbeitung als **Transparenzanforderungen** (vgl. Abschnitt C.V.) vor. Der APPI statuiert außerdem **bestimmte Betroffenenrechte** (vgl. Abschnitt C.V.) für die Verarbeitung persönlicher Informationen.

  Zudem sieht das japanische Datenschutzrecht auch **für die Handhabung anonymisierter Informationen bestimmte Informationspflichten** vor. Auch insoweit stellt der APPI punktuell **höhere Hürden** auf als das deutsche/europäische Datenschutzrecht, das für die Verarbeitung anonymer Informationen überhaupt keine Anwendung findet.

- Der APPI sieht **keine umfassende Dokumentations- und Nachweispflichten** (vgl. Abschnitt C.VI.)vor, allerdings eine punktuelle Dokumentations- und Nachweispflicht für die Übermittlung und den Empfang persönlicher Informationen.

- Auch unter dem APPI verbleibt **erhebliche Rechtsunsicherheit** (vgl. Abschnitt C.VII.), insbesondere bei der Frage des Anwendungsbereichs der Ausnahmen für akademische Verarbeitung sowie bei der Abgrenzung von Anonymisierung und Pseudonymisierung.

- Auch im japanischen Datenschutzrecht bildet schon die **Zersplitterung der Anforderungen im nationalen Recht** (vgl. Abschnitt C.VIII.), die sich im APPI und in den lokalen Gemeindeverordnungen finden, gewisse Hürden.

  Weitere Hürden ergeben sich im japanischen Datenschutzrecht daraus, dass **unterschiedliche Rechtsrahmen für private und öffentliche Akteure** gelten.

- Auch unter dem APPI gilt eine **Unabdingbarkeit des Datenschutzrechts** (vgl. Abschnitt C.IX.), betroffene Personen können also auf die Einhaltung der datenschutzrechtlichen Anforderungen ebenfalls nicht einfach verzichten.

Im Ergebnis lässt sich festhalten, dass der APPI im Vergleich zum deutschen/europäischen Datenschutzrecht etwas weniger bzw. niedrigere Hürden aufstellt. Allerdings stellt das japanische Datenschutzrecht punktuell zusätzliche Hürden auf.

c) Spielräume bei der Erprobung digitaler Innovationen in Japan

Vergleichbar zum deutschen/europäischen Datenschutzrecht (dazu oben Abschnitt D) lassen sich (entsprechend) auch im japanischen Datenschutzrecht folgende Spielräume für die Erprobung digitaler Innovationen nutzbar machen:

- Personenbezogene Daten vermeiden (vgl. Abschnitt D.I.)
- Anreize für betroffene Personen setzen und betroffene Personen aktiv an Reallaboren teilhaben lassen (vgl. Abschnitt D.II.)
- Erforderliche Datenschutzmaßnahmen durch Reduzierung der Risiken der Verarbeitung minimieren (vgl. Abschnitt D.IV.)
- Privilegien für Forschung nutzen (vgl. Abschnitt D.V.)
- Bildsymbole für die Gestaltung von Datenschutzinformationen verwenden (vgl. Abschnitt D.VI.)
- Genehmigte Verhaltensregeln und Zertifizierungen nutzen (vgl. Abschnitt D.VII.)
- Aufsichtsbehörden konsultieren (vgl. Abschnitt D.VIII.)

Im Unterscheid zum deutschen/europäischen Datenschutzrecht (dazu oben Abschnitt D) stehen im japanischen Datenschutzrecht folgende Spielräume für die Erprobung digitaler Innovationen nicht zur Verfügung:

- Interessenabwägung in der Praxis nutzen und positiv beeinflussen (vgl. Abschnitt D.III.): Das japanische Datenschutzrecht kennt kein dem deutschen/europäischen Datenschutzrecht vergleichbares generelles „Verarbeitungsverbot mit Erlaubnisvorbehalt“, das eine Interessenabwägung vorsieht.

- Privilegien für Statistik nutzen (vgl. Abschnitt D.V.): Das japanische Datenschutzrecht sieht keine Privilegien für statistische Zwecke vor.

Dafür eröffnet das im japanischen Datenschutzrecht vergleichsweise stark ausgeprägte Instrument der Einwilligung weiteren Gestaltungsspielraum, da umfassende Einwilligungen in die Verarbeitung persönlicher Informationen möglich sind und betroffene Personen erteilte Einwilligungen nicht ohne Weiteres widerrufen können.

d) „Regulatorische Sandkästen“ / „Reallabore“ in Japan

aa) Rechtsrahmen für „regulatorische Sandkästen“

2018 hat die japanische Regierung einen **Rechtsrahmen für „projektbasierte regulatorische Sandkästen“** eingeführt.

Zweck dieses Rahmens ist es, innovative Technologien für eine begrenzte Zeit ohne die Einschränkung geltender Vorschriften zu testen. In diesem Rahmen muss ein Unternehmen einen Testplan vorlegen und eine Genehmigung von der Regierung einholen. Auf der Grundlage des Testergebnisses und der gesammelten Daten legt die Regierung den Regulierungsansatz für die neuen Technologien fest. Derzeit laufen zwanzig Projekte in diesem Rahmen in verschiedenen Sektoren wie IoT, Gesundheitswesen, Finanzen oder Mobilität.

Im Jahr 2020 führte die japanische Regierung außerdem einen **Rechtsrahmen für „regionale regulatorische Sandkästen“** ein.

Dieser ist dem projektbasierten regulatorischen Sandkasten insofern ähnlich, als er es Unternehmen ermöglicht, neue innovative Technologien ohne die von geltenden Vorschriften ausgehenden Einschränkun-

gen zu testen. Im Unterschied zum projektbasierten regulatorischen Sandkasten gilt der regionale regulatorische Sandkasten allerdings nur für bestimmte Anwendungsszenarien (insbesondere autonomes Fahren und Drohnen) und erlaubt die Erprobung dieser Technologien nur in von der Regierung bestimmten Sonderverwaltungsbezirken.

Dabei zielen die die vorgesehenen regulatorischen Sandkästen nicht speziell darauf ab, datenschutzrechtliche Hürden zu überwinden. Tatsächlich gab es bislang soweit ersichtlich keinen Fall, in dem im Rahmen dieser Sandkästen besondere Ausnahmen von den datenschutzrechtlichen Anforderungen gewährt wurden. Der Grund hierfür liegt könnte darin liegen, dass das japanische Datenschutzrecht ohnehin schon genügend Spielräume für die Erprobung digitaler Innovationen bietet.

bb) Sonderbefreiung von geltenden Vorschriften

Darüber hinaus gibt es in Japan noch die Möglichkeit von Sonderbefreiungen von geltenden Vorschriften.

In diesem Rahmen kann die Regierung eine bestimmte Organisation von der Einhaltung geltender Vorschriften befreien. Dieses Instrument kann verwendet werden, wenn die Sicherheit des Geschäftsmodells trotz Befreiung von den geltenden Vorschriften nachgewiesen werden kann. In der Praxis ist es allerdings nicht einfach, die Sicherheit neuer Geschäftsmodelle nachzuweisen. Unter anderem deswegen hat der Japanische Gesetzgeber die Rechtsrahmen für regulatorische Sandkästen (vgl. oben) geschaffen.

II. Europäischer Vergleich

1. Frankreich

a) Überblick über Datenschutzrecht in Frankreich

Wie in Deutschland findet im EU-Mitgliedsstaat Frankreich die DS-GVO unmittelbare Anwendung. Die im europäischen Datenschutzrecht identifizierten Hürden für die Erprobung digitaler Innovationen (dazu **Abschnitt C**) gelten also auch in Frankreich.

Daneben gibt es in Frankreich nationale datenschutzrechtliche Regelungen, insbesondere das Französische Datenschutzgesetz[139] sowie das Dekret zur Anwendung des Gesetzes[140].

Datenschutzaufsichtsbehörde ist in Frankreich die Nationale Kommission für Informatik und Freiheiten (*Commission Nationale de l'Informatique et des Libertés,* ***„CNIL"***)[141].

b) Regelungsansätze im französischen Recht zur Erleichterung der Erprobung digitaler Innovationen

aa) Gestaltung fachrechtlicher Anforderungen zur Schaffung von datenschutzrechtlichen Rechtfertigungstatbeständen

Wie in Deutschland (dazu **Abschnitt E.II.1.**) erscheint es auch in Frankreich grundsätzlich denkbar, dass der nationale Gesetzgeber durch Gestaltung fachrechtlicher Verpflichtungen zur Verarbeitung personenbezogener Daten im Kontext der Erprobung von Innovationen Anknüpfungspunkte für datenschutzrechtliche Rechtfertigungstatbestände schafft.[142]

Derzeit sind uns in Frankreich zwar keine gesetzgeberischen Maßnahmen bekannt, die ausdrücklich zur Verarbeitung konkreter personenbezogener Daten im Kontext von Erprobungen verpflichten (und die Bedingungen für eine solche Verarbeitung festlegen).

Im Kontext **autonomer Fahrzeuge** gibt es in Frankreich allerdings gesetzliche Regelungen für Tests solcher Fahrzeuge mit Genehmigung des französischen Verkehrsministeriums, bei denen bestimmte Daten aufgezeichnet werden müssen. Das Dekret, das die Bedingungen für die Erteilung der Genehmigung spezifiziert, sieht insbesondere vor, dass das Fahrzeug mit einem Aufzeichnungsgerät ausgestattet sein muss, um jederzeit feststellen zu können, ob das Fahrzeug zu einem bestimmten Zeitpunkt vollständig oder teilweise autonom fuhr. Das Dekret enthält Regelungen zur automatisierten Löschung der Daten des Aufzeichnungsgeräts sowie der Speicherung im Falle eines Unfalls. Die Regelun-

---

139 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, https://www.cnil.fr/fr/la-loi-informatique-et-libertes.

140 Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038528420?r=GO5MfyCVUL.

141 http://www.cnil.frhttps://www.naih.hu/.

142 Vgl. Art. 6 (1) (c) DS-GVO.

gen beziehen sich zwar nicht konkret auf personenbezogene Daten. Es lässt sich aber annehmen, dass die aufgezeichneten Daten personenbezogene Daten enthalten können.

bb) Nutzung des nationalen Regelungsspielraums der DS-GVO im französischen Datenschutzrecht

Darüber hinaus erscheint wie in Deutschland (dazu **Abschnitt E.II.2.**) auch in Frankreich in dem relativ engen Regelungsspielraum, den die DS-GVO dem nationalen Gesetzgeber lässt, zumindest eine punktuelle Gestaltung denkbar, um die Erprobung von Innovationen zu erleichtern.

In Frankreich hat der Gesetzgeber im nationalen Recht bislang insbesondere von folgenden Gestaltungsspielräumen Gebrauch gemacht:

- Schaffung besonderer Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zur Erprobung neuer Technologien, die im öffentlichen Interesse liegen.[143]

- Beschränkung von Betroffenenrechten für die Verarbeitung personenbezogener Daten zur Erprobung neuer Technologien, die im öffentlichen Interesse liegen[144] oder zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecke.[145]

Anders als der deutsche Gesetzgeber hat der französische Gesetzgeber bislang nicht von seinem sich aus der DS-GVO ergebenden Regelungsspielraum im Beschäftigungskontext[146] Gebrauch gemacht.

Für Erprobungen hat der französische Gesetzgeber beispielsweise in folgenden Anwendungsfeldern im Kontext von Verarbeitungen im öffentlichen Interesse von seinen Gestaltungsmöglichkeiten Gebrauch gemacht:

- In einem Dekret aus 2016 hat der Gesetzgeber Bedingungen festgelegt, unter denen **öffentliche Verkehrsunternehmen** auf Versuchsbasis und für eine Dauer von 3 Jahren **audiovisuelle Aufzeichnung** vornehmen dürfen. Das Dekret regelt die Details der

[143] Vgl. Art. 6 (1) (e), (3) DS-GVO.
[144] Vgl. Art. 23 DS-GVO.
[145] Vgl. Art. 89 (2) DS-GVO
[146] Vgl. Art. 88 DS-GVO.

Verarbeitung personenbezogener Daten. Außerdem beschränkt das Dekret das **Widerspruchsrecht** betroffener Personen.

- In einem Gesetz aus 2018 zur Harmonisierung der Nutzung mobiler Videoüberwachung durch Sicherheitsbehörden und einem Dekret aus 2019 hat der Gesetzgeber Bedingungen festgelegt, unter denen die **Feuerwehr** auf Versuchsbasis bis 2022 **audiovisuelle Aufzeichnung** vornehmen darf. Das Dekret regelt die Details der Verarbeitung personenbezogener Daten. Außerdem beschränkt das Dekret das **Widerspruchsrecht** betroffener Personen. Das Dekret sieht zudem eine Einschränkung des **Auskunftsrechts** vor.

Es erscheint denkbar, dass der französische Gesetzgeber zukünftig weitere Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im öffentliches Interesse und diesbezügliche Beschränkungen von Betroffenenrechten erlässt, auch im Kontext von Erprobungsszenarien. Derzeit ist uns allerdings keine Gesetzgebung bekannt, die nichtöffentlichen Einrichtungen die Erprobung neuer Technologien ermöglichen würde.

Das Französische Datenschutzgesetz sieht außerdem die Möglichkeit der Beschränkung von Betroffenenrechten im Rahmen des Regelungsspielraums der DS-GVO[147] per Dekret für Verarbeitungstätigkeiten zu wissenschaftlichen oder historischen Forschungszwecken und für statistische Zwecke vor. Etwaige auf Grundlage eines Dekrets vorgenommene Beschränkungen könnten auch für die Erprobung digitaler Innovationen relevant sein.

c) „Regulatorische Sandkästen“ / „Reallabore“ in Frankreich

Uns sind keine „regulatorischen Sandkästen“ oder „experimentelle Gesetzgebung“ in Frankreich bekannt, die die datenschutzrechtlichen Hürden für die Erprobung digitaler Innovationen verringern oder beseitigen würden. Insbesondere enthält das Französische Datenschutzgesetz keine Regelungen, die sich konkret mit der Erprobung neuer Technologien befassen.

[147] Vgl. Art. 23 DS-GVO.

d) Behördliche Maßnahmen oder Stellungnahmen zu „Regulatorischen Sandkästen“ / „Reallaboren“ in Frankreich

2020 veröffentlichte die CNIL ihren Jahresbericht für 2019, der ein Kapitel zu „regulatorischen Sandkästen“ enthält.

Die CNIL erwähnt in ihrem Jahresbericht, dass „regulatorische Sandkästen“ in Frankreich bereits in verschiedenen Regelungsbereichen eingeführt wurden. Speziell mit Blick auf Datenschutzrecht merkt die CNIL allerdings Folgendes an:

- Ausnahmen von den Verpflichtungen der DS-GVO, auch experimentelle, seien nicht möglich, da die DS-GVO ein direkt anwendbares europäisches Rechtsinstrument zur Harmonisierung ist, das keine ausdrücklich formalisierten „Sandkästen“ vorsieht.

- Durchaus möglich sei aber eine progressive und dynamische Anwendung der Regelung der DS-GVO durch die CNIL in einem „Sandkasten“-Vorgehen. Insbesondere könne die CNIL die Anwendung der Regelungen der DS-GVO durch verschiedene (durch die CNIL nicht näher definierte) Compliance-Instrumente (von der CNIL entworfene Dokumente) definieren/erklären/ausarbeiten.

Dem Jahresbericht zufolge erwägt die CNIL derzeit ein formelleres und konkreteres Verfahren für „Sandkästen“. Aus dem Bericht geht jedoch klar hervor, dass dies nicht die Implementierung von Ausnahmeregelungen für die Verpflichtungen der DS-GVO beinhalten würde, sondern eher aus einer Strukturierung und Formalisierung einer experimentelleren Herangehensweise. Dies bestünde laut der CNIL darin, intensive Unterstützung anzubieten, auch für junge Unternehmen, die im Ergebnis, wenn sich aus der Erprobung die Notwendigkeit dafür zeigt, in eine Anpassung der Instrumente und der Auslegungen der CNIL resultieren könnte.

2. Ungarn

a) Überblick über Datenschutzrecht in Ungarn

Wie in Deutschland findet im EU-Mitgliedsstaat Ungarn die DS-GVO unmittelbare Anwendung. Die im europäischen Datenschutzrecht identifizierten Hürden für die Erprobung digitaler Innovationen (dazu **Abschnitt C**) gelten also auch in Ungarn.

Daneben gibt es in Ungarn nationale datenschutzrechtliche Regelungen, insbesondere das Ungarische Datenschutzgesetz[148] sowie das Ungarische Gesundheitsdatenschutzgesetz[149].

Datenschutzaufsichtsbehörde ist in Ungarn die Nationale Behörde für Datenschutz und Informationsfreiheit (*Nemzeti adatvédelmi és információsabadság Hatóság,* ***„NAIH“***)[150].

b) Regelungsansätze im ungarischen Recht zur Erleichterung der Erprobung digitaler Innovationen

aa) Gestaltung fachrechtlicher Anforderungen zur Schaffung von datenschutzrechtlichen Rechtfertigungstatbeständen

Wie in Deutschland (dazu **Abschnitt E.II.1.**) erscheint es auch in Ungarn grundsätzlich denkbar, dass der nationale Gesetzgeber durch Gestaltung fachrechtlicher Verpflichtungen zur Verarbeitung personenbezogener Daten im Kontext der Erprobung von Innovationen Anknüpfungspunkte für datenschutzrechtliche Rechtfertigungstatbestände schafft.[151]

Der ungarische Gesetzgeber hat von diesen Gestaltungsmöglichkeiten im Kontext der Erprobung neuer Technologien bislang für die **Verarbeitung personenbezogener Daten im Rahmen von Tests autonomer Fahrzeuge zu Entwicklungszwecken** Gebrauch gemacht:

2018 trat die neue ungarische Regulierung für das Testen autonomer Fahrzeuge auf öffentlichen Straßen in Kraft, die auch datenschutzrechtliche Bestimmungen enthält:

- Die Regulierung schafft zum einen eine rechtliche Verpflichtung für die Verarbeitung personenbezogener Daten bei Bild- und Tonaufzeichnungen als Anknüpfungspunkt für eine datenschutzrechtliche Rechtsgrundlage.[152]

- Zum anderen legt die Regulierung Umfang und Zwecke der Datenverarbeitung fest.

---

[148] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, https://net.jogtar.hu/jogszabaly?docid=A1100112.TV

[149] 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, https://net.jogtar.hu/jogszabaly?docid=99700047.TV

[150] https://www.naih.hu/.

[151] Vgl. Art. 6 (1) (c) DS-GVO.

[152] Vgl. Art. 6 (1) (c) DS-GVO.

Weitere fachrechtliche Anforderungen könnte der ungarische Gesetzgeber zukünftig für die Verwendung von **Drohnen** formulieren. Im Kontext unbemannter Luftfahrzeuge hat der ungarische Gesetzgeber bereits detaillierte datenschutzrechtliche Regelungen angekündigt. Hierzu formulierte die NAIH Empfehlungen für den Gesetzgeber:

- Datenschutzfragen sollen in einer separaten Rechtsnorm geregelt werden.
- Es soll eine neue Rechtsgrundlage bestimmt werden. Es könne die Datenverarbeitung erleichtern, wenn auch spezielle Rechtsgrundlagen eingeführt würden.
- Die Zweckbindung soll in einem Genehmigungsverfahren geprüft werden.
- Für den kommerziellen Betrieb von Drohnen sollen die Erleichterungen nicht gelten.

Derzeit ist allerdings offen, ob und ggf. wie der ungarische Gesetzgeber die Vorschläge der NAIH umsetzen wird.

bb) Nutzung des nationalen Regelungsspielraums der DS-GVO im ungarischen Datenschutzrecht

Darüber hinaus erscheint wie in Deutschland (dazu **Abschnitt E.II.2.**) auch in Ungarin in dem relativ engen Regelungsspielraum, den die DS-GVO dem nationalen Gesetzgeber lässt, zumindest eine punktuelle Gestaltung denkbar, um die Erprobung von Innovationen zu erleichtern.

In Ungarn hat der Gesetzgeber beispielsweise im Gesundheitsdatenschutzgesetz **gesetzliche Ausnahmen vom Verbot der Verarbeitung personenbezogener Daten** geschaffen, insbesondere für die Verarbeitung zu **statistischen Zwecken** und für **wissenschaftliche Forschungszwecke**.[153] Diese Regelungen schaffen auch für die Erprobung von Innovationen gewisse Flexibilität.

Soweit ersichtlich hat der ungarische Gesetzgeber jedoch innerhalb der Regelungsspielräume der DS-GVO bislang keine speziellen Regelungen für die Erprobung digitaler Innovationen geschaffen.

[153] Vgl. Art. 9 (2) (j) DS-GVO.

c) „Regulatorische Sandkästen“ / „Reallabore“ in Ungarn

Uns sind keine „regulatorischen Sandkästen“ oder „experimentelle Gesetzgebung“ in Ungarn bekannt, die die datenschutzrechtlichen Hürden für die Erprobung digitaler Innovationen verringern oder beseitigen würden.

d) Behördliche Maßnahmen oder Stellungnahmen zu „Regulatorischen Sandkästen“ / „Reallaboren“ in Ungarn

Uns sind keine behördlichen Maßnahmen oder Stellungnahmen zu „Regulatorischen Sandkästen“ oder „Reallaboren“ in Ungarn bekannt.

*****