EUROPEAN DATA PROTECTION SUPERVISOR

Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit

11. April 2017

INHALT

I. Welchen Zweck hat dieses Toolkit und wie ist es zu verwenden?

Grundrechte, in der Charta der Grundrechte der Europäischen Union (nachstehend „die Charta“) verankert sind, gehören zu den Kernwerten der Europäischen Union[1]. Diese Rechte sind zu wahren, wenn Organe und Einrichtungen der EU neue Maßnahmen konzipieren und umsetzen oder neue Rechtsvorschriften annehmen. In der Rechtsordnung der EU spielen aber auch noch andere Grundrechtsnormen eine wichtige Rolle, insbesondere die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK).

Dieses Toolkit ist die Antwort auf von EU-Organen vorgetragene Ersuchen um Orientierungshilfe bezüglich der sich aus Artikel 52 Absatz 1 der Charta ergebenden besonderen Anforderungen, dem zufolge Einschränkungen der Ausübung des Rechts auf Schutz personenbezogener Daten (Artikel 8 der Charta) nur vorgenommen werden dürfen, wenn sie „erforderlich“ sind und einer dem Gemeinwohl dienenden Zielsetzung oder dem Erfordernis des Schutzes der Rechte und Freiheiten anderer entsprechen[2].

Seitdem sind die Bedingungen für eventuelle Einschränkungen der Ausübung von Grundrechten zu den wichtigsten Merkmalen der Charta geworden, weil sie darüber entscheiden, in welchem Umfang die Rechte tatsächlich genossen werden können.

Die Erforderlichkeit ist eine wesentliche Voraussetzung, die jede vorgeschlagene Maßnahme, die eine Verarbeitung personenbezogener Daten mit sich bringt, zu erfüllen hat.

Dieses Toolkit ist als Hilfestellung bei der Beantwortung der Frage gedacht, ob vorgeschlagene Maßnahmen mit dem EU-Datenschutzrecht in Einklang stehen. Es wurde als Rüstzeug für Entscheidungsträger und Gesetzgeber der EU erarbeitet, die für die Ausarbeitung oder Prüfung von Maßnahmen zuständig sind, die die Verarbeitung personenbezogener Daten beinhalten und das Recht auf Schutz personenbezogener Daten oder andere in der Charta niedergelegte Rechte und Freiheiten einschränken.

Der EDSB respektiert in vollem Umfang die Verantwortung des Gesetzgebers für die Beurteilung der Erforderlichkeit und Verhältnismäßigkeit einer Maßnahme. Dieses Toolkit soll daher nicht endgültig die Frage beantworten (und könnte dies auch gar nicht tun), ob eine konkrete vorgeschlagene Maßnahme als erforderlich gelten kann. Es bietet vielmehr eine praxisbezogene, in einzelne Schritte unterteilte Checkliste für die Beurteilung der Erforderlichkeit neuer Legislativmaßnahmen und gleichzeitig eine rechtliche Analyse des Begriffs der Erforderlichkeit mit Blick auf die Verarbeitung personenbezogener Daten.

Es ergänzt und vertieft bereits bestehende Orientierungshilfen der Kommission und des Rates zu den Einschränkungen von Grundrechten ganz allgemein, in denen es beispielsweise um Folgenabschätzungen und Kompatibilitätsprüfungen geht[3].

Das Toolkit besteht aus dieser Einleitung, in der Inhalt und Zweck des Toolkits dargestellt werden, einer praktischen, in einzelne Schritte untergliederten Checkliste für die Beurteilung der Erforderlichkeit neuer Legislativmaßnahmen und einer rechtlichen Analyse der Prüfung der Erforderlichkeit der Verarbeitung personenbezogener Daten. Die Checkliste ist das Herzstück des Toolkits und kann auch unabhängig von dem Rest des Dokuments verwendet werden.

Grundlage des Toolkits sind die Rechtsprechung[4] des Gerichtshofs der Europäischen Union (nachstehend EuGH), des Europäischen Gerichtshofs für Menschenrechte (EGMR) sowie frühere Stellungnahmen des EDSB und der Artikel 29-Datenschutzgruppe. Es lehnt sich an ein 2016 für eine Konsultation der Öffentlichkeit veröffentlichtes Hintergrundpapier an[5].

Wir bedanken uns bei allen Teilnehmern für ihre Rückmeldungen, die wir zur Verbesserung des Dokuments herangezogen haben.

Anmerkung zur Terminologie

Mit Blick auf die Rechte in der Charta der Grundrechte werden in der politischen Diskussion und sogar in Rechtstexten, darunter der Rechtsprechung des EuGH, scheinbar auswechselbar mehrere ähnliche Begriffe wie „Einschränkung", „Beschränkung", „Eingriff" und „Einfluss" und deren Ableitungen verwendet. Zwecks Vereinfachung hält sich dieses Toolkit an Artikel 52 der Charta und spricht mit Ausnahme von Zitaten durchgehend von „Einschränkung".

II. Rechtliche Analyse: Anwendung der Prüfung der Erforderlichkeit auf das Recht auf Schutz personenbezogener Daten

1. Die Prüfung der Erforderlichkeit zur Beurteilung der Rechtmäßigkeit vorgeschlagener Maßnahmen, die die Verarbeitung personenbezogener Daten zur Folge haben

In Artikel 8 der Charta ist das Recht auf Schutz personenbezogener Daten verankert. Dieses Recht ist nicht absolut und kann eingeschränkt werden, sofern die Einschränkungen den in Artikel 52 Absatz 1 der Charta formulierten Bedingungen entsprechen[6]. Gleiches gilt für das in Artikel 7 der Charta niedergelegte Recht auf Achtung des Privatlebens.

Jede Einschränkung der Ausübung der durch die Charta geschützten Grundrechte muss, damit sie rechtmäßig ist, den folgenden, in Artikel 52 Absatz 1 der Charta niedergelegten Kriterien entsprechen:

- Sie muss gesetzlich vorgesehen sein;
- sie muss den Wesensgehalt des Rechts achten;
- sie muss tatsächlich den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer entsprechen;
- sie muss erforderlich sein (Gegenstand dieses Toolkits), und
- sie muss verhältnismäßig sein.

Diese Kriterienliste gibt die verlangte Reihenfolge bei der Beurteilung der Rechtmäßigkeit wieder. Zunächst einmal ist zu prüfen, ob ein zugängliches und vorhersehbares Gesetz[7] eine Einschränkung vorsieht, und ob der **Wesensgehalt des Rechts** geachtet wird, ob also das Recht weitgehend seines Inhalts beraubt ist und die Person das Recht nicht ausüben kann[8]. Wird das Wesen des Rechts berührt, ist die Maßnahme unrechtmäßig und muss nicht näher untersucht werden, ob die Maßnahme mit den Vorschriften in Artikel 52 Absatz 1 der Charta vereinbar ist.

Als nächstes ist der Frage nachzugehen, ob die Maßnahme **einer dem Gemeinwohl dienenden Zielsetzung** entspricht. Die dem Gemeinwohl dienende Zielsetzung bildet den Hintergrund, vor dem die Erforderlichkeit der Maßnahme beurteilt werden kann. Es ist daher wichtig, die dem Gemeinwohl dienende Zielsetzung so detailliert wie möglich zu bestimmen, damit festgestellt werden kann, ob die Maßnahme erforderlich ist.

Der nächste Schritt besteht darin, die **Erforderlichkeit** einer vorgeschlagenen legislativen Maßnahme zu beurteilen, die die Verarbeitung personenbezogener Daten mit sich bringt.

Ist diese Frage zur Zufriedenheit beantwortet, wird die **Verhältnismäßigkeit** der vorgeschlagenen Maßnahme bewertet. Sollte die Erforderlichkeit des Maßnahmenentwurfs nicht festgestellt werden, besteht kein Bedarf an einer Prüfung seiner Verhältnismäßigkeit. Eine Maßnahme, die als nicht erforderlich eingestuft wurde,

sollte erst dann wieder vorgeschlagen werden, wenn sie so geändert wurde, dass sie die Bedingung der Erforderlichkeit erfüllt.

Mit der Überprüfung der Verhältnismäßigkeit, die bei jeder Einschränkung von Grundrechten durchzuführen ist, wird sich der EDSB in einem eigenen Dokument befassen.

Eine genaue Beschreibung der fraglichen Maßnahme ist wichtig, da sie mehrere der oben genannten Kriterien betreffen kann. Es kommt daher vor, dass die Gerichte die Kriterien paarweise prüfen. So kann beispielsweise eine unklar formulierte oder zu breit angelegte Maßnahme die Beantwortung der Frage verhindern, ob sie „gesetzlich vorgesehen" und „erforderlich" ist[9].

2. Beziehung zwischen Verhältnismäßigkeit und Erforderlichkeit

Die **Verhältnismäßigkeit** ist ein allgemeiner Grundsatz des EU-Rechts, demzufolge *„die Maßnahmen der Union inhaltlich wie formal nicht über das zur Erreichung der Ziele der Verträge erforderliche Maß hinausgehen"*[10]. Nach der ständigen Rechtsprechung des Gerichtshofs *„verlangt der Grundsatz der Verhältnismäßigkeit, dass die Handlungen der Unionsorgane geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist"*[11]. Daher *„schränkt er die Behörden in der Ausübung ihrer Befugnisse ein, weil er ein Gleichgewicht zwischen den eingesetzten Mitteln und dem angestrebten Ziel (oder dem erreichten Ergebnis) verlangt"*[12].

Artikel 52 Absatz 1 der Charta besagt: *„Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen [der Ausübung von Grundrechten] nur vorgenommen werden, wenn sie erforderlich sind (...)*".

Verhältnismäßigkeit im weiteren Sinne umfasst sowohl die Erforderlichkeit als auch die **Angemessenheit** einer Maßnahme, also das Ausmaß, in dem eine logische Verknüpfung zwischen der Maßnahme und dem verfolgten (legitimen) Ziel besteht. Damit eine Maßnahme ferner dem in Artikel 52 Absatz 1 der Charta niedergelegten Grundsatz der Verhältnismäßigkeit Genüge tut, sollten die sich aus der Maßnahme ergebenden Vorteile nicht durch die Nachteile aufgewogen werden, die die Maßnahme im Hinblick auf die Achtung vor der Ausübung der Grundrechte mit sich bringt[13]. Dieses letzte Element beschreibt die Verhältnismäßigkeit in einem engeren Sinne und stellt den Prüfung der Verhältnismäßigkeit dar. Sie sollte klar von der **Erforderlichkeit** unterschieden werden.

Erforderlichkeit impliziert das Erfordernis einer kombinierten, faktengestützten Bewertung der Wirksamkeit der Maßnahme mit Blick auf das angestrebte Ziel und auf die Frage, ob sie im Vergleich zu anderen Optionen für das Erreichen desselben Ziels weniger eingreifend ist.

„Erforderlichkeit" ist auch ein Grundsatz der Datenqualität und ein in praktisch allen im Datenschutzsekundärrecht der EU formulierten Anforderungen an die Rechtmäßigkeit der Verarbeitung personenbezogener Daten immer wieder auftretender Faktor[14]. Ferner besteht eine Verknüpfung zwischen Artikel 8 Absatz 2 der Charta und dem Sekundärrecht, denn Artikel 8 Absatz 2 spricht von der „gesetzlich geregelten" legitimen Grundlage für die Verarbeitung, und die Erläuterung zu Artikel 8 verweist auf dieses Sekundärrecht mit den Worten, die Richtlinie 95/46 und die Verordnung (EG)

Nr. 45/2001 „enthalten Bedingungen und Beschränkungen für die Wahrnehmung des Rechts auf den Schutz personenbezogener Daten".

Dieses Toolkit stützt sich auf die Annahme, dass nur bei einer erwiesenermaßen *erforderlichen* Maßnahme eine Prüfung der Verhältnismäßigkeit stattfindet. In der jüngeren Vergangenheit hat der EuGH in Rechtssachen die Verhältnismäßigkeit gar nicht mehr geprüft, nachdem er befunden hatte, dass die Einschränkungen von in Artikel 7 und 8 der Charta verankerten Rechten nicht unbedingt erforderlich waren[15]. So sollte beispielsweise bei einer Strafverfolgungsmaßnahme, sofern sie für erforderlich gehalten wird, geprüft werden, ob sie bei einer Beschränkung auf lediglich schwere Straftaten verhältnismäßiger wäre. Eine Prüfung der Verhältnismäßigkeit könnte auch die Klärung der Frage beinhalten, welche Vorschriften für eine Überwachungsmaßnahme vor oder nach ihrer Genehmigung gelten sollten: Solche Vorschriften, häufig als „Garantien" bezeichnet, könnten die von der geplanten Maßnahme aufgeworfenen Risiken für die Grundrechte verringern.

In der Praxis kann ein spezifischer Aspekt oder eine Bestimmung in einem Maßnahmenentwurf für die Beurteilung sowohl der Erforderlichkeit als auch der Verhältnismäßigkeit von Belang sein. So kann beispielsweise die Frage, ob eine Maßnahme auf alle Straftaten oder nur auf schwere Straftaten abheben sollte, als Frage der Erforderlichkeit betrachtet werden; sollte jedoch eine solche Bestimmung als erforderlich eingestuft werden, müsste noch immer ihre Verhältnismäßigkeit und die Frage untersucht werden, ob sie die Werte einer demokratischen Gesellschaft untergräbt. In der Praxis kommt es daher zu gewissen Überschneidungen zwischen den Begriffen Erforderlichkeit und Verhältnismäßigkeit, und je nach der fraglichen Maßnahme können die beiden Prüfungen parallel oder auch in umgekehrter Reihenfolge durchgeführt werden[16].

Generell gilt jedoch, dass zunächst bestimmt werden muss, ob eine Einschränkung eines Grundrechts erforderlich ist; erst dann sollte die Verhältnismäßigkeit geprüft werden.

3. Die Charta und die EMRK

Das **Recht auf Achtung des Privatlebens** (auch als Recht auf Privatsphäre bezeichnet) ist Gegenstand der Charta (Artikel 7) und der EMRK (Artikel 8), während das **Recht auf den Schutz personenbezogener Daten** als eigenständiges Grundrecht in der Charta (Artikel 8) geschützt ist[17].

Nach dem Inkrafttreten des Vertrags von Lissabon wurde die **Charta** zum wichtigsten Bezugspunkt, mit dessen Hilfe die Konformität des EU-Sekundärrechts mit den Grundrechten beurteilt wird[18]. In der ständigen Rechtsprechung des EuGH heißt es, dass die EMRK, *„solange die Union ihr nicht beigetreten ist, kein Rechtsinstrument darstellt, das formell in die Unionsrechtsordnung übernommen worden ist"*[19]. Folglich hat der EuGH in jüngerer Zeit in seiner Rechtsprechung bekräftigt, dass eine Prüfung der Gültigkeit einer Bestimmung des EU-Sekundärrechts *„allein anhand der durch die Charta garantierten Grundrechte vorzunehmen ist"*[20].

Im Einklang mit Artikel 6 Absatz 3 EUV hat der EuGH jedoch auch daran erinnert, dass die spezifischen Bestimmungen der EMRK *„zum Zweck der Auslegung"* der entsprechenden Bestimmungen der Charta heranzuziehen sind[21]. In Artikel 6 Absatz 3

EUV heißt es insbesondere: *„Die Grundrechte, wie sie in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, sind als allgemeine Grundsätze Teil des Unionsrechts".* Und auch die Charta selber fordert dies: *„Soweit diese Charta Rechte enthält, die den durch die [EMRK] garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der [EMRK] verliehen wird"*, während das Recht der Union einen weiter gehenden Schutz gewähren kann (Artikel 52 Absatz 3 der Charta).

Einerseits entspricht das Recht auf Achtung des Privatlebens in Artikel 7 der Charta unmittelbar Artikel 8 EMRK. Andererseits ist das Recht auf den Schutz personenbezogener Daten in der Charta, nicht jedoch in der EMRK formuliert und ist daher nicht unter den Rechten aufgeführt, denen ein gemäß Artikel 52 Absatz 2 der Charta durch die EMRK geschütztes Recht entspricht[22]. Die Erläuterung zu Artikel 8 der Charta besagt jedoch, dass sich dieses Recht unter anderem auf Artikel 8 EMRK stützt. Daher ist die Rechtsprechung des EGMR zu Artikel 8 EMRK bei der Beantwortung der Frage, ob eine Einschränkung im Einklang mit der Charta steht, zwar relevant, jedoch nicht zwangsläufig ausschlaggebend[23]. EuGH und EGMR stehen auch in einem ständigen Dialog, wie an zahlreichen Verweisen in der Rechtsprechung des jeweils anderen Gerichtshofs abzulesen ist[24].

Die in Artikel 8 Absatz 2 EMRK und Artikel 52 Absatz 1 der Charta aufgeführten Kriterien für eine rechtmäßige Einschränkung des Rechts auf Achtung des Privatlebens sind einander ähnlich[25]. Artikel 8 Absatz 2 EMRK besagt darüber hinaus, dass die Einschränkung „in einer demokratischen Gesellschaft" notwendig sein muss. Auch wenn Artikel 52 Absatz 1 nicht dieselbe Formulierung verwendet, ist das Element der „demokratischen Gesellschaft" doch auch in der EU-Rechtsordnung vorhanden, denn es ergibt sich aus den Kernwerten der EU, zu denen die Achtung der Demokratie gehört (Artikel 2 EUV).

Daher sind die wichtigsten Bezugspunkte für eine Beurteilung der Erforderlichkeit von Maßnahmen, die die Ausübung der in Artikel 8 der Charta garantierten Rechte einschränken, Artikel 52 Absatz 1 sowie die Rechtsprechung des EuGH. Darüber hinaus sollten auch die Kriterien in Artikel 8 Absatz 2 EMRK und hier vor allem die Bedingung, dass eine Einschränkung in einer demokratischen Gesellschaft erforderlich sein muss[26], wie in der Rechtsprechung des EGMR ausgelegt, in der Analyse Berücksichtigung finden.

4. Maßnahmen sollten *unbedingt erforderlich* sein

Die Rechtsprechung des EuGH prüft, ob Einschränkungen der Rechte auf Schutz personenbezogener Daten und die Achtung des Privatlebens bei der Verarbeitung personenbezogener Daten *unbedingt erforderlich* sind: *„Ausnahmen und Beschränkungen in Bezug auf den Schutz personenbezogener Daten **müssen sich auf das absolut Notwendige beschränken**"*. Der EGMR prüft die *absolute Notwendigkeit* je nach Kontext und allen Gegebenheiten, beispielsweise mit Blick auf geheime Überwachungsmaßnahmen[27].

Aus der Rechtsprechung des EuGH ergibt sich, dass die Bedingung der unbedingten Notwendigkeit eine horizontale Bedingung ist, und dies unabhängig von dem Bereich, um den es geht, wie Strafverfolgung oder kommerzieller Sektor[28]. Das Erfordernis der

„unbedingten Notwendigkeit“ ist eine Folge der wichtigen Rolle, die die Verarbeitung personenbezogener Daten für eine Reihe von Grundrechten spielt, darunter die Meinungsfreiheit. Auch wenn es für den Bereich der Strafverfolgung spezifische Rechtsvorschriften gibt, wie beispielsweise die Richtlinie 2016/680[29], rechtfertigt dies nicht eine andere Bewertung der Erforderlichkeit.

Das Erfordernis der unbedingten Notwendigkeit hat insofern noch eine weitere Konsequenz, als die gerichtliche Überprüfung der Maßnahme auch streng ist; mit anderen Worten: Der Spielraum des Gesetzgebers bei der Auswahl der Maßnahme ist beschränkt. Die Bedingungen für eine strenge gerichtliche Überprüfung des Gestaltungsspielraums des Gesetzgebers werden also auch aus dem Blickwinkel der Schwere der Einschränkung betrachtet, die eine bestimmte Maßnahme verursachen kann[30]. Auch der EDSB unterstrich in der anhängigen Rechtssache bezüglich des Entwurfs eines PNR-Abkommens zwischen der EU und Kanada, dass in Anbetracht der systematischen und besonders die Privatsphäre verletzenden Verarbeitung personenbezogener Daten, die das Abkommen vorsieht, eine strenge gerichtliche Überprüfung erforderlich ist[31].

5. Einschränkung eines Grundrechts

Die Überprüfung der Erforderlichkeit sollte in Fällen vorgenommen werden, in denen die vorgeschlagene Legislativmaßnahme die Verarbeitung personenbezogener Daten zur Folge hat.

Der EuGH bewertet Einschränkungen der Ausübung von im EU-Recht garantierten Rechten und Freiheiten auf der Grundlage von Artikel 52 Absatz 1 der Charta. Der Gerichtshof stellte fest, dass eine Handlung „einen Eingriff in das durch Artikel 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten dar, da sie eine Verarbeitung personenbezogener Daten vorsieht“[32]. Daher ist vom Grundsatz her jeder im Gesetz vorgesehene Verarbeitungsvorgang (wie die Erhebung, Speicherung, Verwendung, Weitergabe von Daten) eine Einschränkung des Rechts auf den Schutz personenbezogener Daten, und dies unabhängig davon, ob diese Einschränkung möglicherweise gerechtfertigt ist.

Darüber hinaus hat der EuGH in der überwiegenden Zahl der Rechtssachen, in denen es um Rechtsvorschriften ging, festgestellt, dass eine Verarbeitung sowohl das Recht auf Schutz personenbezogener Daten als auch das Recht auf Achtung der Privatsphäre einschränkt[33]. Der Gerichtshof befand ferner, dass es für die Feststellung einer Einschränkung *„nicht darauf ankommt, ob die übermittelten Informationen als sensibel anzusehen sind oder ob die Betroffenen durch den Vorgang irgendwelche Nachteile erlitten haben“*[34].

Mit Blick auf das in Artikel 8 EMRK geschützte Recht auf Privatleben besagt die Rechtsprechung des EGMR, dass die Verarbeitung personenbezogener Daten das Recht je nach den Gegebenheiten, wie dem sensiblen Charakter der Daten und der Weise, wie die Daten verwendet werden, einschränken kann[35].

6. Schlussfolgerung: Erforderlichkeit im Datenschutzrecht - ein fall- und faktengestütztes Konzept, das der Bewertung durch den EU-Gesetzgeber bedarf

Eine vorgeschlagene Maßnahmen sollte sich auf Belege stützen, aus denen hervorgeht, welches Problem mit der Maßnahmen gelöst werden soll, wie es mit der Maßnahme gelöst werden soll, und warum bestehende oder weniger in die Privatsphäre eindringende Maßnahmen es nicht hinreichend lösen können.

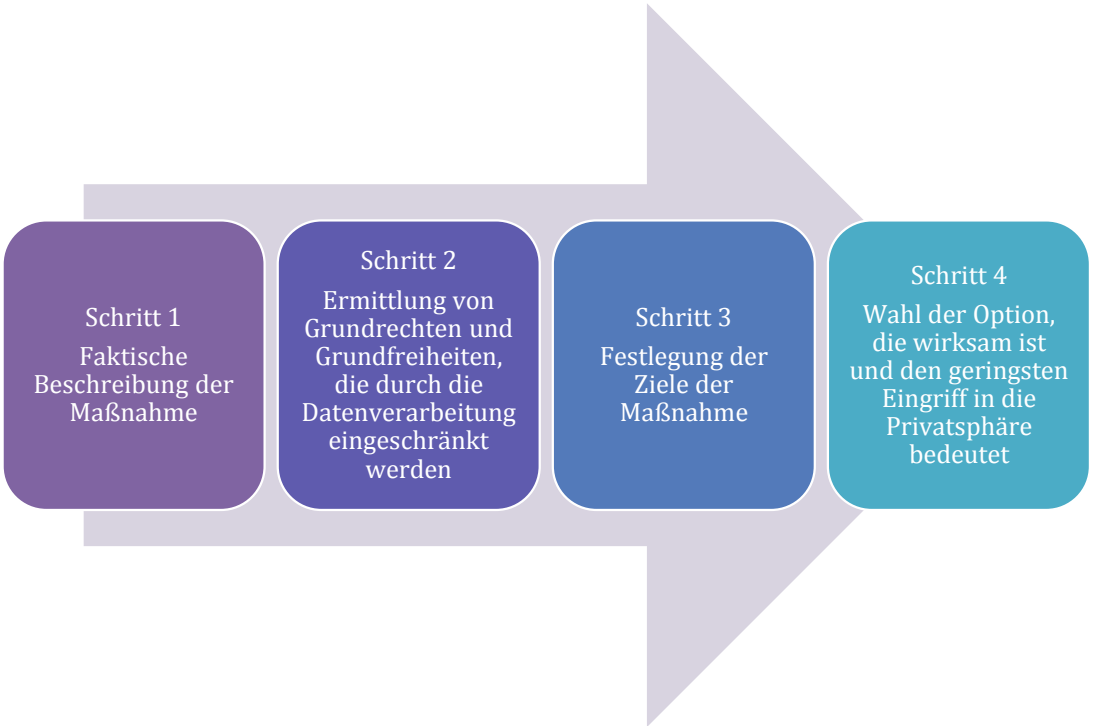
Eine Analyse der Rechtsprechung des EuGH und des EGMR erbringt, dass Erforderlichkeit im Datenschutzrecht ein faktenbasiertes Konzept und nicht ein nur abstrakter Begriff ist, und dass das Konzept vor dem Hintergrund der konkreten Gegebenheiten eines Falls sowie der Bestimmungen der Maßnahme und des mit ihr verfolgten konkreten Zwecks zu betrachten ist[36].

III. Checkliste für die Beurteilung der Erforderlichkeit neuer Legislativmaßnahmen

Die Checkliste für die Beurteilung der Erforderlichkeit besteht aus vier aufeinander folgenden Schritten. Jeder Schritt entspricht einer Reihe von Fragen, die die Beurteilung der Erforderlichkeit erleichtern.

- **Schritt 1** ist einleitender Art; er verlangt **eine detaillierte faktische Darstellung** der vorgeschlagenen Maßnahme und ihres Zwecks, die jeder Beurteilung vorausgeht.
- **Schritt 2** hilft bei der Beantwortung der Frage, ob die vorgeschlagene Maßnahme **eine Einschränkung** des Rechts auf Schutz personenbezogener Daten oder des Rechts auf Achtung des Privatlebens (auch als Recht auf Privatsphäre bezeichnet) und möglicherweise noch anderer Rechte bedeutet.
- In **Schritt 3** wird das **Ziel der Maßnahme** betrachtet, anhand dessen die Erforderlichkeit einer Maßnahme beurteilt werden sollte.
- **Schritt 4** bietet **Orientierung bezüglich der spezifischen Aspekte, auf die** bei der Prüfung der Erforderlichkeit **einzugehen ist**; so sollte die Maßnahme insbesondere **wirksam sein** und **den geringsten Eingriff in die Privatsphäre bedeuten.**

Führt die Beurteilung eines der in den Schritten #2 bis #4 aufgeführten Elemente zu dem Schluss, dass eine Maßnahme möglicherweise dem Erfordernis der Notwendigkeit nicht Genüge tut, sollte die Maßnahme entweder erst gar nicht vorgeschlagen oder unter Berücksichtigung der Ergebnisse der Analyse überdacht werden.



Schritt 1: Faktische Beschreibung der vorgeschlagenen Maßnahme

Eine detaillierte Beschreibung der ins Auge gefassten Maßnahme ist nicht nur Voraussetzung für die Prüfung der Erforderlichkeit, sondern sie hilft auch beim Nachweis der Einhaltung der ersten Bedingung in Artikel 52 Absatz 1 der Charta, also der Qualität des Rechts.

Erläuterung

- ✓ Die Maßnahme sollte hinreichend beschrieben werden, damit klar wird, was genau für welchen Zweck vorgeschlagen wird.
    - Vor allem kommt es darauf an, präzise anzugeben, in welchem Umfang die vorgeschlagene Maßnahme die Verarbeitung personenbezogener Daten vorsieht, und welche(s) das/die Ziele und der/die konkrete(n) Zwecke(e) der Maßnahme ist/sind.
    - Wie bereits erwähnt (Abschnitt II.1), kann eine verschwommen definierte Maßnahme durchaus noch andere Bedingungen für eine rechtmäßige Einschränkung von Grundrechten berühren und würde sie die Ermittlung der möglicherweise betroffenen Rechte erschweren.

Vorgehensweise

- ✓ **Beschreiben Sie die Maßnahme**
    - Beantworten Sie die Frage, ob die Maßnahme die Verwendung personenbezogener Daten vorsieht.
        - Der Ausdruck **personenbezogene Daten** ist sehr weit gefasst, denn er bezeichnet *„alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als „bestimmbar" wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind"*[37]. Daher gelten Name, Vorname, Fahrzeugkennzeichen, Telefonnummer, Passnummer, IP-Adresse oder jede andere eindeutige Kennung als personenbezogene Daten[38].
    - Werden personenbezogene Daten verarbeitet, beschreiben Sie:
        - die mit der Maßnahme verfolgte dem Gemeinwohl dienende Zielsetzung;
        - den genauen Zweck der Verarbeitung personenbezogener Daten, dessen Erläuterung detaillierter sein sollte als die der Zielsetzung;
        - die Datenkategorien;
        - die Personen, deren Daten verarbeitet werden (z. B. Passagiere, Arbeitnehmer, Migranten);

- wer die Daten verarbeitet und wer Zugriff auf sie hat (z. B. ein Privatunternehmen, eine öffentliche Organisation);
- welche Verarbeitungsvorgänge vorgesehen sind (z. B. Erhebung, Speicherung, Abruf, Übermittlung);
- alle anderen relevanten Bestimmungen wie die Dauer der Verarbeitung.

Sachdienliche Beispiele

BEISPIEL 1: EDSB, Beitrag *zu der von der Kommission abgehaltenen öffentlichen Konsultation (siehe Rat der Europäischen Union, Dok. 6370/13) zu der Änderung des Vorschlags der Kommission KOM (2011) 628 endgültig/2 für eine Verordnung des Europäischen Parlaments und des Rates über die Finanzierung, die Verwaltung und das Kontrollsystem der Gemeinsamen Agrarpolitik* (Vorschriften angenommen, um in Einklang mit dem Urteil in der Rechtssache *Schecke* betreffend die Veröffentlichung personenbezogener Daten von Begünstigten im Rahmen der Gemeinsamen Agrarpolitik zu stehen - nunmehr Verordnung 1306/2013, insbesondere Artikel 111 - 113 und Erwägungsgründe 73 - 87)

„Der EDSB weist darauf hin, dass für eine Beurteilung der Einhaltung der Anforderungen des Schutzes der Privatsphäre und des Datenschutzes ein klarer und genau definierter Zweck zwingend erforderlich ist, dem die geplante Maßnahmen dienen soll. .. In seinen Ausführungen zum Kontrollziel führte der Vertreter des EDSB aus, die Kommission solle daher klar zum Ausdruck bringen, ob zum Ziel der Maßnahme auch gehöre, eine gewisse Form der öffentlichen Kontrolle über die Ausgabe von EU-Geldern durch die Empfänger zu erlauben, womit die Offenlegung der Identität der Empfänger unerlässlich würde. Sollte es bei der Zielsetzung jedoch nur um die öffentliche Kontrolle über die EU-Einrichtungen und darum gehen, wie der EU-Haushalt ausgegeben wird, liegt weniger auf der Hand, dass die Öffentlichkeit die Identität der Empfänger erfahren sollte...".

Schritt 2: Ermittlung der Grundrechte und Grundfreiheiten, die durch die Verarbeitung personenbezogener Daten eingeschränkt werden

Erläuterung

- ✓ Ist in der Maßnahme die Verarbeitung personenbezogener Daten vorgesehen, stellt die Maßnahme eine Einschränkung des Rechts auf Schutz personenbezogener Daten gemäß Artikel 52 Absatz 1 der Charta dar.
- ✓ Je nach der Art der Daten und der Art ihrer Verwendung kann die vorgeschlagene Maßnahme auch das Recht auf Achtung des Privatlebens (auch als Recht auf Privatsphäre bezeichnet) einschränken (siehe Abschnitt II.5).
- ✓ Diesbezüglich heißt es in der ständigen Rechtsprechung der EuGH, dass „es für die Feststellung eines Eingriffs in das Grundrecht auf Achtung des Privatlebens **nicht darauf ankommt, ob die Informationen sensibel sind oder ob die Betroffenen irgendwelche Nachteile erlitten haben"**[39].
- ✓ Des Weiteren hat der EGMR wiederholt festgestellt, dass die **Speicherung durch eine Behörde von Daten**, die mit dem Privatleben einer Person zu tun haben,

einer Einschränkung des Rechts auf Achtung ihres Privatlebens gleichkommt[40], und dies unabhängig von der Verwendung der Daten[41].

- ✓ Unterschiedliche Verarbeitungsvorgänge oder eine Reihe von Verarbeitungsvorgängen (also Erhebung und ein weiterer Vorgang, wie Speicherung oder Übermittlung oder Abruf von Daten) können eigenständige Einschränkungen des Rechts auf den Schutz personenbezogener Daten und gegebenenfalls des Rechts auf Achtung des Privatlebens darstellen. So befand der EuGH beispielsweise Folgendes: Beinhaltet die Maßnahme den **Zugriff der zuständigen einzelstaatlichen Behörden** auf die verarbeiteten Daten, bedeutet dieser Zugriff einen weiteren Eingriff in das Grundrecht auf Achtung des Privatlebens[42].

- ✓ Wird dem Betroffenen die Gelegenheit verweigert, den gespeicherten und abgerufenen Daten zu widersprechen (also das Recht auf Auskunft über die Daten und auf deren Berichtigung), kommt dies ebenfalls einer Einschränkung seines Rechts auf Achtung des Privatlebens gleich[43].

Es können noch andere Rechte und Freiheiten durch die vorgeschlagene Maßnahme **beeinträchtigt werden,** worauf im Folgenden eingegangen wird. Beeinträchtigt werden können beispielsweise das Recht auf einen wirksamen Rechtsbehelf bei Gericht[44], das Recht auf Nichtdiskriminierung[45] oder das Recht auf freie Meinungsäußerung[46].

- ✓ Gemäß Artikel 52 Absatz 1 der Charta **sollte** der **„Wesensgehalt" des Rechts geachtet werden** (siehe Abschnitt II.1). Das bedeutet, dass die Einschränkung nicht so weit gehen darf, dass das Recht seiner Kernbestandteile beraubt wird und damit die Ausübung des Rechts verhindert wird.

Vorgehensweise

- ✓ **Beantworten Sie die Frage, ob die vorgeschlagene Maßnahme in irgendeiner Weise die Verwendung personenbezogener Daten vorsieht. Wenn dem so ist, beschreiben Sie:**
  - Welche Art von Verarbeitung ist geplant (z. B. Erhebung, Speicherung, Weitergabe, Übermittlung usw.)?
  - Wer verarbeitet die Daten (z. B. private Stellen, öffentliche Stellen, Organisationen, zuständige Behörden, bestimmte natürliche Personen usw.)?
  - Wer hat Zugriff auf sie?
  - Wie lange werden die Daten gespeichert?[47]
  - Die Umstände, unter denen die personenbezogenen Informationen verwendet werden (z. B. systematisch, nur in bestimmten Fällen, während eines bestimmten Zeitraums usw.).

- Auf wen beziehen sich die Daten (z. B. bestimmte Personenkategorien, Nutzer eines Dienstes, einer Straftat verdächtigte Personen, Ausländer, Inländer usw.)?

✓ **Ermitteln Sie, welche Grundrechte und Grundfreiheiten eingeschränkt werden**

- Prüfen Sie, inwieweit die Datenverarbeitung das Recht auf Achtung des Privatlebens einschränkt;
- ermitteln Sie, ob möglicherweise Personen „unterschiedlich behandelt" werden und es so zu Diskriminierung kommen könnte;
- bewerten Sie die Konsequenzen für die Möglichkeit für Personen, wirksame Rechtsbehelfe bei Gericht einzulegen;
- bewerten Sie, inwieweit Rede- und Gedankenfreiheit und die Freiheit, Informationen zu erhalten, eingeschränkt werden;
- bewerten Sie, ob der Wesensgehalt des Rechts beeinträchtigt wird.

Ergebnis

✓ **Wird ein Recht eingeschränkt**, bedeutet dies für sich genommen noch nicht, dass die Maßnahme nicht vorgeschlagen werden sollte. Allerdings sollte die Maßnahme die in Artikel 52 Absatz 1 der Charta niedergelegten Bedingungen einschließlich der Erforderlichkeit erfüllen.

✓ Wird der **Wesensgehalt des Rechts** durch die Maßnahme beeinträchtigt, ist die Einschränkung nicht rechtmäßig und sollte die Maßnahme zurückgezogen oder vor Einleitung der nächsten Schritte abgeändert werden (siehe Abschnitt I.1).

Sachdienliche Beispiele

BEISPIEL 2: *Huber* (EuGH, Rechtssache C-524/06)

Der Gerichtshof befasste sich mit der Rechtmäßigkeit einer von den deutschen Behörden eingerichteten Datenbank, die personenbezogene Daten über Drittstaatsangehörige und andere EU-Bürger enthielt, die nicht die deutsche Staatsangehörigkeit haben. Der Gerichtshof befand unter anderem, dass das Recht auf Nichtdiskriminierung aufgrund der Staatsangehörigkeit innerhalb der EU *„dahin auszulegen ist, dass es einem Mitgliedstaat verwehrt, zur Bekämpfung der Kriminalität ein System zur Verarbeitung personenbezogener Daten zu errichten, das nur Unionsbürger erfasst, die keine Staatsangehörigen dieses Mitgliedstaats sind"* (Rn. 81). Bevor er zu dieser Schlussfolgerung kam, trug der Gerichtshof der Tatsache Rechnung, dass *„sich die Kriminalitätsbekämpfung ... zwingend auf die Verfolgung von Verbrechen und Vergehen unabhängig von der Staatsangehörigkeit der Täter bezieht"* (Rn. 78). *„Folglich kann für einen Mitgliedstaat die Situation seiner Staatsangehörigen im Hinblick auf das Ziel der Bekämpfung der Kriminalität nicht anders sein als die der Unionsbürger, die keine Staatsangehörigen dieses Mitgliedstaats sind und sich in seinem Hoheitsgebiet aufhalten"* (Rn. 79).

BEISPIEL 3: EDSB, Stellungnahme 3/2016 *zum Austausch von Informationen über Drittstaatsangehörige mit Hilfe des Europäischen Strafregisterinformationssystems (ECRIS)*, 13. April 2016

Mit dem Legislativvorschlag soll ein besonderes System für den Austausch von Informationen zwischen den Mitgliedstaaten über strafrechtliche Verurteilungen von Drittstaatsangehörigen eingerichtet werden, das auch Daten über EU-Bürger enthalten würde, die die Staatsangehörigkeit eines Drittlandes besitzen. Sie würden daher anders als die EU-Bürger behandelt, die nicht die Staatsangehörigkeit eines Drittlandes besitzen. Der EDSB stellte fest: *„Die im Vorschlag vorgesehene unterschiedliche Behandlung dürfte für das Erreichen des verfolgten Zwecks nicht erforderlich sein, wenn man berücksichtigt, dass im Falle von EU-Bürgern die bestehenden ECRIS-Verfahren angewandt werden können, damit Behörden Informationen austauschen können“* und: *„Diese Ungleichbehandlung kann zu Diskriminierung führen, die wiederum ein Verstoß gegen Artikel 21 Absatz 1 der EU-Charta wäre“* (Punkt 33).

BEISPIEL 4: *Rechnungshof* (EuGH, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01)

Der Gerichtshof befand: *„Zwar kann die bloße Speicherung personenbezogener Daten über die an das Personal gezahlten Gehälter durch einen Arbeitgeber als solche keinen Eingriff in die Privatsphäre begründen“*. Dann heißt es allerdings: *„... doch stellt die Weitergabe dieser Daten an einen Dritten - im vorliegenden Fall eine Behörde - ... eine Beeinträchtigung des Rechts der Betroffenen auf Achtung ihres Privatlebens ... dar“* (Rn. 74).

BEISPIEL 5: *Schecke* (EuGH, verbundene Rechtssachen C-92/09 und C-93/09)

Die Veröffentlichung im Internet der Namen von Empfängern und der Beträge öffentlicher Gelder, die sie erhalten haben, stellt einen Eingriff in ihr Privatleben im Sinne von Artikel 7 der Charta dar (Rn. 58).

BEISPIEL 6: *Digital Rights Ireland*, (EuGH, verbundene Rechtssachen C-293/12 und C-594/12)

In der Rechtssache, in der es um die Richtlinie über die Vorratsdatenspeicherung ging, befand der Gerichtshof, dass die Verpflichtung für Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsdienste Kommunikationsdaten wie die Telefonnummer des Anrufenden und des Angerufenen, die E-Mail-Adressen, die für den Internetzugang verwendeten IP-Adressen für einen Zeitraum zwischen sechs Monaten und zwei Jahren zu speichern, *„als solche einen Eingriff in die durch Artikel 7 der Charta garantierten Rechte darstellt“* (Rn. 34). *„Zudem stellt der Zugang der zuständigen nationalen Behörden zu den Daten einen zusätzlichen Eingriff in dieses Grundrecht dar“* (Rn. 35). Der Gerichtshof stellte ferner fest: „Desgleichen greift die Richtlinie 2006/24 in das durch Artikel 8 der Charta garantierte Grundrecht auf den Schutz personenbezogener Daten ein, da sie eine Verarbeitung personenbezogener Daten vorsieht“ (Rn. 36).

Schritt 3: Legen Sie die Ziele der Maßnahme fest

Erläuterung

- ✓ Gemäß Artikel 52 Absatz 1 der Charta **muss** die Maßnahme
  - **einer von der Union anerkannten dem Gemeinwohl dienenden Zielsetzung oder**
  - **den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.**
- ✓ Zu den **dem Gemeinwohl dienenden Zielsetzungen der Union** gehören beispielsweise die in Artikel 3 und Artikel 4 Absatz 2 EUV erwähnten Zielsetzungen und andere Interessen, die durch spezifische Bestimmungen in den Verträgen[48] geschützt und in der Rechtsprechung des Gerichtshofs ausgelegt werden.
  - Artikel 23 der Datenschutz-Grundverordnung 2016/679 enthält eine Auflistung von Zielen, aufgrund derer legitimerweise die Rechte natürlicher Personen, wie z. B. das Recht auf Auskunft über die eigenen personenbezogene Daten, und die Pflichten des Verantwortlichen eingeschränkt werden können.
  - Transparenz und öffentliche Kontrolle sind ebenfalls legitime Ziele (Artikel 1 und Artikel 15 Absatz 1 EUV), die eine bessere Beteiligung am Entscheidungsprozess ermöglichen[49].
- ✓ Die **Rechte anderer** sind zunächst einmal die in der Charta niedergelegten.
  - Das Recht auf Schutz personenbezogener Daten muss möglicherweise gegen andere Rechte abgewogen werden, darunter das Recht auf Schutz des geistigen Eigentums und das Recht auf einen wirksamen Rechtsbehelf, auf Meinungsfreiheit und auf unternehmerische Tätigkeit[50].
- ✓ Die Beschreibung der Maßnahme ist zwar von der Prüfung der Erforderlichkeit getrennt, doch ist sie Voraussetzung für deren Beurteilung, da die Erforderlichkeit anhand des/der angestrebten Ziels/Ziele zu bewerten ist.
  - Es ist das **Problem** zu spezifizieren, **das mit der Maßnahme gelöst werden soll**, also der Zweck der Verarbeitung personenbezogener Daten. Dies ist noch wichtiger, wenn eine dem Gemeinwohl dienende Zielsetzung möglicherweise verschiedene Aspekte umfasst oder eine Maßnahme sich mit mehreren dem Gemeinwohl dienenden Zielsetzungen befassen sollte. So kann beispielsweise das Ziel der Wahrung der öffentlichen Sicherheit dahingehend gedeutet werden, dass es die innere und die äußere Sicherheit gleichermaßen umfasst[51], weshalb in einer Maßnahme klar darzulegen ist, ob es dort entweder um die innere oder die äußere Sicherheit oder um beide Aspekte geht.
- ✓ Das zu lösende Problem sollte real und nicht rein hypothetischer Natur sein. Daher sollten **objektive Belege für das Problem** vorgelegt werden. Bei diesen Belegen sollte es sich um Fakten oder statistische Daten handeln, und sie sollten eine

wissenschaftliche Überprüfung erlauben und die Existenz des Problems überzeugend nachweisen.

- ✓ Für den EGMR gilt eine Einschränkung für einen legitimen Zweck als **„in einer demokratischen Gesellschaft erforderlich", „wenn sie einem zwingenden gesellschaftlichen Bedürfnis entspricht".** Das zu lösende Problem muss nicht nur real, bereits vorhanden oder unmittelbar bevorstehend, sondern auch von zentraler Bedeutung für das Funktionieren der Gesellschaft sein.

- ✓ Wird mit einer Maßnahme mehr als eine Zielsetzung verfolgt, ist jede von ihnen zu begründen[52].

Vorgehensweise

- ✓ **Stellen Sie fest, ob die mit der Maßnahme verfolgte Zielsetzung legitim ist und bewerten Sie diese Legitimität:**
    - Stellen Sie sicher, dass das Problem hinreichend und klar beschrieben wird;
    - fügen Sie als Nachweis der Existenz des Problems ausreichende und wissenschaftlich nachprüfbare Belege bei;
    - definieren Sie genau die dem Gemeinwohl dienende Zielsetzung oder das Recht anderer, um die/das es in der Maßnahme geht;
    - sorgen Sie dafür, dass der Zweck der Verarbeitung personenbezogener Daten tatsächlich darauf abhebt, einer von der Union anerkannten dem Gemeinwohl dienenden Zielsetzung oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer zu entsprechen;
    - erläutern Sie die Bedeutung der zu erreichenden Zielsetzung und inwiefern sie für das Funktionieren der Gesellschaft von zentraler Bedeutung ist.

Ergebnis

- ✓ **Ist das zu lösende Problem nicht hinreichend beschrieben**, sollte es besser erläutert und dargestellt werden. Andernfalls ist eine Beurteilung der Erforderlichkeit der Maßnahme nicht möglich.

- ✓ **Liegen für das Problem keine ausreichenden Belege vor**, sollte nach weiteren Belegen gesucht werden.

- ✓ **Entspricht die Maßnahme nicht tatsächlich einer von der Union anerkannten dem Gemeinwohl dienenden Zielsetzung oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer**, sollte die Maßnahme nicht vorgeschlagen werden.

- ✓ **Entspricht die Maßnahme einer solchen Zielsetzung** und wird dies hinreichend durch einschlägige Nachweise belegt, kann als nächstes die Erforderlichkeit der Maßnahme im Einklang mit Schritt 4 beurteilt werden.

Sachdienliche Beispiele

BEISPIEL 7: *Digital Rights Ireland* (EuGH, verbundene Rechtssachen C-293/12 und C-594/12)

Bei der Prüfung der Rechtmäßigkeit der Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24) berücksichtigte der EuGH die Schlussfolgerungen des Rates „Justiz und Inneres" vom 19. Dezember 2002, denen zufolge die beträchtliche Zunahme der Möglichkeiten bei der elektronischen Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig sind und daher ein wertvolles Mittel bei der Verhütung von Straftaten und der Bekämpfung der Kriminalität, insbesondere der organisierten Kriminalität, darstellen (Rn. 43). Der EuGH stellte ferner fest, dass seiner Rechtsprechung nach die Bekämpfung des internationalen Terrorismus zur Wahrung des Weltfriedens und der internationalen Sicherheit eine dem Gemeinwohl dienende Zielsetzung darstellt. Das Gleiche gilt für die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit (Rn. 42). Daher stellte der Gerichtshof fest, dass *„die durch die Richtlinie 2006/24 vorgeschriebene Vorratsdatenspeicherung von Daten zu dem Zweck, sie gegebenenfalls den zuständigen nationalen Behörden zugänglich machen zu können, eine dem Gemeinwohl dienende Zielsetzung darstellt"* (Rn. 44).

BEISPIEL 8: *Promusicae* (EuGH, Rechtssache C-275/06)

Nach Auffassung des EuGH ist der Schutz des Rechts auf geistiges Eigentum eine legitime Zielsetzung für die Verarbeitung von Kommunikationsdaten (IP-Adressen). und er verweist hier auf Artikel 13 der Richtlinie 95/46/EG, in dem die legitimen Ziele von Einschränkungen des Rechts auf Achtung vor dem Privatleben bei der Verarbeitung personenbezogener Daten geregelt sind (Rn. 26).

BEISPIEL 9: EDSB, Stellungnahme vom 9. Oktober 2012 *zur Änderung des Vorschlags der Kommission KOM (2011) 628 endgültig/2 für eine Verordnung des Europäischen Parlaments und des Rates über die Finanzierung, die Verwaltung und das Kontrollsystem der Gemeinsamen Agrarpolitik* (Vorschriften angenommen, um in Einklang mit dem Urteil in der Rechtssache Schecke betreffend die Veröffentlichung personenbezogener Daten von Begünstigten im Rahmen der Gemeinsamen Agrarpolitik zu stehen - nunmehr Verordnung 1306/2013, insbesondere Artikel 111 - 113 und Erwägungsgründe 73 - 87)

Zwar räumt der EDSB ein, dass Transparenz und öffentliche Kontrolle dem Gemeinwohl dienende Zielsetzungen sind, wie es auch in dem Urteil *Schecke* heißt (Rn. 65, 68, 69, 75), er ist jedoch der Auffassung, dass die Verringerung von Kontrollen und Vor-Ort-Kontrollen durch die Behörden aufgrund wirtschaftlicher Zwänge nicht unter die genannte Zielsetzung fallen: *„Transparenz und öffentliche Kontrolle sind für sich genommen legitime Ziele und können nicht als Ersatz für konkrete Kontrollen und Vor-Ort-Kontrollen durch zuständige Behörden dargestellt werden. ..."* (Punkt 17).

BEISPIEL 10: EDSB, Stellungnahme 3/2016 *zum Austausch von Informationen über Drittstaatsangehörige mit Hilfe des Europäischen Strafregisterinformationssystems (ECRIS)*

Nach Ansicht des EDSB ist der ECRIS-Vorschlag der Kommission für einen leichteren Zugriff auf strafrechtliche Verurteilungen von Drittstaatsangehörigen dem Bereich der Bekämpfung von Terrorismus und der Bekämpfung schwerer Kriminalität zur Aufrechterhaltung der öffentlichen

Sicherheit als einer im EU-Recht anerkannten dem Gemeinwohl dienenden Zielsetzung zuzuordnen. *„Die vorgeschlagenen Maßnahmen dienen somit einem dem Gemeinwohl dienenden Ziel und lassen sich vorbehaltlich der Wahrung des Grundsatzes der Verhältnismäßigkeit rechtfertigen“* (Punkt 9).

Schritt 4: Wahl der Option, die wirksam ist und den geringsten Eingriff in die Privatsphäre bedeutet

In Abschnitt II.2 haben wir festgehalten, dass ein Unterschied zwischen der *Angemessenheit* und der *Wirksamkeit* einer Maßnahme besteht. Auch wenn die gewählte Maßnahme angemessen ist, sollte sie doch auch wirksam sein und die Privatsphäre weniger verletzen als andere Optionen, die für das Erreichen desselben Ziel bestehen.

Eine Maßnahme, die angemessen ist, ist in der Lage, das angestrebte Ziel zu erreichen:

- Es muss **eine logische Verbindung zwischen der Einschränkung und** den ermittelten legitimen Zielen bestehen;
- das angestrebte Ziel muss als unmittelbare Folge der Maßnahme erreicht werden;
- eine angemessene Maßnahme muss sich jedoch nicht mit allen Einzelaspekten des Problems befassen[53].

Erläuterungen zu Wirksamkeit und Grad des Eindringens in die Privatsphäre

- ✓ **Die Maßnahme sollte tatsächlich wirksam sein**, also für das Erreichen der dem Gemeinwohl dienenden Zielsetzung wesentlich sein.
  - Nicht alles, was „sich für einen bestimmten Zweck als nützlich erweisen könnte“, ist „wünschenswert oder kann als in einer demokratischen Gesellschaft notwendig angesehen werden“[54]. Nur Bequemlichkeit oder Kosteneinsparung[55] reichen nicht aus.
  - Die ausgewählten Kategorien betroffener Personen, die Kategorien erhobener und verarbeiteter personenbezogener Daten, die Speicherfrist für die Daten usw. sollten einen wirksamen Beitrag zum Erreichen des angestrebten Ziels leisten.
  - Sieht die vorgeschlagene Maßnahme auch die Verarbeitung **sensibler Daten** vor, sollte bei der Beurteilung der Wirksamkeit die Messlatte höher angelegt werden.
    - Zu sensiblen Daten gehören unter anderem Daten, die Auskunft geben über ethnische oder rassische Herkunft, politische Meinungen, religiöse oder ähnliche Überzeugungen, Gesundheitszustand. Einen ähnlichen Status haben Daten über strafrechtliche Verurteilungen und Straftaten[56]. Genetische und biometrische Daten werden in den neuen Rechtsakten über den Schutz personenbezogener Daten als sensible Daten anerkannt[57].

Auf die „Sensibilität“ solcher Daten hat allerdings die Artikel 29-Datenschutzgruppe schon wiederholt hingewiesen[58].

- Bei anderen Datenkategorien, die zwar nicht als sensibel im engeren Sinne eingestuft sind, kann sich in bestimmten Zusammenhängen ein größeres Risiko für die betroffene Person ergeben und die Anwendung einer höheren Schwelle als unbedingt erforderlich auslösen. Dies trifft beispielsweise auf eindeutige Kennungen wie nationale Kennziffern oder Finanzdaten zu.

✓ Die geplante Maßnahme sollte sich **möglichst wenig auf die fraglichen Rechte auswirken.**

- Es sollte nach Alternativmaßnahmen gesucht werden, die weniger schwerwiegend in das Recht auf Schutz personenbezogener Daten und das Recht auf Achtung des Privatlebens eingreifen.
- Als Alternative kommt auch eine Kombination von Maßnahmen in Frage.
- Alternativen sollten real und im Hinblick auf das zu lösende Problem hinreichend und vergleichbar wirksam sein[59].
- Wird eine Einschränkung nur für einen Teil der Bevölkerung/des geografischen Gebiets verhängt, ist dies ein weniger schwerer Eingriff als eine Einschränkung, die für die gesamte Bevölkerung/das ganze geografische Gebiet gilt; eine kurzfristige Einschränkung ist weniger schwerwiegend als eine langfristige; die Verarbeitung einer Datenkategorie ist im Allgemeinen ein geringerer Eingriff als die Verarbeitung mehrerer Datenkategorien[60].
- Einsparungen bei den Ressourcen sollten sich auf die Alternativmaßnahmen nicht auswirken; dieser Aspekt ist bei der Prüfung der Verhältnismäßigkeit zu analysieren, weil er ein Abwägen mit anderen konkurrierenden dem Gemeinwohl dienenden Zielsetzungen verlangt (siehe Abschnitt II.2).

✓ **Jeder einzelne Aspekt** der Maßnahme ist einer strengen Prüfung der Erforderlichkeit zu unterziehen.

- Dabei können sich manche spezifische Bestimmungen, betreffend beispielsweise die Verarbeitung einer Kategorie personenbezogener Daten, die Kategorien betroffener Personen, die Speicherfrist für die Daten, als erforderlich herausstellen, andere hingegen nicht. Voraussetzung für die Beurteilung einer Maßnahme sind „klare und präzise Regeln für die Tragweite und die Anwendung einer Maßnahme“[61]. Wie schon in Abschnitt II.1 erwähnt, sind klare und präzise Regeln auch wichtig, damit den meisten der anderen Kriterien in Artikel 52 Absatz1 der Charta Genüge getan wird.
- Sieht eine Maßnahme den Zugriff von Behörden auf die Daten vor, müssen in der Maßnahme **objektive Kriterien** niedergelegt sein, die insbesondere

die Zahl der zum Zugriff auf die Daten befugten Personen und die Verwendung der Daten auf das absolut Notwendige beschränken[62].

- Die Maßnahme sollte **differenzieren**, **einschränken** und **Ausnahmen vorsehen** bei den Personen, deren Daten mit Blick auf das angestrebte Ziel verwendet werden[63].

- Bei der Festlegung einer **Speicherfrist** für die Daten sollte die Maßnahme **zwischen den Datenkategorien** nach Maßgabe ihres **etwaigen Nutzens** für das verfolgte Ziel eine **Unterscheidung treffen** und muss sie objektive Kriterien für die Festlegung der Speicherfrist heranziehen[64].

- Die Einschränkung des **Rechts auf Information** über die Verarbeitung personenbezogener Daten sollte ebenfalls für den von der vorgeschlagenen Maßnahme verfolgten Zweck notwendig sein. So kann beispielsweise der Zweck geheimer Überwachungsmaßnahmen die Einschränkung der Unterrichtung der betroffenen Personen rechtfertigen. *„Sobald Informationen gegeben werden können, ohne dass der Zweck der Maßnahme nach Beendigung der Überwachungsmaßnahme gefährdet wird, sollten die betroffenen Personen jedoch in Kenntnis gesetzt werden."*[65]

✓ In der Maßnahme sollte detailliert auf die **Gründe** eingegangen werden, **aus denen ein Tätigwerden erforderlich ist**; dabei sollte Folgendes erläutert werden:

- Warum sind bestehende Maßnahmen für eine Lösung des Problems nicht ausreichend?

- Warum sind alternative, weniger in die Privatsphäre eingreifende Maßnahmen für eine Lösung des Problems nicht ausreichend?

- Warum kann die vorgeschlagene Maßnahme das **Problem wirksamer als andere** lösen?

- Zu allen diesen Aspekten sollten objektive Belege vorgelegt werden, darunter Fakten oder statistische Daten, die einer wissenschaftlichen Überprüfung Stand halten und die vorgeschlagene Maßnahme überzeugend unterstützen.

- Die Prüfung der Erforderlichkeit muss nicht für jeden einzelnen Mitgliedstaat vorgenommen werden, auch wenn sie für die Folgenabschätzung von Belang ist, die sich mit dem Mehrwert eines Tätigwerdens der EU befasst[66].

Vorgehensweise

✓ **Beschreiben Sie, wie und warum die Maßnahme für die Deckung des entstandenen Bedarfs wesentlich ist:**

- Warum sind bestehende Maßnahmen für eine Lösung des Problems nicht ausreichend?

- Warum und wie kann die Maßnahme das Ziel erreichen?

- ✓ **Prüfen Sie, ob alternative, weniger in die Privatsphäre eingreifende Maßnahmen beim Erreichen des verfolgten Ziels vergleichbar wirksam sein könnten.**

- ✓ Legen Sie wissenschaftlich überprüfbare Belege vor, die wirklich die Behauptung stützen können, dass bestehende Maßnahmen und weniger in die Privatsphäre eingreifende Alternativmaßnahmen das Problem nicht wirksam lösen können.

Ergebnis

- ✓ **Erwägen Sie die korrekte Umsetzung bestehender Maßnahmen an Stelle neuer in die Privatsphäre eingreifender Maßnahmen.**

- ✓ **Erwägen Sie eine Alternativmaßnahme, deren Wirksamkeit vergleichbar ist, die aber geringere Auswirkungen auf den Schutz personenbezogener Daten oder das Recht auf Achtung des Privatlebens hat.** Der Aspekt höherer Kosten kann bei der Prüfung der Verhältnismäßigkeit betrachtet werden.

- ✓ **Nur wenn** nach einer evidenzgestützten Analyse **keine bestehenden oder weniger in die Privatsphäre eingreifenden Maßnahmen zur Verfügung stehen**, und nur wenn eine solche Analyse erbringt, dass die geplante Maßnahme für das Erreichen der dem Gemeinwohl dienenden Zielsetzung **wesentlich und auf das absolut Notwendige beschränkt** ist, sollte diese Maßnahme auf ihre Verhältnismäßigkeit geprüft werden (siehe Abschnitt II.2).

Sachdienliche Beispiele

BEISPIEL 11: *Österreichischer Rundfunk u. a.* (EuGH, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01)

In Beantwortung der Frage, ob eine weitreichende Veröffentlichung von Namen zusammen mit den Bezügen von Arbeitnehmern verschiedener vom Rechnungshof kontrollierter Rechtsträger mit dem Recht auf Privatleben vereinbar ist, forderte der EuGH die nationalen Gerichte auf, zu untersuchen, ob der mit einer solchen weitreichenden Veröffentlichung verfolgte Zweck *„nicht ebenso wirksam erreicht werden könnte, wenn die personenbezogenen Daten nur den Kontrollorganen zugänglich gemacht würden“* (Rn. 88).

BEISPIEL 12: *Schecke* (EuGH, verbundene Rechtssachen C-92/09 und C-93/09)

Bei der Prüfung der Notwendigkeit der Veröffentlichung der personenbezogenen Daten aller Empfänger öffentlicher Gelder wies der Gerichtshof darauf hin, dass der Gesetzgeber keine alternativen, weniger in die Privatsphäre eindringenden Maßnahmen berücksichtigt hat, wie die Beschränkung der Veröffentlichung auf die Empfänger, die in bestimmten Zeiträumen Beihilfen erhalten haben, oder auf die Häufigkeit oder die Art und den Umfang der erhaltenen Beihilfen. Des Weiteren unterstrich der Gerichtshof, dass sich ein geringerer Eingriff in die Privatsphäre auch mit einer Kombination dieser Maßnahmen erreichen lässt: *„Mit einer in dieser Weise beschränkten namentlichen Veröffentlichung könnten gegebenenfalls einschlägige Erläuterungen in Bezug auf die übrigen natürlichen Personen, die Empfänger von Mitteln aus diesen Fonds sind, und auf die daraus erhaltenen Beträge einhergehen“.* Der Gerichtshof befand: *„In Anbetracht der*

Tatsache, dass sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten auf das absolut Notwendige beschränken müssen (Urteil Satakunnan Markkinapörssi und Satamedia, Rn. 56) und dass Maßnahmen vorstellbar sind, die dieses Grundrecht der natürlichen Personen weniger stark beeinträchtigen, den Zielen der in Rede stehenden Unionsrechtsvorschriften aber ebenso in wirksamer Weise dienen, ...“. (Rn. 81, 82, 83, 86).

BEISPIEL 13: *Tele2 Sverige AB* (EuGH, verbundene Rechtssachen C-203/15 und C-698/15)

In seinen Schlussanträgen führte der Generalanwalt erneut aus: *„In Anbetracht des Erfordernisses des absolut Notwendigen ist es unerlässlich, dass die Gerichte sich nicht mit der Prüfung des bloßen Nutzens einer generellen Verpflichtung zur Vorratsspeicherung begnügen, sondern genau untersuchen, ob eine andere Maßnahme oder eine Kombination von Maßnahmen, insbesondere aber eine gezielte Vorratsspeicherungspflicht, mit der andere Ermittlungsinstrumente einhergehen, bei der Bekämpfung schwerer Kriminalität nicht dieselbe Wirksamkeit aufweisen. Ich weise insoweit darauf hin, dass eine Reihe von Studien, die dem Gerichtshof vorgelegt worden sind, die Erforderlichkeit dieser Art von Verpflichtung zur Bekämpfung schwerer Kriminalität in Frage stellen.“* Solche anderen Maßnahmen sollten im Hinblick auf das verfolgte Ziel wirksam sein. „Diese *Verpflichtung kann nämlich je nach den von ihr erfassten Nutzern, geografischen Gebieten und Kommunikationsmitteln einen mehr oder weniger weiten materiellen Umfang haben.“* (Rn. 209, 211).

Der EuGH befand, eine gezielte Speicherung könne unter der Voraussetzung gerechtfertigt sein, dass die Speicherung auf das für das Ziel der Bekämpfung schwerer Kriminalität unbedingt Erforderliche beschränkt ist: *„...die zur Bekämpfung schwerer Straftaten vorgenommene gezielte Vorratsspeicherung von Verkehrs- und Standortdaten [sollte] hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt sein.“* Und weiter: *„...muss sich die nationale Regelung auf objektive Anknüpfungspunkte stützen, die es ermöglichen, Personenkreise zu erfassen, deren Daten geeignet sind, einen zumindest mittelbaren Zusammenhang mit schweren Straftaten sichtbar zu machen, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Begrenzung lässt sich durch ein geografisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht, dass solche Taten vorbereitet oder begangen werden.“* Nach Auffassung des Gerichtshofs muss sich der Zugriff zuständiger Behörden auf diese Daten auf objektive Kriterien stützen; in der Regel sollte er nur für Daten Verdächtiger gelten. Ausnahmsweise könnte in Situationen *„... wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt wird, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten können.“* (Rn. 102, 103, 108, 111, 115, 119).

BEISPIEL 14: Gutachten 1/15 des Generalanwalts (Gutachtenantrag des Europäischen Parlaments) *zu dem Entwurf eines Abkommens zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen*

Zu der unbedingten Erforderlichkeit der Maßnahme unterstrich der Generalanwalt: Die Bestimmungen des Entwurfs des PNR-Abkommens *„müssen zudem solche Maßnahmen vorsehen,*

die am wenigsten in die durch die Artikel 7 und 8 der Charta gewährten Rechte eingreifen, und trotzdem zu dem von dem geplanten Abkommen verfolgten Ziel der öffentlichen Sicherheit wirksam beitragen. ... Diese Alternativmaßnahmen müssen auch hinreichend wirksam sein, d. h., sie müssen ... ebenso wirksam sein wie die vom geplanten Abkommen zur Erreichung des von ihm verfolgten Ziels der öffentlichen Sicherheit vorgesehenen Maßnahmen." Mit Blick auf diese Prüfung der Erforderlichkeit geht der Generalanwalt auf verschiedene Aspekte der Maßnahme ein, wie z. B.: *„... die Kategorien von Daten im Anhang des geplanten Abkommens ... müssten prägnanter und präziser abgefasst werden und sollten den Fluggesellschaften oder den zuständigen kanadischen Behörden hinsichtlich der konkreten Tragweite dieser Kategorien keinen Ermessensspielraum lassen." „Dies lässt mangels besser untermauerter Erläuterungen im geplanten Abkommen zur unbedingten Erforderlichkeit der Verarbeitung sensibler Daten darauf schließen, dass das Ziel der Bekämpfung des Terrorismus und der grenzüberschreitenden schweren Kriminalität ebenso wirksam verwirklicht werden kann, ohne dass solche Daten nach Kanada übermittelt werden." „Um die Straftaten, bezüglich deren die Verarbeitung von PNR-Daten gestattet ist, auf das unbedingt Erforderliche zu beschränken, und um die Rechtssicherheit der Fluggäste, deren Daten an die kanadischen Behörden übermittelt werden, zu gewährleisten, bin ich jedoch der Ansicht, das die Straftaten... abschließend aufgeführt werden müssten...".* Zur Dauer der Speicherung führte der Generalanwalt aus: *„...gibt das geplante Abkommen die objektiven Gründe nicht an, die die Vertragsparteien veranlasst haben, die Dauer der Speicherung der PNR-Daten auf höchstens fünf Jahre zu verlängern."* (Rn. 208, 220, 222, 235, 261, 267).

BEISPIEL 15: Stellungnahme des EDSB *zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität*, 25. März 2011

Der EDSB stellte fest, die Folgenabschätzung für die vorgeschlagene Richtlinie enthalte ausführliche Erläuterungen und Statistiken zur Begründung der Maßnahme, diese Elemente seien jedoch nicht überzeugend. Zur Veranschaulichung werde in der Beschreibung der Bedrohung durch Terrorismus und schweres Verbrechen in der Folgenabschätzung und in der Begründung zum Vorschlag die Zahl von 14 000 Straftaten pro 100 000 Einwohner in den Mitgliedstaaten genannt. Diese Zahl wirke zwar beeindruckend, beziehe sich jedoch auf undifferenzierte Kategorien von Kriminalität und sei nicht geeignet zur Rechtfertigung eines Vorschlags, der nur auf begrenzte Kategorien schwerer, grenzüberschreitender Kriminalität und Terrorismus abziele. Als weiteres Beispiel werde ein Bericht über „Probleme" mit Drogen angeführt, ohne dass die Statistik mit dem im Vorschlag thematisierten Typ des Drogenhandels verknüpft sei; dies ist nach Ansicht des EDSB keine gültige Referenz (Punkt 11). Der EDSB kam zu dem Schluss, die Hintergrunddokumentation sei nicht so relevant und genau, als dass sie die Erforderlichkeit des Instruments belegen könne (Punkt 12).

BEISPIEL 16: Artikel 29-Datenschutzgruppe, Stellungnahme 7/2010 *zur Mitteilung der Europäischen Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer*, 12. November 2010

Bei ihrer Bewertung der Erforderlichkeit von Übermittlungen von PNR-Daten an Drittländer riet die Artikel 29-Datenschutzgruppe: Die Kommission sollte, bevor sie etwaige neue Abkommen abschließt, *„prüfen, ob von Drittländern gestellten Ersuchen um Übermittlung von PNR-Daten nicht bereits im Rahmen der bestehenden Systeme und Mechanismen nachgekommen werden könnte."* Die Arbeitsgruppe betonte ferner: *„Wegen der aus derartigen Beschlüssen resultierenden Eingriffe in die Privatsphäre sollten vor einer etwaigen Einführung eines solchen Systems alternative Optionen gründlich geprüft werden - und zwar weitgehend automatisch, auf der Grundlage der üblichen Muster und im Lichte der Schwierigkeiten des Einzelnen, derartige Beschlüsse anzufechten"* (S. 5).

BEISPIEL 17: EDSB, Stellungnahme 3/2016 *zum Austausch von Informationen über Drittstaatsangehörige mit Hilfe des Europäischen Strafregisterinformationssystems (ECRIS), 13. April 2016*

Der zu prüfende Legislativvorschlag sieht eine Verpflichtung für die Mitgliedstaaten vor, biometrische Daten (Fingerabdrücke) aller verurteilten Drittstaatsangehörigen in ECRIS einzugeben, und dies mit dem Argument, dies sei für Identifizierungszwecke erforderlich. Der EDSB forderte mehr Nachweise für die Notwendigkeit der Speicherung von Fingerabdrücken: *„Man kann also nicht davon ausgehen, dass es keine andere Möglichkeit der sicheren Identifizierung der Personen gibt als die Verwendung von Fingerabdrücken, weshalb die Notwendigkeit einer obligatorischen Verwendung von Fingerabdrücken bei Drittstaatsangehörigen im ECRIS noch nachzuweisen wäre"* (Punkt 15).

BEISPIEL 18: Stellungnahme 5/2015 des EDSB *zu dem Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen*

Der EDSB unterstreicht Folgendes: *„Nach den vorliegenden Informationen zeigen die aktuellen Fassungen des Vorschlags nicht, dass eine angemessene Beurteilung gemäß des EuGH-Urteils hinsichtlich verbleibender Lücken im Kampf gegen den Terrorismus und hinsichtlich der Möglichkeiten, diese mit den den Mitgliedstaaten derzeitig zur Verfügung stehenden Instrumenten zu klären, stattgefunden hat." Während in dieser Beurteilung auch neue Untersuchungsansätze genannt werden sollten, um der Polizei und den Justizbehörden eine effektivere Überwachung bekannter Verdächtiger zu ermöglichen, weisen zahlreiche Vorfälle, die in letzter Zeit in der EU stattgefunden haben, auf Lücken bei der polizeilichen Erkenntnisgewinnung hin, die nicht in Zusammenhang mit Flugreisenden stehen. Auch zeigt sich, dass ein gezielter Einsatz von Mitteln und verstärkte Bemühungen bei bekannten Verdächtigen in einigen Fällen effektiver sein können, als die standardmäßige Erstellung von Millionen von Passagierprofilen."* (Punkt 14).

BEISPIEL 19: Artikel 29-Datenschutzgruppe, Schreiben an den LIBE-Ausschuss zu *EU PNR*, 19. März 2015

Die Artikel 29-Datenschutzgruppe betonte, die Erforderlichkeit von EU-PNR solle nachgewiesen werden; unter anderem solle belegt werden, warum die bestehenden Instrumente (SIS, API) nicht ausreichen, warum mit weniger eingreifenden Alternativen der Zweck nicht erreicht würde, und inwiefern das EU-PNR, im Gegensatz zu weniger eingreifenden Maßnahmen, die zum Ziel führende Lösung sei. Die Erklärungen sollten gestützt werden durch Belege, möglicherweise Statistiken, und durch Studien der EU oder von Mitgliedstaaten.

BEISPIEL 20: EDSB, Stellungnahme 07/2016 zum ersten Reformpaket zur Überarbeitung des Gemeinsamen Europäischen Asylsystems (Eurodac-Verordnung, EASO-Verordnung und Dublin-Verordnung)

Der EDSB betonte, dass das Erfordernis der Hinzufügung einer zweiten Kategorie biometrischer Daten, nämlich von Gesichtsbildern, zu einer groß angelegten Datenbank auf einer *„Beurteilung"* beruhen sollte, *„bei der eine einheitliche Studie oder ein auf klaren Fakten gestützter Ansatz verwendet werden"*.
Mit Blick auf die Speicherfrist unterstrich der EDSB, dass eine Verlängerung der Speicherfrist auf fünf Jahre zur Angleichung an andere Instrumente *„insoweit irrelevant ist, als diese Rechtsakte unter Umständen andere Zwecke verfolgen und ihre Speicherfrist durch andere Elemente gerechtfertigt sein kann"*. In seiner Stellungnahme vertrat der EDSB die Ansicht, die Speicherfrist von fünf Jahren sei nicht ausreichend begründet worden, und er empfahl, weitere Belege zugunsten dieser Frist vorzulegen (Punkte 22, 30, 31).

Endnoten

[1] In Artikel 2 des Vertrags über die Europäische Union (EUV) heißt es: *„Die Werte, auf die sich die Union gründet, sind die Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und die Wahrung der Menschenrechte einschließlich der Rechte der Personen, die Minderheiten angehören"*. Ferner werden in Artikel 6 Absatz 1 EUV die Rechte, Freiheiten und Grundsätze anerkannt, die in der Charta der Grundrechte der Europäischen Union vom 7. Dezember 2000 in der am 12. Dezember 2007 in Straßburg angepassten Fassung niedergelegt sind, die den Verträgen rechtlich gleichrangig ist, und Artikel 6 Absatz 3 EUV besagt: *„Die Grundrechte, wie sie in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben, sind als allgemeine Grundsätze Teil des Unionsrechts"*.

[2] Die Absicht des EDSB zur Veröffentlichung dieses Toolkits wurde am 24. Mai 2016 im Ausschuss für bürgerliche Freiheiten des Europäischen Parlaments angekündigt.

[3] Siehe „Tool#24 on Fundamental Rights & Human Rights" als Teil der „Better Regulation Toolbox", abrufbar unter: http://ec.europa.eu/smart-regulation/guidelines/tool_24_en.htm und die vertiefende Analyse in der Arbeitsunterlage der Kommissionsdienststellen „Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments", SEC (2011) 567 final. Siehe ferner Rat, „Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council's preparatory bodies", 5377/15, 20. Januar 2015. Diese Dokumente sind eher allgemein gehalten, auch wenn mehrere Beispiele der Rechtsprechung in diesen Leitlinien auf die in Artikel 7 und 8 der Charta verankerten Rechte verweisen, da sich der EuGH in mehreren wichtigen Urteilen zur Einschränkung dieser Rechte geäußert hat.

[4] Einen Überblick über die einschlägige Rechtsprechung von EuGH und EGMR bietet das „Handbuch zum europäischen Datenschutzrecht", das im Juni 2014 von der Europäischen Agentur für Grundrechte herausgegeben wurde. Siehe ferner das „Factsheet - Personal data protection", herausgegeben im November 2016 von der Pressestelle des EGMR, abrufbar unter: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[5] Siehe „Developing a „toolkit" for assessing the necessity of measures that interfere with fundamental rights", abrufbar unter:https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Papers/16-06-16_Necessity_paper_for_consultation_EN.pdf.

[6] In den verbundenen Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke*, hieß es im Schlussantrag der Generalanwältin: *„Wie eine Reihe klassischer Rechte nach der EMRK genießt das Recht auf Schutz der Privatsphäre keinen absoluten Vorrang. Artikel 8 Absatz 2 EMRK erkennt ausdrücklich die Möglichkeit von Ausnahmen von diesem Recht an, wie auch Artikel 9 des Übereinkommens Nr. 108 hinsichtlich des Schutzes von personenbezogenen Daten. Artikel 52 der Charta stellt beispielsweise (in allgemeinen Worten) entsprechende Kriterien auf, die, wenn sie erfüllt sind, Ausnahmen von den Rechten nach der Charta (oder Abweichungen hiervon) zulassen"*, Rn. 73. Dieser Linie folgte dann der EuGH in seinem Urteil, Rn. 48-50.

[7] Zum Begriff „gesetzlich vorgesehen" sollten die vom Europäischen Gerichtshof für Menschenrechte entwickelten Kriterien herangezogen werden, wie es verschiedentlich von Generalanwälten des EuGH in ihren Schlussanträgen angeregt wurde; siehe beispielsweise die Schlussanträge der Generalanwälte in den verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, Rn. 137-154, C-70/10, *Scarlet Extended,* Rn. 88-114, und C-291/12, *Schwarz*, Rn. 43. Diesem Ansatz folgt auch die Datenschutz-Grundverordnung 2016/679, Erwägungsgrund 41.

[8] Zwar gibt es nicht im Übermaß Rechtsprechung zu den Bedingungen, unter denen das Wesen eines Rechts als berührt gelten kann, doch kann man wohl sagen, das dies der Fall wäre, wenn die Einschränkung so weit ginge, dass sie das Recht seiner Kernbestandteile beraubte und damit die Ausübung dieses Rechts verhinderte. In *Schrems* befand der EuGH, dass das Wesen des Rechts auf einen wirksamen Rechtsbehelf berührt war. *„Eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, verletzt den Wesensgehalt des in Artikel 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz"* (Rn. 95). Er fuhr dann nicht mit der Prüfung der Frage fort, ob eine solche Einschränkung erforderlich war, sondern erklärte, auch aus anderen Gründen, die Entscheidung der Kommission über die Angemessenheit der „Grundsätze des „sicheren Hafens" zum Datenschutz" für ungültig. In *Digital Rights Ireland* stellte der EuGH zum Wesensgehalt des Rechts auf Achtung des Privatlebens fest, dass dieser nicht angetastet war, da die Richtlinie über die Vorratsdatenspeicherung die Kenntnisnahme des Inhalts elektronischer Kommunikation als solchen nicht gestattet. Desgleichen befand der EuGH, der Wesensgehalt des Rechts auf Schutz personenbezogener Daten sei nicht angetastet, weil die Richtlinie über die Vorratsdatenspeicherung die grundlegende Bestimmung enthalte, der zufolge geeignete technische und organisatorische Maßnahmen zu treffen sind, um die gespeicherten Daten gegen zufällige oder unrechtmäßige Zerstörung sowie zufälligen Verlust oder zufällige Änderung zu schützen (Rn. 39, 40). Erst danach befasste sich der Gerichtshof mit der Prüfung der Erforderlichkeit der Maßnahme. Die Vorenthaltung einer Überwachung durch eine unabhängige Stelle der Einhaltung des vom Unionsrecht garantierten Schutzniveaus könnte ebenfalls den Wesensgehalt des Rechts auf Schutz personenbezogener Daten antasten, da eine solche Überwachung in Artikel 8 Absatz 3 der Charta ausdrücklich verlangt wird, und *„Anderenfalls würde den Personen, deren personenbezogene Daten gespeichert wurden, das durch Artikel 8 Absatz 1 und 3 der Charta garantierte Recht vorenthalten, sich zum Schutz ihrer Daten mit einer Eingabe an die nationalen Kontrollstellen zu wenden"*, siehe *Tele2 Sverige AB*, Rn. 123.

[9] In *Szabo und Vissy/Ungarn*, 12. Januar 2016, befand der EGMR, dass der Begriff *„betroffene Personen, die … als Personenkreis identifiziert werden"* jede Person umfassen könnte, ohne dass die Behörden verpflichtet wären, die Beziehung zwischen den Personen und der Verhinderung eines terroristischen Anschlags nachzuweisen. Eine solche Maßnahme erfüllt nicht die Bedingungen der Vorhersehbarkeit und Erforderlichkeit (Rn. 58, 62, 66, 67).

[10] Siehe Artikel 5 Absatz 4 EUV.

[11] Rechtssache C-62/14, *Gauweiler (OMT)*, Rn. 67.

[12] K. Lenaerts, P. Van Nuffel, *European Union Law*, Sweet and Maxwell, 3rd edition, London, 2011, p. 141. (Rechtssache C-343/09 *Afton Chemical*, Rn. 45; verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke und Eifert*, Rn. 74; Rechtssachen C-581/10 und C-629/10, *Nelson u. a.,* Rn. 71; Rechtssache C-283/11, *Sky Österreich*, Rn. 50, und Rechtssache C-101/12, *Schaible*, Rn. 29).

[13] Siehe beispielsweise Rechtssache C-83/14 *Razpredelenie Bulgaria Ad,* Rn. 123. Dort stellt der Gerichtshof fest, dass *„…das vorlegende Gericht, falls keine andere ebenso wirksame Maßnahme wie die streitige Praxis ermittelt werden kann, weiter zu prüfen haben wird, ob die durch diese Praxis verursachten Nachteile im Hinblick auf die angestrebten Ziele nicht unverhältnismäßig sind und ob diese Praxis nicht eine übermäßige Beeinträchtigung der legitimen Interessen derjenigen Personen bewirkt, die in den betroffenen Stadtteilen wohnen".* Siehe ferner die Schlussanträge des Generalanwalts in den verbundenen Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, Rn. 132,172, 247, 248, wo es heißt, der EuGH habe in *Digital Rights Ireland* den Aspekt der Verhältnismäßigkeit nicht geprüft, *„da die Regelung der Richtlinie 2006/24 über das für die Bekämpfung schwerer Kriminalität absolut Notwendige hinausging".* Weiter führt er aus: *„Das Erfordernis der Verhältnismäßigkeit in einer demokratischen Gesellschaft - oder Verhältnismäßigkeit im engeren Sinne - ergibt sich sowohl aus Artikel 15 Absatz 1 der Richtlinie 2002/58 als auch aus Artikel 52 Absatz 1 der Charta, und aus der ständigen Rechtsprechung. Nach dieser ständigen Rechtsprechung kann eine grundrechtsverletzende Maßnahme nur dann als verhältnismäßig angesehen werden, wenn die verursachten Nachteile nicht außer Verhältnis zu den verfolgten Zielen stehen"*. Er unterstreicht dann, dass das Erfordernis der Verhältnismäßigkeit in dem Sonderfall der Vorratsspeicherung einer so großen Datenmenge der

„Ausgangspunkt ist für eine Debatte über die Werte, die in einer demokratischen Gesellschaft gelten sollen, und letztlich über die Art von Gesellschaft, in der wir leben wollen". In seinem Urteil stellt der Gerichtshof in den Randnummern 102 und 103 seine Analyse dar mit Erwägungen, die eher mit der Verhältnismäßigkeit zu tun haben, wenn er sagt, die Bekämpfung von Kriminalität und sogar schwerer Kriminalität rechtfertige eine allgemeine und unterschiedslose Speicherung von Daten über elektronische Kommunikation. Der Gerichtshof stellt fest: *„Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen".* Weiter stellt er fest, dass nur die Bekämpfung schwerer Kriminalität eine gezielte Speicherung und den Zugriff auf Daten der elektronischen Kommunikation rechtfertigen könnte. *„In Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte durch eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung die Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, vermag allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen". „Da außerdem der mit der Regelung verfolgte Zweck im Verhältnis zur Schwere des mit dem Zugang einhergehenden Eingriffs in die Grundrechte stehen muss, vermag folglich im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung schwerer Straftaten einen solchen Zugang zu den auf Vorrat gespeicherten Daten zu rechtfertigen"*.

[14] Siehe Artikel 6 Absatz 1 Buchstabe c und Artikel 7 der Richtlinie 95/46, Artikel 4 Absatz 1 Buchstabe c und Artikel 5 der Verordnung (EG) Nr. 45/2001, Artikel 5 Absatz 1 Buchstabe c und Artikel 6 Absatz 1 der Verordnung (EU) 2016/679 sowie deren Erwägungsgrund 49, in dem die strenge Prüfung der Erforderlichkeit der Verarbeitung personenbezogener Daten für Zwecke der Sicherung der Netz- und Informationssicherheit der Systeme des Verantwortlichen unterstrichen werden, und Artikel 8 Absatz 1 der Richtlinie 2016/680.

In seinen Leitlinien für die EU-Organe zur Prüfung der Frage, ob im Einklang mit der Verordnung (EG) Nr. 45/2001 Videoüberwachungsmaßnahmen erforderlich sind, führte der EDSB aus: *„Es sollten keinen Systeme installiert werden, die nicht effizient genug sind, um ihren Zweck zu erfüllen, etwa dann, wenn sie nur die Illusion von mehr Sicherheit vermitteln"* (Abschnitt 5.4) und *„wenn angemessene Alternativen zur Verfügung stehen. Eine Alternative gilt als angemessen, es sei denn, sie ist nicht machbar oder erheblich ineffizienter als die Videoüberwachung ... Die Tatsache an sich, dass eine Technologie zu relativ geringen Kosten verfügbar ist, reicht als Begründung für den Einsatz der Videotechnologie noch nicht aus."* (Abschnitt 5.5). Erst dann prüfte er, ob die Maßnahme verhältnismäßig ist: *„Und schließlich sollte ein Organ, das zu der Schlussfolgerung gelangt, dass ein eindeutiger Bedarf am Einsatz der Videoüberwachung besteht und es keine anderen Methoden gibt, die weniger stark in die Privatsphäre eingreifen, diese Technologie nur dann nutzen, wenn die Vorteile der Videoüberwachung ihre negativen Auswirkungen überwiegen."* (Abschnitt 5.6). Siehe EDSB, Leitlinien zur Videoüberwachung, Brüssel, 17. März 2010, abrufbar unter:https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_DE.pdf. Im Zusammenhang mit einer Meldung zur Vorabkontrolle gemäß Artikel 27 der Verordnung (EG) Nr. 45/2001 einer Maßnahme, bei der Fingerabdrücke zur Kontrolle der Arbeitszeit verwendet werden sollten, vertrat der EDSB die Auffassung, eine solche Verarbeitung sei nicht erforderlich. *„Der EDSB warnt davor, dass der Einsatz fingerabdruckgestützter Systeme für die Kontrolle der Arbeitszeit von Mitarbeitern nicht als erforderlich gilt und daher gemäß dem genannten Artikel 5 (der Verordnung (EG) Nr. 45/2001) nicht rechtmäßig ist. Die Bedingung, dass die Verarbeitung personenbezogener Daten im Hinblick auf das Ziel erforderlich sein muss, verpflichtet den für die Verarbeitung Verantwortlichen zu einer Prüfung der Frage, ob sich der Zweck der Verarbeitung nicht auch mit weniger die Privatsphäre verletzenden Mitteln erreichen lässt. Statt nämlich ein System zu wählen, das biometrische Daten verwendet, hätten von [der Einrichtung der Union] in diesem Zusammenhang andere Systeme erwogen werden sollen, wie Anmelden, Anwesenheitslisten oder Arbeitszeiterfassungssysteme mit Hilfe von Magnetausweisen"* (Abschnitt 3), siehe Schreiben des EDSB zur Meldung zur Vorabkontrolle der „Verarbeitung von Urlaub und Gleitzeit", 13.10.2014, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Prior checks/Letters/2014/14-10-13_Letter_Mr_Mifsud_EBA_EN.pdf.

[15] In den verbundenen Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, stellte der Gerichtshof zunächst fest, Verhältnismäßigkeit bestehe aus den Schritten Angemessenheit und Erforderlichkeit (Rn. 46), befand dann, die Einschränkungen der in Artikel 7 und 8 geschützten Rechte seien nicht erforderlich (siehe Rn. 65), und kam daher zu dem Schluss, die Einschränkungen seien nicht

verhältnismäßig (Rn. 69). Ähnlich in der Rechtssache C-362/14, *Schrems*, Rn. 92 und 93, wo der EuGH die Erforderlichkeit prüfte und die Safe Harbour-Entscheidung für ungültig erklärte, ohne auf dem Weg zu dieser Schlussfolgerung die Verhältnismäßigkeit auch nur zu erwähnen (Rn. 98).

[16] Beispielsweise in den verbundenen Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, stellt der Gerichtshof in den Randnummern 102 und 103 seine Analyse dar mit Erwägungen, die eher mit der Verhältnismäßigkeit zu tun haben, wenn er sagt, die Bekämpfung von Kriminalität und sogar schwerer Kriminalität rechtfertige eine allgemeine und unterschiedslose Speicherung von Daten über elektronische Kommunikation. Der Gerichtshof stellt fest: *„Zudem kann zwar die Wirksamkeit der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen; eine solche dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorsieht, für die Kriminalitätsbekämpfung nicht rechtfertigen".* Weiter stellt er fest, dass nur die Bekämpfung schwerer Kriminalität eine gezielte Speicherung und den Zugriff auf Daten der elektronischen Kommunikation rechtfertigen könnte. *„In Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte durch eine nationale Regelung, die für Zwecke der Kriminalitätsbekämpfung die Vorratsspeicherung von Verkehrs- und Standortdaten vorsieht, vermag allein die Bekämpfung der schweren Kriminalität eine solche Maßnahme zu rechtfertigen". „Da außerdem der mit der Regelung verfolgte Zweck im Verhältnis zur Schwere des mit dem Zugang einhergehenden Eingriffs in die Grundrechte stehen muss, vermag folglich im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten nur die Bekämpfung schwerer Straftaten einen solchen Zugang zu den auf Vorrat gespeicherten Daten zu rechtfertigen"*. Erst dann nimmt er eine Analyse der Anforderungen an die Erforderlichkeit einer gezielten Speicherung von Kommunikationsdaten vor (Rn. 108).

[17] Siehe auch die Stellungnahme 4/2007 der Artikel 29-Datenschutzgruppe zum Begriff „personenbezogene Daten", S. 8.

[18] Deutlich wird dies an den neueren richtungsweisenden Entscheidungen des EuGH zum Datenschutz, insbesondere *Digital Rights Ireland* und *Schrems*.

[19]Siehe EuGH, C-617/10, *Åkerberg Fransson*, Rn. 44, C-398/13 P, *Inuit Tapiriit Kanatami u. a. / Kommission,* Rn. 45, C-601/15, PPU *J.N. / Staatssecretaris van Veiligheid en Justitie*, Rn. 45, und verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, Rn. 127-129.

[20] Siehe EuGH, Rechtssache C-199/11, *Otis u. a.,* Rn. 47, Rechtssache C-398/13 P, *Inuit Tapiriit Kanatami u. a. / Kommission*, Rn. 46, und Rechtssache C-601/15 PPU, *J.N. / Staatssecretaris van Veiligheid en Justitie*, Rn. 46.

[21] Siehe Rechtssache C-601/15 PPU, *J.N. / Staatssecretaris van Veiligheid en Justitie*, Rn. 77.

[22] Siehe die Erläuterung zu Artikel 52 der Charta.

[23] Siehe H. Kranenborg, Article 8, pg. 235, in S. Peers and J. Kenner, *EU Charter of Fundamental Rights*, 2014 and S. Peers, Article 52, pg. 1515 et. seq., ibid.

[24] Siehe beispielsweise EuGH, verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke*, Rn. 59, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 35, verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, Rn. 119 und 120, und EGMR, *Zakharov / Russland*, 4. Dezember 2015, und *Szabo und Vissy / Ungarn*, 12. Januar 2016, Rn. 23.

[25] Artikel 8 Absatz 2 EMRK: „*Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und* ***in einer demokratischen Gesellschaft notwendig ist*** *für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer*".. Bezüglich der Charta siehe Artikel 52 Absatz 1 – *„Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Vorbehaltlich des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie* ***erforderlich*** *sind und den von der EU anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen*".

[26] Für eine detaillierte Analyse der Rechtsprechung des EGMR zur Anwendung der Anforderungen in Artikel 8 Absatz 2 der Konvention siehe die Stellungnahme 01/2014 der Artikel 29-Datenschutzgruppe der

Konzepte der Erforderlichkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung, 27. Februar 2014.

[27] EGMR, *Szabo und Vissy / Ungarn*, 12. Januar 2016, Rn. 73.

[28] Siehe EuGH, Rechtssache C-73/07, *Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy, Satamedia Oy*, Rn. 56; verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke*, Rn. 77; Rechtssache C-473/12, *IPI*, Rn. 39; verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland and Seitlinger u. a.*, Rn. 52; Rechtssache C-212/13, *Rynes*, Rn. 28; Rechtssache C-362/14, *Schrems,* Rn. 92; verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, Rn. 96 und Gutachten 1/15 des Generalanwalts (Gutachtenantrag des Europäischen Parlaments) zum Entwurf eines Abkommens zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen, Rn. 226.

[29] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4.5.2016.

[30] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 47 und 48.

[31] EDSB, Vortrag in der mündlichen Verhandlung in der Rechtssache betreffend den Entwurf des PNR-Abkommens zwischen der EU und Kanada, abrufbar unter: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2016/16-04-05_Pleading_Canada_PNR2_EN.pdf; im Gutachten 1/15 des Generalanwalts (Gutachtenantrag des Europäischen Parlaments) zu dem Entwurf eines Abkommens zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen heißt es, dass die strenge Kontrolle des Spielraums des Gesetzgebers auf der Bedeutung der Verarbeitung personenbezogener Daten in der Gesellschaft und auf der Schwere des Eingriffs durch die fragliche Maßnahme beruht (Rn. 201). Siehe ferner EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 47.

[32] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 34 - 36; siehe auch verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke*, Rn. 58.

[33] Siehe beispielsweise verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke*, Rn. 55, und verbundene Rechtssachen C-468/10 und C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) und Federación de Comercio Electrónico y Marketing Directo (FECEMD), / Administración del Estado*, Rn. 41. Nur in einer Rechtssache vertrat der EuGH die Auffassung, dass keine Einschränkung des Rechts auf Privatleben vorliegt, wenn die mit Lohn und Gehalt zusammenhängenden personenbezogenen Daten von den Arbeitgebern für ihren ursprünglichen Zweck verarbeitet werden; siehe EuGH, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Rechnungshof u. a. / Österreichischer Rundfunk*, Rn. 74.

[34] EuGH, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Rechnungshof u. a. / Österreichischer Rundfunk*, Rn. 75, und verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 33.

[35] EuGH, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Rechnungshof u. a. / Österreichischer Rundfunk*, Rn. 75; verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 33. EGMR, *S. und Marper / Vereinigtes Königreich*, 4. Dezember 2008, Rn. 67. Der Gerichtshof führte aus: *„Bei der Beantwortung der Frage, ob die von den Behörden gespeicherten personenbezogenen Daten irgendeinen der oben erwähnten Aspekte des Privatlebens umfassen, wird der Gerichtshof allerdings dem spezifischen Kontext angemessen Rechnung tragen, in dem die fraglichen Informationen erhoben und gespeichert wurden, der Art der Datensätze, der Weise, in der diese Datensätze verwendet und verarbeitet werden, und den Ergebnissen, die möglicherweise erzielt werden (siehe sinngemäß Friedl, op. cit., Rn. 49-51, und Peck, op.cit., Rn. 59)“*.

[36] Des Weiteren hat die Erforderlichkeit, wie der EuGH festgestellt hat, im EU-Sekundärrecht seine eigene unabhängige Bedeutung. Zur unabhängigen Bedeutung des Konzepts der Erforderlichkeit in Artikel 7 Buchstabe e der Richtlinie 95/46/EG siehe EuGH, Rechtssache C-524/06, *Huber / Bundesrepublik Deutschland*, Rn. 52.

[37] Siehe Richtlinie 95/45/EG, Artikel 1 Buchstabe a.

[38] Siehe Artikel 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.

[39] EuGH, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Österreichischer Rundfunk u. a.*, Rn. 75, und verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 33.

[40] EGMR, *Leander / Schweden*, 26.März 1987, Rn. 48.

[41] EGMR, *Amman / Schweiz*, 16. Februar 2000, Rn. 65, 69 und 80.

[42] Zu Artikel 8 EMRK siehe *Leander / Schweden,* 26. März 1987, Rn. 48; *Rotaru / Rumänien,* 4. Mai 2000, Rn. 46, und *Weber und Saravia / Deutschland*, 29. Juni 2006, Rn. 79, EGMR 2006-XI. Zu Artikel 7 der Charta siehe EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 35.

[43] EGMR, *Leander / Schweden,* 26. März 1987, Rn. 48; *Rotaru / Rumänien*, 4. Mai 2000, Rn. 46.

[44] EuGH, Rechtssache C-362/14, *Schrems*, Rn. 97.

[45] EuGH, Rechtssache C-524/06, *Huber*, Rn. 75, 79, 80, 81.

[46] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 28; verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, Rn. 92. Siehe ferner C. Docksey, *Four Fundamental rights: finding the balance*, (2016) 6 International Data Privacy Law, pp. 2.

[47] Gutachten 1/15 des Generalanwalts (Gutachtenantrag des Europäischen Parlaments) zu dem Entwurf eines Abkommens zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen, Rn. 274-281.

[48] Beispielsweise die Artikel 36 und 346 AEUV. Zu den dem Gemeinwohl dienenden Zielsetzungen siehe auch die Erläuterung zu Artikel 52 der Charta.

[49] EuGH, verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke*, Rn. 65, 68, 69, 75.

[50] EuGH, C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, Rn. 65; C-70/10, *Scarlet Extended SA / Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Rn. 46, 49, 53.

[51] EuGH, C-145/09, *Tsakouridis*, zum Begriff der öffentlichen Sicherheit, Rn. 43 und 44; C-601/15 PPU, *J. N. / Staatssecretaris voor Veiligheid en Justitie*, Rn. 66.

[52] EDSB, Stellungnahme 02/2016 zum Vorschlag für eine Verordnung über die Europäische Grenz- und Küstenwache, Punkt 8.

[53] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 49-50.

[54] Artikel 29-Datenschutzgruppe, Stellungnahme 9/2004 zum Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, WP 99, 9. November 2004.

[55] Artikel 29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, WP 193, 27. April 2012, S. 9.

[56] Siehe Artikel 8 der Richtlinie 95/46, Artikel 9 und 10 der Datenschutz-Grundverordnung 2016/679 und die Richtlinie 2016/680.

[57] Artikel 9 der Verordnung 2016/679 und Artikel 10 der Richtlinie 2016/680.

[58] Siehe beispielsweise Artikel-29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, S. 4.

[59] EuGH, C-291/12, *Schwarz*. Der Gerichtshof führte aus: *„Unter diesen Umständen ist festzustellen, dass dem Gerichtshof nicht zur Kenntnis gebracht worden ist, dass es Maßnahmen gäbe, die hinreichend wirksam zum Ziel des Schutzes vor betrügerischer Verwendung von Reisepässen beitragen könnten und dabei weniger schwerwiegend in die durch die Artikel 7 und 8 der Charta anerkannten Rechte eingriffen als das auf Fingerabdrücken beruhende Verfahren“* (Rn. 53); siehe ferner Gutachten 1/15 des Generalanwalts (Gutachtenantrag des Europäischen Parlaments) zum Entwurf eines Abkommens zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen, dem zufolge das PNR-Abkommen aus Maßnahmen bestehen muss, die die in Artikel 7 und 8 der Charta anerkannten Rechte möglichst wenig beeinträchtigen, aber gleichzeitig einen wirksamen Beitrag zum Ziel der öffentlichen Sicherheit leisten (Rn. 208, 244).

[60] Dies gilt jedoch nicht für Kennzeichen von allgemeiner Bedeutung. Siehe Artikel 87 der Verordnung 2016/679

[61] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 54, und die bereits zitierte Rechtsprechung des EGMR (*Liberty u. a. / Vereinigtes Königreich*, Rn. 62 und 63; *Rotaru / Rumänien*, Rn. 57-59, und *S. und Marper / Vereinigtes Königreich*, Rn. 99).

[62] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 60; C-362/14, *Schrems*, Rn. 93.

[63] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 57; C-362/14, *Schrems*, Rn. 93.

[64] EuGH, verbundene Rechtssachen C-293/12 und C-594/12, *Digital Rights Ireland*, Rn. 63-64.

[65] EGMR, *R. Zakharov / Russland*, 4. Dezember 2015, Rn. 287. Siehe ferner EGMR, *Szabo und Vissy / Ungarn*, 12. Januar 2016, Rn. 86.

[66] Siehe zum Subsidiaritätsgrundsatz „Tool#3 on Legal Basis, Subsidiarity and Proportionality" als Teil der „Better Regulation Toolbox", abrufbar unter: http://ec.europa.eu/smart-regulation/guidelines/tool_3_en.htm.