Bundesministerium
für Wirtschaft
und Energie

Reallabore
Testräume für Innovation
und Regulierung

Praxishilfe zum Datenschutz in Reallaboren

bmwi.de

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Stand
März 2021

Diese Broschüre wird ausschließlich als Download angeboten.

Gestaltung
PRpetuum GmbH, 80801 München

Bildnachweis
fandijki / Adobe Stock / Titel
your123 / Adobe Stock / S. 2
Maksim Kabakou / Adobe Stock / S. 5
Eoneren / iStock / S. 18

Zentraler Bestellservice für Publikationen der Bundesregierung:
E-Mail: publikationen@bundesregierung.de
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

I. Einleitung

Reallabore machen es möglich, Innovationen im realen Umfeld zu erproben, erlebbar zu machen und über ihre Wirkungen zu lernen. Von großem Nutzen ist das besonders auch für solche Technologien und Geschäftsmodelle, die auf der Nutzung und Auswertung großer Mengen an realen Daten basieren.

Immer dann, wenn dabei personenbezogene Daten verarbeitet werden, wird auch deren Schutz zum wichtigen Thema. Die europäische Datenschutzgrundverordnung (DS-GVO) bietet hierfür seit dem 25. Mai 2018 einen einheitlichen und unmittelbar geltenden Rechtsrahmen, der gerade auf den freien Verkehr personenbezogener Daten in der Europäischen Union abzielt.

Für die Unternehmen ist die Umsetzung der datenschutzrechtlichen Vorgaben jedoch häufig mit Herausforderungen verbunden. Laut einer Umfrage des Digitalverbandes BITKOM im Herbst 2020 hat jedes zweite Unternehmen aufgrund der DS-GVO bereits auf neue, innovative Projekte verzichtet – entweder wegen direkter Vorgaben oder wegen Unklarheiten in der Auslegung der DS-GVO.

Ziel dieser Praxishilfe ist es, die wichtigsten datenschutzrechtlichen Anforderungen an die Erprobung von Innovationen in Reallaboren aufzuzeigen und Hinweise zu geben, wie Unternehmen damit umgehen können. Die datenschutzrechtlichen Regelungen enthalten an vielen Stellen Spielräume, die sich gerade für die Erprobung digitaler Innovationen nutzbar machen lassen. Das Datenschutzrecht gibt dem Rechtsanwender eine Reihe flexibler Instrumente an die Hand, die eine rechtskonforme Erprobung digitaler Innovationen zulassen und in der Praxis oftmals unterschätzt werden.

Ausgehend von der Darstellung der wichtigsten datenschutzrechtlichen Anforderungen an die Erprobung von Innovationen in Reallaboren (Kapitel II) stellt die Praxishilfe konkrete Instrumente und Gestaltungsspielräume vor, mit denen diese Anforderungen – zumindest teilweise – bewältigt werden können (Kapitel III).[1]

Im Überblick: Datenschutzrechtliche Spielräume für Reallabore

- Anonyme Informationen und synthetische Daten nutzen (Kapitel III.1)
- Anreize für betroffene Personen setzen und sie aktiv einbinden (Kapitel III.2)
- Interessenabwägung nutzen und positiv beeinflussen (Kapitel III.3)
- Risiken reduzieren (Kapitel III.4)
- Privilegien für Forschung und Statistik nutzen (Kapitel III.5)
- Bildsymbole für die Gestaltung von Datenschutzinformationen verwenden (Kapitel III.6)
- Genehmigte Verhaltensregeln und Zertifizierungen nutzen (Kapitel III.7)
- Aufsichtsbehörden konsultieren (Kapitel III.8)

Die Inhalte dieser Broschüre stellten eine gekürzte Fassung des Gutachtens „Hürden und Gestaltungsspielräume im deutschen und europäischen Datenschutzrecht für die Erprobung digitaler Innovationen“ (Rücker et al., 2021) dar, das die Kanzlei Noerr im Auftrag des BMWi und im Rahmen der BMWi-Reallabore-Strategie (siehe Infobox) erstellt hat. Neben den hier dargestellten Informationen, die

1 Die Broschüre bietet einen allgemeinen Überblick, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann die rechtliche Analyse oder Beratung im Einzelfall nicht ersetzen.

sich vorwiegend an Praktikerinnen und Praktiker richten, umfasst das vollständige Gutachten auch Verweise auf die einschlägigen Gesetzesnormen, weitere Quellennachweise und Hintergrundinformation sowie Empfehlungen zur Weiterentwicklung des datenschutzrechtlichen Rahmens.

INFOBOX

Das Unterstützungsangebot des BMWi: Die Reallabore-Strategie

Im Dezember 2018 hat das BMWi die technologie- und branchenübergreifende **Reallabore-Strategie** veröffentlicht, die durch die Geschäftsstelle Reallabore im BMWi umgesetzt wird. Drei Zielsetzungen stehen im Mittelpunkt.

Mehr Spielräume für Innovationen

Um neue rechtliche Spielräume für die Erprobung von Innovationen zu schaffen, sind in zahlreichen Rechtsbereichen zusätzliche Experimentierklauseln erforderlich. Daher unterstützt das BMWi die zuständigen Stellen in der Bundesregierung bei der **Schaffung und Überarbeitung von Experimentierklauseln**. Zudem stellt das BMWi themenübergreifende Hilfestellungen und Gutachten zur Verfügung, so etwa die Broschüre „**Recht flexibel – Arbeitshilfe zur Formulierung von Experimentierklauseln**“ oder die vorliegende **Praxishilfe zum Datenschutz in Reallaboren**. Darüber hinaus arbeitet das BMWi an den Grundzügen eines möglichen **Bundesexperimentiergesetzes,** das einen einheitlichen und leistungsstarken Rechtsrahmen für die Erprobung in Reallaboren bereitstellen soll. Auf europäischer Ebene hat der Rat der Europäischen Union im Rahmen der deutschen Präsidentschaft **Ratsschlussfolgerungen zu Reallaboren und Experimentierklauseln** beschlossen. So wurden ein europaweites Verständnis von Reallaboren sowie die Grundlage für eine stärkere Verankerung von Experimentierklauseln in europäischem Recht geschaffen. Grundlage des Austausches innerhalb der Bundesregierung ist die regelmäßig tagende **interministerielle Arbeitsgruppe Reallabore**.

Vernetzen und Informieren

Ebenso ist es Ziel der Reallabore-Strategie, Reallabore in Deutschland zu vernetzen und zu informieren. Dazu wurde das **Netzwerk Reallabore** ins Leben gerufen, in dem sich mittlerweile mehr als 500 Mitglieder aus Unternehmen, Verbänden, Forschung und Verwaltung für den Austausch in Veranstaltungen und Workshops zusammengeschlossen haben. Mit dem **Handbuch Reallabore** hat das BMWi eine umfassende Praxishilfe für die Umsetzung von Reallaboren veröffentlicht. Alle Informationen zur Reallabore-Strategie finden sich auf der **Website** www.reallabore-bmwi.de.

Reallabore unterstützen und begleiten

Herausragende Reallabore sichtbar machen, innovative Ideen würdigen und zu neuen Reallaboren ermuntern – das sind die Ziele des **Innovationspreises Reallabore – Testräume für Innovation und Regulierung** des BMWi. Erstmals wurde der Innovationspreis im Jahr 2020 an neun Preisträger verliehen.

II. Datenschutzrechtliche Anforderungen

Im Rahmen der Erprobung innovativer digitaler Technologien und Geschäftsmodelle werden häufig personenbezogener Daten verarbeitet. Das folgende Kapitel zeigt, welche zentralen datenschutzrechtlichen Anforderungen dabei zu berücksichtigen sind. Hierbei differenziert das Datenschutzrecht bislang nicht zwischen der Erprobung von Innovationen in Reallaboren und ihrer unbefristeten Anwendung.

1. Generelles „Verarbeitungsverbot mit Erlaubnisvorbehalt“

Das zentrale Wesensmerkmal des deutschen und europäischen Datenschutzrechts ist der so genannte 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 der betroffenen Person ergeben. Daneben existiert ein eng begrenzter Kanon so genannter gesetzlicher Rechtsgrundlagen, etwa für Verarbeitungen, die zur Erfüllung eines Vertrages mit der betroffenen Person oder zur Erfüllung gesetzlicher Pflichten erforderlich sind. Die DS-GVO hält damit den Rechtsanwender ganz allgemein dazu an, jeglichen Umgang mit personenbezogenen Daten vorab dahingehend zu hinterfragen, ob eine ausreichende Rechtsgrundlage einschlägig ist.

BEISPIEL

Unbeabsichtigte Verarbeitung personenbezogener Daten als „Nebenprodukt“ bei der Erprobung autonomer Fahrzeuge

Szenario: Der Entwickler[2] 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.

Anforderung: Auch für diese unbeabsichtigte Verarbeitung personenbezogener Daten ist eine Rechtsgrundlage erforderlich.

2 Aufgrund der besseren Lesbarkeit gilt in der vollständigen Publikation bei Verwendung der männlichen Form stets, dass alle Geschlechter eingeschlossen sind.

2. Spezielles Verarbeitungsverbot für „besondere Kategorien personenbezogener Daten“

Für so genannte „besondere Kategorien personenbezogener Daten“ sieht die DS-GVO einen erhöhten Schutz vor. Hierunter fallen etwa Gesundheitsdaten oder biometrische Daten. Die Verarbeitung solcher Daten erfordert nicht nur eine Rechtsgrundlage, sondern darüber hinaus einen besonderen Ausnahmetatbestand, der gerade die Verarbeitung besonderer Kategorien personenbezogener Daten gestattet.

Solche Ausnahmetatbestände zielen jeweils auf vergleichsweise konkrete Verarbeitungssituationen ab, beispielsweise die Verarbeitung personenbezogener Daten durch Fachpersonal für Zwecke der Gesundheitsvorsorge.

BEISPIEL 1

Einwilligungserfordernis für innovative Gesundheits-Apps

Szenario: Ein Unternehmen möchte eine cloud-basierte App betreiben, die es registrierten Nutzern 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.

Anforderung: Ginge es hier nicht um Gesundheitsdaten, sondern um „normale“ Daten, ließe sich die Verarbeitung zur Erfüllung des mit dem Anwender bestehenden Nutzungsvertrages grundsätzlich 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 gilt. 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 Verarbeitung personenbezogener Daten legitimieren.

BEISPIEL 2

Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte

Szenario: Ein Arzt nutzt eine innovative Software-as-a-Service-Lösung (SaaS) zur von künstlicher Intelligenz gestützten Auswertung von CT-Aufnahmen und der 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.

Anforderung: Blickt man isoliert auf die Rechtsgrundlage der Anonymisierung, ließe sich die Anonymisierung im Regelfall auf eine Interessenabwägung stützen. Die anonymen Daten würden dann nicht mehr dem Anwendungsbereich des Datenschutzrechts unterfallen, wären also weitgehend uneingeschränkt verwendbar. 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 nur mit einer ausdrücklichen (und jederzeit frei widerruflichen) Einwilligung der jeweiligen Patienten zulässig.

3. 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. 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). 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“ (Art. 5 (1) (b) DS-GVO) dürfen. Bereits bei der Planung einer Verarbeitungstätigkeit sind daher alle angestrebten Zwecke zu ermitteln und zu berücksichtigen.

> 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 nur erhoben/verarbeitet werden, soweit das für den im Voraus festgelegten Zweck auch tatsächlich erforderlich ist.

> Die Erhebung des Geburtsdatums wäre zur Abwicklung einer Onlinebestellung 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.

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“ (Art. 5 (1) (e) DS-GVO).

> Werden personenbezogene Daten nur zur Abwicklung einer Onlinebestellung 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 defi-

nierende Zwecke. Der Verantwortliche müsste jeweils im Detail prüfen, welche konkreten Daten er für diese Zwecke in welchem Umfang verarbeiten darf und wann welche Daten zu löschen sind.

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.

BEISPIEL 1

Big-Data-Analysen und explorative Statistiken

Szenario: Ein Unternehmen im Gesundheitssektor verfügt über umfangreiche Datensätze zu Kunden seiner verschiedenen Geschäftsbereiche, unter anderem aus dem Betrieb einer Gesundheits-App (siehe auch das Praxisbeispiel „Einwilligungserfordernis für innovative Gesundheits-Apps“ → II.2). Die bestehenden Datensätze sowie zusätzliche, aus zahlreichen Onlinequellen (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.

Anforderung: 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. 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.

BEISPIEL 2

Blockchainbasierte Zahlungstechnologie

Szenario: Der Betreiber einer elektronischen Geldbörse möchte Transaktionen mittels blockchaingestützter Technologien protokollieren. Wesensmerkmal der Blockchain-Technologie ist die Unveränderlichkeit in der Blockchain abgelegter Informationen.

Anforderung: Die dauerhafte und nicht reversible Speicherung personenbezogener Daten in der Blockchain steht in Konflikt mit dem Grundsatz der Speicherbegrenzung.

4. Grundsätzliches Verbot „automatisierter Entscheidungen“

Technische Innovationen erlauben mehr und mehr die Verlagerung menschlicher Tätigkeiten und Entscheidungen auf Maschinen, wenn diese Maschinen mittels künstlicher Intelligenz zunehmend komplexere Problemstellungen lösen können. 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“ (Art. 22 (1) DS-GVO). Insbesondere bei Anwendungen künstlicher Intelligenz ist dieses Verbot automatisierter Entscheidungen besonders zu berücksichtigen.

BEISPIEL 1

KI-gestützte Automatisierung der Kundenkommunikation

Szenario: 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.

Anforderung: Bei diesem System wäre zunächst im Detail zu prüfen, ob „automatisierte Entscheidungen“ im Sinne der DS-GVO getroffen werden. In diesem Fall wäre nicht nur die Datenverarbeitung durch das System an sich zu rechtfertigen. Zusätzlich wäre zu prüfen, ob für das grundsätzliche Verbot automatisierter Entscheidungen ein Ausnahmetatbestand greift.

BEISPIEL 2

Vollautomatisiertes Depotmanagement über Robo-Advisor

Szenario: Ein FinTech-Start-up 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.

Anforderung: Beim Betrieb des Robo-Advisors greift das grundsätzliche Verbot automatisierter Entscheidungsfindungen. Darüber hinaus muss das Unternehmen seinen Kunden „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ (Art. 13 (2) (f) DS-GVO) zur Verfügung stellen.

5. Transparenzanforderungen und Betroffenenrechte

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

Umfang und Komplexität von Datenschutzerklärungen

Die DS-GVO sieht umfangreiche Informationspflichten vor. 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 kann das in der Praxis zu einem schwer auflösbaren Konflikt zwischen umfassender Erfüllung der Informationspflichten und gleichzeitiger Wahrung der erforderlichen Transparenz führen.

BEISPIEL

Datenschutzinformationen für ein smartes Hausautomatisierungssystem

Szenario: Ein Unternehmen hat ein smartes Hausautomatisierungssystem entwickelt, das über zahlreiche Sensoren und Schaltelemente (Mikrofone, 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.

Anforderung: Der Nutzer (Hausbewohner) sowie sämtliche anderen 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 weiterentwickelte Verarbeitungsvorgänge wären die Nutzer zu unterrichten.

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. Anfragen zur Geltendmachung dieser Rechte sind unverzüglich, grundsätzlich jedenfalls aber innerhalb eines Monats vom Verantwortlichen zu beantworten.

Verantwortliche müssen bereits vorab robuste Prozesse etablieren, um diese Zeitvorgabe in der Praxis einzuhalten und 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 Betroffenenrechte gelten. 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.

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 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.

6. Accountability: Dokumentations- und Nachweispflichten

Verarbeitungsverzeichnis und weitere allgemeine Dokumentationspflichten

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

Eine besondere Ausprägung dieses Grundsatzes der Rechenschaftspflicht ist etwa die Pflicht, ein Verarbeitungsverzeichnis zu führen. Das Verarbeitungsverzeichnis muss 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.

So ist etwa bei Verarbeitungstätigkeiten, die auf Grundlage einer Interessenabwägung 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 oder zur gemeinsamen Verantwortung.

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.

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. 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.

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. Beide Aufsichtsbehörden zeigen, dass eine detaillierte und kleinteilige Auseinandersetzung mit allen erdenklichen Risiken erforderlich ist (https://www.lda.bayern.de/de/thema_dsfa.html).

Verbleibende Rechtsunsicherheit

In einer Umfrage des Digitalverbandes BITKOM im Herbst 2020 beschreiben 74 Prozent der befragten Unternehmen eine anhaltende Rechtsunsicherheit durch die Regeln der DS-GVO. Typischerweise geht es aufgrund der Neuartigkeit des Rechtsrahmen wie auch aufgrund der hohen Dynamik und Komplexität der betreffenden Technologien um neuartige Fragestellungen, zu denen sich bislang weder durch Rechtsprechung oder Behördenstellungnahmen noch in der rechtlichen Literatur robuste Leitlinien für die konkrete Anwendung und Auslegung des Datenschutzrechts herausgebildet haben.

BEISPIEL 1

Abgrenzung Anonymisierung und Pseudonymisierung

Szenario: Der Anbieter einer SaaS-Lösung für Ärzte (Praxisbeispiel „Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“ → II.2) 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.

Anforderung: Beim Thema Anonymisierung und Pseudonymisierung stehen Unternehmen vor zahlreichen ungelösten Rechtsfragen, die ganz erhebliche Auswirkungen haben können. Klar ist nur, dass die Verarbeitung anonymer Informationen nicht dem Datenschutzrecht unterliegt und dass die Verwendung von Pseudonymen sich zumindest positiv auf die Risiken der Verarbeitung und damit auch auf die Rechtfertigung auswirkt.

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. 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 Re-Identifizierung 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.

BEISPIEL 2

Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars

Szenario: Zahlreiche Funktionen eines Fahrzeugs lassen sich „on demand" vom Fahrer buchen, 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.

Anforderung: Stellt ein Fahrzeugeigentümer einen Auskunftsanspruch und verlangt eine Kopie seiner Daten vom Hersteller, stellt sich zunächst die Frage, wie weit dieser Anspruch reicht. Einerseits ist unklar, welche Fahrzeugdaten 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. Außerdem lässt sich für den Hersteller kaum ermitteln, um wessen personenbezogene Daten es sich handelt. Schließlich könnte der Fahrzeugeigentümer sein Fahrzeug auch verliehen haben. Die entstandenen Daten wären dann dem eigentlichen Fahrer zuzuordnen und dürften dem Eigentümer grundsätzlich nicht offengelegt werden.

BEISPIEL 3

Forschung und Statistik zur Verbesserung von Produkten und Dienstleistungen

Szenario: 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" → II.2).

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" → II.3)

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

Anforderung: 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.

7. Unterschiedliche Anforderungen im nationalen Recht der EU-Mitgliedstaaten

Die DS-GVO verfolgt als EU-weit unmittelbar anwendbare Verordnung das Ziel, eine gleichmäßige und einheitliche Anwendung des Datenschutzrechts sicherzustellen. In der EU existieren trotz weitreichender Harmonisierung durch die DS-GVO nach wie vor sehr viele unterschiedliche Regelungen zum Datenschutz. In bestimmten Bereichen gibt es signifikante Unterschiede 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 können für bestimmte Details abweichendes nationales oder sogar Landesrecht bestehen.

BEISPIEL

Nutzung von Cloud-Diensten durch Krankenhäuser

Szenario: Ein Träger von Krankenhäusern möchte die im Praxisbeispiel „Anonymisierung von Patientendaten zur Entwicklung KI-gestützter Medizinprodukte“ (→ II.2) vorgestellte SaaS-Lösung bei der Behandlung seiner Patienten nutzen.

Anforderung: Vereinzelte deutsche Landesgesetze lassen den Einsatz von Auftragsverarbeitern außerhalb von Krankenhäusern zumindest ihrem Wortlaut nach nicht zu. Diese Regelungen gestatten zwar beispielsweise Auftragsverarbeiter zur Mikroverfilmung von Patientenakten innerhalb des Krankenhauses, nicht aber cloudbasierte Lösungen. Der Cloud-Dienstleister muss daher nicht nur die DS-GVO, das deutsche Bundesdatenschutzgesetz und die Vorgaben des Strafgesetzbuches einhalten, sondern muss auch alle einschlägigen landesrechtlichen und berufsrechtlichen Regelungen im Blick haben.

8. Unabdingbarkeit des Datenschutzrechts

Nicht zuletzt kann auch die Unabdingbarkeit des Datenschutzrechts in der Praxis eine signifikante Herausforderung darstellen. 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-Folgenabschätzungen. Nach überwiegender Meinung ist beispielsweise auch ein freiwilliger Verzicht betroffener Personen auf die Erfüllung von Informationspflichten und Datensicherheitsanforderungen nicht möglich.

BEISPIEL

Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts

Szenario: Um seine Gesundheits-App in einer Betaphase unter Realbedingungen testen zu können, hat der App-Betreiber (siehe Praxisbeispiel „Einwilligungserfordernis für innovative Gesundheits-Apps“ → II.2) einige wenige Testpersonen gefunden, die die App nutzen und ihm Feedback geben wollen. Die Tester sind von dieser Technologie begeistert und Datenschutz ist ihnen hierbei nicht wichtig. 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.

Anforderung: 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.

III. Praxisempfehlungen: Spielräume bei der Erprobung digitaler Innovationen nutzen

Wenngleich die skizzierten Anforderungen des Datenschutzrechts die Entwicklung und Anwendung innovativer Technologien auf den ersten Blick vor große Herausforderungen stellen, lassen die datenschutzrechtlichen Regelungen bei näherer Betrachtung viele Spielräume, die sich gerade für die Erprobung digitaler Innovationen nutzbar machen lassen. Im Folgenden wird ein Überblick über die bedeutsamsten Gestaltungsinstrumente im bestehenden Rechtsrahmen gegeben. Dabei werden zur Veranschaulichung auch die im vorgehenden Kapitel herangezogenen Praxisbeispiele aufgegriffen.

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

Das Datenschutzrecht ist nur auf die Verarbeitung „personenbezogener Daten“ anwendbar, nicht aber auf die Nutzung anonymer Informationen. Ein in der Praxis nicht selten übersehenes, aber oftmals sehr wirkungsvolles Gestaltungsinstrument ist die Vermeidung personenbezogener Datenverarbeitung – sofern es das jeweilige Geschäftsmodell zulässt. Oft sind in der Praxis innovative Technologien bei näherer Betrachtung ebenso gut oder mit nur geringen Einschränkungen auch ohne Verarbeitung personenbezogener Daten realisierbar. Schon eine gezielte Reduzierung des Umfangs personenbezogener Datenverarbeitung auf ein absolutes Minimum reduziert den Aufwand für die Einhaltung datenschutzrechtlicher Anforderungen dabei oft erheblich.

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.

Die Erprobung von Sicherheitseinrichtungen eines neuen autonomen Fahrzeugs lässt sich technisch so gestalten, dass eine Videokamera dauerhaft Aufzeichnungen der Umgebung macht, die 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“ → II.1). Um die Verarbeitung personenbezogener Daten zu vermeiden, könnten anstelle der Videokamera spezielle Sensoren an Bord des Fahrzeuges genutzt werden, die keine Bildaufzeichnung erfordern – sofern technisch machbar.

Bei der blockchainbasierten Speicherung von Transaktionsdaten zu einer elektronischen Geldbörse (dazu Praxisbeispiel „Blockchainbasierte Zahlungstechnologie“ → II.3) erscheint es denkbar, in der Blockchain keine personenbezogenen Transaktionsdaten zu speichern. Zum erforderlichen Nachweis dafür, dass die Daten nicht verändert wurden, könnten nur nicht direkt personenbezogene Hash-Werte/Quersummen gespeichert werden. Die personenbezogenen Transaktionsdaten würden

dann nur in einem separaten System außerhalb der Blockchain gespeichert. Das lässt auch eine spätere Löschung dieser Daten zu.

Anonymisierte Informationen nutzen

Mit der Auswertung anonymisierter Informationen kann in vielen Fällen die Verarbeitung personenbezogener Daten vermieden werden. Die Anonymisierung bearbeitet personenbezogene Daten so, dass die betroffene Person auf Grundlage der bearbeiteten Daten nicht mehr identifiziert werden kann. 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, 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“ → II.2 und „Abgrenzung Anonymisierung und Pseudonymisierung“ → II.7). Für eine rechtssichere Anonymisierung wären die in einer Kopie des Originaldatensatzes enthaltenen Informationen so zu aggregieren, dass auch zusammen dem 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 im Zuge des technischen Fortschritts später 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.

Erprobung digitaler Innovationen anhand synthetischer Daten

Auch mit synthetischen Daten kann die Verarbeitung personenbezogener Daten oft vermieden werden. Eine einfache Anonymisierung kann oft nur mit einer Verringerung der Datenqualität erreicht werden. 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 erscheint die Nutzung solcher nahezu realen Daten als eine attraktive und erwägenswerte Alternative.

Im Praxisbeispiel „Big-Data-Analysen und explorative Statistiken“ (→ II.3) 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, nicht personenbezogenen Daten gilt das Datenschutzrecht allerdings nicht mehr.

2. Anreize für betroffene Personen setzen und 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 sich positiv auf die datenschutzrechtliche Rechtfertigung auswirken.

„Einwilligung“ als Gestaltungsinstrument

Mit der Rechtsgrundlage der „Einwilligung“ ermöglicht die DS-GVO einen erheblichen Gestaltungsspielraum für die Rechtfertigung der Verarbeitung personenbezogener Daten. Mit ihrer Einwilligung kann die betroffene Person grundsätzlich die Verarbeitung jedweder 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 so genannten „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. 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“ (→ II.3) beschriebenen Auswertungen großer Mengen an (Gesundheits-) Daten aus verschiedensten Quellen zu 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.

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 begrenzte 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 – argumentieren, dass die Krankenhäuser Auftragsverarbeiter auf Grundlage einer Einwilligung ihrer Patienten einsetzen dürfen (dazu Praxisbeispiel „Nutzung von Cloud-Diensten durch Krankenhäuser“ → II.8). 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 cloudbasierte 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.

„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“ ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn 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“ (→ II.4) 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 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 nicht ausreichen.

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

Betreibt im Praxisbeispiel „Einwilligungserfordernis für innovative Gesundheits-Apps“ (→ II.2) 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 berufen, um das spezielle Verarbeitungsverbot zu überwinden.

Für „normale“ Unternehmen greift meist keiner der gesetzlichen Ausnahmetatbestände, sodass selbst die vertragserforderliche Verarbeitung von Gesundheitsdaten einer ausdrücklichen Einwilligung der Nutzer bedarf. 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.

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

Setzen von Anreizen für die Teilhabe an Reallaboren

Es kann sich in manchen Fällen anbieten, betroffenen Personen Vorteile zu gewähren, wenn Sie an einem Reallabor durch Abschluss entsprechender Verträge und Erklärung von Einwilligungen teilnehmen. 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 diejenigen, die umfangreichen Big-Data-Analysen zur Entwicklung neuer Produkte zustimmen, als Anreiz etwa Pizzagutscheine ausgeben (hierzu Praxisbeispiele „Big-Data-Analysen und explorative Statistiken“ → II.3) und „Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts“ (→ II.9)

- 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“ → II.2, „KI-gestützte Automatisierung der Kundenkommunikation“ → II.4).

3. Interessenabwägung in der Praxis nutzen und positiv beeinflussen

Als zentrale Abwägungsklausel bietet der Rechtfertigungstatbestand der „Interessenabwägung“ einen erheblichen Gestaltungsspielraum. Hierbei lässt sich auch der **begrenzte Umfang von Reallaboren als Kriterium für die Interessenabwägung nutzen.**

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).

Über die Interessenabwägung haben Verantwortliche die Flexibilität, grundsätzlich jede beliebige „interessengerecht gestaltete“ Verarbeitung vorzunehmen (mit Ausnahme solcher Verarbeitungstätigkeiten, die unter das spezielle Verarbeitungsverbot für „besondere Kategorien personenbezogener Daten“ fallen.) 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. Die Erforderlichkeit lässt sich jedoch zumindest in einem gewissen Umfang auch durch die Gestaltung der jeweiligen Verarbeitungsschritte und der Zweckdefinition beeinflussen. Auf die Erforderlichkeit ist ein besonderes Augenmerk zu legen. In der Praxis fehlt es 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. In vielen Fällen begründen Aufsichtsbehörden die Unzulässigkeit einer Verarbeitung allein mit fehlender Erforderlichkeit.

Interessenabwägung positiv beeinflussen

Unter welchen Voraussetzungen eine Interessenabwägung in einem Reallabor (oder sonstigen Szenarien) zugunsten 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. 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.

  Wie im Praxisbeispiel „Abgrenzung Anonymisierung und Pseudonymisierung“ → II.8) 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 nur pseudonymisierte Daten zu Teilnehmenden an Studien, die aus sich heraus nicht unmittelbar personenbezogen sind. Ein unabhängiger Datentreuhänder führt hingegen eine Zuordnungsliste dieser Daten zu den jeweiligen Probanden und fungiert als externe Kontrollinstanz bei einer erforderlichen Aufhebung der Pseudonymisierung. Nur unter im Vorfeld konkret festgelegten Bedingungen würde das Forschungsinstitut dann die Kontaktdaten der jeweiligen Probanden erhalten, beispielsweise zur Klärung von Rückfragen mit Teilnehmenden der Studie. Vergleichbare Modelle erscheinen beispielsweise bei Reallaboren im Bereich der wissenschaftlichen Forschung erwägenswert.

- Gewährt ein Verantwortlicher in transparenter Weise ein überobligatorisches, bedingungsloses und leicht auszuübendes Widerspruchsrecht, wiegen die schutzwürdigen Belange der betroffenen Person geringer. Sie hat es selbst in der Hand, 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.

  In den Praxisbeispielen „Big-Data-Analysen und explorative Statistiken“ (→ II.3) sowie „KI-gestützte Automatisierung der Kundenkommunikation“ (→ II.4) 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. 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 auf einer Website, anstatt nur in den Datenschutzinformationen).

- 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 Abwägung 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).

- Eine sehr enge Zweckbindung und eine sehr kurze Verarbeitungsdauer lassen sich bei der Interessenabwägung als Argument zugunsten des Verantwortlichen heranziehen.

  Wie im Praxisbeispiel „Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars“ (→ II.7) gezeigt, fallen beim Hersteller von Connected Cars unüberschaubar viele Daten zur Fahrzeugnutzung an (z. B. zur Verbesserung und Weiterentwicklung dieser Fahrzeuge). Hier besteht beispielsweise das Risiko, dass diese Daten auch zulasten der Fahrzeughalter/Fahrer verwendet werden könnten. Denkbar wäre 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.

  Bei für Testfahrten eines autonomen Fahrzeugs notwendigen Videoaufzeichnungen kann die Interessenabwägung dadurch positiv beeinflusst werden, 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“ → II.1).

Durch Interessenabwägung nicht gestaltbare Aspekte

- **Keine Überwindung spezieller Verarbeitungsverbote durch einfache Interessenabwägung**: Dort, wo es spezielle Verarbeitungsverbote gibt, ist eine Verarbeitung 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“ → II.9). 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 “.

- **Interessenabwägung nur sehr eingeschränkt für behördliche Verarbeitungen anwendbar:** Die DS-GVO gestattet Behörden, die in Erfüllung ihrer Aufgaben handeln, die „Interessenabwägung“ als Rechtsgrundlage nicht. Zwar ist bislang 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.

- **Dokumentationspflichten:** Die Durchführung einer Interessenabwägung macht die Dokumentation der Verarbeitungsaktivitäten nicht entbehrlich. Im Gegenteil: Die Interessenabwägung zieht sogar höhere Dokumentationspflichten nach sich. Für die Erfüllung der datenschutzrechtlichen Rechenschaftspflicht ist nicht nur eine Dokumentation der eigentlichen Verarbeitungsaktivität erforderlich, sondern auch eine detaillierte Dokumentation der Abwägung der Interessen des Verantwortlichen, Dritter und der betroffenen Personen.

- Die Dokumentation ist in der Praxis vergleichsweise aufwendig. Jedoch kann der Verantwortliche den sehr offen gehaltenen Rechtfertigungstatbestand in konkrete Bahnen lenken und besser 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.

4. Mit Reduzierung der Risiken durch die Verarbeitung die erforderlichen Datenschutzmaßnahmen 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,**
- **Gestaltung der Sicherheitsmaßnahmen,**
- **Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.**

Beispielsweise 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. Beides dürfte in einem Reallabor typischerweise niedriger ausfallen als etwa in einem vollständigen nationalen oder internationalen Roll-out eines Geschäftsmodells.

Der App-Betreiber im Praxisbeispiel „Erprobung neuer Technologien unter Abbedingung des Datenschutzrechts“ (→ II.9) 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).

5. 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:

- **Weite Zweckdefinition und „Broad Consent“ für wissenschaftliche Forschung,**
- **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“ (EG 159 DS-GVO).

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. Unter dem Begriff „statistische Zwecke" verstehen die Erwägungsgründe der DS-GVO jeden „für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche[n] Vorgang der Erhebung und Verarbeitung personenbezogener Daten" (EG 162 DS-GVO). 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 und Innovation leisten, ist es durchaus denkbar, 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" (→ II.2) 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 ist es denkbar, anstelle der Einwilligung gesetzliche Ausnahmetatbestände zu nutzen, die die Verarbeitung von Gesundheitsdaten zulassen. So könnte man 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" → II.7).

Eine ähnliche Argumentation ist auch im Praxisbeispiel „Big-Data-Analysen und explorative Statistiken" (→ II.3) denkbar, insbesondere wenn der App-Betreiber seine Auswertungen auf Grundlage wissenschaftlich anerkannter Standards durchführt und hieraus 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.

6. Bildsymbole für die Gestaltung von Datenschutzinformationen verwenden

Als Gestaltungsmittel für die transparente Information über die Datenverarbeitung sieht die DSGVO die Nutzung standardisierter Bildsymbole vor. Diese Bildsymbole sollen nicht die nach der DS-GVO erforderlichen Detailinformationen 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, könnten aussagekräftige Bildsymbole verwendet werden, um den Nutzern auch am kleinen Smartphone-Display zumindest einen guten Überblick über die Verarbeitung zu verschaffen (hierzu Praxisbeispiel „Datenschutzinformationen für ein smartes Hausautomatisierungssystem“ → II.5). 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.

7. 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 dem Nachweis der Einhaltung der DS-GVO.

„Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten“ (Art. 40 (2) DS-GVO), 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.

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 hohe Unsicherheitsfaktoren gibt, etwa bei der konkreten Zweckbestimmung einer Big-Data-Analyse (so etwa im Praxisbeispiel „Big-Data-Analysen und explorative Statistiken“ → II.3). Auch 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“ → II.4).

Die konkrete Rechtswirkung von Verhaltensregeln und Zertifizierungen ist zwar umstritten. Allerdings sieht die DS-GVO etwa bei folgenden Aspekten eine Berücksichtigung vor. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens:

- kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen;
- kann als Faktor herangezogen werden, um die Erfüllung der Anforderungen an technische und organisatorische Sicherheitsmaßnahmen nachzuweisen;
- ist bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag gebührend zu berücksichtigen.

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

Grenzen dieser Selbstregulierungsmechanismen

- **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 noch nicht durchgesetzt. Nach aktuellem Kenntnisstand gibt es bislang in Deutschland nur eine einzige genehmigte Verhaltensregel (die „Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien“[3]). Zertifizierungen nach der DS-GVO wurden, soweit ersichtlich, bislang noch überhaupt nicht erteilt. Es gibt auch noch keine akkreditierten Zertifizierungsstellen.

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.

3 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.

- **Nur Präzisierung, aber keine Schaffung neuer Rechtfertigungstatbestände**
  Verhaltensregeln bzw. 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).

8. 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. Die praktische Erfahrung zeigt jedoch, dass die Aufsichtsbehörden auch außerhalb dieses gesetzlichen Rahmens auf informeller Grundlage unterstützen. So hat die deutsche Datenschutzkonferenz (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“.

Auch zu ganz konkreten Einzelfragen erscheint eine Abstimmung mit den Aufsichtsbehörden denkbar, etwa zu den in den Praxisbeispielen „Big-Data-Analysen und explorative Statistiken“ (→ II.3), „Reichweite von Auskunfts- und Portabilitätsansprüchen bei Connected Cars“ (→ II.7), „Forschung und Statistik zur Verbesserung von Produkten und Dienstleistungen“ (→ II.7) und „Nutzung von Cloud-Diensten durch Krankenhäuser“ (→ II.8) beschriebenen Anforderungen des Datenschutzrechts.

Selbstverständlich hat eine solche informelle Abstimmung keinerlei normative Wirkung, sondern bewirkt nur eine gewisse Selbstbindung der beteiligten Aufsichtsbehörden. Dadurch lässt sich die Rechtsunsicherheit 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.[4]

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

INFOBOX

Zentrale Begriffe der DS-GVO

- „**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.

- „**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).

- „**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).

- „**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).

- „**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).

- „**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).