EUROPEAN DATA PROTECTION SUPERVISOR

Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken

Inhalt

I. Welchen Zweck haben diese Leitlinien und wie sind sie zu verwenden?

Die in der Charta der Grundrechte der Europäischen Union (im Folgenden „**Charta**“) verankerten **Grundrechte** zählen zu den **zentralen Werten** der Europäischen Union, die auch im Vertrag über die Europäische Union (im Folgenden „EUV“) festgelegt sind.[1] Zu diesen Rechten zählen die in den Artikeln 7 und 8 der Charta verankerten Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten. Diese Grundrechte sind von den Organen und Einrichtungen der EU zu wahren, auch wenn diese neue Maßnahmen konzipieren und umsetzen oder neue Rechtsvorschriften erlassen. In der Rechtsordnung der EU spielen auch noch andere Grundrechtsnormen eine einflussreiche Rolle, insbesondere die, die in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (im Folgenden „**EMRK**“) verankert sind.[2]

Die **Bedingungen für eventuelle Einschränkungen** der Ausübung von Grundrechten sind zu den wichtigsten Merkmalen der Charta geworden, weil sie darüber entscheiden, **in welchem Umfang die Rechte tatsächlich genossen werden können**.[3]

Die **Erforderlichkeit** und die **Verhältnismäßigkeit** einer legislativen Maßnahme, die eine Einschränkung der Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten mit sich bringt, stellen eine wesentliche **doppelte Anforderung** dar, die jede vorgeschlagene Maßnahme, die eine Verarbeitung personenbezogener Daten beinhaltet, erfüllen muss. Soll jedoch gewährleistet sein, dass der **Datenschutz** ein **fester Bestandteil der politischen Entscheidungsprozesse in der EU** wird, ist nicht nur das Verständnis der im Rechtsrahmen und in der Rechtsprechung festgelegten Grundsätze erforderlich, sondern auch eine **praxisbezogene und kreative Ausrichtung** auf Lösungen für komplexe Probleme mit häufig miteinander konkurrierenden strategischen Prioritäten.[4]

Der **Gerichtshof der Europäischen Union** (im Folgenden „EuGH“) hat anerkannt, dass EU-Rechtsvorschriften häufig **mehreren Zielen öffentlichen Interesses** dienen sollen, die einander mitunter widersprechen, und dass ein **ausgewogenes Verhältnis** zwischen den verschiedenen öffentlichen Interessen und den durch die EU-Rechtsordnung geschützten

---

[1] Artikel 2 EUV lautet: „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 einer Minderheit angehören**.“ Zudem werden in Artikel 6 Absatz 1 EUV die **Rechte, Freiheiten und Grundsätze anerkannt, die in der Charta festgelegt sind**; die Charta und die Verträge sind rechtlich gleichrangig. (Hervorhebung hinzugefügt)

[2] In Artikel 6 Absatz 3 EUV heißt es: „Die Grundrechte, wie sie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den **gemeinsamen Vertragsüberlieferungen der Mitgliedstaaten** ergeben, sind als **allgemeine Grundsätze Teil des Unionsrechts**.“ (Hervorhebung hinzugefügt)

[3] Nach Artikel 52 Absatz 1 der Charta muss „(j)ede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten (...) gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.“

[4] Siehe **Strategiepapier „Der EDSB als Berater von EU-Organen in Fragen der Strategie und Gesetzgebung: ein Rückblick auf die Erfahrungen aus zehn Jahren“** vom 4. Juni 2014, abrufbar unter: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-advisor-eu-institutions-policy-and-legislation_de.

Grundrechten hergestellt werden muss.[5] Zu diesen in der Charta verankerten Rechten und Interessen können gehören: das Recht auf Leben (Artikel 2) und das Recht auf Unversehrtheit (Artikel 3); das Recht auf Freiheit und Sicherheit (Artikel 6); Freiheit der Meinungsäußerung (Artikel 11); unternehmerische Freiheit (Artikel 16); das Eigentumsrecht einschließlich des geistigen Eigentums (Artikel 17); das Recht auf Zugang zu Dokumenten (Artikel 42).

Diese Leitlinien sind als **Hilfestellung** bei der Beantwortung der Frage gedacht, ob die vorgeschlagenen Maßnahmen mit dem EU-Datenschutzrecht in Einklang stehen. Sie wurden 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 die Rechte auf den Schutz personenbezogener Daten und der Privatsphäre einschränken. Sie sind darauf ausgerichtet, die Entscheidungsträger und Gesetzgeber nach Ermittlung der Maßnahmen, die sich auf den Datenschutz auswirken, und der Prioritäten und Ziele, die diesen Maßnahmen zugrunde liegen, bei der Suche nach Lösungen zu unterstützen, die die Konflikte zwischen diesen Prioritäten möglichst klein halten und verhältnismäßig sind.

Der EDSB betont, dass es in der Verantwortung des Gesetzgebers liegt, die Verhältnismäßigkeit einer Maßnahme zu beurteilen. Die vorliegenden Leitlinien sollen daher nicht endgültig die Frage beantworten (und können dies auch gar nicht), ob eine konkrete vorgeschlagene Maßnahme als verhältnismäßig gelten kann. Vielmehr bieten sie eine **praktische, schrittweise Methode** zur Bewertung der Verhältnismäßigkeit neuer legislativer Maßnahmen und liefern Erläuterungen sowie konkrete Beispiele**.** Sie erfüllen den Wunsch der Organe der EU nach Empfehlungen zu den besonderen Anforderungen, die sich aus Artikel 52 Absatz 1 der Charta ergeben.

Die Leitlinien **ergänzen** das Toolkit des EDSB „Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken“ (im Folgenden „**Necessity Toolkit**“)[6] und vertiefen die bestehenden Leitlinien in Bezug auf die Rechte auf Privatsphäre und den Schutz personenbezogener Daten[7], die von der Europäischen Kommission, dem Rat der EU und der Agentur der Europäischen Union für Grundrechte (im Folgenden „FRA“) zu den Einschränkungen der Grundrechte im Allgemeinen, z. B. in Bezug auf Folgenabschätzungen und Vereinbarkeitsprüfungen, erstellt wurden.[8]

---

[5] Rechtssache C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, ECLI:EU:C:2008:54, Rn. 68. In den verbundenen Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, erklärt Generalanwalt Saugmandsgaard Øe in seinen Schlussanträgen ECLI:EU:C:2016:572, Rn. 247, dass „*(d)as Erfordernis der Verhältnismäßigkeit in einer demokratischen Gesellschaft – oder Verhältnismäßigkeit „im engeren Sinne“ – 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 ergibt. 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.*“ (Hervorhebung hinzugefügt) In Rn. 248 wies er auch darauf hin, dass das Erfordernis der Verhältnismäßigkeit in diesem besonderen Fall der Vorratsspeicherung großer Datenmengen „*(d)er Ausgangspunkt für eine Debatte über die Werte ist, die in einer demokratischen Gesellschaft gelten sollen, und letztlich über die Art von Gesellschaft, in der wir leben wollen*“.

[6] EDSB, „Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener einschränken: Ein Toolkit“, 11. April 2017, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_de.pdf.

[7] In diesen Leitlinien wird häufig auf den Begriff „Datenschutz“ Bezug genommen, um sowohl auf das Recht auf **Privatsphäre** als auch auf den **Schutz personenbezogener Daten** zu verweisen. Wir weisen jedoch darauf hin, dass es sich hierbei um verschiedene Rechte handelt. Eine Erläuterung des Unterschieds zwischen den beiden Begriffen finden Sie auf: https://edps.europa.eu/data-protection/data-protection_de.

[8] Siehe Europäische Kommission **Instrument Nr. 24**, **Grundrechte und Menschenrechte als Teil des Instrumentariums für eine bessere Rechtsetzung**, abrufbar unter: https://ec.europa.eu/info/law/law-making-

Ziel dieser Leitlinien ist es, Fragen im Zusammenhang mit den Auswirkungen auf die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten eingehender zu erörtern und entsprechende Beispiele zu liefern. Dabei wird insbesondere näher auf das **Instrument Nr. 24** des **Instrumentariums für eine bessere Rechtsetzung** der Kommission und die **Operativen Leitlinien zur Berücksichtigung der Grundrechte bei Folgenabschätzungen der Kommission** eingegangen, die ergänzt werden.

Der EDBS stellt fest, dass der Schutz personenbezogener Daten in den letzten Jahren an Bedeutung gewonnen hat und als Dimension, die der Gesetzgeber in sämtlichen Politikbereichen und bei nahezu allen Initiativen der Kommission berücksichtigen muss, eine immer wichtigere Rolle spielt. Dies ist nicht nur auf eine verstärkte Sensibilisierung der Öffentlichkeit zurückzuführen, sondern auch auf die **stark gestiegene Kapazität bei der**

Um die Arbeit der Kommission zu erleichtern und diese Schlüsseldimension **bereits zum Zeitpunkt der Erstellung der Folgenabschätzung proaktiv** zu berücksichtigen, wird im operativen Teil dieser Leitlinien auch auf die **Terminologie der Folgenabschätzungsmethodik der Kommission verwiesen** (nämlich: ***Faktoren***, ***Ursachen***, ***Problemdefinition***, ***Auswirkungen***).

Angesichts der Komplexität und der Besonderheiten dieser Aufgabe ist der EDSB auch **bemüht und bereit, die Dienststellen der Kommission zu unterstützen, indem er unter anderem zur Folgenabschätzung beiträgt** und eine wichtige Informationsquelle zum Datenschutz als Grundrecht bietet.

Bei Fragen zu diesen Leitlinien und zur Beurteilung der Auswirkungen von Rechtsakten auf die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten kann das Referat Politik und Beratung des EDSB kontaktiert werden. Zu diesem Zweck steht die funktionale E-Mail-Adresse des Referats Politik und Beratung zur Verfügung: POLICY-CONSULT@edps.europa.eu.

process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_de

und die vertiefende Analyse in der **Arbeitsunterlage der Kommissionsdienststellen „Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments“** (Operative Leitlinien zur Berücksichtigung der Grundrechte bei Folgenabschätzungen der Kommission), SEC(2011) 567 final, abrufbar unter: http://ec.europa.eu/smart-regulation/impact/key_docs/docs/sec_2011_0567_en.pdf.

Siehe ferner **Leitlinien des Rates zu den methodischen Schritten für die in den Vorbereitungsgremien des Rates vorzunehmende Prüfung der Vereinbarkeit mit den Grundrechten**, 5377/15 vom 20. Januar 2015, abrufbar unter:
https://www.consilium.europa.eu/media/30209/qc0214079enn.pdf

sowie **Handbuch der FRA„Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level“** (Die Anwendung der Charta der Grundrechte der Europäischen Union im Rechtswesen und bei der Politikgestaltung auf nationaler Ebene), Leitlinien, Mai 2018, abrufbar unter: http://fra.europa.eu/en/publication/2018/national-guidance-application-eu-charter.

Diese Dokumente umfassen sämtliche Grundrechte und verweisen daher auch auf verschiedene Beispiele aus der Rechtsprechung des EuGH, die sich auf die in den Artikeln 7 und 8 der Charta verankerten Rechte beziehen.

Datenverarbeitung (die bis vor Kurzem noch unbedenklich erschien), **die erhebliche Auswirkungen auf das Leben jedes einzelnen Bürgers hat**.

Es muss betont werden, dass die **Erforderlichkeit und Verhältnismäßigkeit**, auch wenn sie eng miteinander verbunden sind (beide Bedingungen müssen von der Regelung erfüllt sein), **zwei verschiedene Prüfungen** nach sich ziehen. Dies wird in Abschnitt III der vorliegenden Leitlinien deutlich gemacht. Hier wird eine praktische Checkliste zur schrittweisen Überprüfung der Verhältnismäßigkeit vorgestellt und ein erster umfassender Überblick über den **gesamten Arbeitsablauf** gegeben.

Die Leitlinien enthalten eine **Einleitung**, in der ihr Inhalt und Zweck dargelegt werden, eine **rechtliche Analyse** der Verhältnismäßigkeitsprüfung, die für die Verarbeitung personenbezogener Daten durchgeführt wird, sowie eine **praktische Checkliste zur schrittweisen** Bewertung der Verhältnismäßigkeit neuer legislativer Maßnahmen. Die Checkliste ist das Herzstück der Leitlinien und kann auch unabhängig vom Rest des Dokuments verwendet werden.

Die Leitlinien stützen sich auf die **Rechtsprechung** [9] des EuGH, des Europäischen Gerichtshofs für Menschenrechte (im Folgenden „EGMR"), die Stellungnahmen des Europäischen Datenschutzbeauftragten und der Artikel-29-Datenschutzgruppe (im Folgenden „WP29") sowie auf die Leitlinien des Europäischen Datenschutzausschusses (im Folgenden „EDSA").

Zusammen mit dem **Necessity Toolkit** soll mit den Leitlinien **ein gemeinsamer Ansatz für die Beurteilung der Erforderlichkeit und Verhältnismäßigkeit** legislativer Maßnahmen im Hinblick auf das Recht auf Privatsphäre und den Schutz personenbezogener Daten geschaffen werden.

II. Rechtliche Analyse: Anwendung der Verhältnismäßigkeitsprüfung auf die Rechte auf Privatsphäre und den Schutz personenbezogener Daten

1. Die **Prüfung der Verhältnismäßigkeit** zur Beurteilung der Rechtmäßigkeit vorgeschlagener Maßnahmen, die die Verarbeitung personenbezogener Daten umfassen

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 festgelegten Bedingungen entsprechen. Gleiches gilt für das in Artikel 7 der Charta festgelegte **Recht auf Achtung des Privatlebens**.[10]

---

[9] Einen Überblick über die diesbezügliche **Rechtsprechung** des EuGH und des EGMR finden Sie im **Handbuch der FRA zum europäischen Datenschutzrecht**, Ausgabe 2018, abrufbar unter: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law.
Siehe auch das „Informationsblatt - Schutz personenbezogener Daten", das im September 2018 vom EGMR herausgegeben wurde und unter folgender Adresse abgerufen werden kann: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[10] In den verbundenen Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke und Hartmut Eifert*, erklärt Generalanwältin Sharpston in ihrem Schlussanträgen, ECLI:EU:C:2010:353, Rn. 73, dass *„(d)as Recht auf Schutz der Privatsphäre wie eine Reihe klassischer Rechte nach EMRK **keinen absoluten Vorrang genießt**.*

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

- Sie muss **gesetzlich vorgesehen sein**,
- sie muss den **Wesensgehalt der Rechte achten**,
- sie muss den von der Union anerkannten **dem Gemeinwohl dienenden Zielsetzungen** oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen,
- sie muss **erforderlich** sein – der Schwerpunkt des Necessity Toolkits –, und
- sie muss **verhältnismäßig** sein – das Hauptthema dieser Leitlinien.

Diese Liste von **Makrokriterien** legt die **Reihenfolge** fest, in der die **Bewertung** der Rechtmäßigkeit einer Einschränkung bei der Ausübung eines Grundrechts erfolgen muss.

1. Zunächst ist zu prüfen, ob das Gesetz, das eine Beschränkung vorsieht, **zugänglich und vorhersehbar** ist.[11] Ist diese Voraussetzung nicht erfüllt, ist die Maßnahme rechtswidrig

---

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." (Hervorhebung hinzugefügt) Dieser Ansatz wurde durch das Urteil des EuGH, ECLI:EU:C:2010:662, Rn. 48-50 bestätigt.

Erläuterungen zum Schutz personenbezogener Daten als „kein uneingeschränktes" Recht, siehe Erwägungsgrund 4 der Verordnung (EU) 2016/679 („Datenschutz-Grundverordnung", im Folgenden „DSGVO"): „Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das **Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht**; es muss **im Hinblick auf seine gesellschaftliche Funktion** gesehen und **unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.**" (Hervorhebung hinzugefügt)

Zum Unterschied zwischen **uneingeschränkten Rechten** (wie dem Verbot der Folter und unmenschlicher oder erniedrigender Strafe oder Behandlung gemäß Artikel 4 der Charta) und Rechten, die **Einschränkungen unterliegen** (wie das Recht auf Privatsphäre und den Schutz personenbezogener Daten), siehe Arbeitsunterlage der Kommissionsdienststellen, Operative Leitlinien zur Berücksichtigung der Grundrechte in Folgenabschätzungen der Kommission, SEC (2011) 567 final, Seite 9, und Handbuch der FRA „Die Anwendung der Charta der Grundrechte der Europäischen Union im Rechtswesen und bei der Politikgestaltung auf nationaler Ebene", Leitlinien, Mai 2018, Seite 70.

Eine wichtige Folge dieser Unterscheidung besteht darin, dass **absolute Rechte nicht eingeschränkt werden können und daher nicht gegen andere Rechte oder Interessen abgewogen werden können**. In Fällen, in denen das **Recht auf Privatsphäre mit einem absoluten Recht** (z. B. dem Recht, nicht gefoltert zu werden) **einhergeht** (in dieselbe Richtung geht), werden daher **beide (miteinander einhergehenden) Rechte nicht gegen andere Rechte oder Interessen (z. B. nationale Sicherheit) abgewogen.**

[11] Gemäß Artikel 52 Absatz 3 der Charta gilt: „Soweit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weitergehenden Schutz gewährt." Was den Ausdruck „**gesetzlich vorgesehen**" gemäß Artikel 52 Absatz 1 der Charta anbelangt, sollten die vom EGMR erarbeiteten Kriterien so verwendet werden, wie in mehreren Schlussanträgen der Generalanwälte des EuGH vorgeschlagen, siehe z. B. Schlussanträge in den verbundenen Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, Rn. 137-154, und in Rechtssache C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, Rn. 88-114. Daher kann unter anderem auf das Urteil des EGMR in der Rechtssache *Weber und Saravia / Deutschland*, Rn. 84, verwiesen werden: „Der Gerichtshof weist erneut darauf hin, dass der Ausdruck „gesetzlich vorgesehen" im Sinne von Artikel 8 Absatz 2 [der EMRK] voraussetzt, dass die angegriffene Maßnahme eine gewisse innerstaatliche Rechtsgrundlage haben muss; er betrifft auch die Qualität

und bedarf keiner weiteren Prüfung.[12]

2. Wenn die Maßnahme die Prüfung der Qualität des Gesetzes nach Punkt 1 oben bestanden hat, ist zweitens zu prüfen, ob der **Wesensgehalt des Rechts** geachtet wird, d. h. ob also das Recht weitgehend seines Inhalts **beraubt** ist und die Person das Recht nicht ausüben kann. Wird der Wesensgehalt des Rechts berührt, ist die Maßnahme unrechtmäßig und es muss nicht näher untersucht werden, ob die Maßnahme mit den Vorschriften in Artikel 52 Absatz 1 der Charta vereinbar ist.[13]

---

des in Rede gestellten Gesetzes, wobei vorausgesetzt ist, dass es der betroffenen Person zugänglich ist, die zudem seine Folgen absehen können muss. Außerdem muss er mit der Rechtsstaatlichkeit vereinbar sein."
Siehe auch Erwägungsgrund 41 der DSGVO: „Eine solche [Rechtsgrundlage oder] legislative Maßnahme sollte **klar** und **präzise** sein, und ihre Anwendung sollte für die ihr **unterliegenden Personen vorhersehbar** sein, im Einklang mit der Rechtsprechung des Gerichtshofs der Europäischen Union (...) und des Europäischen Gerichtshofs für Menschenrechte." (Hervorhebung hinzugefügt)
- Was den Ausdruck „**Vorhersehbarkeit**" im Zusammenhang mit der **Überwachung des Kommunikationsverkehrs** anbelangt, siehe EGMR, *Zakharov / Russland*, Rn. 229: „Der Gerichtshof hat wiederholt entschieden, dass „Vorhersehbarkeit" im Zusammenhang mit der Überwachung des Kommunikationsverkehrs nicht dasselbe sein kann wie in vielen anderen Bereichen. Im besonderen Zusammenhang mit geheimen Überwachungsmaßnahmen wie der Überwachung des Kommunikationsverkehrs kann Vorhersehbarkeit nicht bedeuten, dass der Bürger vorhersehen können sollte, wann die Behörden wahrscheinlich Maßnahmen zur Überwachung seiner Kommunikation treffen werden, sodass er sein Verhalten entsprechend anpassen kann. Insbesondere bei geheimer Ausübung der Exekutivgewalt ist die Gefahr von Willkür jedoch offensichtlich. Daher sind klare, ausführliche Vorschriften für das Abhören von Telefongesprächen unerlässlich, insbesondere da sich die hierfür zur Verfügung stehende Technologie ständig weiterentwickelt. Das inländische Recht muss hinreichend klar formuliert sein, damit die Bürger angemessen auf die Umstände und Voraussetzungen hingewiesen werden, unter denen Behörden befugt sind, diese Maßnahmen vorzunehmen." (Hervorhebungen hinzugefügt) Siehe zuletzt in diesem Sinne *Big Brother Watch u. a. / Vereinigtes Königreich*, EGMR, 13. September 2018, Rn. 306.
- Siehe auch Rechtssache *Shimovolos / Russland*, EGMR, 21. Juni 2011.

[12] Siehe Rechtssache des EGMR, *Benedik / Slowenien*, Rn. 132*:* „Der Gerichtshof ist der Ansicht, dass dem Gesetz, auf das die strittige Maßnahme gestützt wurde, nämlich die Offenlegung von Teilnehmerinformationen in Zusammenhang mit der fraglichen dynamischen IP-Adresse durch die Polizei (...) und der Art und Weise, wie es von den innerstaatlichen Gerichten angewendet wurde, **an Klarheit fehlte** und keine ausreichenden Garantien gegen einen willkürlichen Eingriff in die Rechte nach Artikel 8 geboten wurden. Unter diesen Umständen befindet der Gerichtshof, dass der Eingriff in das Recht des Antragstellers auf Achtung seines Privatlebens **nicht** wie von Artikel 8 Absatz 2 EMRK gefordert **„gesetzlich vorgesehen"** war. Daher braucht der Gerichtshof **nicht zu prüfen, ob die strittige Maßnahme ein legitimes Ziel verfolgte und verhältnismäßig war**." (Hervorhebung hinzugefügt)
Siehe auch Rechtssache *Rechnungshof (C-465/00) / Österreichischer Rundfunk u. a. und Christa Neukomm (C-138/01) und Joseph Lauermann (C-139/01) / Österreichischer Rundfunk.*, ECLI:EU:C:2003:294, Rn. 77-80; Schlussanträge des Generalanwalts in dem Gutachten zum PNR-Abkommen mit Kanada 1/15, ECLI:EU:C:2017:592, Rn. 191-192: „*In Bezug auf die Speicherung personenbezogener Daten ist festzustellen, dass die fragliche Regelung u. a. stets objektive Kriterien genügen muss, die einen Zusammenhang zwischen den zu speichernden personenbezogenen Daten und dem verfolgten Ziel herstellen (vgl. in diesem Sinne Urteile vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93 und vom 21. Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Rn. 110). Was die Verwendung rechtmäßig gespeicherter personenbezogener Daten durch eine Behörde angeht, ist darauf hinzuweisen, dass der Gerichtshof entschieden hat, dass der Zugang zu solchen Daten einem der in der Regelung genannten Zwecke zu entsprechen hat, sondern auch die* ***materiell- und verfahrensrechtlichen Voraussetzungen für die Verwendung der Daten festlegen muss*** *(vgl. entsprechend Urteil vom 21 Dezember 2016, Tele2 Sverige und Watson u. a., C-203/15 und C-698/15, EU:C:2016:970, Randnummern 117 und 118 und die dort angeführte Rechtsprechung).*"

[13] Zwar gibt es nicht im Übermaß Rechtsprechung zu den Bedingungen, unter denen **der Wesensgehalt** eines Rechts als berührt gelten kann, doch könnte man wohl argumentieren, dass 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 der Rechtssache **C-362/14**, *Schrems*, ECLI:EU:C:2015:650, Rn. 94 und 95, befand der EuGH dass **der Wesensgehalt des Rechts auf Achtung des Privatlebens und einen wirksamen Rechtsbehelf** berührt war:

3. Als Drittes 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. Wie im Necessity Toolkit erklärt, ist es daher wichtig, die dem Gemeinwohl dienende Zielsetzung so detailliert wie möglich zu bestimmen, um feststellen zu können, ob die Maßnahme erforderlich ist.

4. Der nächste Schritt besteht darin, die **Erforderlichkeit** einer vorgeschlagenen legislativen Maßnahme zu beurteilen, die die Verarbeitung personenbezogener Daten mit sich bringt (Prüfung der Erforderlichkeit).[14]

5. Fällt diese Prüfung zur Zufriedenheit aus, ist die **Verhältnismäßigkeit** der vorgeschlagenen Maßnahme zu bewerten (Prüfung der Verhältnismäßigkeit). Der Begriff der Verhältnismäßigkeit ist ein im EU-Recht fest verankerter Rechtsbegriff. Es handelt sich um **einen allgemeinen Grundsatz** des EU-Rechts, demzufolge *„die Maßnahmen der Union inhaltlich wie formal **nicht über das zur Erreichung der Ziele der Verträge erforderliche Maß hinausgehen**“.*[15] (Hervorhebung hinzugefügt) Er baut auf den Verfassungstraditionen verschiedener Mitgliedstaaten auf.[16]

---

*„eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, ist als Verletzung des Wesensgehalts des durch Artikel 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens anzusehen (...). Ebenso verletzt 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, **den Wesensgehalt des in Artikel 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz**.“* (Rn. 94 und 95) (Hervorhebung hinzugefügt) Der Gerichtshof fuhr nicht mit der Prüfung der Frage fort, ob eine solche Einschränkung erforderlich war und erklärte, auch aus anderen Gründen, die **Entscheidung der Kommission** über die Angemessenheit der „Grundsätze des „sicheren Hafens“ zum Datenschutz“ für **ungültig**.

- In den verbundenen Rechtssachen **C-293/12 und C-594/12,** *Digital Rights*, ECLI:EU:C:2014:238, Rn. 39, 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 nicht gestattet** (sondern nur von „Metadaten“).

Desgleichen befand der EuGH, dass der **Wesensgehalt des Rechts auf *Schutz personenbezogener Daten*** nicht angetastet sei, 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 und 40). Erst nachdem festgestellt worden war, dass der Wesensgehalt des betreffenden Grundrechts nicht beeinträchtigt war, befasste sich der Gerichtshof mit der Prüfung **der Erforderlichkeit** der Maßnahme.

- In den verbundenen Rechtssachen **C-203/15 und C-698/15**, *Tele2 Sverige AB,* ECLI:EU:C:2016:970, Rn. 123, stellte der Gerichtshof fest, dass die **Vorenthaltung einer Überwachung** durch eine unabhängige Stelle der Einhaltung des vom Unionsrecht garantierten Schutzniveaus **den Wesensgehalt des Rechts auf Schutz personenbezogener Daten ebenfalls antasten** könnte, da eine solche Überwachung in Artikel 8 Absatz 3 der Charta ausdrücklich verlangt wird und *„(a)nderenfalls 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“.*

[14] Unsere Analyse der **Prüfung der Erforderlichkeit** finden Sie im Necessity Toolkit des EDSB unter: https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_de.

[15] Siehe Artikel 5 Absatz 4 EUV.

[16] Der Grundsatz wurde vom EuGH in der Rechtssache *Internationale Handelsgesellschaft*, **C-11/70,** ECLI:EU:C:1970:114, erarbeitet. Ähnlich wie im deutschen Verwaltungsrecht besteht die Prüfung zur Feststellung der Erforderlichkeit und Verhältnismäßigkeit einer Maßnahme auch auf EU-Ebene aus drei Schritten: (i) Angemessenheit, (ii) Erforderlichkeit und (iii) Verhältnismäßigkeit *im engeren Sinne*. Siehe diesbezüglich, C.

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 (...)." Nach der ständigen Rechtsprechung des EuGH *„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"*.[17] Daher umfasst die **Verhältnismäßigkeit im weiteren Sinne** (laut EuGH) **sowohl die Erforderlichkeit als auch die Angemessenheit** (**Verhältnismäßigkeit *im engeren Sinne***) einer Maßnahme, also das Ausmaß, in dem eine logische Verknüpfung zwischen der Maßnahme und dem verfolgten (legitimen) Ziel besteht.[18]

Damit eine Maßnahme dem in Artikel 52 Absatz 1 der Charta festgelegten 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 von Grundrechten mit sich bringt. Daher „***schränkt er die Behörden*** *in der Ausführung ihrer Befugnisse ein, weil er* ***ein Gleichgewicht*** *zwischen den eingesetzten* ***Mitteln*** *und* ***dem angestrebten Ziel (oder dem erreichten Ergebnis) verlangt***".[19]

So hat der EuGH im *Digital Rights-Urteil*[20] beschlossen, dass der **Gestaltungsspielraum des Gesetzgebers** verkleinert wird, wenn Grundrechte eingeschränkt werden: *„da Grundrechtseingriffe in Rede stehen, kann der Gestaltungsspielraum des Unionsgesetzgebers anhand einer Reihe von Gesichtspunkten eingeschränkt sein; zu ihnen gehören u. a. der betroffene Bereich, das Wesen des fraglichen durch die Charta gewährleisteten Rechts, Art und Schwere des Eingriffs sowie dessen Zweck".*[21] Die Frage: „Welches **Ausmaß hat der (eingeschränkte) Gestaltungsspielraum des Unionsgesetzgebers**?" beantwortete der EuGH in der Sache wie folgt: „*Daher* ***muss*** *die fragliche Unionsregelung klare und präzise Regeln*

Bagger Tranberg, *Proportionality and data protection in the case law of the European Court of Justice*, International Data Privacy Law, 2011, Vol. 1, Nr. 4, Seite 240.

[17] Rechtssache C-62/14, *Gauweiler (OMT)*, ECLI:EU:C:2015:400, Rn. 67. Siehe auch Rechtssache C-331/88, *Fedesa u. a.*, ECLI:EU:C:1990:391, Rn. 13: „*Was die Prüfung der Verhältnismäßigkeit angeht verlangt der Grundsatz der Verhältnismäßigkeit, der zu den allgemeinen Grundsätzen des Gemeinschaftsrechts gehört, dass die Maßnahmen der Gemeinschaftsorgane nicht die Grenzen dessen überschreiten, was zur Erreichung der mit der fraglichen Regelung zulässigerweise verfolgten Ziele geeignet und erforderlich ist, wobei, wenn mehrere geeignete Maßnahmen zur Auswahl stehen, die am wenigsten belastende zu wählen ist und die verursachten Nachteile nicht außer Verhältnis zu den angestrebten Zielen stehen dürfen.*"

[18] Als mögliches Beispiel für **Verhältnismäßigkeit im weiteren Sinne**, das sowohl die Prüfung der Erforderlichkeit als auch die Prüfung der Verhältnismäßigkeit umfasst, siehe C-594/12, *Digital Rights*, wobei die Erforderlichkeit (Rn. 65: *„Aus dem Vorstehenden folgt, dass die Richtlinie 2006/24 keine klaren und präzisen Regeln zur Tragweite des Eingriffs in die in Artikel 7 und 8 der Charta verankerten Grundrechte vorsieht. Somit ist festzustellen, dass die Richtlinie 2006/24 einen Eingriff in diese Grundrechte beinhaltet, der in der Rechtsordnung der EU von großem Ausmaß und von besonderer Schwere ist, ohne dass sie Bestimmungen enthielte, die zu gewährleisten vermögen, dass sich der Eingriff tatsächlich auf das* ***absolut Notwendige*** *beschränkt.")* und die Verhältnismäßigkeit (Rn. 69: „*Aus der Gesamtheit der vorstehenden Erwägungen ist zu schließen, dass der Unionsgesetzgeber beim Erlass der Richtlinie 2006/24 die Grenzen überschritten hat, die er zur Wahrung des Grundsatzes der* ***Verhältnismäßigkeit*** *im Hinblick auf die Artikel 7, 8 und 52 Absatz 1 der Charta einhalten musste.")* vom EuGH explizit angesprochen werden. Mit anderen Worten: Der EuGH entscheidet erst *nach* der Prüfung der Erforderlichkeit über die Verhältnismäßigkeit.

[19] K. Lenaerts, P. Van Nuffel, *European Union Law*, Sweet and Maxwell, 3. Auflage, London, 2011, S. 141 (Rechtssache C-343/09, *Afton Chemical*, Rn. 45; verbundene Rechtssachen C-92/09 und C-93/09, *Volker und Markus Schecke und Hartmut Eifert*, ECLI:EU:C:2010:662, 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).

[20] Verbundene Rechtssachen C-293/12 und C-594/12, ECLI:EU:C:2014:238.

[21] Ibid., Rn. 47.

für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen."[22] (Hervorhebung hinzugefügt)

Das letztgenannte Element (das verlangte Gleichgewicht) beschreibt die **Verhältnismäßigkeit im engeren Sinne (*stricto sensu*)** und begründet die Prüfung der Verhältnismäßigkeit, die Gegenstand der vorliegenden Leitlinien ist. Sie sollte sowohl aus konzeptioneller als auch aus praktischer Sicht klar von der Erforderlichkeit (siehe Abschnitt III unten) unterschieden werden.

2. Erläuterungen zum **Zusammenhang** zwischen Verhältnismäßigkeit und Erforderlichkeit

Wie im Necessity Toolkit vorgesehen, „**impliziert Erforderlichkeit 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**". Die Prüfung der Erforderlichkeit sollte als **erster Schritt** angesehen werden, den eine vorgeschlagene Maßnahme, die die Verarbeitung personenbezogener Daten umfasst, erfüllen muss. 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 anderen Worten: **Die Erforderlichkeit ist eine Voraussetzung für die Verhältnismäßigkeit**.[23]

Diese Leitlinien stützen sich daher auf die Annahme, dass nur bei einer erwiesenermaßen erforderlichen Maßnahme eine Prüfung der Verhältnismäßigkeit stattfinden sollte. Wie im Necessity Toolkit erwähnt, hat der EuGH in der jüngeren Vergangenheit in einigen 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.[24]

---

[22] Ibid., Rn. 54.
- Siehe auch **zweite Stellungnahme des EDSB 5/2015 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen (PNR) zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität**, Seite 6-7: „Im Rahmen einer **Verhältnismäßigkeitsprüfung** kann der **Gestaltungsspielraum des EU-Gesetzgebers anhand einer Reihe von Gesichtspunkten eingeschränkt sein**. Zu ihnen zählen insbesondere der betroffene Bereich, die Art der fraglichen Rechte, die Art und die Schwere des Eingriffs sowie das Ziel, das mit dem Eingriff verfolgt werden soll. Der Gerichtshof wies nachdrücklich darauf hin, dass diese Einschränkungen und Schutzbestimmungen umso bedeutsamer sind, wenn die personenbezogenen Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht." Die Stellungnahme des EDSB ist abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_de.pdf.

[23] In den verbundenen Rechtssachen **C-465/00, C-138/01 und C-139/01**, *Rechnungshof*, ECLI:EU:C:2003:294, Rn. 91, befand der EuGH: *„Sollten die vorlegenden Gerichte die den Ausgangsverfahren zugrunde liegende nationale Regelung für **unvereinbar** mit Artikel 8 EMRK halten, so kann diese Regelung **auch nicht dem Erfordernis der Verhältnismäßigkeit** nach Artikel 6 Absatz 1 Buchstabe c und Artikel 7 Buchstaben c oder e der Richtlinie 95/46 genügen."* (Hervorhebung hinzugefügt)

[24] In den verbundenen Rechtssachen **C-293/12 und C-594/12**, *Digital Rights*, ECLI:EU:C:2014:238, stellte der Gerichtshof zunächst fest, Verhältnismäßigkeit bestehe aus den Schritten Angemessenheit und Erforderlichkeit

Sobald eine legislative Maßnahme jedoch als **erforderlich** erachtet wird, sollte sie auf ihre **Verhältnismäßigkeit** geprüft werden. **Bei der Prüfung der Verhältnismäßigkeit wird im Allgemeinen bewertet, welche „Garantien" mit einer Maßnahme einhergehen sollten** (z. B. bei der Überwachung), um die mit der geplanten Maßnahme verbundenen Risiken für die Grundrechte und -freiheiten der betroffenen Personen auf ein „akzeptables"/angemessenes Maß zu reduzieren.

Ein weiterer Faktor, der bei der Prüfung der Verhältnismäßigkeit einer vorgeschlagenen Maßnahme zu berücksichtigen ist, ist **die Effektivität der vorhandenen Maßnahmen** gegenüber der geplanten.[25] Liegen bereits Maßnahmen für einen ähnlichen oder den gleichen Zweck vor, sollte deren Effektivität im Rahmen der Beurteilung der Verhältnismäßigkeit systematisch bewertet werden. Wird die Effektivität bestehender Maßnahmen, die einen ähnlichen oder gleichen Zweck verfolgen, nicht bewertet, kann die Prüfung der Verhältnismäßigkeit für eine neue Maßnahme nicht als ordnungsgemäß durchgeführt angesehen werden.

3. **Schlussfolgerung**: Verhältnismäßigkeit im Datenschutzrecht. Ein faktengestütztes Konzept, das der Einzelfallbewertung durch den EU-Gesetzgeber bedarf

Das „Aufkommen eines Verhältnismäßigkeitserfordernisses" gilt als „**eine der auffälligsten Entwicklungen** im europäischen Datenschutzrecht in den letzten zehn Jahren".[26]

Der Grundsatz der Verhältnismäßigkeit wurde in Artikel 5 Absatz 1 des **überarbeiteten Übereinkommens 108**[27] aufgenommen, in dem es heißt: „Die Datenverarbeitung muss in Bezug auf den verfolgten legitimen Zweck **verhältnismäßig** sein und in allen Phasen der Verarbeitung ein **ausgewogenes Verhältnis** zwischen allen betroffenen Interessen, seien sie öffentlich oder privat, und den betroffenen Rechten und Freiheiten widerspiegeln." (Hervorhebung hinzugefügt)

Im Mittelpunkt des Begriffs der Verhältnismäßigkeit steht das Konzept der **Abwägung**: die Abwägung der **Intensität des Eingriffs** *im Vergleich* zur **Bedeutung** („Legitimität", unter Verwendung des Wortlauts der Rechtsprechung) des **im gegebenen Kontext** erreichten Ziels.

Für eine gut durchgeführte Prüfung ist die ausdrückliche Festlegung der Elemente, von denen die Abwägung abhängt, sowie deren Strukturierung nach einem einheitlichen System erforderlich. Nur so kann die Prüfung vollständig und genau sein.

Daher ist die **Klarheit der Maßnahme**, die die Grundrechte auf Privatsphäre und/oder Datenschutz einschränkt, eine Voraussetzung für die Feststellung der Intensität des Eingriffs. Letztere ist wiederum erforderlich, um prüfen zu können, ob die Auswirkungen auf diese

---

(Rn. 46). Anschließend befand er, die Einschränkungen der in Artikel 7 und 8 geschützten Rechte seien **nicht erforderlich** (Rn. 65), und kam daher zu dem Schluss, die Einschränkungen seien nicht verhältnismäßig (Rn. 69). - Ähnlich in der Rechtssache **C-362/14**, *Schrems*, ECLI:EU:C:2015:650, Rn. 92 und 93, in der 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).

[25] Siehe Stellungnahme 01/2014 der WP29 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung vom 27. Februar 2014, Seite 9, abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_de.pdf.

[26] Lee A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford University Press, 2014, Seite 147.

[27] Europarat, **Überarbeitetes Übereinkommen über den Schutz des Menschen bei der Verarbeitung personenbezogener Daten,** Konsolidierte Fassung, abrufbar unter: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

Grundrechte „in einem angemessenen Verhältnis zum Ziel“ stehen (d. h. zu dem Ziel, das mit der zu prüfenden Regelung verfolgt wird).

Wie der EuGH erklärt hat, ist unbedingt darauf hinzuweisen, dass es sich bei der Verhältnismäßigkeit um eine ***konkrete*** Bewertung handelt (von Fall zu Fall):

> *„Nach dem Grundsatz der **Verhältnismäßigkeit** hat das vorlegende **Gericht alle Umstände der Rechtssache, mit der es befasst ist**, insbesondere die Dauer der Zuwiderhandlung gegen die die Richtlinie 95/46 durchführenden Vorschriften und die Bedeutung, die der Schutz der verbreiteten Daten für die Betroffenen hat, zu berücksichtigen.“*[28] (Hervorhebung hinzugefügt)

Mit anderen Worten: Die Bewertung der Verhältnismäßigkeit hängt stets vom **Kontext** ab[29]: Wie in diesen Leitlinien näher erläutert wird, kann diese Bewertung nicht durchgeführt werden, ohne zuvor den Kontext der zu prüfenden Maßnahme zu ermitteln (z. B.: *Gibt der für die Verarbeitung Verantwortliche die Informationen zu der betreffenden Person weiter oder gewährt er Zugriff darauf? An wen? Und zu welchem Zweck?*).

Entsprechende Hinweise finden sich im Tenor dieser Leitlinien. Ähnlich wie die Methodik der Kommission zur Folgenabschätzung in Bezug auf Datenschutzfragen zielen die Leitlinien zur Verhältnismäßigkeit im Wesentlichen darauf ab, **dem Gesetzgeber dabei zu helfen, die richtigen Fragen zu stellen**, und zwar unter Berücksichtigung der relevantesten und am häufigsten auftretenden Datenschutzfragen. Die folgende Checkliste in diesen Leitlinien (ein vierstufiges Analyseinstrument) soll ebenfalls zum „Querdenken“ anregen und innovative politische *Ex-ante*-Entscheidungen zur Folge haben und bei der Kontrolle sowie der Ex-post-Bewertung der Maßnahmen helfen.

III. Checkliste für die Beurteilung der Verhältnismäßigkeit neuer Legislativmaßnahmen

1. Allgemeine Beschreibung der Arbeitsabläufe

Die Gesamtbewertung der Notwendigkeit und der Verhältnismäßigkeit (**zusammenfassender Überblick**) läuft wie folgt ab:

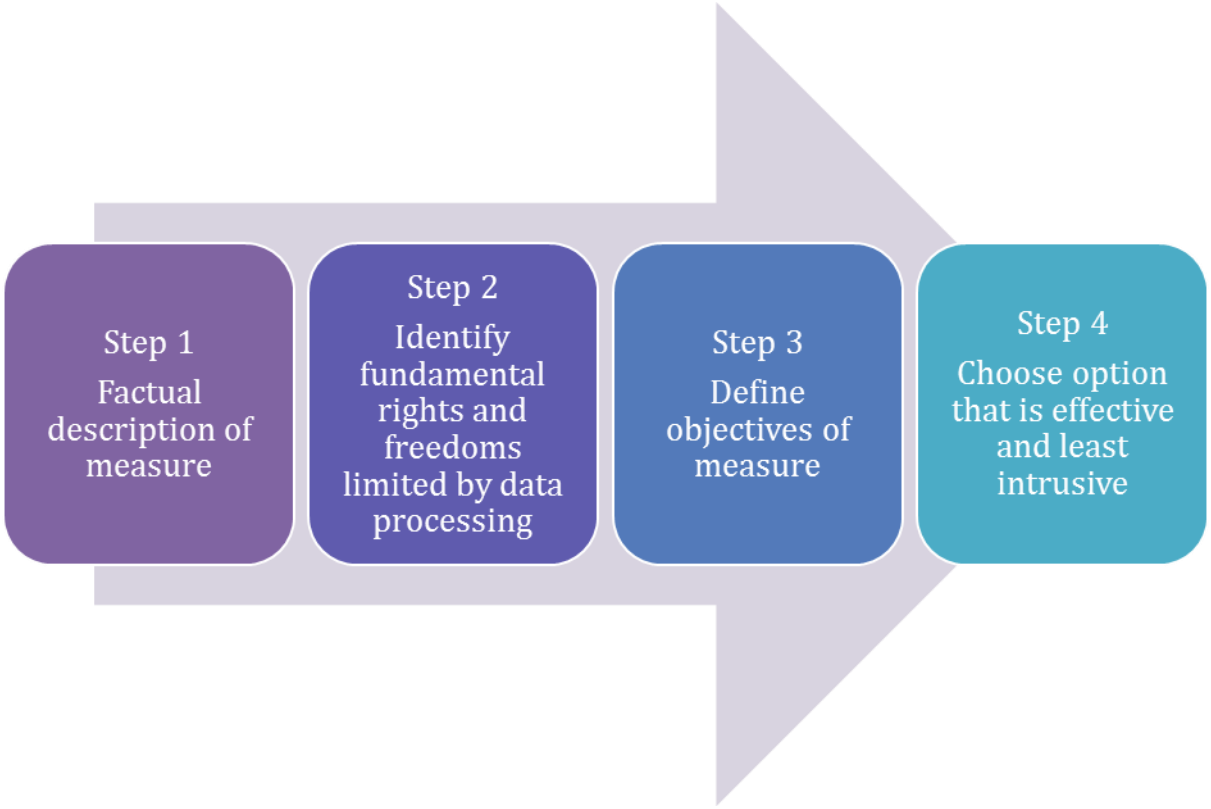
Prüfung 1: In Bezug auf die Erforderlichkeit (Prüfung der Erforderlichkeit) werden im Necessity Toolkit folgende Schritte empfohlen[30]:

[28] EuGH, Rechtssache C-101/01, *Linqvist*, ECLI:EU:C:2003:596, Rn. 89.

[29] Siehe beispielsweise EGMR, *M.K. / Frankreich*, Rn. 46: „Der Gerichtshof ist der Auffassung, dass der beklagte Staat **seinen Ermessensspielraum in dieser Angelegenheit** überschritten hat, da die Bestimmungen, über die Speicherung der Fingerabdrücke von Personen, die verdächtigt werden, Straftaten begangen zu haben, aber nicht verurteilt worden sind, in der umstrittenen Datenbank, **die im vorliegenden auf den Antragsteller angewandt wurden**, kein ausgewogenes Verhältnis zwischen den betreffenden konkurrierenden öffentlichen und privaten Interessen schaffen. Folglich muss die Speicherung der Daten als **unverhältnismäßiger Eingriff** in das Recht des Antragstellers auf Achtung seines Privatlebens angesehen werden und kann in einer demokratischen Gesellschaft nicht als notwendig angesehen werden.“ (Hervorhebung hinzugefügt)

[30] Siehe Seite 9 des EDSB-Necessity Toolkits.

- **Schritt 1** ist einleitender Art; er verlangt **eine detaillierte faktische Darstellung** der vorgeschlagenen Maßnahme und ihres Zwecks, die jeder weiteren 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.
- **Schritt 3** betrachtet das **Ziel der Maßnahme**, 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.**



Step	Schritt
Factual description of measure	Faktische Beschreibung der Maßnahme
Identify fundamental rights and freedoms limited by data processing	Ermittlung von Grundrechten und Grundfreiheiten, die durch die Datenverarbeitung eingeschränkt werden
Define objectives of measure	Festlegung der Ziele der Maßnahme
Choose option that is effective and least intrusive	Wahl der Option, die wirksam ist und den geringsten Eingriff in die Privatsphäre bedeutet

Führt die Beurteilung zu dem Schluss, dass eine Maßnahme dem Erfordernis der Erforderlichkeit Genüge tut (**Prüfung 1**), kann die Maßnahme im Rahmen der Verhältnismäßigkeitsprüfung (**Prüfung 2**) anhand folgender Schritte geprüft werden.

Mit anderen Worten: Wir werden im Rahmen von **Prüfung 2** die als erforderlich bewertete Maßnahme erneut prüfen (was bedeutet, dass es sich hierbei um die Maßnahme handelt, mit der das angestrebte Ziel wirksam und mit dem geringsten Eingriff erreicht werden kann). Außerdem werden wir beurteilen, ob die auf diese Weise verursachte Einschränkung (Eingriff) in einem angemessenen Verhältnis zu dem Ziel steht, das wir erreichen möchten.

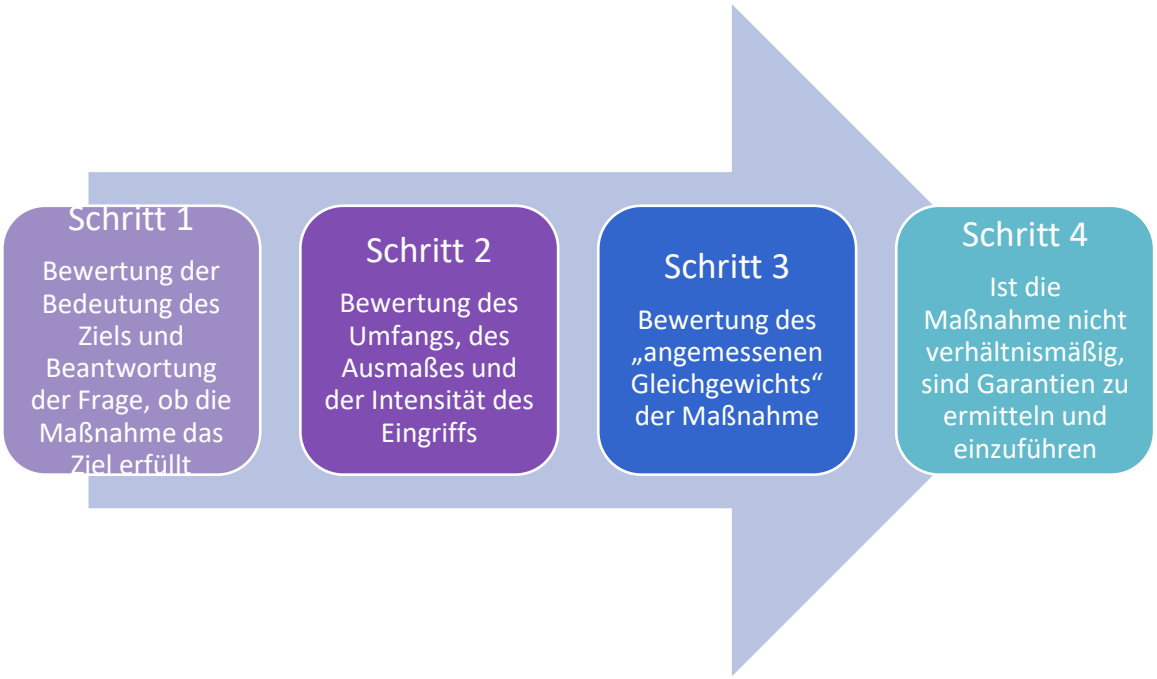
Prüfung 2: In Bezug auf die Verhältnismäßigkeit (Prüfung der Verhältnismäßigkeit) werden folgende Schritte durchgeführt:

- **Schritt 1** (bzw. 5 beider Arbeitsabläufe gemeinsam): Bewertung der **Bedeutung** („**Legitimität**“) **des Ziels** (in Schritt 3 des „Necessity Toolkits“ ermittelt) und Beantwortung der Frage, **ob und inwieweit** die vorgeschlagene Maßnahme dieses Ziel erfüllen und das in der Problemdefinition genannte Problem lösen würde („**tatsächlich** erfüllt“) [dies wäre „der Vorteil/Nutzen“].

- **Schritt 2** (bzw. 6 beider Arbeitsabläufe gemeinsam): Bewertung **des Umfangs, des Ausmaßes und der Intensität** des Eingriffs (in Schritt 2 des „Necessity Toolkits“ ermittelt) im Hinblick auf die Auswirkungen auf die Grundrechte auf Privatsphäre und den Datenschutz [dies wäre(n) „der Nachteil/die Kosten“].

- **Schritt 3** (bzw. 7 beider Arbeitsabläufe gemeinsam): Bewertung des **angemessenen Gleichgewichts (*Vorteil/Nachtteil; Nutzen/Kosten*)** der Maßnahme.

- **Schritt 4** (bzw. 8 beider Arbeitsabläufe gemeinsam): **Eine Entscheidung bezüglich der Maßnahme (durchführbar/nicht durchführbar) treffen**. Wenn das Ergebnis „nicht durchführbar“ lautet, sind unter Berücksichtigung aller Faktoren, die dafür gesorgt haben, dass die Bewertung als unverhältnismäßig eingestuft wurde, Garantien zu ermitteln und (wenn möglich) einzuführen, die dafür sorgen könnten, dass die Maßnahme verhältnismäßig wird.



Step	Schritt
Assess the importance of the objective and whether the measure meets the objective	Bewertung der Bedeutung des Ziels und Beantwortung der Frage, ob die Maßnahme das Ziel erfüllt
Assess the scope, the extend and the intensity of the interference	Bewertung des Umfangs, des Ausmaßes und der Intensität des Eingriffs
Proceed to the ‘fair balance’ evaluation of the measure	Bewertung des „angemessenen Gleichgewichts“ der Maßnahme
If the measure is not proportionate, identify and introduce safeguards	Ist die Maßnahme nicht verhältnismäßig, sind Garantien zu ermitteln und einzuführen

2. Beschreibung der einzelnen Schritte der Verhältnismäßigkeitsprüfung

Schritt 1: Bewertung der Bedeutung („Legitimität“) des Ziels und der Frage, ob und inwieweit die vorgeschlagene Maßnahme dieses Ziel erfüllen würde (Wirksamkeit und Effizienz)

Eine detaillierte Beschreibung des **Zwecks oder der Zwecke** der ins Auge gefassten Maßnahme ist nicht nur **Voraussetzung** für die Prüfung der Verhältnismäßigkeit, sondern sie hilft auch beim Nachweis der Einhaltung der ersten Anforderung von Artikel 52 Absatz 1 der Charta, *also der Qualität des Rechts*.[31]

[31] In den Schlussanträgen des Generalanwalts Mengozzi, ECLI:EU:C:2016:656, Rn. 193 zu dem Entwurf eines Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen heißt es: „*Nach der Rechtsprechung des EGMR verlangt dieser Ausdruck im Wesentlichen, dass die in Rede stehende Maßnahme **zugänglich** und **hinreichend vorhersehbar** ist, also mit anderen Worten klar genug formuliert ist, um jeden hinreichend erkennen zu lassen, unter welchen Umständen und unter welchen*

In der Praxis ist eine *Ex-ante*-Bewertung der Bedeutung des Ziels und der Wirksamkeit der Maßnahme zur Erreichung dieses Ziels nicht möglich, wenn das Gesetz das betreffende Ziel oder die betreffenden Ziele nicht **eindeutig und genau definiert**.

Es ist zu beachten, dass sowohl die **Maßnahme** als auch ihre **Ziele** bereits in den Schritten 1 und 3 der Erforderlichkeitsprüfung (Prüfung 1) **festgelegt** werden sollten. Bei diesem Schritt werden wir diese Ziele erneut prüfen, um – nach wie vor *ex ante*, nun jedoch *konkret* – ihre **Bedeutung** zu ermitteln und festzustellen, inwieweit sie durch die Maßnahme **tatsächlich erfüllt werden**.

In Bezug auf die in der Folgenabschätzung der Kommission verwendete Terminologie geht es hier um die Wirksamkeit *(ist die vorgeschlagene Maßnahme am besten geeignet, um die Ziele zu erreichen?*) und die Effizienz (*Wirkungsgrad*) der Maßnahme (die ermittelte strategische Option) zur Erreichung des Ziels (d. h. zur **Lösung der in der Problemdefinition ermittelten Probleme**).

Die Maßnahmen sollten den **in der Problemanalyse genau bestimmten Erfordernissen** (d. h. den von der Europäischen Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer) Rechnung tragen. Wie der EuGH erklärt hat, muss die **Maßnahme** der **Zielsetzung** „tatsächlich entsprechen", um verhältnismäßig zu sein.[32] Außerdem muss die Zielsetzung die in der Problemanalyse herausgearbeiteten Erfordernisse widerspiegeln.

Bei der Bewertung der Wirksamkeit der Maßnahme muss der Gesetzgeber stets zuerst die Wirksamkeit **bereits bestehender Maßnahmen** überprüfen.[33] Mit anderen Worten: Bevor

---

Voraussetzungen sie den Hoheitsträger ermächtigt, Maßnahmen zu ergreifen, die seine von der EMRK geschützten Rechte beeinträchtigen." (Hervorhebung hinzugefügt)

- In den verbundenen Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, führt Generalanwalt Saugmandsgaard Øe in seinen Schlussanträgen ECLI:EU:C:2016:572, Rn. 139-140 weiter aus: *„Nach dieser Rechtsprechung beinhaltet der Ausdruck „gesetzlich vorgesehen", dass die gesetzliche Grundlage hinreichen zugänglich und vorhersehbar ist, d. h.* ***so genau formuliert ist, dass der Einzelne sein Verhalten, gegebenenfalls nach Einholung sachkundigen Rates, danach richten kann.*** *Diese gesetzliche Grundlage muss auch geeigneten Schutz gegen Willkür bieten und damit den Umfang und die Art und Weise der Ausübung der den zuständigen Behörden verliehenen Befugnis hinreichend klar definieren (Grundsatz der Rechtsstaatlichkeit). Meiner Ansicht nach muss dem in Artikel 52 Absatz 1 der Charta verwendeten Ausdruck „gesetzlich vorgesehen" (...) dieselbe Bedeutung beigemessen werden, wie sie dieser Ausdruck im Zusammenhang mit der EMRK hat."*
Siehe hierzu auch EGMR, *Catt / Vereinigtes Königreich*, 24. Januar 2019, Rn. 6 der übereinstimmenden Stellungnahme von Richter Koskelo und Richter Felici: „**Die allgemeinen Grundsätze des Datenschutzrechts**, z. B. die Forderung, dass die zu verarbeitenden Daten für den Zweck angemessen, relevant und nicht übermäßig sein müssen, **werden verwässert, möglicherweise bis hin zur praktischen Bedeutungslosigkeit, wenn der eigentliche Zweck ohne eine sinnvolle Definition oder Einschränkung bleibt**." (Hervorhebung hinzugefügt)

[32] EuGH, verbundene Rechtssachen C-203/15 und C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, Rn. 94: *„Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen der Ausübung dieser Rechte und Freiheiten nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer* ***tatsächlich entsprechen****."* (Hervorhebung hinzugefügt)

[33] In der Stellungnahme 01/2014 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung (abrufbar unter:https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_de.pdf) erklärt die WP29: „Wie auch immer diese Bewertung durchgeführt wird, sie sollte eine nachweisgeführte Erklärung beinhalten, warum die vorhandenen Maßnahmen für die Erfüllung dieses Bedürfnisses nicht mehr ausreichen."

neue Maßnahmen vorgeschlagen und ergriffen werden, sollte der Gesetzgeber prüfen, ob die „bestehende Maßnahme“ in der Praxis **umgesetzt** wird und ob eine **Ausweitung und/oder Vertiefung** dieser Maßnahme das in der Problemanalyse festgestellte Problem bereits zufriedenstellend lösen würde. Wird die Wirksamkeit bestehender Maßnahmen, die einen ähnlichen oder gleichen Zweck verfolgen, nicht systematisch bewertet, kann die Prüfung der Verhältnismäßig für eine neue Maßnahme nicht als ordnungsgemäß durchgeführt angesehen werden. Bei einer bereits bestehenden Maßnahme muss die Wirksamkeit bei der Abwägung nicht in absoluten Zahlen, sondern im Hinblick auf den Mehrwert der Maßnahme betrachtet werden.

Vorgehensweise

- Die **Erfordernisse** sollten in der Problemanalyse hinreichend beschrieben werden, um ein klares Verständnis dafür zu ermöglichen, *was* genau Auslöser für die Initiative für einen Gesetzgebungsvorschlag war. Der Gesetzgeber muss über vollständige und genaue Informationen über die **zu lösenden Probleme** (die **Ursachen** des Problems) und über die verfügbaren Optionen verfügen.

- Insbesondere sollte sich der Gesetzgeber in Bezug auf das zu lösende Problem (**Problemdefinition**) der Dringlichkeit des **betreffenden öffentlichen Interesses** (z. B. öffentliche Sicherheit) bewusst sein und in der Maßnahme **eindeutig darauf hinweisen** (indem er beispielsweise erklärt, dass mit der Maßnahme einer vorübergehenden hochgradigen Bedrohung begegnet werden soll). Dies ließe sich in folgender Frage zusammenfassen: „Besteht für uns ein *drängendes gesellschaftliches Bedürfnis*, das Recht (auf Privatsphäre und/oder Datenschutz) einzuschränken?“[34]

In der **Stellungnahme 06/2016 zum zweiten Paket „Intelligente Grenzen“ der EU** vom 21. September 2016 (Seite 3) (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_de.pdf) wies der EDSB auf Folgendes hin: „Notwendigkeit und Verhältnismäßigkeit der [EES-Regelung] sind sowohl insgesamt, **unter Berücksichtigung der bereits in der EU bestehenden IT-Großsysteme**, als auch spezifisch, für jeden Einzelfall dieser Drittstaatsangehörigen, zu bewerten, die ja rechtmäßige Besucher der EU sind.“

- In der **Stellungnahme 3/2017 zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)** vom 6. März 2017 (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_de.pdf), machte der EDSB klar, dass (Seite 8): „bei einer Datenschutzfolgenabschätzung des ETIAS **eine Bestandsaufnahme aller auf EU-Ebene ergriffenen Maßnahmen in den Bereichen Migration und Sicherheitsziele vorgenommen und deren konkrete Umsetzung, Wirksamkeit und Auswirkung auf die Grundrechte natürlicher Personen gründlich analysiert werden sollten, bevor neue Systeme geschaffen werden, in denen wieder personenbezogene Daten verarbeitet werden.** Bei dieser Analyse sollte dem Politikbereich, in dem diese Maßnahmen gelten, und der jeweiligen Rolle der wichtigsten beteiligten Akteure Rechnung getragen werden.“

- Siehe **Stellungnahme des EDSB 5/2015 zu dem Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität** (Seite 15): „Der Vorschlag bietet keine umfassende Bewertung dahingehend, inwieweit die derzeitig vorhandenen Instrumente den Zweck der EU-Regelung für PNR-Daten erfüllen können.“

[34]Siehe beispielsweise Entscheidung des EGMR in der Rechtssache *Weber und Saravia / Deutschland*, Rn. 112: „Die Beschwerdeführerin vertrat die Auffassung, dass diese weitreichenden Überwachungsbefugnisse **keinem drängenden gesellschaftlichen Bedürfnis entsprächen**. Die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland seitens eines ausländischen, über Nuklearwaffen verfügenden Staats, die während des „Kalten Krieges“ bestanden habe, sei entfallen Gegenwärtig bestehe keine andere vergleichbare Bedrohung. Insbesondere stellten Drogenhandel, Geldfälschung und Geldwäsche oder die mutmaßlichen Gefahren der organisierten Kriminalität keine so schwere Gefahr für die öffentliche Sicherheit dar, dass sie einen derart intensiven Eingriff in den Telekommunikationsverkehr von Einzelpersonen rechtfertigen würden. Die Tatsache,

- Die Bezugnahme auf das vorgenannte **Ausmaß der Bedrohung** und die Überwachung/Aktualisierung dieser Ursache ermöglichen es dem Gesetzgeber, die Maßnahme zur Einschränkung des Rechts auf Privatsphäre und den Schutz personenbezogener Daten aufzuheben, sobald dieses Ausmaß nachlässt. Ein unabhängiges Aufsichtssystem, um zu verhindern, dass die vorübergehende Maßnahme zu einer dauerhaften wird, ist ebenfalls von entscheidender Bedeutung.

- Es ist wichtig zu prüfen, ob **der konkrete Zweck oder die konkreten Zwecke** der Maßnahme diese Bedürfnisse **widerspiegelt/widerspiegeln**. Dies ließe sich in folgender Frage zusammenfassen: „Entspricht der vorgesehene Zweck diesem Bedürfnis?“ [mit der der Terminologie der Folgenabschätzung ausgedrückt: „*Sorgt die Maßnahme unter Berücksichtigung ihrer Auswirkungen/Konsequenzen für die Lösung des Problems*?“] Die Bejahung dieser Frage würde eine „allmähliche legislative Zweckentfremdung“ vermeiden (d. h. eine Maßnahme, die das Problem nicht wirklich behebt[35], sondern stattdessen einen anderen Zweck verfolgt).

---

dass die Überwachung infolge der Entscheidung des Bundesverfassungsgerichts auf Inhalte von „*nachrichtendienstlicher Relevanz*“ beschränkt sei, sei nicht geeignet, die Überwachungsbefugnisse des Bundesnachrichtendienstes effektiv zu beschränken.“ (Hervorhebung hinzugefügt)
Zum drängenden gesellschaftlichen Bedürfnis siehe **Stellungnahme der WP29 zur Anwendung der Begriffe der Notwendigkeit und der Verhältnismäßigkeit sowie des Datenschutzes im Bereich der Strafverfolgung**, WP211, 27. Februar 2014, Seite 7 und 8. Siehe auch die Liste der zu berücksichtigenden Aspekte auf den Seiten 9-11. Die Stellungnahme ist abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_de.pdf.

[35] Siehe **Reflexionspapier zur Interoperabilität von Informationssystemen im Raum der Freiheit, der Sicherheit und des Rechts** vom 17. November 2017 (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_de_0.pdf), in dem der EDSB feststellte, dass die Kommission „ferner eindeutig festlegen sollte, **für welche konkreten Zwecke** welche Kategorien personenbezogener Daten im Rahmen ihrer künftigen Initiativen für Interoperabilität verarbeitet werden sollen. Damit wäre auch eine geordnete Debatte über Interoperabilität aus der Grundrechtsperspektive möglich.“ (Seite 3)
Zum selben Thema siehe **Stellungnahme 4/2018 des EDSB zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Großsystemen der EU** vom 16. April 2018, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/18-04-16_edps-opinion-on-interoperability_de.pdf.
41. Der EDSB unterstreicht, dass „Bekämpfung irregulärer Migration und Gewährleistung eines hohen Maßes an Sicherheit“ eine sehr vage Beschreibung von (ansonsten legitimen) Zwecken ist (Seite 12). Er merkt an, dass Artikel 20 den Erlass einer nationalen Rechtsvorschrift verlangt, in der diese näher bestimmt werden. Er erinnert jedoch daran, dass der Gerichtshof der Europäischen Union („EuGH“) in seinem Urteil in Digital Rights Ireland (Rn. 62) befand, dass die Richtlinie 2006/24 *„kein objektives Kriterium vorsieht, das es ermöglicht, den Zugang der zuständigen nationalen Behörden zu den Daten und deren spätere Nutzung zwecks Verhütung, Feststellung oder strafrechtlicher Verfolgung auf Straftaten zu beschränken“*, weil sie *„lediglich allgemein auf die von jedem Mitgliedstaat in seinem nationalen Recht bestimmten Straftaten Bezug nimmt“.* Der Gerichtshof vertrat ferner die Auffassung, der Zugang zu diesen Daten und deren spätere Nutzung sei nicht *„strikt auf die Zwecke der Verhütung und Feststellung genau abgegrenzter schwerer Straftaten oder der sie betreffenden Strafverfolgung“* beschränkt.
42. **Nach Auffassung des EDSB sind die Zwecke der Bekämpfung irregulärer Migration und des Beitrags zu einem hohen Maß an Sicherheit vor dem Hintergrund von Artikel 20 zu breit gefasst und erfüllen in den Vorschlägen nicht die Vorgaben des Gerichtshofs, „*strikt beschränkt*“ und „*genau abgegrenzt*“ zu sein. Er empfiehlt daher, sie in den Vorschlägen genauer zu definieren**. „Irreguläre Migration“ könnte beispielsweise auf die Einreise- und Aufenthaltsbedingungen verweisen, wie sie in Artikel 6 der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates festgelegt sind. Mit Blick auf die Sicherheit empfiehlt der EDSB, auf die Straftaten abzuheben, die ein hohes Maß an Sicherheit besonders bedrohen könnten; hier könnte beispielsweise auf die in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI aufgelisteten Straftaten verwiesen werden,

- Prüfen Sie, ob der im Gesetzgebungsvorschlag verankerte **Zweck (**das **Ziel)** mit dem **öffentlichen/gesellschaftlichen Regelungsbedarf** in Einklang steht, dem begegnet werden soll (der Schaden, dem die Gesellschaft möglicherweise ausgesetzt ist, wenn die Maßnahme nicht ergriffen wird, z. B. weit verbreitete allgemeine Kriminalität oder konkrete Wirtschaftskriminalität).

Wir erinnern daran, dass die **Ziele** laut der Folgenabschätzung der Kommission nach der **SMART**-Formel formuliert werden müssen, d. h. sie müssen **spezifisch** (ausreichend präzise und konkret); **messbar** (Soll-Zustand ist in messbarer Form anzugeben, z. B. Rückgang der Straftaten wird auf ... % geschätzt); **erreichbar**; **realistisch**; und **zeitgebunden** (bezogen auf einen festen Termin oder Zeitraum, bis zu dem die Ergebnisse erreicht werden sollen) sein. Diese Anforderungen, die für die Methode der besseren Rechtsetzung gelten, sind, wie die Beispiele zeigen werden, besonders wichtig, wenn Regelungen den Schutz personenbezogener Daten einschränken oder anderweitig beeinträchtigen.

- Bewerten Sie die **Bedeutung** des Ziels (Soll damit ein verfassungsrechtlicher Wert oder ein Grundrecht geschützt werden?).[36]

- Bewerten Sie die **Wirksamkeit und Effizienz** der Maßnahme zur Erreichung des vorgenannten Ziels.

Sachdienliche Beispiele

Zur Veranschaulichung dieser **Methodik analysieren** wir in den vier grauen Kästen insbesondere die Urteile des EuGH in den Rechtssachen *Tele2* und *Ministerio Fiscal*, die Schlussanträge des Generalanwalts und das Gutachten 1/15 des EuGH zum Abkommen zwischen der EU und Kanada zur Übermittlung von Fluggastdatensätzen (im Folgenden „PNR“) sowie das Urteil des EuGH in der Rechtssache *Bevándorlási és Állampolgársági Hivatal* und geben Beispiele für jeden der vier Schritte.

BEISPIEL 1: Tele2 Sverige AB (EuGH, C-203/15, ECLI:EU:C:2016:970)

Der Gerichtshof **beschrieb die Ziele** der zu prüfenden Maßnahme (kurz: eine Verpflichtung zur Speicherung von Verkehrs- und Standortdaten) wie folgt: „*Artikel 15 Absatz 1 Satz 1 der Richtlinie 2002/58 sieht vor, dass die in dieser* ***Bestimmung*** *genannten Rechtsvorschriften, die vom Grundsatz der Vertraulichkeit von Kommunikationen und der damit verbundenen Verkehrsdaten abweichen, „die* ***nationale Sicherheit (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen*** *“ zum Ziel haben müssen oder einen der anderen Zwecke verfolgen müssen, die in* ***Artikel 13 Absatz 1*** *der Richtlinie*

sofern sie nach nationalem Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind.“

[36] Ein **Überblick über die in der Charta gewährleisteten Rechte, Freiheiten und Grundsätze** findet sich in Anhang II, Seite 28 der Arbeitsunterlage der Kommissionsdienststellen, Operative Leitlinien zur Berücksichtigung der Grundrechte in Folgenabschätzungen der Kommission, SEC (2011) 567 final.

95/46, auf den Artikel 15 Absatz 1 Satz 1 der Richtlinie 2002/58 verweist, genannt sind (...). Hierbei handelt es sich um eine ***abschließende Aufzählung*** *der Zwecke, wie aus Artikel 15 Absatz 1 Satz 2 der Richtlinie 2002/58 hervorgeht, wonach die Rechtsvorschriften aus den in Artikel 15 Absatz 1 Satz 1 dieser Richtlinie „aufgeführten Gründen" gerechtfertigt sein müssen. Die Mitgliedstaaten* ***dürfen demnach solche Vorschriften nicht zu anderen als den in Artikel 15 Absatz 1 Satz 1 der Richtlinie 2002/58 aufgezählten Zwecken erlassen***." (Hervorhebung hinzugefügt) Zwar ist die **Bedeutung** des Ziels (Schutz der öffentlichen Sicherheit und Durchsetzung des Strafrechts) in diesem Fall offensichtlich, doch räumte der Gerichtshof auch ein, dass die Maßnahme die Möglichkeiten zur Nutzung moderner Ermittlungstechniken und damit „*die* ***Wirksamkeit*** *der Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus*" verbessern würde. (Hervorhebung hinzugefügt)

BEISPIEL 2: Ministerio Fiscal (EuGH, C-207/16, ECLI:EU:C:2018:788)

Im Hinblick auf die **Bedeutung der Zielsetzung** stellte der Gerichtshof fest, dass **die Zielsetzung** der Maßnahme auf die ***„Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten im Allgemeinen"*** (in diesem Fall auf den Diebstahl einer Brieftasche und eines Mobiltelefons) und nicht auf die Bekämpfung einer „schweren Straftat" beschränkt ist. Daher kann argumentiert werden, dass der Gerichtshof das „Ausmaß" der Bedeutung der Zielsetzung als relativ **gering** erachtete.

In Bezug auf die **Wirksamkeit der Maßnahme** zum Erreichen des vorgenannten Ziels stellte der Gerichtshof fest, dass die Kriminalpolizei im Rahmen der zu prüfenden Maßnahme „*für die Zwecke strafrechtlicher Ermittlungen um gerichtliche Erlaubnis zum* ***Zugang zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten ersucht****, (...)* ***um die Identität der Inhaber von SIM-Karten festzustellen, die in einem Zeitraum von zwölf Tagen mit der IMEI des gestohlenen Mobiltelefons aktiviert wurden****." „Mit den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Zugangsantrag bezieht (...),* ***kann nur eine Verbindung zwischen der SIM-Karte oder den SIM-Karten, die mit dem gestohlenen Mobiltelefon aktiviert wurden, und der Identität der Inhaber dieser SIM-Karten (auf dem gestohlenen Telefon aktiviert) während eines bestimmten Zeitraums hergestellt werden****. Es liegt daher auf der Hand, dass die Maßnahme* ***wirksam*** *wäre, um den Dieb oder einen Käufer des Telefons (falls er sich entschied, das Telefon zu nutzen und eine SIM-Karte darauf installierte) ausfindig zu machen und so direkt oder indirekt über weitere und auf diese Weise ermöglichte Ermittlungen den Täter zu identifizieren.*" (Hervorhebung hinzugefügt)

BEISPIEL 3: „PNR-Abkommen EU-Kanada" (Schlussanträge des Generalanwalts, ECLI:EU:C:2016:656 und Gutachten 1/15 des EuGH, ECLI:EU:2017:592)

In Rn. 205 seiner Schlussanträge erkannte Generalanwalt Mengozzi sowohl die **Bedeutung des Ziels** als auch **die Wirksamkeit** der Maßnahme zur Erreichung dieses Ziels an: „*Ich denke, dass nichts wirklich dagegen spricht, anzuerkennen, dass der mit dem geplanten Abkommen verbundene Eingriff* ***zur Erreichung des von ihm verfolgten Ziels der öffentlichen Sicherheit,*** *insbesondere der Bekämpfung des Terrorismus und der grenzübergreifenden schweren Kriminalität, geeignet ist. Wie nämlich insbesondere die Regierung des Vereinigten Königreichs und die Kommission geltend gemacht haben, bietet die Übermittlung von PNR-Daten zum Zweck einer Analyse und Speicherung den kanadischen Behörden zusätzliche Möglichkeiten zur Erkennung von bis dahin unbekannten und nicht verdächtigten Fluggästen, die Verbindungen zu anderen, in ein Terroristennetz einbezogenen oder an grenzübergreifender schwerer Kriminalität beteiligten Personen und/oder Fluggästen haben könnten. Diese Daten stellen, wie die von der Regierung des Vereinigten Königreichs und der Kommission übermittelten* ***Statistiken*** *über die frühere Praxis der kanadischen Behörden* ***veranschaulichen****,* ***nützliche Mittel für strafrechtliche Ermittlungen dar****, die insbesondere im Hinblick auf die vom geplanten Abkommen geschaffene polizeiliche Zusammenarbeit auch zur Verhinderung und Aufdeckung einer terroristischen Straftat oder grenzübergreifender schwerer Kriminalität innerhalb der Union beitragen können."* (Hervorhebung hinzugefügt)

Der Gerichtshof berücksichtigte die **bereits bestehenden Maßnahmen** und kam zu dem Schluss, dass die bereits verfügbaren Daten „***nicht hinreichend** sind, um das vom geplanten Abkommen verfolgte Ziel der öffentlichen Sicherheit ebenso wirksam zu erreichen*". (Hervorhebung hinzugefügt)

BEISPIEL 4: *Bevándorlási és Állampolgársági Hivatal* (EuGH, C-473/16, ECLI:EU:C:2018:36)

In diesem Fall handelt es sich bei der zu prüfenden Maßnahme um die Erstellung und Verarbeitung eines **psychologischen Gutachtens** über die sexuelle Orientierung einer Person, die gemäß der Richtlinie 2011/95 die Flüchtlingseigenschaft beantragt. Der Gerichtshof erkannte an, dass **das Ziel** der Maßnahme darin besteht, „*die Suche nach Anhaltspunkten zu rechtfertigen, die eine Einschätzung ermöglichen, inwieweit der Antragsteller tatsächlich internationalen Schutzes bedarf*".

Der Gerichtshof stellte außerdem fest, dass „*ein Gutachten wie das im Ausgangsverfahren streitige nur dann **als geeignet erachtet** werden kann, wenn es sich auf Methoden und Grundsätze stützt, die nach den von der internationalen Wissenschaftsgemeinschaft anerkannten Normen als hinreichend zuverlässig gelten*". (Hervorhebung hinzugefügt)

Zur **Wirksamkeit** der Maßnahme bei der Erreichung des vorgenannten Ziels stellte der Gerichtshof jedoch fest: „*Es **kann nicht davon ausgegangen werden, dass ein solches Gutachten unverzichtbar ist**, um die Aussagen einer um internationalen Schutz nachsuchenden Person zu ihrer sexuellen Orientierung zu bestätigen und damit über einen Antrag auf internationalen Schutz, der mit der Furcht vor Verfolgung wegen dieser Orientierung begründet wird, befinden zu können*." (Hervorhebung hinzugefügt)

Insbesondere befand der Gerichtshof, dass: „*wenn die Mitgliedstaaten den Grundsatz anwenden, wonach der Antragsteller seinen Antrag auf internationalen Schutz begründen muss, dessen Aussagen zu seiner sexuellen Orientierung, für die Unterlagen oder sonstige Beweise fehlen, **keines Nachweises bedürfen, wenn die in dieser Vorschrift genannten Voraussetzungen erfüllt sind, die insbesondere auf die Kohärenz und die Plausibilität dieser Aussagen abstellen** und **in keiner Weise auf die Erstellung oder Verwendung eines Gutachtens Bezug nehmen***". (Hervorhebung hinzugefügt)

„*Selbst wenn ein auf projektive Persönlichkeitstests gestütztes Gutachten wie das im Ausgangsverfahren streitige **dazu beitragen könnte**, mit einiger Zuverlässigkeit die sexuelle Orientierung zu bestimmen, ergibt sich im Übrigen aus den Ausführungen des vorlegenden Gerichts, dass **die Ergebnisse eines solchen Gutachtens lediglich geeignet sind, ein Abbild dieser sexuellen Orientierung zu liefern**. Diese Ergebnisse vermitteln somit allenfalls **ein ungefähres Bild und sind daher für die Beurteilung der Aussagen** einer um internationalen Schutz nachsuchenden Person **nur von begrenztem Interesse**, insbesondere wenn diese Aussagen wie im Ausgangsverfahren keine Widersprüche aufweisen*." (Hervorhebung hinzugefügt)

BEISPIEL 5: Stellungnahme 3/2017 des EDSB zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)

Es ist möglich, dass der Gesetzgeber **das Ziel** der Maßnahme auch als „**zu vermeidendes Risiko**" bezeichnet. Wie vom EDSB betont, sollten auch in diesem Fall die Risiken soweit wie möglich definiert werden. „Gemäß Artikel 1 des Vorschlags dient das ETIAS der Feststellung, ob mit der Anwesenheit eines von der Visumpflicht befreiten Reisenden im Hoheitsgebiet der Mitgliedstaaten ein **Risiko irregulärer Migration oder ein Risiko für die Sicherheit oder die öffentliche Gesundheit verbunden ist**. Der EDSB weist darauf hin, dass der Vorschlag das **Risiko für die öffentliche Gesundheit** durch eine Aufzählung spezifischer Kategorien von Krankheiten **definiert**, aber **Risiken für die Sicherheit oder durch irreguläre Migration nicht definiert**." (Hervorhebung hinzugefügt)

Schritt 2: Bewertung des Eingriffs (dessen Umfang, Ausmaß und Intensität) im Hinblick auf die tatsächlichen Auswirkungen der Maßnahme auf die Grundrechte auf Privatsphäre und Datenschutz

Der andere wichtige Schritt bei der Prüfung der Verhältnismäßigkeit besteht darin, eine eingehende Bewertung dahingehend durchzuführen, inwieweit die geplante Maßnahme in die Grundrechte auf Privatsphäre und Datenschutz eingreift.

Es sei darauf hingewiesen, dass die durch die Maßnahme **eingeschränkten Grundrechte und -freiheiten** bereits in Schritt 2 der Erforderlichkeitsprüfung (Prüfung 1) **ermittelt** wurden. Im vorliegenden Schritt werden wir diese Grundrechte und -freiheiten erneut prüfen, um nach wie vor *ex ante*, nun jedoch *konkret*, zu ermitteln und festzustellen, inwieweit sie betroffen wären. Denn wie im Handbuch der FRA „Die Anwendung der Charta der Grundrechte der Europäischen Union im Rechtswesen und bei der Politikgestaltung auf nationaler Ebene – Leitlinien" erwähnt, „*sollte die Maßnahme den von der Einschränkung betroffenen Personen im Verhältnis zum verfolgten Ziel keine* ***unverhältnismäßige und übermäßige Belastung*** *aufbürden*".[37]

Es sei darauf hingewiesen, dass die Auswirkungen **für die betroffene Person gering** sein können, für das **Kollektiv/die Gesellschaft insgesamt** jedoch **erheblich bzw. äußerst erheblich** (**Auswirkungen auf den Einzelnen** *vs.* **Auswirkungen auf die Gesellschaft insgesamt**).[38]

Die **Kosten** der Maßnahme, die sich auf die Privatsphäre auswirkt, zeigen sich in diesem Zusammenhang durch die **Externalitäten** des mangelnden Datenschutzes (die „Datenverschmutzung"). Hypothetische Beispiele für solche Externalitäten sind: Schaden für den Wahlprozess und den politischen Prozess (Missbrauch von Daten zur politischen Manipulation) [39] ; unrechtmäßige Profilerstellung und Diskriminierung, die Misstrauen gegenüber öffentlichen Behörden hervorrufen; „abschreckende Wirkung" auf die Meinungsfreiheit durch eine allumfassende Überwachungsmaßnahme[40] oder andere negative

---

[37] Vorgenanntes Handbuch der FRA, S. 76 Siehe auch EuGH, Rechtssache C-258/14, *Eugenia Florescu u. a. / Casa Judeţeană de Pensii Sibiu u. a.*, ECLI: EU:2017:448, Rn. 58.

[38] Siehe Omri Ben-Shahar, *Data Pollution*, University of Chicago, Juni 2018, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231 Siehe Seite 3: „Das Datenschutzparadigma basiert auf der Prämisse, dass die Verletzung personenbezogener Daten von privater Natur ist – das „Kernselbst" betrifft –, obwohl diese äußerst privaten Verletzungen durch reine Anhäufung (oder durch differenziertere Kanäle) auch Auswirkungen auf die Gesellschaft haben" und Seite 4: „In der Literatur wurden sämtliche Aspekte der durch die Datenerfassung verursachten privaten Schäden sowie die möglichen Verletzungen der Privatsphäre der Personen, deren Daten erfasst werden, untersucht. Das **Externalitätenproblem** wurde jedoch gänzlich vernachlässigt: Wie wirkt sich die Beteiligung von Menschen an Datenerfassungsdiensten auf **Mitmenschen und die gesamte Öffentlichkeit** aus?"

[39] Siehe Stellungnahme des EDSB zu Online-Manipulation, auf die in Fußnote 42 verwiesen wird.
ICO, "*Democracy disrupted? Personal information and political influence*", 11. Juli 2018, abrufbar unter: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf.
Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: *Action Plan against Disinformation* (JOIN(2018) 36 final), abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zur „Gewährleistung freier und fairer Europawahlen", abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018DC0637&from=EN

[40] In seinen Schlussanträgen, ECLI:EU:C:2013:845, in der Rechtssache *Digital Rights* verwies Generalanwalt Cruz Villalón auf diese abschreckende Wirkung: „*(...) darf (...) nicht vernachlässigt werden, dass das diffuse Gefühl des Überwachtwerdens, das die Umsetzung der Richtlinie 2006/24 erzeugen kann, geeignet ist,*

Auswirkungen auf die Freiheit der Personen, die sich aus einem allgegenwärtigen und systemisch implementierten Profilerstellungs- und Bewertungssystem ergeben[41].

Auch wenn diese Externalitäten in der Praxis schwer zu quantifizieren sind[42], sind sie vom Gesetzgeber bei der Bewertung der „Datenschutzkosten" der Maßnahme zu berücksichtigen.

Im Falle einer vorgeschlagenen Überwachungsmaßnahme ist zu bewerten, **wie stark einschneidend** eine Überwachungsmethode ist. Für diese Bewertung sind die **Dimensionen der Überwachung** zu bewerten. In der einschlägigen Rechtsprechung des EGMR und des EuGH wurden Überwachungsdimensionen festgelegt, angefangen bei der „Dimension der Sinne" (z. B. Audio- und Videoaufzeichnung)[43] bis hin zu den Möglichkeiten zur Analyse, Zusammenführung und Übermittlung der Informationen. Das **Ausmaß des Eingriffs in das Privatleben** der Zielpersonen sowie der mögliche Eingriff in das Privatleben **Dritter** muss von den Behörden, die über die Maßnahme entscheiden, sorgfältig geprüft werden.

Die Auswirkungen dieses Schritts beziehen sich auch auf die möglicherweise schädlichen Folgen der Maßnahme, **die über den Schutz der Privatsphäre hinausgehen** und schließen daher die Risiken für andere Grundrechte ein. Dies entspricht dem Ansatz des EDSB, der ausdrücklich und mehrfach auf die „Risiken für die Rechte und Freiheiten natürlicher Personen" verweist und damit die Tatsache unterstreicht, dass eine negative Auswirkung auf das Recht auf Privatsphäre oft **untrennbar** mit der Verletzung **anderer Grundrechte** wie dem Recht auf **freie Meinungsäußerung, Freizügigkeit,**

Vereinigungsfreiheit[44] und allgemeiner Grundsätze des EU-Rechts wie dem **Grundsatz der**

---

entscheidenden Einfluss auf die Ausübung der Freiheit der Meinungsäußerung und der Informationsfreiheit durch die Unionsbürger auszuüben, und dass folglich auch ein Eingriff in das durch Art. 11 der Charta garantierte Recht vorliegt" (Rn. 52); „*Die Erhebung dieser Daten schafft die Voraussetzungen für eine Überwachung, die, auch wenn sie nur vergangenheitsbezogen bei ihrer Auswertung erfolgt, das Recht der Unionsbürger auf das Geheimnis ihres Privatlebens gleichwohl während der gesamten Dauer der Vorratsspeicherung permanent bedroht. Aufgrund des erzeugten diffusen Gefühls des Überwachtwerdens stellt sich die Frage nach der Dauer der Vorratsdatenspeicherung in besonders eindringlicher Weise*." (Rn. 72)
Der EuGH bestätigte den Ansatz des Generalanwalts und erklärte in Rn. 37 des Urteils, dass: *„(...) der Umstand, dass die Vorratsspeicherung der Daten und ihre spätere Nutzung vorgenommen werden, ohne dass der Teilnehmer oder der registrierte Benutzer darüber informiert wird, geeignet ist, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist*".

[41] In Bezug auf die hypothetischen Beispiele, siehe H.J. Pandit, D. Lewis, *Ease and Ethics of User Profiling in Black Mirror*, 2018, abrufbar unter: https://dl.acm.org/citation.cfm?id=3191614. Siehe als Beispiel für ein Modell zur Folgenabschätzung: „Ethics Canvas", Seite 1582.

[42] Siehe Seite 31 des Artikels *Data Pollution* aus Fußnote 38: „Datenexternalitäten sind häufig qualitativ und beruhen auf Vermutungen. Wie hoch sind die Kosten für verzerrte Ergebnisse bei Präsidentschaftswahlen? Für diskriminierendes rassistisches Profiling?".

[43] In der Rechtssache *Uzun / Deutschland* erachtete der EGMR die Verwendung eines GPS-Geräts zur Standortbestimmung als weniger einschneidende Maßnahme als das Abhören des gesprochenen Worts.
- Zur **Videoüberwachung** (CCTV) siehe **Leitlinien des EDSB zur Videoüberwachung** vom 17. März 2010, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_de.pdf.

[44] Der EDSB plädiert für einen breiter angelegten Ansatz für den Datenschutz, der diese Verbindungen berücksichtigt. Siehe insbesondere **Stellungnahme 3/2018 des EDSB zu Online-Manipulation und personenbezogenen Daten**, S. 13. „Die Privatsphäre und der Schutz personenbezogener Daten gehören zu den „Freiheiten" der EU, zu denen die **Gedanken-, Gewissens- und Religionsfreiheit**, **die Meinungs- und Informationsfreiheit** sowie die **Versammlungs- und Vereinigungsfreiheit** gehören (Artikel 10, 11 und 12). Diese **stehen ebenfalls eindeutig auf dem Spiel**, da die wichtigsten Plattformvermittler die Verbreitung von Informationen entweder erleichtern oder behindern können. Zum Beispiel werden Inhalte, die nicht von einer Internet-Suchmaschine gelistet oder hoch eingestuft werden, mit geringerer Wahrscheinlichkeit ein großes Publikum erreichen oder überhaupt gesehen werden. Alternativ kann ein Suchalgorithmus auch auf bestimmte Arten von Inhalten oder Anbieter von Inhalten ausgerichtet sein, wodurch die Gefahr besteht, dass damit

„Nichtdiskriminierung“[45] verbunden ist. In diesem Sinne verfolgen diese Leitlinien einen „Grundrechtsansatz“.

Vorgehensweise

Die Auswirkungen sollten hinreichend beschrieben werden, um ein klares Verständnis für **die Tragweite, den Umfang und das Ausmaß des Eingriffs** in die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten zu ermöglichen. Besonders wichtig ist es, Folgendes genau zu ermitteln:

- **die Auswirkung[46],** wobei Folgendes zu berücksichtigen ist:

---

verbundene Werte wie Medienpluralismus und Vielfalt beeinträchtigt werden“ und Seite 5: „Die EU-Rechtsvorschriften über den Datenschutz und die Vertraulichkeit der elektronischen Kommunikation gelten für die Datenerhebung, die Profilerstellung und das Mikrotargeting und **sollten bei ordnungsgemäßer Durchsetzung dazu beitragen, den Schaden** durch Versuche, Einzelpersonen und Gruppen zu manipulieren, **zu minimieren**.“ Die Stellungnahme ist abrufbar unter:
https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_de.pdf.

[45] So stellte beispielsweise der Meijers-Ausschuss am 19. Februar 2018 in seiner „Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) vom 12. Dezember 2017, KOM (2017) 794“ die Überschneidung zwischen der **Einschränkung der Privatsphäre** (Erhebung und Verarbeitung personenbezogener Daten, die sich auf eine Gruppe/Personenkategorie beziehen) **und der Verletzung des Grundsatzes der Nichtdiskriminierung** fest. Siehe Seite 3 der Stellungnahme: „Das ausdrückliche Ziel des Vorschlags, die Identitätsprüfungen von Drittstaatsangehörigen durch Polizeibehörden innerhalb des EU-Hoheitsgebiet zu erleichtern, um festzustellen, ob Informationen über diese Person in einer oder mehreren EU-Datenbanken gespeichert sind, wird die Möglichkeit verbessern, dass Drittstaatsangehörige (oder solche, die als Drittstaatsangehörige gelten) für Identitätsprüfungen angehalten werden. In diesem Zusammenhang erinnert der Meijers-Ausschuss an die Rechtssache *Huber / Deutschland*, in der sich der EuGH mit der **unterschiedlichen Behandlung von Staatsangehörigen und Unionsbürgern mit Wohnsitz in Deutschland** im Hinblick auf die **zentrale Speicherung und Mehrfunktionalität personenbezogener Daten in einer Ausländerbehörde, einschließlich die Verwendung zu Strafverfolgungszwecken** befasst hat (EuGH *Huber / Deutschland*, C-524/06, 16. Dezember 2008, Rn. 78-79).“

[46] Die Folgenabschätzung, auf die in diesen Leitlinien Bezug genommen wird, berücksichtigt den **kontextabhängigen datenschutzrechtlichen Schaden und das Schadensrisiko, die sich möglicherweise aus der Bewertung des Ziels der legislativen Maßnahme für die betroffenen Personen und für die gesamte Gesellschaft ergeben**. Daher unterscheidet sie sich (ist allgemeiner) von der Idee der „**unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen**“ von der in Artikel 24 DSGVO die Rede ist.
Ein weiterer Unterschied zur **Datenschutz-Folgenabschätzung** (DSFA) gemäß Artikel 35 DSGVO besteht darin, dass wir in diesen Leitlinien auf die „abstraktere Ebene“ der Bewertung der Verhältnismäßigkeit *der legislativen Maßnahme* Bezug nehmen (und nicht auf eine von einem für die Verarbeitung Verantwortlichen vorgesehene *Form der Verarbeitung*). Dementsprechend könnte die Verhältnismäßigkeit als „*DSFA im Rahmen des Gesetzes*“ angesehen werden (die im Rahmen der beratenden Funktion bei legislativen Maßnahmen, die sich auf das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten auswirken, durchzuführen ist).
Dennoch kann es sinnvoll sein, darauf hinzuweisen, dass **viele der Faktoren, die für die Durchführung der DSFA relevant sind, auch für die Bewertung der Datenschutzkosten einer legislativen Maßnahme relevant sind**.
Siehe diesbezüglich **WP29, jetzt Leitlinien des EDSA zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“**, WP248, zuletzt überarbeitet und angenommen am 4. Oktober 2017, abrufbar unter:
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
Auf die folgenden neun Faktoren (zur Feststellung hoher Risiken) wird auf den Seiten 10-12 hingewiesen: (i) **Bewerten oder Einstufen**, darunter das Erstellen von Profilen und Prognosen; (ii) **Automatisierte Entscheidungsfindung** mit Rechtswirkung oder ähnlich bedeutsamer Wirkung; (iii) **Systematische Überwachung**; (iv) **Vertrauliche Daten** oder höchst persönliche Daten; (v) Datenverarbeitung in **großem**

- *der **Umfang*** der Maßnahme: Ist sie hinreichend begrenzt? *Anzahl der betroffenen Personen*; ob sie „***kollaterale** Eingriffe*“ zur Folge hat, d. h. Eingriffe in die Privatsphäre von Personen, die eigentlich nicht Gegenstand der Maßnahme sind[47];

- *die **Tragweite**: Wie wird das Recht eingeschränkt? Menge der erfassten Informationen; für wie lange; ob die zu prüfende Maßnahme die Erhebung und Verarbeitung besonderer Datenkategorien erfordert*[48];

- *das **Ausmaß der Eingriffe*** unter Berücksichtigung: *der Art der Tätigkeit*, die Gegenstand der Maßnahme ist (ob sie Tätigkeiten betrifft, die unter die Geheimhaltungspflicht fallen oder nicht, Anwalt-Mandanten-Beziehung;

Umfang; (vi) **Abgleichen oder Zusammenführen** von Datensätzen; (vii) Daten zu **schutzbedürftigen Betroffenen**; (viii) Innovative Nutzung oder Anwendung **neuer technologischer oder organisatorischer Lösungen,** wie etwa die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle usw.; (ix) Fälle, in denen die Verarbeitung an sich „**die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert**“. In Anlage I der Leitlinien finden sich **branchenspezifische** Rahmenbestimmung, beispielsweise „**Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme**“, abrufbar unter: http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.
Siehe insbesondere die Seiten 27-31 zur **Identifizierung, Quantifizierung (Schwere und Wahrscheinlichkeit) und Bewertung** des „Risikos“.
- Siehe abschließend den **Entwurf der Liste der zuständigen Aufsichtsbehörde**(n) **bezüglich der Verarbeitungen, für die eine Datenschutz-Folgenabschätzung erforderlich sind (Artikel 35.4 DSGVO),** abrufbar unter: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_de

[47] Siehe *Big Brother Watch u. a. / Vereinigtes Königreich*, EGMR, 13. September 2018, Rn. 2.43: „2.43. Unter **kollateralem Eingriff** versteht man das Einholen von Informationen über Personen, die nichts mit der Ermittlung zu tun haben. Die Berücksichtigung kollateraler Eingriffe ist Teil der Überlegungen zur Verhältnismäßigkeit und gewinnt bei der Beantragung von Verkehrsdaten oder Dienstnutzungsdaten zunehmend an Bedeutung. Anträge sollten Informationen darüber enthalten, **welche kollateralen Eingriffe auftreten könnten und wie sich die angefragten Zeiträume auf die kollateralen Eingriffe auswirken**. Wenn **keine nennenswerten Risiken für kollaterale Eingriffe** bestehen, z. B. bei der Beantragung von Teilnehmerinformationen der Person, gegen die ermittelt wird, **ist darauf hinzuweisen, dass keine Risiken für kollaterale Eingriffe bestehen**.“ (Hervorhebung hinzugefügt)

[48] Siehe EuGH, verbundene Rechtssachen C-465/00, C-138/01 und C-139/01, *Rechnungshof*, ECLI:EU:C:2003:294, Rn. 52: *„Die österreichische Regierung macht insbesondere geltend, im Rahmen der Verhältnismäßigkeitsprüfung sei auch zu berücksichtigen, **wie stark** der Bezug der Daten zum Privatleben sei. So seien Daten, die den **intimsten Kern der Person, die Gesundheit, das Familienleben oder die Sexualität** beträfen, in stärkerem Maße schutzwürdig als Einkommens- und Steuerdaten, die zwar ebenfalls personenbezogen seien, aber in geringerem Maße die Identität der Person beträfen und insofern weniger sensibel seien.“* (Hervorhebung hinzugefügt)
- Zur Verarbeitung von **Gesundheitsdaten**, siehe **Stellungnahme 3/2017 des EDSB zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)**, Seite 13: „Der EDSB bezweifelt, dass eine Verarbeitung dieser besonders sensiblen Datenkategorie in so großem Maßstab und über diesen Zeitraum den Vorgaben von Artikel 52 Absatz 1 der Charta genügt und folglich als erforderlich und verhältnismäßig betrachtet werden kann. Der EDSB stellt die Relevanz der im Vorschlag vorgesehenen Erhebung und Verarbeitung von Gesundheitsdaten in Frage, weil es ihnen an Belastbarkeit mangelt und weil aufgrund der nur schwachen Verbindung zwischen Risiken für die Gesundheit und von der Visumpflicht befreiten Reisenden keine Notwendigkeit hierfür besteht.“
- Besonderes Augenmerk wurde in letzter Zeit auf die Risiken der künstlichen Intelligenz bei der Gesichts- (und „Affekt“-)Erkennung gelegt. Siehe *AI Now Report 2018*, Dezember 2018, abrufbar unter: https://ainowinstitute.org/AI_Now_2018_Report.pdf.
- Zu **biometrischen Daten**, siehe **Stellungnahme 3/2012 der WP29 zu Entwicklungen im Bereich biometrischer Technologien**, Seiten 30-31, zu den spezifischen Risiken biometrischer **Daten; und Stellungnahme 02/2012 der WP29 zur Gesichtserkennung bei Online- und Mobilfunkdiensten**, Abschnitt 5, Spezifische Risiken und Empfehlungen.

medizinische Tätigkeit); *des Kontextes*; ob sie auf ***Profiling*** der betroffenen Personen hinausläuft oder nicht[49]; ob die Verarbeitung die Nutzung eines (teilweise oder vollständig) ***automatisierten*** Entscheidungsfindungssystems mit einer „Fehlermarge" beinhaltet[50];

- ob sie **schutzbedürftige** Personen betreffen oder nicht[51];
- ob sie **auch *andere Grundrechte* betreffen** (es könnte ein „untrennbar verbundenes" Grundrecht geben[52], beispielsweise das Recht auf Schutz der Privatsphäre und das Recht auf freie Meinungsäußerung, wie in den Rechtssachen *Digital Rights* und *Tele2* des EuGH).

In Fällen, in denen einige (oder ein Teil der) Auswirkungen nicht im Voraus festgestellt werden können, könnte es hilfreich sein, das sogenannte **Vorsorgeprinzip** anzuwenden.[53] Als Beispiel

---

[49] In diesem Zusammenhang verstehen wir unter dem Begriff „Profiling" im weiten Sinne „die Profilerstellung der Person", wie in der Rechtssache *Tele2* und nicht unbedingt die Definition nach Artikel 4 Absatz 4 DSGVO: „*Profiling bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen*."

[50] Im Hinblick auf automatisierte Entscheidungen, siehe Gutachten 1/15, ECLI:EU:C:2017:592 des EuGH zum geplanten Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung von PNR-Daten. In der Stellungnahme des Gerichtshofes wurde hervorgehoben, dass das kanadische System für die Risikobewertung von EU-Reisenden systematisch und automatisiert funktioniert und **eine „erhebliche" Fehlerquote** aufweist, was zur Folge hat, dass eine große Anzahl von Personen, die kein Risiko darstellten, der laufenden Kontrolle durch die CBSA und anderer Behörden ausgesetzt waren. In der Stellungnahme wurde betont, dass algorithmische Systeme und Technologien zur Risikobewertung „in **nichtdiskriminierender Weise** angewendet werden müssen" und dass endgültige Entscheidungen „allein auf einer individualisierten, von **Menschen durchgeführten** Bewertung beruhen müssen"). In diesem Fall sei auch darauf hingewiesen, dass das Recht auf Privatsphäre und den Schutz personenbezogener Daten mit anderen Grundrechten und Grundsätzen zusammenhängen kann (hier: Nichtdiskriminierung).
- Für weitere Informationen zu den **Auswirkungen der automatisierten Entscheidungsfindung durch staatliche/öffentliche Behörden**, siehe Australische Regierung, *Automated Assistance in Administrative Decision Making, Better Practice Guide*, Februar 2007 (auch wenn der Leitfaden nicht aktualisiert wurde, enthält er dennoch eine Reihe relevanter Fragen), abrufbar unter: https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf.

[51] EGMR, *S. und Marper*, Rn. 124: „Der Gerichtshof ist ferner der Ansicht, dass die Speicherung von Daten nicht verurteilter Personen im Falle von **Minderjährigen** wie dem Erstantragsteller angesichts ihrer besonderen Situation und der Bedeutung ihrer Entwicklung und Integration in die Gesellschaft **besonders schädlich** sein kann."
- Siehe als Beispiel für die besondere Aufmerksamkeit, die bei der Verarbeitung personenbezogener Daten von Minderjährigen erforderlich ist die **Antwort des EDSB auf die öffentliche Konsultation der Kommission zur Herabsetzung des Alters für die Abnahme von Fingerabdrücken bei Kindern im Visumverfahren von zwölf auf sechs Jahre** vom 9. November 2017, Seite 2: „Der EDSB empfiehlt, die Notwendigkeit und Verhältnismäßigkeit der Abnahme von **Fingerabdrücken bei jüngeren Kindern** in den Mittelpunkt **weiterer Überlegungen und Bewertungen** zu stellen, wie **sie im Rahmen der Folgenabschätzung** für den künftigen Vorschlag der Kommission zur Überarbeitung der VIS-Verordnung angestellt werden". Die vollständige Antwort des EDSB ist abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-11-09_formal_comments_2017-0809_de.pdf.

[52] Siehe Christopher Docksey, *Four fundamental rights: finding the balance*, International Data Privacy Law, 2016, Bd. 6, Nr. 3, Seite 203: „In manchen Zusammenhängen wie der Massenüberwachung und der unabhängigen Regulierung ergänzen sich das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten und auf Meinungsfreiheit völlig und stärken sich gegenseitig."

[53] Hans Jonas war bereits in den 1970er Jahren Verfechter des Vorsorgeprinzips. Am 2. Februar 2000 erklärte die **Europäische Kommission** in ihrer **Mitteilung zum Vorsorgeprinzip** (KOM(2000) 1 endg.): „Obgleich das

für die Anwendbarkeit dieses Prinzips könnte dem Gesetzgeber vorgeschlagen werden, unter Berücksichtigung aller relevanter Umstände des Falles einen „inkrementellen Ansatz“ zu wählen und sich für die Verwendung eines bereits *erprobten und verifizierten* IT-Tools zu entscheiden, statt eines IT-Tools, dessen Wirksamkeit (falsch negative Ergebnisse, falsch positive Ergebnisse) noch nicht vollständig getestet wurde.

Sachdienliche Beispiele

BEISPIEL 1: *Tele2 Sverige AB* (EuGH, C-203/15 und C-698/15, ECLI:EU:C:2016:970)

Der Gerichtshof bewertete den **Eingriff** als **schwerwiegend**, insbesondere angesichts der Tatsache, dass die Maßnahmen die Erstellung eines Profils der betroffenen Person implizieren.

Der Gerichtshof hat Folgendes festgestellt: „*Die Regelung sieht eine **allgemeine und unterschiedslose Vorratsspeicherung** sämtlicher **Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer** in Bezug auf **alle elektronischen Kommunikationsmittel** vor und verpflichtet die Betreiber elektronischer Kommunikationsdienste, diese Daten systematisch und kontinuierlich auf Vorrat zu speichern, und zwar ausnahmslos. Wie aus der Vorlageentscheidung hervorgeht, entsprechen die von dieser Regelung erfassten **Datenkategorien** im Wesentlichen denen, deren Vorratsspeicherung nach der Richtlinie 2006/24 vorgesehen war.*“

„*Die **Daten**, die somit von den Betreibern elektronischer Kommunikationsdienste auf Vorrat zu speichern sind, **ermöglichen die Rückverfolgung und Identifizierung der Quelle und des Adressaten einer Nachricht sowie die Bestimmung von Datum, Uhrzeit, Dauer und Art einer Nachrichtenübermittlung, der Endeinrichtung von Benutzern und des Standorts mobiler Geräte**. Zu diesen Daten gehören **Name und Anschrift des Teilnehmers oder registrierten Benutzers, die***

Vorsorgeprinzip im Vertrag nur im Zusammenhang mit dem **Umweltbereich** ausdrücklich erwähnt wird, ist sein Anwendungsbereich **wesentlich weiter**. So ist es in konkreten Fällen anwendbar, **in denen die wissenschaftlichen Beweise nicht ausreichen, keine eindeutigen Schlüsse zulassen oder unklar** sind, in denen jedoch aufgrund einer vorläufigen und objektiven wissenschaftlichen Risikobewertung **begründeter Anlass zu der Besorgnis** besteht, dass die möglicherweise gefährlichen Folgen für die Umwelt und die Gesundheit von Menschen, Tieren und Pflanzen mit dem hohen Schutzniveau der Gemeinschaft unvereinbar sein könnten.“ Die Mitteilung ist abrufbar unter:
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52000DC0001&from=EN.
Wir sind der Auffassung, dass dieses Prinzip, in Übereinstimmung mit der Metapher des Verlusts der Privatsphäre als „Datenverschmutzung“, auch auf die Risiken für die Privatsphäre und den Schutz personenbezogener Daten anwendbar ist.

- „Wenn über die Entwicklung neuer Technologien, die in die Privatsphäre eingreifen, kein Konsens besteht, erwartet der EGMR von einem Mitgliedstaat, dass er „eine Vorreiterrolle einnimmt“, um „die besondere Verantwortung dafür zu tragen, dass das richtige Gleichgewicht hergestellt wird“, P. Popelier und C. Van De Heyning, *Procedural Rationality*: *Giving Teeth to the Proportionality Analysis*, European Constitutional Law Review, 9, 2013, S. 243, in Bezug auf die Rechtssache *S und Marper / Vereinigtes Königreich*, EGMR.

- IIn seiner **Stellungnahme 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Großsystemen der EU** berücksichtigte der EDSB die unvorhersehbaren Risiken und forderte daher eine umfassendere, evidenzbasierte Debatte (über die Interoperabilität), *„die Entscheidung für Interoperabilität ist nicht vorrangig eine technische, sondern an erster Stelle eine politische Entscheidung, **die in den kommenden Jahren weitreichende rechtliche und gesellschaftliche Konsequenzen haben kann**. Vor dem Hintergrund der sich klar abzeichnenden Tendenz, verschiedene Ziele des EU-Rechts und der EU-Politik miteinander zu vermengen (also Grenzkontrollen, Asyl und Einwanderung, polizeiliche Zusammenarbeit und nun auch justizielle Zusammenarbeit in Strafsachen) sowie der Gewährung des routinemäßigen Zugriffs von Strafverfolgungsbehörden auf Datenbanken anderer Behörden würde die Entscheidung des EU-Gesetzgeber, IT-Großsysteme interoperabel zu machen, nicht nur deren Struktur und Funktionsweise auf Dauer und weitreichend berühren, sondern auch die bisherige Auslegung der Rechtsgrundsätze in diesem Bereich verändern und somit unumkehrbar sein. Aus diesen Gründen fordert der EDSB eine **umfassende Debatte über die Zukunft der Systeme für den Informationsaustausch in der EU, ihre Governance und die Möglichkeiten, in diesen Zusammenhang Grundrechte zu schützen**.“ (Rn. 25)

***Rufnummer des anrufenden und des angerufenen Anschlusses sowie bei Internetdiensten eine IP-Adresse**. Aus diesen Daten **geht insbesondere hervor, mit welcher Person ein Teilnehmer oder registrierter Benutzer auf welchem Weg kommuniziert hat, wie lange die Kommunikation gedauert hat und von welchem Ort aus sie stattfand**. Ferner ist ihnen zu entnehmen, **wie häufig der Teilnehmer oder registrierte Benutzer in einem bestimmten Zeitraum mit bestimmten Personen kommuniziert hat** (vgl. entsprechend, in Bezug auf die Richtlinie 2006/24, Urteil Digital Rights, Rn. 26).“*

„*Aus der **Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten auf Vorrat gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren** (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 27). Diese Daten ermöglichen insbesondere (...) die **Erstellung des Profils der betroffenen Personen**, das im Hinblick auf das Recht auf Achtung der Privatsphäre eine genauso sensible Information darstellt wie der Inhalt der Kommunikationen selbst.“*

„*Der mit einer solchen **Regelung verbundene Eingriff** in die in den Art. 7 und 8 der Charta verankerten Grundrechte ist **von großem Ausmaß** und als **besonders schwerwiegend** anzusehen. Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen **das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist** (vgl. entsprechend, zur Richtlinie 2006/24, Urteil Digital Rights, Rn. 37).“*

*Zu den Auswirkungen der Maßnahme auf **andere Grundrechte**, die mit dem Recht auf Privatsphäre und den Schutz personenbezogener Daten verbunden sind, stellte der Gerichtshof fest, dass: „die Vorratsspeicherung der Verkehrs- und Standortdaten (...) Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und infolgedessen auf die Ausübung der in Art. 11 der Charta gewährleisteten **Freiheit der Meinungsäußerung** durch die Nutzer dieser Mittel haben könnte (vgl. entsprechend in Bezug auf Richtlinie 2006/24 Urteil Digital Rights, Rn. 28)*“. (Hervorhebung hinzugefügt)

Der Gerichtshof berücksichtigte auch die Auswirkungen der Maßnahme „*ratione personae*“, nämlich das durch die Regelung vorgeschriebene Erfordernis, (auch) Daten über **Mitglieder eines Berufsstands, die mit unter dem Schutz des Berufsgeheimnisses stehenden oder anderweitig vertraulichen Informationen umgehen**, zu speichern und zugänglich zu machen: „*besondere Aufmerksamkeit der Erforderlichkeit und der Verhältnismäßigkeit muss gelten, wenn sich die angefragten Daten auf eine Person beziehen, die Mitglied eines Berufsstands ist, der mit unter dem Schutz des Berufsgeheimnisses stehenden oder anderweitig vertraulichen Informationen umgeht*.“ (Hervorhebung hinzugefügt)

BEISPIEL 2: *Ministerio Fiscal* (EuGH, C-207/16, ECLI:EU:C:2018:788)

Der Gerichtshof stellte Folgendes fest: „*Es ist (...) **zu prüfen, ob** nach den Umständen des vorliegenden Falles **der Eingriff in die in den Artikel 7 und 8 der Charta** verankerten Grundrechte, der mit einem Zugang der Kriminalpolizei zu den im Ausgangsverfahren in Rede stehenden Daten einhergeht, **als „schwer“ anzusehen ist***.“

„*Insoweit ist festzustellen, dass der im Ausgangsverfahren in Rede stehende Antrag, mit dem die Kriminalpolizei für die Zwecke strafrechtlicher Ermittlungen um gerichtliche Erlaubnis zum Zugang zu von den Betreibern elektronischer Kommunikationsdienste gespeicherten personenbezogenen Daten ersucht, **ausschließlich darauf abzielt**, die Identität der Inhaber von SIM-Karten festzustellen, die in einem Zeitraum von zwölf Tagen mit der IMEI des gestohlenen Mobiltelefons aktiviert wurden. (...) dieser Antrag bezieht sich **nur** auf den Zugang zu den diesen SIM-Karten entsprechenden Telefonnummern sowie zu den Daten bezüglich der Identität der Karteninhaber wie deren Name, Vorname und gegebenenfalls Adresse. Dagegen **beziehen sich diese Daten (...) weder auf die mittels des gestohlenen Mobiltelefons erfolgte Kommunikation noch auf dessen Ortung**.“*

„*Daher kann mit den Daten, auf die sich der im Ausgangsverfahren in Rede stehende Zugangsantrag bezieht, offenbar nur eine Verbindung zwischen der SIM-Karte oder den SIM-Karten, die mit dem gestohlenen Mobiltelefon aktiviert wurden, und der Identität der Inhaber dieser SIM-Karten während eines bestimmten Zeitraums hergestellt werden. Ohne einen Abgleich mit den Daten bezüglich der mittels dieser SIM-Karten erfolgten Kommunikation und den Standortdaten* ***lassen sich diesen Daten weder das Datum, die Uhrzeit, die Dauer und die Adressaten der mittels der betreffenden SIM-Karte bzw. der betreffenden SIM-Karten erfolgten Kommunikation entnehmen noch die Orte, an denen diese Kommunikation erfolgte, oder die Häufigkeit dieser Kommunikation mit bestimmten Personen während eines bestimmten Zeitraums. Aus diesen Daten lassen sich daher keine genauen Schlüsse auf das Privatleben der Personen ziehen, deren Daten betroffen sind***.“ (Hervorhebung hinzugefügt)

Auf dieser Grundlage stellte der Gerichtshof fest, dass es sich hierbei **nicht um einen schweren Eingriff** handelt. Es lässt sich feststellen, dass die Tatsache, dass **von der betroffenen Person kein Profil erstellt wurde**, ein Hauptgrund dafür war, dass der Gerichtshof den Eingriff als „nicht schwer“ bewertete (die Argumentation erfolgte hier *gegensätzlich* zu Tele2).

BEISPIEL 3: Gutachten 1/15 *PNR-Abkommen mit Kanada* (EuGH, ECLI:EU:C:2017:592)

In der Rechtssache PNR-Abkommen mit Kanada bewertete der Gerichtshof den **Eingriff** insbesondere im Hinblick auf den Umfang, das Ausmaß des Eingriffs und den *persönlichen Geltungsbereich*. Letzterer galt (neben anderen Aspekten) als ein Problem in dem Abkommen. Der Gerichtshof stellte fest, dass: „*der mit dem geplanten Abkommen verbundene Eingriff zwar* ***weniger weitreichend*** *war als der von der Richtlinie 2006/24 vorgesehene* und sich auch **weniger stark** auf das täglichen Leben jedes Einzelnen auswirkt, doch wirft sein **undifferenzierter und allgemeiner Charakter** Fragen auf“. (Hervorhebung hinzugefügt)

Die anderen vom Gerichtshof kritisierten problematischen Aspekte betreffen: (i) die Ermittlung der für die Verarbeitung der Daten zuständigen Behörde; (ii) die automatisierte Verarbeitung (Fehlen von Garantien, vgl. Rn. 258-260); (iii) die Bedingungen für den Zugang für Strafverfolgungsbehörden zu gespeicherten Daten; (iv) die Datenspeicherfrist; (v) die Offenlegung und Übermittlung von Daten; (vi) Aufsicht durch eine unabhängige Behörde. Auf die vorstehenden Probleme hat der EuGH *auch* in den Rechtssachen *Digital Rights* und *Tele2* hingewiesen.

BEISPIEL 4: *Bevándorlási és Állampolgársági Hivatal* (EuGH, C-473/16, ECLI:EU:C:2018:36)

In Bezug auf **den Eingriff** der fraglichen Maßnahme, stellte der Gerichtshof fest: *„Der* ***Eingriff*** *in das Privatleben der um internationalen Schutz nachsuchenden Person, der in der Erstellung und Verwendung eines Gutachtens wie des im Ausgangsverfahren streitigen besteht, ist in Anbetracht seiner Art und seines Gegenstands von* ***besonderer Schwere****.“*

„Denn ein solches Gutachten beruht u. a. darauf, dass der Betroffene ***einer Reihe von Tests unterzogen wird****, die einen wesentlichen Bestandteil seiner Identität feststellen sollen und seine persönliche Sphäre berühren, da es um* ***intime Aspekte seines Lebens geht*** *(...).“*

„*Bei der Beurteilung der* ***Schwere des Eingriffs****, den die Erstellung und Verwendung eines psychologischen Gutachtens wie des im Ausgangsverfahren streitigen darstellt, ist auch Prinzip 18 der Yogyakarta-Prinzipien zur Anwendung internationaler Menschenrechtsnormen und -standards in Bezug auf sexuelle Orientierung und Geschlechtsidentität zu berücksichtigen, auf das die französische und die niederländische Regierung verwiesen haben. Dort heißt es u. a., dass niemand aufgrund seiner sexuellen Orientierung oder seiner geschlechtlichen Identität gezwungen werden darf, sich irgendeiner Form psychologischer Untersuchung zu unterziehen*.“

„*Eine Gesamtschau dieser Gesichtspunkte ergibt, dass* ***die Schwere des Eingriffs*** *in das Privatleben, den die Erstellung und Verwendung eines Gutachtens wie des im Ausgangsverfahren streitigen darstellt, über das hinausgeht, was mit der Würdigung der Aussagen der um internationalen Schutz nachsuchenden Person zur Furcht vor Verfolgung wegen ihrer sexuellen Orientierung oder der*

Heranziehung eines psychologischen Gutachtens mit einem anderen Gegenstand als der Feststellung der sexuellen Orientierung dieser Person notwendigerweise verbunden ist." (Hervorhebung hinzugefügt)

BEISPIEL 5: Stellungnahme 06/2016 des EDSB zum zweiten Paket „Intelligente Grenzen" der EU[54]

„Der EDSB möchte zunächst betonen, dass aus dem Blickwinkel der Artikel 7 und 8 der Charta die **Verarbeitung personenbezogener Daten im Rahmen des EES einen erheblichen Eingriff bedeutet,** bedenkt man die **Zahl der von dieser Regelung betroffenen Personen**, **die Art der verarbeiteten Informationen**, die für die Verarbeitung dieser Informationen **eingesetzten Mittel** und die verschiedenen verfolgten Zwecke, wie weiter unten noch näher ausgeführt wird."

BEISPIEL 6: Stellungnahme 3/2017 des EDSB zu dem Vorschlag für ein Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)

„Der Vorschlag sieht die Prüfung der Anträge aller von der Visumpflicht befreiten Drittstaatsangehörigen nach den ETIAS-Überprüfungsregeln vor, obwohl nur wenige von ihnen wohl tatsächlich ein bestimmtes Risiko darstellen und ihnen daher die Reisegenehmigung verweigert wird. Dieser automatisierte und intransparente Umgang mit personenbezogenen Daten bedeutet an sich schon einen **schweren Eingriff** in die Grundrechte einer **unbegrenzten Zahl von Antragstellern**, die einem **Profiling unterzogen werden**; hier sollte mit Blick auf das erwartete Ergebnis eines solchen Instruments eine Abwägung vorgenommen werden.

Zudem kann je nach der für die Entwicklung der spezifischen Risikoindikatoren **verwendeten Methode**, die sehr weit ausgelegt werden können, **die Zahl der Personen, denen eine automatisierte Genehmigung aufgrund eines auf den Überprüfungsregeln beruhenden Treffers verweigert wird, relativ hoch sein**, auch wenn diese Personen eigentlich kein Risiko darstellen."

Schritt 3: Bewertung des angemessenen Gleichgewichts der Maßnahme

Wenn (und erst ab diesem Zeitpunkt) der Gesetzgeber **alle erforderlichen Informationen** erfasst und die Bewertung der Bedeutung und der Wirksamkeit und der Effizienz der Maßnahme und ihrer Eingriffe in die Privatsphäre und den Schutz personenbezogener Daten vorgenommen hat, sollte er prüfen, ob zwischen diesen beiden Aspekten ein angemessenes Gleichgewicht herrscht.

Bei einer **Informationsasymmetrie**, wenn z. B. die Vorteile bekannt, die Kosten jedoch unbekannt sind oder *umgekehrt*, wird es schwierig, wenn nicht gar unmöglich sein, unter Abwägung aller Faktoren festzustellen, ob die Maßnahme verhältnismäßig ist.

In der Praxis erfordert der Grundsatz der Verhältnismäßigkeit ein **Gleichgewicht** zwischen dem Ausmaß und der Art des Eingriffs und den Gründen für das Eingreifen (den Erfordernissen), was sich in den Zielen niederschlägt, die mit der Maßnahme effektiv verfolgt werden. Der EuGH bekräftigte: *„Sind mehrere grundrechtlich geschützte Rechte und Freiheiten im Spiel, die unter dem Schutz der Unionsrechtsordnung stehen, ist bei der Beurteilung der möglichen Unverhältnismäßigkeit einer unionsrechtlichen Bestimmung darauf zu achten, dass die Erfordernisse des Schutzes dieser verschiedenen Rechte und Freiheiten*

[54] Abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_de.pdf.

miteinander in Einklang gebracht werden *und dass zwischen ihnen ein* ***angemessenes Gleichgewicht*** *besteht.*“[55]

Mit anderen Worten: Der Grundsatz dient als Instrument, um Interessenkonflikte nach einem rationalen Standard abzuwägen. Dies gilt für Fälle, bei denen keinem *von vornherein* der Vorrang gegenüber dem anderen eingeräumt wurde.[56]

Es gibt tatsächlich eine Methode, mit der sich überprüfen ließe, ob ein EU-Rechtsakt als mit den Artikeln 7 und 8 der Charta und mit dem Grundsatz der Verhältnismäßigkeit gemäß Artikel 52 Absatz 1 der Charta vereinbar angesehen werden kann oder nicht. Eine solche Methode würde sich vornehmlich aus den Urteilen des EuGH ergeben, auf die in diesen Leitlinien Bezug genommen wird, insbesondere, aber nicht ausschließlich auf dem Gebiet der „allgemeinen Überwachungsprogramme“.[57]

Vorgehensweise

- Zunächst sollten Sie *vor* der Abwägung prüfen, ob eine **Informationsasymmetrie** vorliegt: *Wurden alle relevanten Informationen erfasst und sowohl eine Bewertung des „Nutzens“ als auch der „Kosten“ der Maßnahme durchgeführt?*
- **Vergleichen** Sie anschließend die Einschränkungen der Privatsphäre und des Datenschutzes mit dem Nutzen (die **Abwägung**): *Sind die zur Erreichung des Ziels vorgesehenen Maßnahmen angesichts der Einschränkungen des Datenschutzes und des Rechts auf Privatsphäre eine verhältnismäßige Reaktion auf das einem Gesetzesvorschlag zugrunde liegende Erfordernis?*
- Stellen Sie nach der Abwägung sicher, dass ausreichende **Nachweise** erbracht und gegebenenfalls veröffentlicht wurden, aus denen hervorgeht, dass die **Analyse durchgeführt wurde** (*Bericht über die Prüfung der Verhältnismäßigkeit*, d. h. eine synthetische Analyse des **Ergebnisses** der durchgeführten Bewertung).
- **Bewahren (erfassen und speichern) Sie alle sachdienlichen Unterlagen auf**, die Sie während der Durchführung der **Abwägung** und des Entwurfs des *Berichts über die Prüfung der Verhältnismäßigkeit* erhalten oder erstellt haben. Diese Unterlagen sollten

[55] EuGH Rechtssachen, C-283/11, *Sky Österreich GmbH / Österreichischer Rundfunk* (GC), ECLI:EU:C:2013:28, Rn. 60; C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, ECLI: EU:C:2008:54, Rn. 65 und 66 und C-544/10, *Deutsches Weintor*, ECLI:EU:C:2012:526, Rn. 47; EGMR Urteil, *Big Brother Watch u. a. / Vereinigtes Königreich*, 13. September 2018, „2.42. Eine Prüfung der Verhältnismäßigkeit des Antrags sollte insbesondere die Rechte (insbesondere auf Privatsphäre und gegebenenfalls auf Meinungsfreiheit) des Einzelnen und eine Abwägung dieser Rechte gegenüber dem Nutzen der Überprüfung umfassen.“

[56] Siehe insbesondere Rechtssache C-28/08 des EuGH, *Bavarian Lager*, Rn. 56: „*Die Verordnungen Nrn. 45/2001 und 1049/2001 sind kurz nacheinander erlassen worden. Sie enthalten keine Bestimmungen, die ausdrücklich den Vorrang der einen gegenüber der anderen dieser Verordnungen vorsähen*.“

[57] In der Stellungnahme **4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Großsystemen der EU** stellte der EDSB auf Seite 13 klar, dass: „die neuen Datenverarbeitungsverfahren, die eine **korrekte Identifizierung der Personen ermöglichen**, einen **Eingriff in die nach den Artikeln 7 und 8 der Charta geschützten Grundrechte dieser Personen** bedeuten. Folglich sind sie auf ihre Notwendigkeit und Verhältnismäßigkeit zu testen (Artikel 52 Absatz 1 der Charta).“
- Siehe auch *S und Marper / Vereinigtes Königreich*, EMGR, Rn. 67: „**Allein das Speichern von Daten, die sich auf das Privatleben eines Einzelnen** beziehen, stellt einen Eingriff nach Artikel 8 dar (...). Die spätere Verwendung der gespeicherten Informationen hat keinen Einfluss auf diese Feststellung (...). 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.“

für die Begründung (oder zur Ermittlung kritischer Punkte) der zu prüfenden Maßnahme sachdienlich und ausreichend sein (Ziel der Bewertung) und dem Bericht als Anhang beiliegen.[58]

Sachdienliche Beispiele

BEISPIEL 1: *Tele2 Sverige AB* (EuGH, C-203/15 und C-698/15, ECLI:EU:C:2016:970)

In der Rechtssache *Tele2* befand der Gerichtshof Folgendes: *„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 (...).“* (Hervorhebung hinzugefügt)

Der Gerichtshof hatte einerseits die Bedeutung und Wirksamkeit der Maßnahme klar vor Augen, andererseits die **Tragweite** (nicht beschränkt auf Daten, die sich auf einen bestimmten Zeitraum beziehen und/oder ein bestimmtes geographisches Gebiet und/oder auf Personen, die in schwere Kriminalität verwickelt sein könnten) und das **Ausmaß/die Intensität** (u. a. Profiling) des Eingriffs.

[58] In seinen Schlussanträgen ECLI:EU:C:2013:845, in den verbundenen Rechtssachen C-293/12 und C-594/12, *Digital Rights*, wies der Generalanwalt auf das **Fehlen relevanter und ausreichender Gründe** für die in der Richtlinie vorgeschriebene **zweijährige Vorratsdatenspeicherung** als Hauptgrund für die Ablehnung der Verhältnismäßigkeit der zweijährigen Vorratsdatenspeicherung hin (im Gegensatz zu der gerechtfertigten Speicherungsfrist von weniger als einem Jahr). Siehe Rn. 148-149: „*Es lässt sich sagen, dass eine „nach Monaten bemessene“ Speicherungsfrist personenbezogener Daten durchaus von einer „nach Jahren bemessenen“ Frist zu unterscheiden ist. Erstere entspräche derjenigen, die in dem als gegenwärtig wahrgenommenen Leben angesiedelt ist, und Letztere derjenigen, die in dem als Erinnerung wahrgenommenen Leben angesiedelt ist. Der Eingriff in das Recht auf Achtung des Privatlebens ist aus diesem Blickwinkel jeweils ein anderer, und die Erforderlichkeit jedes dieser Eingriffe muss gerechtfertigt werden können. Auch wenn die Erforderlichkeit des Eingriffs in der Dimension der gegenwärtigen Zeit als hinreichend gerechtfertigt erscheint, habe ich jedoch* ***keine Rechtfertigung für einen Eingriff gefunden, der sich bis in die vergangene Zeit erstrecken soll****. Direkter ausgedrückt – und ohne zu leugnen, dass es Straftaten gibt, die lange im Voraus vorbereitet werden – habe ich in den verschiedenen Stellungnahmen, in denen die Verhältnismäßigkeit von Artikel 6 der Richtlinie 2006/24 verteidigt wird, keine hinreichende Rechtfertigung dafür gefunden, dass die von den Mitgliedstaaten festzulegende Frist für die Vorratsdatenspeicherung nicht innerhalb eines Rahmens von weniger als einem Jahr bleiben sollte.*“
- Siehe auch verbundene Rechtssachen *Volker und Markus Schecke und Hartmut Eifert*, **C-92/09 und C-93/09**, ECLI:EU:C:2010:662, Rn. 81: „***Es gibt nämlich keinen Hinweis darauf****, dass der Rat und die Kommission beim Erlass von Artikel 44a der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 Modalitäten der Veröffentlichung von Informationen über die betroffenen Empfänger erwogen hätten, die im Einklang mit dem Zweck einer solchen Veröffentlichung gestanden, zugleich aber auch in das Recht dieser Empfänger auf Achtung ihres Privatlebens im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen weniger stark eingegriffen hätten (...).*“ (Hervorhebung hinzugefügt)
- In der **Stellungnahme 7/2018** zu dem Vorschlag für eine Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und anderer Dokumente vom 10. August 2018 (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_de_0.pdf)) weist der EDSB auf Seite 3 darauf hin, „*dass die Folgenabschätzung zum Vorschlag* ***anscheinend die von der Kommission gewählte Option nicht unterstützt****, nämlich die obligatorische Aufnahme sowohl von Gesichtsbildern als auch von (zwei) Fingerabdrücken in Personalausweise (und Aufenthaltsdokumente).* (...) *Der EDSB empfiehlt daher, vor diesem Hintergrund die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung biometrischer Daten (Gesichtsbild in Kombination mit Fingerabdrücken) erneut zu prüfen.*“
- Gleichermaßen befand der EDSB auf Seite 3 in seiner **Stellungnahme 7/2017 zur neuen Rechtsgrundlage für das Schengener Informationssystem** vom 2. Mai 2017 (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_de.pdf), „(...) *dass die Einführung neuer Kategorien von Daten, darunter neuer biometrischer Identifikatoren, die Frage nach der Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Änderungen aufwirft, und daher sollten die Vorschläge durch eine Abschätzung der Folgen für das in der Charta der Grundrechte der EU verankerte Recht auf Privatsphäre und Datenschutz ergänzt werden*“.

Nach Abwägung der beiden Faktoren entschied der Gerichtshof Folgendes: „*Die Wirksamkeit der Bekämpfung schwerer Kriminalität kann für sich genommen die Erforderlichkeit einer nationalen Regelung, die die allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten für die Kriminalitätsbekämpfung vorsieht, nicht rechtfertigen.*“ Die Maßnahme *„**überschreitet somit die Grenzen des absolut Notwendigen** und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden“*. (Hervorhebung hinzugefügt)

BEISPIEL 2: *Ministerio Fiscal* (EuGH, C-207/16, ECLI:EU:C:2018:788)

In der Rechtssache *Ministerio Fiscal* befand der Gerichtshof, dass die zu prüfende Maßnahme **verhältnismäßig** ist (sie hat die Prüfung der Verhältnismäßigkeit erfolgreich bestanden und ist daher sowohl nach den Grundsätzen der Erforderlichkeit als auch nach den Grundsätzen der Verhältnismäßigkeit rechtmäßig).

Ausschlaggebend für diese Bewertung ist die Tatsache, dass der Eingriff als „nicht schwerwiegend“ eingestuft wurde und daher nicht schwerer wog als die (ebenfalls nicht schwerwiegende/hohe) Bedeutung des Ziels, das durch die Maßnahme tatsächlich erreicht wurde.

Der Gerichtshof stellte Folgendes fest: *„Ist der mit (der Maßnahme) verbundene **Eingriff nicht schwer**, kann (die Maßnahme) durch einen Zweck der **Verhütung, Ermittlung, Feststellung und Verfolgung von „Straftaten“ im Allgemeinen gerechtfertigt sein**.“* Dagegen kann „nach dem Grundsatz der Verhältnismäßigkeit ein **schwerer** Eingriff im **Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten** (nur) **durch einen Zweck der Bekämpfung einer ebenfalls als „schwer“ einzustufenden Kriminalität gerechtfertigt sein**“. (Hervorhebung hinzugefügt)

BEISPIEL 3: Gutachten 1/15 *PNR-Abkommen mit Kanada* (EuGH, ECLI:EU:C:2017:592)

Bei der in dieser Rechtssache zu prüfenden Maßnahme handelt es sich um eine **Informationsasymmetrie** zwischen dem erwarteten Nutzen und den Auswirkungen auf das Grundrecht auf Privatsphäre und den Schutz personenbezogener Daten. Dies ist insbesondere darauf zurückzuführen, dass die **Kategorien der zu verarbeitenden personenbezogenen Daten** nicht **klar und präzise** formuliert sind; auch die Regeln für die automatische Vorabkontrolle von Fluggästen werden in der Maßnahme **nicht festgelegt**.

Das Fehlen dieser Angaben macht nicht nur die Vergleichbarkeit unmöglich, sondern sorgt auch dafür, dass der Gerichtshof die Vereinbarung in ihrer derzeitigen Fassung umgehend für **unvereinbar** mit den Artikeln 7 und 8 und Artikel 52 Absatz 1 der Charta erklärt.

BEISPIEL 4: *Bevándorlási és Állampolgársági Hivatal* (EuGH, C-473/16, ECLI:EU:C:2018:36)

In dieser Rechtssache gelangte der Gerichtshof unter Berücksichtigung aller Aspekte zur Bedeutung und Wirksamkeit der Maßnahme sowie der Intensität des Eingriffes (in dieser Rechtssache in Bezug auf eine bestimmte Person) zu dem Schluss, dass: „*Artikel 4 der Richtlinie 2011/95 im Licht von Artikel 7 der Charta dahin auszulegen ist, **dass er es untersagt, zur Beurteilung der Frage, ob die behauptete sexuelle Orientierung einer um internationalen Schutz nachsuchenden Person tatsächlich besteht, ein psychologisches Gutachten** wie das im Ausgangsverfahren streitige zu erstellen und heranzuziehen, das auf der Grundlage eines projektiven Persönlichkeitstests die sexuelle Orientierung dieser Person abbilden soll*“. (Hervorhebung hinzugefügt)

Mit anderen Worten: Der Gerichtshof befand die zu prüfende Maßnahme für **nicht verhältnismäßig**, da es sich bei der Maßnahme um einen äußerst schwerwiegenden Eingriff handelt, aber auch aufgrund der mangelnden Wirksamkeit bei der Erreichung des verfolgten Ziels.

BEISPIEL 5: *Scarlet Extended* (EuGH, C-70/10, ECLI:EU:C:2011:771)

Diese Rechtssache ist insofern interessant, als sie zeigt, dass das R**echt auf Schutz personenbezogener Daten** ein mit anderen Rechten *einhergehendes Recht* sein kann, das nicht das sein muss, das in erster

Linie von der Maßnahme betroffen ist, das jedoch **zusammen** mit anderen Rechten (unternehmerische Freiheit; Freiheit, Informationen zu erhalten oder weiterzugeben) dafür sorgen kann, dass die Maßnahme (mit dem Ziel, die Rechte des geistigen Eigentums besser zu schützen) als unverhältnismäßig erachtet wird.

Es folgen die wichtigsten Auszüge dieses Urteils: „*die Anordnung, das streitige **Filtersystem** einzurichten, ist als Missachtung des Erfordernisses der Gewährleistung eines **angemessenen Gleichgewichts** zwischen dem **Schutz des Rechts des geistigen Eigentums**, das Inhaber von Urheberrechten genießen, und dem Schutz der **unternehmerischen Freiheit**, der Wirtschaftsteilnehmern wie den Providern zukommt, einzustufen.*

*Darüber hinaus würden sich die Wirkungen dieser Anordnung nicht auf den betroffenen Provider beschränken, weil das streitige Filtersystem **auch Grundrechte der Kunden dieses Providers beeinträchtigen kann, und zwar ihre durch die Artikel 8 und 11 der Charta geschützten Rechte auf den Schutz personenbezogener Daten** und auf **freien Empfang oder freie Sendung von Informationen**.(...)*

*Somit ist festzustellen, dass das fragliche nationale Gericht, erließe es die Anordnung, mit der der Provider zur Einrichtung des streitigen Filtersystems verpflichtet würde, **nicht das Erfordernis beachten** würde, **ein angemessenes Gleichgewicht zwischen dem Recht des geistigen Eigentums einerseits** und der **unternehmerischen Freiheit**, dem **Recht auf den Schutz personenbezogener Daten** und dem **Recht auf freien Empfang oder freie Sendung von Informationen andererseits zu gewährleisten***." (Hervorhebung hinzugefügt)

BEISPIEL 6: Stellungnahme 1/2017 des EDSB zu einem Vorschlag der Kommission zur Änderung der Richtlinie (EU) 2015/849 und der Richtlinie 2009/101/EG. Zugang zu Informationen über den wirtschaftlichen Eigentümer und Implikationen für den Datenschutz

In dieser Stellungnahme sowie im Vorschlag wird das Ziel als „zu vermeidendes Risiko" bezeichnet (in diesem Fall das Risiko von Geldwäsche und Terrorismusfinanzierung). In der Regel sollten die Erhebung und Verarbeitung personenbezogener Daten, um dem Zweck angemessen zu sein, an das von den Betroffenen ausgehende Risiko (z. B. für die „ökonomische öffentliche Ordnung") „angepasst" (berücksichtigt) werden. Dies würde die **Optimierung** des Eingriffs in das Recht auf Privatsphäre und den Schutz personenbezogener Daten ermöglichen.

In der Stellungnahme des EDSB zu dem Vorschlag zur Änderung der Geldwäscherichtlinie wurde festgestellt, dass entgegen dem vorgenannten Ansatz: „der Vorschlag (...) bestehende Garantien streicht, die ein **gewisses Maß an Verhältnismäßigkeit** gewährleistet hätten. Beispielsweise bei der Festlegung der Voraussetzungen für den Zugang von zentralen Meldestellen zu Informationen über finanzielle Transaktionen sieht der Vorschlag vor, dass in Zukunft der Bedarf zentraler Meldestellen an zusätzlichen Informationen **nicht länger und nicht nur durch verdächtige Transaktionen ausgelöst werden kann** (wie es jetzt der Fall ist [der sogenannte „risikobasierte Ansatz" zur Bekämpfung der Geldwäsche]), sondern auch durch eigene Analysen und Erkenntnisse der zentralen Meldestelle, und **dies sogar ohne dass zuvor verdächtige Transaktionen gemeldet wurden**. Aufgabe der Meldestellen ist es daher, sich als Einrichtungen nicht mehr auf *„Untersuchungen"*, sondern auf *„Erkenntnisse"* zu stützen. Letztere Vorgehensweise ähnelt eher der Datenminimierung als einer gezielten Untersuchung und hat natürlich Auswirkungen auf den Schutz personenbezogener Daten."

BEISPIEL 7: Leitlinien des EDSB zur Videoüberwachung

Der gleiche Ansatz, der darin besteht, **die Optimierung der Eingriffe in das Recht auf Privatsphäre und den Schutz personenbezogener Daten mit dem mit der Maßnahme verfolgten Ziel** (z. B. Sicherheit der Räumlichkeiten) zu ermitteln, wird in den Leitlinien des EDSB zur Videoüberwachung angewandt: „Wenn Videoüberwachungssysteme pragmatisch auf der Basis der beiden Grundsätze der Selektivität und der **Verhältnismäßigkeit** eingesetzt werden, können sie den Sicherheitserfordernissen gerecht werden und zugleich unsere Privatsphäre achten. Kameras können und sollten intelligent und

ausschließlich zur Lösung genau ermittelter Sicherheitsprobleme eingesetzt werden, um auf diese Weise das Zusammentragen von Bildmaterial, das nicht von Belang ist, auf ein Mindestmaß zu reduzieren. Damit werden nicht nur Eingriffe in die Privatsphäre auf ein Minimum reduziert, sondern es ist zugleich auch gewährleistet, dass die Videoüberwachung **zielgerichteter und letztendlich auch effizienter** eingesetzt werden kann." Die Leitlinien enthalten konkrete Hinweise (u. a. zu: Standorten von Kameras und Blickwinkeln; Zahl der Kameras; Zeiten der Überwachung; Auflösung und Bildqualität; besondere Datenkategorien; Bereiche, in denen verstärkte Erwartungen an den Schutz der Privatsphäre gestellt werden; Hightech- und/oder intelligente Videoüberwachung; Zusammenschaltung von Videoüberwachungssystemen).

BEISPIEL 8: Stellungnahme 5/2015 des EDSB zu dem Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität

„Nichtsdestotrotz **erfüllt der Vorschlag nach wie vor nicht** die wesentliche Voraussetzung für ein PNR-System, d. h. eine Einhaltung der Grundsätze der Notwendigkeit und der **Verhältnismäßigkeit**. Im Vorschlag wird nicht detailliert analysiert, inwieweit weniger einschneidende Maßnahmen den Zweck der EU-Regelung für PNR-Daten erfüllen könnten. Letztendlich führt die nicht zielgerichtete und umfangreiche Erhebung und Verarbeitung von Daten im Rahmen des PNR-Systems zu einer Maßnahme der allgemeinen Überwachung. Nach Ansicht des EDSB wäre der einzige Zweck, der dem Erfordernis der Transparenz und Verhältnismäßigkeit entspricht, die Verwendung der PNR-Daten auf Einzelfallbasis, allerdings ausschließlich im Fall einer ernsthaften und konkreten Bedrohung, die aufgrund konkreter Hinweise gegeben ist. Da **keine Informationen dahingehend vorliegen, dass die Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Maßnahmen angemessen belegt wurden**, ist der EDSB der Meinung, dass der Vorschlag **auch in geänderter Fassung nach wie vor nicht** den Anforderungen von Artikel 7, 8 und 52 der Charta der Grundrechte der Union, Artikel 16 AEUV und Artikel 8 der EMRK entspricht. Der EDSB fordert den Gesetzgeber auf, die Durchführbarkeit **selektiverer und weniger einschneidender Überwachungsmaßnahmen gegen aktuelle Bedrohungen anhand spezifischeren Initiativen zu untersuchen und sich gegebenenfalls auf gezielte Flugkategorien, Passagiere und Länder zu konzentrieren**."

Schritt 4: Analyse der Schlussfolgerungen zur Verhältnismäßigkeit der vorgeschlagenen Maßnahme. Lautet die Schlussfolgerung „nicht verhältnismäßig“, sind Garantien zu ermitteln und einzuführen, die für die Verhältnismäßigkeit der Maßnahme sorgen könnten.

Wenn die in Schritt 3 beschriebene Abwägung zu der Schlussfolgerung führt, dass eine vorgeschlagene Maßnahme **nicht** der Anforderung der Verhältnismäßigkeit entspricht, dann sollte die Maßnahme entweder **nicht vorgeschlagen** oder so **geändert** werden, dass sie diesen Anforderungen entspricht.

Vorgehensweise

- Führen Sie wie im *Bericht über die Prüfung der Verhältnismäßigkeit* beschrieben eine synthetische Analyse des **Ergebnisses** der in Schritt 3 durchgeführten Bewertung durch. Heben Sie hierbei insbesondere **die Faktoren** hervor, die zu der Schlussfolgerung geführt haben, dass „keine Verhältnismäßigkeit“ („negative Verhältnismäßigkeitsprüfung“) vorliegt;
- **Überarbeiten** Sie den Vorschlag und erarbeiten Sie, wenn möglich, eine oder mehrere **Verbesserungsmöglichkeiten**, die die kritischen Punkte ansprechen (**definieren** Sie den Zweck, die Kategorien und die Menge der zu verarbeitenden personenbezogenen Daten [59] enger und verringern Sie auf diese Weise die Auswirkungen, die die Maßnahme auf die Privatsphäre und den Datenschutz hat);
- Sehen Sie **Garantien** vor, die die Auswirkungen des Vorschlags auf die betreffenden Grundrechte verringern (sorgen Sie *beispielsweise* dafür, dass die Überprüfung durch Menschen erforderlich wird, falls im Rahmen von Regelungen vollautomatische Maßnahmen geplant sind) und führen Sie diese ein.[60]

---

[59] Siehe beispielsweise Seite 3 der **förmlichen Stellungnahme des EDSB zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Kreditdienstleister, Kreditkäufer und die Verwertung von Sicherheiten**, in der empfohlen wird, die Kategorien und die Menge der Dokumente (die personenbezogene Daten enthalten), die gemäß dem Vorschlag verarbeitet werden sollen, genauer festzulegen. Die förmliche Stellungnahme ist abrufbar unter:
https://edps.europa.eu/sites/edp/files/publication/19-01-24_comments_proposal_directive_european_parliament_de.pdf.

[60] Als Beispiel für **Garantien**, siehe **Stellungnahme des EDSB 4/2018 zu den Vorschlägen für zwei Verordnungen über die Einrichtung eines Rahmens für die Interoperabilität von IT-Großsystemen der EU**, Seite 18: „Die verschiedenen Instrumente machen **eine Überprüfung der Frage durch eine unabhängige Behörde** erforderlich, ob vor dem Zugang die genannten Bedingungen erfüllt sind. Im Fall von ETIAS, EES und Eurodac sind die Strafverfolgungsbehörden außerdem verpflichtet, **zunächst andere einschlägige Systeme abzufragen** (z. B. nationale Datenbanken, Europol-Daten, Prüm, VIS).“
- Siehe auch die Stellungnahme der FRA zum Thema „Auswirkungen auf die Interoperabilität und die Grundrechte“ vom 11. April 2018 in Bezug auf die Notwendigkeit einer unterschiedlichen Behandlung (Schutzvorkehrungen) schutzbedürftiger Personen, Bemerkungen (Seite 33): „Wird das Kaskadensystem durch einen optimierten Mechanismus wie die vorgeschlagene Überprüfung nach dem „Treffer/kein Treffer“-Verfahren anhand des gemeinsamen Speichers für Identitätsdaten ersetzt, bedeutet das, dass die Daten aller Personen als gleich sensibel angesehen werden und dass die Daten von Personen in einer **prekären Situation** (z. B. von Personen, die um internationalen Schutz nachsuchen) keine **verstärkten Schutzvorkehrungen** erfordern würden.“
- Bezüglich der Schutzvorkehrungen (Überprüfung durch Menschen, aussagekräftige Erläuterungen, Berichterstattung) im Zusammenhang mit einem möglichen Einsatz automatisierter Maßnahmen siehe **förmliche Stellungnahme des EDSB zu dem Vorschlag der Kommission zur Verhinderung der Verbreitung terroristischer Online-Inhalte**, Seite 9: „Gemäß Artikel 8 Absatz 1 unter den „Transparenzanforderungen“ müssen Hostingdiensteanbieter in ihren Nutzungsbedingungen ihre Strategie zur Verhinderung der Verbreitung terroristischer Inhalte darlegen, **gegebenenfalls** mit einer aussagekräftigen Erläuterung der Funktionsweise proaktiver Maßnahmen, einschließlich der Verwendung automatisierter Werkzeuge.“ (Hervorhebung

- Sorgen Sie für eine **Neubewertung** und für **Verfallsklauseln**: Höchstwahrscheinlich ist die zu klärende Situation sowohl aus technologischer als auch aus gesellschaftlicher Sicht durch ein sehr dynamisches Umfeld gekennzeichnet. Diese Ungewissheit könnte dazu beigetragen haben, dass die Maßnahme aus „aufsichtsrechtlichen Gründen" (Vorsorgeprinzip) als nicht verhältnismäßig eingestuft wurde, da Ungewissheiten hinsichtlich der tatsächlichen Auswirkungen der Maßnahme bestehen (z. B. aufgrund der vorgesehenen technologischen Werkzeuge). In diesem Fall ist es ratsam, zusätzlich zu weiteren Schutzvorkehrungen eine genaue **Neubewertung** (regelmäßige Überprüfungen/*nachträgliche* Bewertung der Auswirkungen, bei der auch unerwartete Folgen berücksichtigt werden) und **Verfallsklauseln** vorzusehen („sofern die Maßnahme nicht angepasst oder überarbeitet wird, *gilt sie ab dem... nicht mehr*"). Ferner könnten auch **bestimmte Aufsichtsmechanismen/-behörden** in Betracht gezogen werden.[61]
- Führen Sie die Bewertung der Erforderlichkeit und der Verhältnismäßigkeit **erneut** durch (beide Prüfungen, da die eingeführte Änderung dazu führen könnte, dass die einzelnen Schritte von Prüfung 1 und 2 erneut durchgeführt werden müssen).

Sachdienliche Beispiele

BEISPIEL 1: *Tele2 Sverige AB* (EuGH, C-203/15 und C-698/15, ECLI:EU:C:2016:970)

In der Rechtssache *Tele2* ist das **Ergebnis** der Bewertung der Verhältnismäßigkeit (als „strikte Erforderlichkeit" bezeichnet) **negativ**. Der Gerichtshof weist auf die **Faktoren** hin, die zu seiner negativen Bewertung geführt haben: Diese Faktoren beziehen sich insbesondere auf den (fehlenden) Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und der Bedrohung der öffentlichen Sicherheit, dem mit der Maßnahme entgegengewirkt werden soll (siehe Rn. 106 des Urteils).

Im Umkehrschluss legte der Gerichtshof auch ausdrücklich die Merkmale fest, die eine verhältnismäßige Maßnahme aufzuweisen hat. Insbesondere muss die Maßnahme „*erstens klare und*

hinzugefügt) Gemäß Artikel 9 Absatz 1 wird außerdem festgelegt, dass Hostingdiensteanbieter, die automatisierte Werkzeuge verwenden, wirksame und geeignete Schutzvorkehrungen treffen, um sicherzustellen, dass insbesondere Entscheidungen zur Entfernung oder Sperrung von Inhalten zutreffend und fundiert sind. Gemäß Artikel 9 Absatz 2 bestehen diese Schutzvorkehrungen, „**soweit angemessen**, in einer Aufsicht und Überprüfung durch Menschen, aber in jedem Fall immer dann, wenn eine eingehende Beurteilung des betreffenden Kontexts erforderlich ist, [...]". (Hervorhebung hinzugefügt) Hinsichtlich dieser Schutzvorkehrungen empfiehlt der EDSB, in Artikel 8 Absatz 1 und Artikel 9 Absatz 2 die Formulierung „soweit angemessen" durch „auf jeden Fall" zu ersetzen oder alternativ die Formulierung „soweit angemessen" zu streichen. Der EDSB merkt des Weiteren an, dass gemäß Artikel 6 Absatz 2 Hostingdiensteanbieter der für die Überwachung der Durchführung der proaktiven Maßnahmen gemäß Artikel 17 Absatz 1 Buchstabe c zuständigen Behörde einen Bericht über die ergriffenen proaktiven Maßnahmen, einschließlich der Verwendung automatisierter Werkzeuge, vorlegen sollten. Der EDSB empfiehlt, in Erwägungsgrund 18 des Vorschlags festzulegen, dass Hostingdiensteanbieter den zuständigen Behörden alle notwendigen Informationen über die verwendeten automatisierten Werkzeuge vorlegen sollten, um eine gründliche öffentliche Aufsicht über die Wirksamkeit der Werkzeuge zu gestatten und um sicherzustellen, dass diese nicht zu diskriminierenden, ungezielten, unspezifischen oder ungerechtfertigten Ergebnissen führen." Die förmliche Stellungnahme ist abrufbar unter: https://edps.europa.eu/data-protection/our-work/publications/comments/formal-comments-edps-preventing-dissemination_de.

[61] **Siehe Arbeitsunterlage 01/2016 der WP29 über die Rechtfertigung von Eingriffen in die Grundrechte auf Schutz der Privatsphäre und Datenschutz durch Überwachungsmaßnahmen bei der Übermittlung personenbezogener Daten (wesentliche europäische Garantien)**, WP237 vom 13. April 2016, Abschnitt 6 „Garantie C – **Es sollte ein unabhängiger Aufsichtsmechanismus bestehen"**, Seite 9-10. Das Dokument ist abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640363.

präzise Regeln über die Tragweite und die Anwendung einer solchen Maßnahme der Vorratsdatenspeicherung vorsehen und Mindesterfordernisse aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen. Sie muss insbesondere angeben, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der Vorratsdatenspeicherung vorbeugend getroffen werden darf, um so zu gewährleisten, dass eine derartige Maßnahme auf das absolut Notwendige beschränkt wird. Zweitens (...) muss die Vorratsdatenspeicherung objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen. Diese Voraussetzungen müssen insbesondere in der Praxis geeignet sein, den Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise wirksam zu begrenzen.

Bei der Begrenzung einer solchen Maßnahme im Hinblick auf die potenziell betroffenen Personenkreise und Situationen 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*." (Hervorhebung hinzugefügt)

Weitere **Bedingungen** für die Verhältnismäßigkeit der Maßnahme und für den Zugang zu den gespeicherten Daten durch die Strafverfolgungsbehörden sind in den Rn. 120-122 festgelegt, und zwar die vorherige Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle; das in Kenntnis setzen der betroffenen Person, sobald dies die Ermittlungen nicht mehr beeinträchtigen kann; die Bestimmung, dass die Daten in der Europäischen Union zu speichern sind; die Bestimmung, die Daten nach Ablauf ihrer Speicherungsfrist unwiderruflich zu vernichten. Diese weiteren Bedingungen können tatsächlich als **Schutzvorkehrungen** angesehen werden, die zusammen mit der Festlegung des Umfangs der Maßnahme dafür sorgen können, dass die Maßnahme verhältnismäßig wird.

In dem Urteil wird auch darauf Bezug genommen, dass *„die Einhaltung des Schutzniveaus, das das Unionsrecht im Rahmen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten garantiert, durch eine unabhängige Stelle überwacht wird, da eine solche Überwachung in Artikel 8 Absatz 3 der Charta ausdrücklich gefordert wird und nach ständiger Rechtsprechung des Gerichtshofs ein wesentlicher Bestandteil der Wahrung des Schutzes der Betroffenen bei der Verarbeitung personenbezogener Daten ist. 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 (vgl. in diesem Sinne Urteile Digital Rights, Rn. 68, und vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 41 und 58)."* (Hervorhebung hinzugefügt) Diese letzte Anforderung bezieht sich auf die Bedingung, **den Wesensgehalt des Grundrechts zu achten** und zählt zu **Prüfung 1 (Prüfung der Erforderlichkeit)**.

Bisher hat der Gesetzgeber ***keinen*** **neuen Vorschlag** für eine Richtlinie zur Vorratsdatenspeicherung vorgelegt. Für den Fall, dass er sich dazu entschließt, sollte er sowohl Prüfung 1 als auch Prüfung 2 durchführen, d. h. die Prüfungen der Erforderlichkeit und der Verhältnismäßigkeit.

BEISPIEL 2: *Ministerio Fiscal* (EuGH, C-207/16, ECLI:EU:C:2018:788)

In der Rechtssache *Ministerio Fiscal* wurde die Maßnahme vom Gerichtshof als **verhältnismäßig** in Bezug auf das Ziel betrachtet. Der Gerichtshof hat keine Anmerkung zu den kritischen Punkten gemacht, die der Gesetzgeber zu lösen hat. Daher ist es nicht erforderlich, die Maßnahme zu überarbeiten (den Zweck, die Tragweite und das Ausmaß des Eingriffs neu festzulegen; weitere oder

andere Schutzvorkehrungen vorzusehen) und/oder die Bewertung der Erforderlichkeit und Verhältnismäßigkeit **erneut durchzuführen**.

BEISPIEL 3: Gutachten 1/15 *PNR-Abkommen mit Kanada* (EuGH, ECLI:EU:C:2017:592)

Der Gerichtshof hielt die Maßnahme für **nicht** mit den Artikeln 7 und 8 sowie Artikel 52 Absatz 1 der Charta vereinbar. Die Faktoren, die zu einer solchen Schlussbewertung führten, betrafen im Wesentlichen: a) die mangelnde Klarheit und Spezifizierung der Maßnahme (und damit die Unmöglichkeit, die Auswirkungen zu messen); b) das Fehlen von Schutzvorkehrungen (z. B. Kontrolle durch eine unabhängige Behörde).

Gleichzeitig **erläuterte der Gerichtshof die Bedingungen** (die Formulierungen „*vorausgesetzt*“, „*soweit*“ wären voranzustellen), unter denen die Maßnahme verhältnismäßig wäre. Auf der einen Seite ist die Ermessensbefugnis des Gesetzgebers in dieser Rechtssache daher erheblich eingeschränkt, da er den Anweisungen des Gerichtshofs fristgerecht Folge zu leisten hat. Auf der anderen Seite wird die Arbeit des Gesetzgebers eindeutig erleichtert, denn wenn bei der Neuformulierung der Maßnahme die Empfehlungen des Gerichtshofes befolgt werden, sollte das Risiko einer erneuten Unvereinbarkeitserklärung des Gerichtshofes ausgeschlossen sein.

BEISPIEL 4: *Bevándorlási és Állampolgársági Hivatal* (EuGH, C-473/16, ECLI:EU:C:2018:36)

Der Gerichtshof war der Auffassung, dass Artikel 7 der Charta dahin auszulegen sei, dass er es **untersagt**, zur Beurteilung der Frage, ob die behauptete sexuelle Orientierung einer um internationalen Schutz nachsuchenden Person tatsächlich besteht, ein psychologisches Gutachten wie das im Ausgangsverfahren streitige zu erstellen und heranzuziehen, das auf der Grundlage eines projektiven Persönlichkeitstests die sexuelle Orientierung dieser Person abbilden soll.

In diesem Fall scheint es insbesondere angesichts der **sehr hohen Intensität** des Eingriffs schwierig, **Schutzvorkehrungen** vorzusehen, die die Anwendungder zu prüfenden Maßnahme verhältnismäßig machen könnten.