Bericht zur Bewertung der Auswirkungen einer Datenschutz-Grundverordnung auf die Polizeigesetze der Länder

Stand: 08.04.2015

Inhalt

I. Auftragslage und Schilderung der nachfolgend behandelten Fragestellung

Die von der Kommission im Januar 2012 vorgeschlagene Datenschutzreform besteht aus dem Entwurf einer *„Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafverfolgung sowie zum freien Datenverkehr*“, KOM [2012] 10. (DS-RL) sowie einem Entwurf der *„Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“* KOM [2012] 11 (DS-GVO). Eine Bund-Länder-Arbeitsgruppe hat zu der von der Europäischen Kommission vorgeschlagenen DS-RL Stellung genommen und hierzu einen Bericht erstellt (vgl. Beschluss der 197. IMK am 23/24.05d2015 zu TOP 7). Der AK II hat in seiner 241. Sitzung am 9./10. April 2014 mit seinem Beschluss zu TOP 26 den UA RV beauftragt, seine Arbeitsgruppe „Entwicklungen im EU-Datenschutz“ ergänzend zur bereits erfolgten Beurteilung möglicher Auswirkungen der DS-RL nun auch eine Bewertung der Auswirkungen der DS-GVO auf die Polizeigesetze der Länder vornehmen zu lassen. Ebenso wird das Bundespolizeigesetz in den Blick genommen, da innerhalb der sonderpolizeilichen Zuständigkeit auch die Gefahrenabwehr erfasst ist.

Der Auftrag erhält seine besondere Schwierigkeit durch den Umstand, dass es neben dem Kommissionsentwurf (VO-KOM) mittlerweile einen Standpunkt des Europäischen Parlaments gibt (VO-EP) und die Verhandlungen für einen Standpunkt des Rates auf Hochtouren laufen. Alle drei Entwürfe unterscheiden sich auch in wesentlichen Punkten z. T. erheblich. Hinzu kommt, dass sich der Standpunkt des Rates in den laufenden Verhandlungen noch stark verändert. Die Lettische Präsidentschaft beabsichtigt, spätestens im JI-Rat am 16. Juni 2015 einen (informellen) Standpunkt des Rates („allgemeine politische Ausrichtung“) zu beschließen, der dann gemeinsam mit der VO-KOM und VO-EP im sogenannten Trilog verhandelt wird. Die im Trilog erzielte Endfassung soll anschließend vom Rat als formeller Standpunkt beschlossen und vom Europäischen Parlament formell bestätigt werden. Welche endgültige Gestalt die DS-GVO dabei annehmen wird, ist angesichts der z.T. erheblichen Abweichungen der bisherigen Standpunkte bzw. Verhandlungsergebnisse unklar.

Im vorliegenden Bericht werden nach Möglichkeit die drei unterschiedlichen Entwürfe - Kommissionsentwurf, Entwurf des Europäischen Parlaments und der Ratsentwurf der Verordnung berücksichtigt.

Bezüglich des Entwurfes des Rates wird die von der Italienischen Präsidentschaft am 19. Dezember 2014 vorgelegte Fassung zugrunde gelegt (im Folgenden: VO-Rat-15395/14)[1]. Angesichts des Umfangs und der Komplexität der Themenstellung konzentriert sich der Bericht der AG auf wesentliche Kernfragen.

Eine weitere Schwierigkeit besteht darin, dass die Datenschutz-Grundverordnung bewusst als Grundverordnung konzipiert wurde, in ihrer Systematik weitgehend der Richtlinie 95/46/EG *„Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“* folgt und an unterschiedlichsten Stellen auf die nähere Ausgestaltung durch die Mitgliedstaaten angewiesen ist, was dem Regelungsinstrument Verordnung an sich grundsätzlich fremd ist. Die Frage, welche Spielräume den Mitgliedsstaaten am Ende verbleiben bzw. inwieweit es europarechtlich zulässig sein wird, etwa Regelungen der DS-GVO in Bezug zu nehmen oder gar zu wiederholen, ist unter Europarechtsexperten noch nicht eingehend diskutiert worden und somit weitgehend offen.

Die AG hat sich vor diesem Hintergrund von dem Ziel leiten lassen, der politischen Ebene möglichst rasch einen Überblick über wesentliche Problemstellungen der unterschiedlichen Lösungsansätze in Kommission, EP und Rat zu verschaffen.

---

[1] Fehlt ein ergänzender Hinweis im Text, so wurde diese Fassung zugrunde gelegt. Artikel ohne Kennzeichnung sind solche der Verordnung dieser Fassung.

II. Anwendungsbereich der DS-GVO und Abgrenzung zum Anwendungsbereich der DS-RL

1. Anwendungsbereich im Entwurf der Kommission

Die DS-GVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO) „Verarbeitung“ ist dabei jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung sowie das Löschen oder Vernichten der Daten (Art. 4 Abs. 3 DS-GVO). Da Informationstechnologien auch bei den Polizeien flächendeckend genutzt werden, wäre die DS-GVO umfassend anwendbar, wenn die DS-GVO nach ihrem Anwendungsbereich auf die polizeiliche Tätigkeit Anwendung fände.

Die Abgrenzung zwischen DS-GVO und DS-RL ist – nach bislang allen Fassungen der beiden Rechtsakte – nicht behördenbezogen, sondern zweckbezogen. D.h. ob eine Datenverarbeitung der DS-RL oder der DS-GVO unterfällt, entscheidet sich in erster Linie nach dem Zweck der beabsichtigten oder vorgenommenen Datenverarbeitung. Dabei korrespondieren die Anwendungsbereiche der beiden Rechtsakte derart, dass sämtliche Datenverarbeitungen von einem der beiden Rechtsakte umfasst sind, um zu verhindern, dass eine Schutzlücke entsteht. Nachfolgend zunächst eine Übersicht der derzeitigen Entwürfe[2] zur Abgrenzung:

Entwurf Kommission **Art. 2 Abs. 2e**	**Entwurf Rat in der Fassung vom** **19.12.2014 - Art. 2 Abs. 2e**
Die Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird	Die Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird
e) zur Verhütung, Aufdeckung,	e) zur Verhütung, Aufdeckung,

[2] In der Fassung des Europäischen Parlamentes wurde Art. 2 Abs. 2e nicht verändert.

Untersuchung oder Verfolgung einer Straftat oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden.	Untersuchung oder Verfolgung einer Straftat und *zu diesen Zwecken zur Aufrechterhaltung der öffentlichen Ordnung* oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen *staatlichen* Behörden.

Der von der KOM gewählte Ansatzpunkt rekurriert auf den „Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden“ und grenzt die Rechtsakte wie folgt ab:

Nach Art. 1 Abs. 1, 2 Abs. 1 DS-RL unterliegt Datenverarbeitung zum Zweck der Straftatenverhütung, Strafverfolgung, Straftatenaufdeckung und -vollstreckung der DS-RL. Korrespondierend dazu schließt die DS-GVO in der Fassung der Kommission in Art. 2 Abs. 2 e aus, dass diese auf die Verhütung, Aufdeckung, Untersuchung oder Verfolgung einer Straftat und zu diesen Zwecken auf die Aufrechterhaltung der öffentlichen Ordnung oder auf die Vollstreckung strafrechtlicher Sanktionen durch die zuständigen staatlichen Behörden Anwendung findet. Wesentlich für diese von der Kommission vorgeschlagene zweckbezogene Abgrenzung ist zunächst der Begriff der „Straftatenverhütung“. Nach deutschem Verständnis ist die Straftatenverhütung ein Unterfall der Gefahrenabwehr[3]. Nach den Polizeigesetzen der Länder[4] sind unter Straftaten in diesem Sinne rechtswidrige Taten zu verstehen, die den Tatbestand eines Strafgesetzes verwirklichen, wobei es nicht darauf ankommt, ob Schuld- oder Strafausschließungsgründe vorliegen. Während das Polizeirecht der Länder[5] zwischen der Verhütung (Verwirklichung des Tatbestands steht bevor) und der Unterbindung (Verwirklichung des Tatbestands hat bereits begonnen) differenziert, widerspräche eine solche Unterscheidung dem Zweck von DS-RL und DS-GVO. Eher stellt sich die Frage, ab welchem Zeitpunkt bei Datenerhebungen von einer Straftatenverhütung ausgegangen werden kann, wenn der Sachverhalt sehr unklar ist, aber u.U. eine Straftat im Raum stehen könnte. Selbst bei einer weiten Auslegung des Begriffs der Straftatenverhütung würde der zweckbezogene Ansatz der KOM dazu führen, dass nahezu zwangsläufig Zwecke verbleiben, auf die (auch) die Polizei angewiesen ist und die der DS-GVO unterfallen. Bereits frühzeitig wurden, auch von Seiten der Länder, Bedenken hiergegen geäußert. Der Anwendungsbereich der Ratsfassung vom 19.12.2014, der indessen noch Gegenstand

[3] vgl. z.B. Art. 11 Abs. 2 S. 1 Nr. 1 BayPAG für die Polizei, Art. 7 Abs. 2 Nr. 1 Bay LStVG für die Sicherheitsbehörden
[4] vgl. z.B. Art. 11 Abs. 2 S. 2 BayPAG
[5] vgl. Art. 11 Abs. 2 S. 1 Nr. 1 BayPAG

weiterer Verhandlungen im Rat ist, greift diese Bedenken lediglich vordergründig auf und lässt sich wie folgt zusammenfassen:

Die Anwendung der DS-GVO soll danach ebenso wie bei der Kommission für die Straftatenverhütung und -verfolgung ausgeschlossen sein. Ergänzend ist die Anwendung auch nach der Ratsfassung ausgeschlossen, wenn die Datenverarbeitung ***zu diesen Zwecken*** der Aufrechterhaltung der öffentlichen Ordnung dient. Der Einschub „zu diesen Zwecken“ führt im Ergebnis dazu, dass der Anwendungsbereich gleich bleibt, weil stets auch ein Zweck der Straftatenverhütung oder Verfolgung gegeben sein muss. Auch nach dieser in der in der derzeitigen Ratsfassung vom 19. Dezember 2014 vorgesehen Erweiterung unterfiele die reine nicht-straftatenbezogene Gefahrabwehr daher der DS-GVO. In diesem Fall wären die Rechtsgrundlagen zur Datenverarbeitung durch die Polizeien (auch) an der DS-GVO zu messen. Es wäre dann Art. 6 Abs. 3 i.V.m. Abs. 1e DS-GVO heranzuziehen, wenn man die europarechtliche Zulässigkeit einer nicht-straftatenbezogenen Maßnahme bewerten will. Soweit der von der Arbeitsgruppe favorisierte Ansatz die polizeiliche Tätigkeit einheitlich unter dem Regime der DS-RL zur regeln, nicht durchsetzbar sein sollte, sollte zumindest klargestellt sein, dass Vorschriften der deutschen Polizeigesetze einerseits der Umsetzung der DS-RL dienen können und gleichzeitig ein und dieselbe Norm als Rechtsgrundlage eines Mitgliedstaates im Sinne des Art. 6 Abs. 3 Abs. 1e DS-GVO herangezogen werden kann. Hier könnte sich die Aufnahme eines entsprechenden Erwägungsgrundes anbieten.

2. Derzeitige Debatte um die Abgrenzung und Vorschläge des Europäischen Parlaments und Rates

Bereits frühzeitig wurden, auch von Seiten der Länder, Bedenken geäußert, die gefahrenabwehrende Tätigkeit der Polizei unten den Anwendungsbereich der DS-GVO fallen zu lassen. Die Bundesregierung teilt diese Bedenken und hat sich bei den Verhandlungen zur DS-GVO dafür eingesetzt, die Anwendungsbereiche der beiden Rechtsakte besser abzugrenzen. In der Folge wurde die Frage durch die lettische Ratspräsidentschaft auf dem informellen JI-Rat in Riga erörtert. Die Mitgliedsstaaten wurden gebeten anzugeben, ob sie den Anwendungsbereich des Richtlinienentwurfs

- so wie von der Kommission vorgeschlagen beibehalten möchten, d. h. beschränkt auf die Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung, oder

- auf die „Aufrechterhaltung von Recht und Ordnung und den Schutz der öffentlichen Sicherheit“ ausweiten möchten.

Die Mehrzahl der Mitgliedsstaaten hat sich in der Folge für die zweite Option ausgesprochen. Kommission und Vertreter des Europäischen Parlaments haben deutlich gemacht, dass sie eine entsprechende Regelung nicht mittragen könnten. Eines der Kernprobleme aus polizeilicher Sicht bleibt damit vorerst ungelöst.

Aus Sicht der Arbeitsgruppe sollte weiterhin einem Vorschlag gefolgt werden, nach dem auch die gefahrenabwehrende Tätigkeit der Polizei einheitlich von der DS-RL erfasst wird. Sollte dieser Vorschlag nicht durchsetzbar sein, wäre zum einen die Auslegung des Begriffes „Straftatenverhütung“ für DS-GVO und DS-RL zu klären. Zum anderen sollte eine „Zweifels-Regelung“ aufgenommen werden. Diese könnte so aussehen, dass Datenverarbeitungen, bei denen die Straftatenverhütung ein denkbarer Zweck unter mehreren ist bzw. sein könnte, aber eine Zuordnung zu einem Zweck nicht oder noch nicht möglich ist, „im Zweifel“ generell der DS-RL unterfallen.

3. Datenverarbeitung durch die Polizeien von Bund und Ländern, die unter den Anwendungsbereich der DS-GVO fallen

a) Ausgangslage

Legt man den Geltungsbereich der DS-GVO wie von der Kommission vorgeschlagen und vom Europäischen Parlament bereits beschlossen zugrunde und berücksichtigt die Legaldefinition zur Datenverarbeitung so fallen sämtliche Befugnisse zur Datenerhebung, -verarbeitung und –nutzung, die der Polizei zur Erfüllung ihrer Aufgaben (Gefahrenabwehr, Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen, Erfüllung von durch andere Rechtsvorschriften zugewiesenen weiteren Aufgaben, wie z. B. Verfolgung und Ahndung von Ordnungswidrigkeiten, Schutz privater Rechte, Leistung von Vollzugshilfe für andere Behörden) zur Verfügung stehen, in den Anwendungsbereich der DS-GVO, soweit sie nicht den Zwecken der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten dienen und soweit die Verarbeitung der Daten ganz oder teilweise automatisiert erfolgt oder wenn nicht automatisiert erhobene oder erlangte Daten in einer Datei gespeichert sind bzw. werden sollen. Eine Datenverarbeitung i. S. der DS-GVO findet also lediglich dann nicht statt, wenn für die polizeilichen Maßnahmen eine mündliche oder fernmündliche Datenverarbeitung (Erhebung/Übermittlung) ausreicht und ein (automatisierter) Datenabgleich sowie die spätere Speicherung personenbezogener Daten aus dem Einsatz in einer Datei nicht erforderlich und nicht vorgesehen ist (z. B. bei sog.

schlichthoheitlichem Handeln während des Streifendienstes). Aber bereits die Aufzeichnung des Funkverkehrs durch die Einsatzleitstelle bei einem polizeilichen Einsatz stellt in der Regel eine automatisierte Verarbeitung personenbezogener Daten dar, ebenso der Abgleich personenbezogener Daten mit dem Inhalt polizeilicher Dateien und die Speicherung der Daten im elektronischen Einsatztagebuch, dem „Journal“. Es ist mithin kaum noch eine polizeiliche Maßnahme vorstellbar, die nicht wenigstens teilweise automatisiert erfolgt.

Nachfolgend werden die Bereiche polizeilicher Datenverarbeitung aufgeführt, in denen die DS-GVO Anwendung finden würde.

b) Polizeiliche Datenverarbeitung, die sowohl der DS-RL als auch der DS-GVO unterfällt

Zwar gibt es bei den Polizeien bereits heute rein strafprozessuale Dateien, beispielsweise Fall- und Analysedateien. Viele Dateien trennen allerdings nicht zwischen Daten, die zum Zweck der Strafverfolgung oder Straftatenverhütung erhoben wurden und Daten, die ausschließlich der nicht straftatenbezogenen Gefahrenabwehr dienen. Dies gilt beispielsweise für elektronisch geführte Einsatztagebücher oder Einsatzleitstellensysteme oder für das System EPOST810, das zur Übermittlung von personenbezogenen Daten von den Polizeien genutzt wird. Die Daten sind im System für ein Jahr für alle Nutzer einer Endstelle recherchierbar und können innerhalb dieser Frist erneut aufgerufen werden. Eine Differenzierung zwischen Gefahrenabwehr und Strafverfolgung/Straftatenverhütung ist in solchen Systemen nicht möglich bzw. nicht angestrebt. Ähnliches gilt, wie bereits für das Schengener Informationssystem ausgeführt, auch für Dateien, die Fahndungszwecken dienen, wie beispielsweise INPOL. Alle Fahndungsdaten zu Personen sind – unabhängig von Gefahrenabwehr oder Strafverfolgung – in **INPOL** gespeichert. Eine Differenzierung wäre zwar im Einzelfall in der Regel möglich, gleichwohl ist es denkbar, dass nach einer Person sowohl zur Aufenthaltsermittlung in einem Vermisstenfall als auch zur Vollstreckung eines Haftbefehls gefahndet wird. Diese Person würde sonst in zwei Dateien gespeichert werden müssen. Die Polizei müsste dann in zwei Systemen prüfen. Dies soll anhand folgender Beispiele näher aufgezeigt werden:

(1) Vermisstenfälle

In Deutschland werden vermisste Personen im polizeilichen Fahndungssystem (INPOL) zur Fahndung ausgeschrieben. INPOL stützt sich auf die Erfassung der Personendaten, die in Personaldokumenten aufgeführt sind. Personenbeschreibungen können nur in sehr begrenztem Umfang erfasst werden. Sofern eine vermisste Person im Besitz eines dieser Dokumente angetroffen wird, oder diese Angaben selbst machen kann, reicht INPOL aus.

Wird die vermisste Person jedoch als unbekannte hilflose Person angetroffen oder als unbekannte Leiche aufgefunden, sind weitere Identifizierungshilfsmittel erforderlich und müssen recherchierfähig dargestellt werden. Aus diesem Grunde wird eine Datei über „Vermisste, unbekannte Tote und unbekannte hilflose Personen (Vermi/Utot)“ beim Bundeskriminalamt geführt. In dieser werden im Inland vermisste Personen, unbekannte Leichen und unbekannte hilflose Personen aufgenommen. Da bei den meisten Vermisstenfällen kein Strafverfahren anhängig ist, fehlt jeder Bezug zur Straftatenverfolgung. Bei unbekannten Leichen, die Opfer eines Tötungsdelikts geworden sind, wäre die Anwendung der Regelungen der DS-GVO ausgeschlossen. Innerhalb einer Datei wären somit Daten gespeichert, die den Anwendungsbereich der DS-GVO eröffnen und Daten, die unter die in Umsetzung der DS-RL ergangenen Normen fallen.

Besonders augenfällig wird die Abgrenzungsproblematik, wenn zunächst unklar ist, ob eine Straftat vorliegt oder nicht. Wird ein Kind vermisst, kann es sich um einen Ausreißer handeln (dann Anwendbarkeit der DS-GVO), es kann aber auch eine Entführung oder ein Tötungsdelikt vorliegen (dann Anwendbarkeit der DS-RL). Die ermittelnde Polizei weiß zunächst nicht, welchem Rechtsregime die vorzunehmenden Datenverarbeitungen unterliegen. Dies stellt sich erst im Nachhinein heraus. Das anwendbare Recht kann aber weder ex post, noch willkürlich ex ante festzulegen sein. Zum Zeitpunkt der Vornahme einer jeden Handlung muss die Polizei rechtssicher und für Betroffene nachvollziehbar feststellen können, welches Datenschutzregime Anwendung findet.

Aus Sicht der Arbeitsgruppe muss daher gewährleistet sein, dass Dateien, in denen Daten, die sowohl der nicht-straftatenbezogenen Gefahrabwehr dienen als auch für die straftatenbezogene Gefahrenabwehr zu Recherchezwecken vorgehalten werden, weiterhin nach einheitlichen Regelungen eingerichtet und genutzt werden können. Hier ist eine klare Abgrenzung der Anwendungsbereiche beider Rechtsakte dringend geboten. Eine Klarstellung in der DS-RL und der DS-GVO wäre sinnvoll.

(2) Grenzpolizeiliche Aufgabenwahrnehmung

Die grenzpolizeiliche Aufgabenwahrnehmung umfasst, abgeleitet aus Art. 87 Abs. 1 S. 2 GG, die *polizeiliche Überwachung der Grenzen* einschließlich der Abwehr von Gefahren für die Grenzen wie auch die *Kontrolle des grenzüberschreitenden Verkehrs* (BVerfGE 97, 198, 214 = NVwZ 1998, 495, 496). Diese umfasst somit auch die Verhinderung von Straftaten, typischerweise der unerlaubten Einreise. Daneben dient sie auch der reinen Gefahrenabwehr, die nicht notwendigerweise einen Bezug zu Straftaten hat. Diese Aufspaltung von reiner Gefahrenabwehr und Verhinderung grenzspezifischer Delikte findet

sich auch in den einschlägigen Rechtsakten der EU. Nach Erwägungsgrund 6 des Schengener Grenzkodex (SGK) dienen Grenzkontrollen der Bekämpfung der illegalen Zuwanderung, Menschenhandel, Bedrohung der inneren Sicherheit, der öffentlichen Ordnung und der öffentlichen Gesundheit (*"internal security, public policy, public health and international relations").* Allein aus dieser Aufzählung ergibt sich, dass eine klare Zuordnung der Grenzkontrollen als Kernstück der grenzpolizeilichen Aufgabenwahrnehmung zur Straftatenverhütung und -verfolgung nicht vorgenommen werden kann, da aufgrund des SGK Bereiche umfasst sind, die entweder keinen Bezug zur Straftatenverhütung haben (öffentliche Gesundheit) oder nicht notwendigerweise der Straftatenverhütung dienen (*public policy*, *international relations*). Deutlich wird dies auch bei den Ausgleichsmaßnahmen für den Wegfall der Grenzkontrollen, dem Schengener Informationssystem (SIS). So ist in Art. 97 SDÜ die Ausschreibung von Vermissten und hilflosen Personen vorgesehen. Handelt es sich beispielsweise um einen "jugendlichen Ausreißer" fehlt jeder Bezug zur Straftatenverhütung oder -verfolgung. Die in der Richtlinie gewählte Technik, den Anwendungsbereich an den Zweck zu koppeln und nicht an die speichernde Stelle, führt für das Schengener Informationssystem dazu, dass Datenverarbeitungen aufgrund von Art. 97 SDÜ ohne Straftatenbezug sich nach der DS-GVO richten. Die von Art. 6 Abs. 3 DS-DVO geforderte Rechtsgrundlage wäre das SDÜ. Hinsichtlich der Auskunftserteilung verweist dieses auf das nationale Recht. Da die Auskunftserteilung detailliert in der DS-GVO geregelt ist, wären auf Ausschreibungen nach Art. 97 SDÜ - sofern keine Straftat (z. B. Kindesentführung) Anlass für die Ausschreibung war - zukünftig die Informationspflichten der DS-GVO anzuwenden. Für Ausschreibungen nach Art. 95 und 96 wäre weiterhin § 19 BDSG oder eine in Umsetzung der DS-RL ergangene entsprechende Regelung einschlägig, da aufgrund Art. 2 Abs. 2e DS-GVO die Anwendung der DS-GVO in diesen Fällen ausgeschlossen ist.

Auch dieses Beispiel zeigt, dass eine Abgrenzung der Rechtsakte, die allein auf Straftatenverhütung abstellt, im Ergebnis dazu führt, dass Daten innerhalb eines polizeilichen Informationssystems z. T. der DS-RL und z. T. der DS-GVO unterfallen. Aus Sicht der Arbeitsgruppe ist es auch hier zielführend, wenn dies weiterhin im nationalen Recht einheitlich ausgestaltet werden kann.

c) Polizeiliche Datenverarbeitung, die ausschließlich der DS-GVO unterfällt

(1) Reine Gefahrenabwehrmaßnahmen

Als Gefahrenabwehrbehörde übernimmt die Polizei vielfältige Aufgaben ohne jeglichen Straftatenbezug. Hier sind viele Fallgestaltungen denkbar, bei denen in unterschiedlichem

Maße personenbezogene Daten zu verarbeiten sind, beispielsweise die Einrichtung einer Personenauskunftsstelle (PAST) bei Unglücksfällen wie Zugunglücken u.ä. Neben Gefahrenabwehrmaßnahmen, die aufgrund der ihr allein zustehenden Befugnisse in die originäre Zuständigkeit der Polizei fallen, wird die Polizei auch häufig im Eilfall für andere Behörden tätig, denen Aufgaben der Gefahrenabwehr obliegen, wie z.B. der Feuerwehr, der Baubehörde oder der Gesundheitsbehörde. In diesen Fällen werden personenbezogene Daten erhoben, die durch die Polizei – soweit erforderlich – verarbeitet und genutzt werden. Häufig ist es zum Zeitpunkt des Eingreifens auch unklar, ob eine Straftat vorliegt oder nicht.

(2) Schutz privater Rechte

Der staatliche Schutz privater Rechte vor Gefährdung, Verletzung oder Vereitelung obliegt an sich der Zivilgerichtsbarkeit. Ist zivilgerichtlicher Schutz nicht rechtzeitig zu erlangen und besteht ohne polizeiliche/behördliche Hilfe die Gefahr, dass die Verwirklichung des Rechts vereitelt oder wesentlich erschwert wird, so ist die Polizei subsidiär zuständig. Sämtliche Polizeigesetze[6] enthalten Regelungen zur subsidiären Zuständigkeit der Polizei zum Schutz privater Rechte. Zwar kann auch hier der Zusammenhang mit einer Straftat bestehen, typische praxisrelevante Fälle haben jedoch oft keinen Bezug zur Straftatenverhütung oder -verfolgung, beispielsweise die Identitätsfeststellung zur Ermöglichung der Geltendmachung versicherungsrechtlicher Ansprüche eines Geschädigten gegenüber einem Schadensverursacher oder die Sicherstellung eines Kfz zum Schutz des Eigentums und des Besitzes.

(3) Ordnungswidrigkeiten

Der Entwurf der DS-GVO betrifft ausschließlich *„criminal offences“*, also Straftaten. Da im bereits vorgelegten Bericht zur DS-RL davon ausgegangen wurde, dass die Ordnungswidrigkeiten nicht der DS-RL unterfallen, ist auch für diesen Bericht davon auszugehen, dass die gesamte Datenverarbeitung im Bereich der Ordnungswidrigkeiten der DS-GVO unterfallen dürfte.

Aus Sicht der Arbeitsgruppe muss es auch nach Inkrafttreten der DS-GVO möglich sein, für alle Bereiche des Ordnungswidrigkeitenrechts spezifische Regelungen, insbesondere

[6] § 2 II PolG BW; Art. 2 II BayPAG; § 1 IV ASOG Bln; § 1 II BbgPolG; § 1 II BremPolG; § 3 III HbgSOG; § 1 III HessSOG; § 1 III SOG MV; § 1 III NdsSOG; § 1 II PolG NW; § 1 III POG RP; § 1 III PolG SL; § 2 II Sächs-PolG; § 1 II SOG LSA; § 162 II LVwG SH; § 2 II ThürPAG, § 2 II ThürOBG. – Für die Bundespolizei § 1 IV BPolG

Verfahrensregelungen zu erlassen, die es erlauben, diese Rechtsmaterie entsprechend der ihr innewohnenden Besonderheiten auf nationaler Ebene zu regeln.

(4) Zuverlässigkeitsüberprüfungen / Sicherheitsüberprüfungen

Die leichte Verwundbarkeit der für die Daseinsvorsorge bedeutenden Infrastruktur und die Entwicklungen bei terroristischen Gefährdungslagen führten in der Vergangenheit zu einer Erweiterung der Zuverlässigkeits- und Sicherheitsüberprüfungen. Bundes- und Landesgesetze sehen solche Überprüfungen deshalb für Personen vor, die in sicherheitsempfindlichen Bereichen (z. B. Flughäfen, Atomanlagen) tätig werden wollen oder einen Aufenthaltstitel begehren oder eingebürgert werden wollen. Zuverlässigkeits- und Sicherheitsüberprüfungen werden u. a. in folgenden Bereichen durchgeführt: Luftsicherheit, Atomsicherheit, Waffen, Sprengstoff, Einbürgerung, Akkreditierungsverfahren bei Großveranstaltungen, Einsatz von Fremdfirmen in sicherheitsrelevanten Bereichen, Einsatz von Dolmetschern in polizeilichen Verfahren.

Hierzu werden in verschiedenen behördlichen Systemen personenbezogene Daten (Nachname, Vorname, Geburtsdatum, Geburtsname Mitgliedschaften in Vereinen oder Organisationen usw.) der Betroffenen abgefragt. Dabei soll festgestellt werden, ob bei den betroffenen Personen gegebenenfalls Anhaltspunkte vorliegen, die gegen ihre Zuverlässigkeit sprechen. Die Überprüfung erfolgt durch die Polizei mittels eines Softwaretools (in Hessen beispielsweise das Abfragemanagement Softwaretool (AFM), das einen Datenabgleich mit verschiedenen polizeilichen automatisierten Systemen vornimmt wie Polas Hessen, Inpol Zentral, Schengener Informationssystem, Inpol-Fall-Dateien Crime-Dateien). Soweit beispielsweise die Mitgliedschaft in Vereinen oder Organisationen, die unter Beobachtung des Staatsschutzes stehen, abgefragt werden, können auch Daten zu religiösen oder politischen Anschauungen, mithin besonders geschützte Daten, verarbeitet werden.

Hinsichtlich der Abgrenzung der Anwendbarkeit von der DS-RL und der DS-GVO ist auf die ratio legis der Zuverlässigkeits- und Sicherheitsüberprüfungen abzustellen. Die Ermächtigungsgrundlagen ergeben sich zwar nicht aus den Polizeigesetzen der Länder. Vielmehr sind diese spezialgesetzlich geregelt. Es handelt sich jedoch bei allen Überprüfungsarten um eine reine Aufgabe der Gefahrenabwehr. Beispielsweise ist die waffenrechtliche Zuverlässigkeitsüberprüfung gem. § 5 WaffG zwingende Voraussetzung für sämtliche waffenrechtlichen Erlaubnisarten. Das Waffenrecht ist i. w. S. ein speziell geregeltes Sicherheitsrecht und hat materielle Polizeiaufgaben zum Gegenstand. Bei dem Umgang mit Waffen sollen die Belange der öffentlichen Sicherheit und Ordnung gewahrt

werden, § 1 Abs. 1 WaffG. Auch bei der Überprüfung nach dem Luftsicherheitsgesetz sollen aufgrund des hohen Gefährdungspotenzials des Luftverkehrs für die Allgemeinheit drohende Gefahren abgewendet werden. Damit unterfällt der Bereich der Zuverlässigkeits- / Sicherheitsüberprüfungen der DS-GVO. Fraglich ist, ob die Anwendung der DS-GVO nachteilige Auswirkungen auf die Durchführung der Zuverlässigkeits- und Sicherheitsüberprüfungen hätte. Anzudenken wäre, ob bei der Rechtmäßigkeit der Verarbeitung nach Art. 6 der DS-GVO, Einschränkungen zu erwarten sind. Dies wäre nicht der Fall, wenn die Datenübermittlung von der Polizei an die anfragende Stelle von dem Art. 6 DS-GVO gedeckt wäre.

In Betracht kommen Rechtsgrundlagen nach Art. 6 Nr. 1 c) DS-GVO oder nach Art. 6 Nr. 1 e) DS-GVO. Die Verarbeitung der Daten ist zur Gefahrenabwehr notwendig. Entweder aufgrund einer spezialgesetzlichen Ermächtigungsgrundlage (Art. 6 Nr. 1 c) oder um eine öffentliche Aufgabe zu erfüllen, die regelmäßig durch ein entsprechendes nationales Gesetz zugewiesen ist (Art. 6 Nr. 1 e). Sofern der Art. 6 der DS-GVO inhaltlich keine weiteren Einschränkungen erfährt, dürften die nationalen Regelungen im Bereich der Zuverlässigkeits- und Sicherheitsüberprüfungen als nähere Ausgestaltung von Art. 6 Abs. 1 c) und e) anzusehen sein.

Aus Sicht der Arbeitsgruppe muss gewährleistet sein, dass für Sicherheits- und Zuverlässigkeitsüberprüfungen auch innerhalb des Anwendungsbereichs der DS-GVO nationale Regelungen geschaffen werden können, die einen automatisierten Abgleich mehrerer Dateien vorsehen und die auch besondere Kategorien von Daten umfassen können.

4. Bedeutung der Öffnungsklauseln der DS-GVO

Wie soeben am Beispiel der Sicherheitsüberprüfungen noch einmal näher ausgeführt, besteht eine wesentliche Herausforderung darin, dass die DS-GVO an unterschiedlichsten Stellen auf die nähere Ausgestaltung durch die Mitgliedstaaten angewiesen ist. Dies ist dem Regelungsinstrument einer Verordnung grundsätzlich fremd. Aus Sicht der Arbeitsgruppe ist die Frage, welche Spielräume den Mitgliedsstaaten am Ende verbleiben, von großer Bedeutung. Sollte die nicht straftatenbezogene Gefahrenabwehr der DS-GVO unterfallen, so kann ein einheitliches Gefahrenabwehrrecht nur erhalten werden, wenn weitgehende Öffnungsklauseln bestehen, die eine einheitliche Regelung innerhalb beider Rechtsinstrumente ermöglichen. Im Einzelnen:

Die DS-GVO ist als Verordnung gemäß § 288 Abs. 2 S. 2 AEUV in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Nationales Recht, das einer Verordnung entgegensteht, bleibt zwar gültig, wird aber unanwendbar. Dies folgt aus dem Anwendungsvorrang des Unionsrechts gegenüber dem mitgliedstaatlichen Recht. Aus der Unmittelbarkeit der Geltung einer Verordnung ergibt sich, dass es mitgliedstaatlicher Umsetzung oder Ausführungsakte nicht bedarf und diese zudem unzulässig sind, wenn sie die unmittelbare Geltung der Verordnung verbergen könnten. In Bezug auf mitgliedstaatliches Recht, das von einer Verordnung abweicht, gilt ebenfalls der Anwendungsvorrang des Unionsrechts. Zwar bleibt abweichendes mitgliedstaatliches Recht in Kraft, denn weder der Unionsgesetzgeber noch der EuGH können es außer Kraft setzen. Rechtsnormen, die Wiederholungen oder Abweichungen enthalten, verstoßen aber gegen Art. 288 AEUV und die entsprechende Verordnung, was je nach Bedeutung und Tragweite der Normen Anlass für ein Vertragsverletzungsverfahren sein kann. Das nationale Recht müsste daher bereinigt bzw. angepasst werden. Ausnahmen von diesen Grundsätzen bestehen nur auf der Grundlage und im Rahmen von Öffnungsklauseln und soweit diese unionsrechtlich zulässig sind.

Die Kommission hielt die Anwendung der DS-GVO auf den öffentlichen Bereich für zwingend. Auch wenn hieran aus Sicht der Arbeitsgruppe Zweifel bestehen, verblieb es bei der Anwendung der DS-GVO auch auf den öffentlichen Bereich. Den besonderen Bedürfnissen soll durch entsprechende Öffnungsklauseln Rechnung getragen werden. Wesentlich sind dabei insbesondere folgende Möglichkeiten:

- Art. 6 Abs. 3e ermöglicht es den Mitgliedstaaten Rechtsgrundlagen für die Datenverarbeitung im nationalen Recht zu schaffen;

- Art. 1 Abs. 2a stellt klar, dass die Mitgliedstaaten in diesen Bereichen spezifische Regelungen erhalten, bzw. schaffen können,

- Art. 21 erlaubt es, die Rechte des Betroffenen in bestimmten Bereichen zu beschränken.

Aus Sicht der Arbeitsgruppe sollte für den polizeilichen Bereich gewährleistet werden, dass sowohl die Systematik als auch die Regelungen zur polizeilichen Datenverarbeitung weitestgehend erhalten werden können. Insoweit sind die Änderungen durch den Rat, insbesondere Art. 1 Abs. 2a und die Klarstellung im Erwägungsgrund zu begrüßen. Insbesondere wenn es bei der Abgrenzung zwischen der DS-GVO und der DS-RL, wie von der Kommission vorgeschlagen, bleibt, sollte es möglich bleiben, die polizeiliche

Datenverarbeitung für die Gefahrenabwehr einheitlich zu regeln. Dies ist nur dann gewährleistet, wenn die Öffnungsklauseln der DS-GVO einen ausreichenden Umsetzungsspielraum gewähren.

Im Hinblick auf die fehlende Rechtssicherheit einer Verordnung mit Öffnungsklauseln sollte ggf. in einem Erwägungsgrund klargestellt werden, dass der Umfang der Regelungsbefugnis der Mitgliedstaaten im Bereich der Öffnungsklauseln dem einer Richtlinie entspricht.

5. Zusammenfassende Bewertung

Nach allen bislang vorliegenden Fassungen findet die DS-GVO auf die nicht straftatenbezogene polizeiliche Tätigkeit Anwendung. Wie dargestellt, betrifft dies wesentliche Bereiche der polizeilichen Datenverarbeitung. Die Meinungsbildung im Rat ist hierzu jedoch noch nicht abgeschlossen. **Aus Sicht der Arbeitsgruppe sollte - entsprechend dem deutschen Vorschlag und den Erörterungen beim informellen JI-Rat in Riga im Januar 2015 - die Datenverarbeitung für die gesamte Gefahrenabwehr einheitlich der DS-RL unterstellt werden**.

Ergänzend sollte jedenfalls klargestellt werden, dass Datenverarbeitungen bei denen eine Zuordnung noch nicht möglich ist oder wenn die Straftatenverhütung ein Zweck unter vielen ist, generell der DS-RL unterfallen. Eine entsprechende Zweifelsregelung sollte in die DS-GVO aufgenommen und durch Erwägungsgründe erläutert und abgesichert werden. Eine solche Klarstellung, wonach doppel- oder mehrfachfunktionale Datenverarbeitungen nach der DS-RL zu bewerten wären, könnte die damit verbundenen Probleme weitgehend auflösen.

Zudem muss gewährleistet werden, dass **die bestehenden Öffnungsklauseln erhalten werden und so ausgestaltet sind, dass eine einheitliche Umsetzung von übergreifenden Regelungen der DS-RL und der DS-GVO möglich ist.** Eine Vorschrift eines Polizeigesetzes muss also sowohl als Umsetzung der DS-RL als auch als Vorschrift zur Ausfüllung einer Öffnungsklausel der DS-GVO herangezogen werden können.

III. Datenverarbeitung durch die Polizei auf Basis der DS-GVO - wesentliche Problemstellungen

1. Rechtsgrundlage gemäß der DS-GVO bei Datenerhebung und Verarbeitung durch die Polizei

Ausgangspunkt für die Datenverarbeitung der öffentlichen Stellen in der DS-GVO ist Art. 6 Abs. 1e. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde. In diesem Fall muss die Verarbeitung gemäß Art. 6 Abs. 3 DS-GVO eine Rechtsgrundlage entweder im Unionsrecht oder im innerstaatlichen Recht des Mitgliedstaates haben. Daraus folgt, dass Rechtsgrundlage für Datenverarbeitungen durch die Polizeien weiterhin die mitgliedstaatlichen Gesetze sind, auch soweit eine durch die Polizei vorgenommene Datenverarbeitung in den Anwendungsbereich der DS-GVO fällt. Nach Möglichkeit sollten dies die bestehenden nationalen Gesetze sein.

In der entsprechenden mitgliedstaatlichen Rechtsgrundlage muss gemäß Art. 6 Abs. 1e und Art. 6 Abs. 3 (Ratsfassung) entweder der Zweck der Verarbeitung festgelegt werden oder die Verarbeitung für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt. Dabei können „im Rahmen dieser Verordnung der für die Verarbeitung Verantwortliche, die Verarbeitungsvorgänge und -verfahren einschließlich von Maßnahmen zur Gewährleistung einer rechtmäßigen und nach Treu und Glauben vorgenommenen Verarbeitung in der entsprechenden Rechtsgrundlage aufgeführt werden“.

Am Beispiel des Polizeigesetzes des Landes Sachsen-Anhalt werden nachfolgende typische Datenerhebungs- und Verarbeitungsnormen genannt, die nicht oder nicht ausschließlich dem Zweck der Straftatenverhütung dienen:

- die Datenerhebung zur Abwehr einer Gefahr, zur Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen, zur Erfüllung von durch andere Rechtsvorschriften zugewiesenen weiteren Aufgaben, zum Schutz privater Rechte und zur Leistung von Vollzugshilfe (z. B. § 15 Abs. 1, 2 SOG LSA),

- die Erhebung von Telekommunikations- und Telemedienbestandsdaten zur Abwehr einer Gefahr, zum Schutz privater Rechte oder im Rahmen der Leistung von Vollzugshilfe zur Abwehr einer Gefahr (z. B. § 17a SOG LSA)

- die Identitätsfeststellung zur Abwehr einer Gefahr, zur Erfüllung von durch andere Rechtsvorschriften zugewiesenen weiteren Aufgaben oder zum Schutz privater Rechte (z. B. § 20 Abs. 1 SOG LSA),

- die Entnahme und molekulargenetische Untersuchung von Körperzellen hilfloser Personen oder Leichen und Speicherung der festgestellten DNA-Identifizierungsmuster zum Zwecke des Abgleichs mit denjenigen einer vermissten Person zur Identitätsfeststellung (z. B. § 20a SOG LSA),

- die Durchführung erkennungsdienstlicher Maßnahmen, wenn dies zur Feststellung der Identität angeordnet ist (z. B. § 21 Abs. 2 Nr. 1 SOG LSA),

- die Speicherung, Veränderung und Nutzung von rechtmäßig erhobenen oder „aufgedrängten“ Daten, soweit es zur Erfüllung der Aufgaben erforderlich ist sowie zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns (z. B. § 22 SOG LSA),

- die Aufzeichnung von Telefon- und Funkgesprächen durch die Lage- und Führungszentren der Polizei in dieser Funktion und darüber hinaus, soweit es im Einzelfall zur polizeilichen Aufgabenerfüllung erforderlich ist (z. B. § 23a SOG LSA),

- der Auskunftsanspruch der Polizei gegenüber Diensteanbietern nach TKG/TMG zur Ermittlung des Aufenthaltsortes gefährdeter Personen und der Einsatz technischer Mittel zur Standortermittlung eines von der gefährdeten Person mitgeführten Mobilfunkendgerätes (z. B. § 23b SOG LSA),

- das Verarbeiten oder Nutzen personenbezogener Daten über die zulässige Speicherungsdauer hinaus für Zwecke der Aus- und Fortbildung (z. B. § 25 Abs. 1 SOG LSA),

- die Übermittlung rechtmäßig erlangter personenbezogener Daten

    - zwischen Polizeidienststellen (einschließlich Bund und Länder) zur Erfüllung polizeilicher Aufgaben,

    - zwischen Sicherheitsbehörden und Polizei, soweit die Kenntnis der Daten für die Aufgabenerfüllung des Dritten, an den übermittelt wird, erforderlich

erscheint und im Übrigen von der Polizei an öffentliche Stellen zur Erfüllung polizeilicher Aufgaben, zur Abwehr einer Gefahr oder aufgrund tatsächlicher Anhaltspunkte zur Wahrnehmung einer sonstigen Gefahrenabwehraufgabe durch den Dritten, an den übermittelt wird, zur Verhütung oder Beseitigung erheblicher Nachteile für das Allgemeinwohl oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person (z. B. § 27 SOG LSA),

- die Übermittlung personenbezogener Daten von der Polizei an nichtöffentliche Stellen zur Erfüllung polizeilicher Aufgaben, Verhütung oder Beseitigung erheblicher Nachteile für das Allgemeinwohl oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person (z. B. § 28 SOG LSA),

- der Abgleich personenbezogener Daten von Störern oder - wenn aufgrund tatsächlicher Anhaltspunkte zur Erfüllung einer bestimmten polizeilichen Aufgabe erforderlich – von anderen Personen mit dem Inhalt polizeilicher Dateien und mit dem Fahndungsbestand (z. B. § 30 SOG LSA).

Es handelt sich um polizeirechtliche Befugnisse, mithin Befugnisse zur Gefahrabwehr. Diese dienen nach deutschem Rechtsverständnis dem Rechtsgüterschutz unabhängig davon, ob die Gefahr durch die Begehung einer Straftat oder durch sonstige Handlungen oder Ereignisse verursacht wird.“ Es sollte deshalb vermieden werden, dass ein bisher einheitlich geregeltes Rechtsgebiet, das auf einem differenzierten Ausgleich zwischen hoheitlichen Eingriffen, Grundrechten Betroffener und Schutzinteressen Dritter beruht, aufgrund unterschiedlicher Datenschutzregelungen aufgrund unterschiedlicher Datenschutz-regelungen auf europäischer Ebene nicht einheitlich geregelt werden kann. Wie bereits ausgeführt, ist es wichtig, dass Regelungen, wie die oben beispielhaft angeführten, auch durch den nationalen Gesetzgeber aufrechterhalten werden können, wenn diese der nicht straftatenbezogenen Gefahrenabwehr dienen.

Auch hier ist der Regelungsspielraum, der dem nationalen Gesetzgeber für den öffentlichen Bereich verbleibt, wesentlich. Klarstellende Regelungen, die deutlich machen, dass dem nationalen Gesetzgeber dieser Regelungsspielraum auch erhalten bleibt, obwohl dies dem Rechtsinstrument der Verordnung im Grundsatz fremd ist, sind unverzichtbar.

2. Verarbeitung besonderer Kategorien von personenbezogenen Daten

Ähnliche Unklarheiten, die der Wahl des Instrumentes einer „Grund"-Verordnung mit Öffnungsklausel geschuldet sind, bestehen auch bei Art. 9 DS-GVO. Danach sind besondere Kategorien von personenbezogenen Daten geschützt und dürfen nur in den in Art. 9 Abs. 2 genannten Ausnahmen verarbeitet werden. Für die polizeiliche Aufgabenwahrnehmung ist vor allem Art. 9 Abs. 2g DS-GVO einschlägig. Dazu muss die Verarbeitung erforderlich sein, um auf der Grundlage des Rechts eines Mitgliedstaats, das angemessene Garantien zur Wahrung der berechtigten Interessen der betroffenen Person vorsieht, aus Gründen des öffentlichen Interesses eine Aufgabe zu erfüllen.

Eine Speicherung von besonderen Kategorien von Daten bei Polizeien erfolgt beispielsweise im Bereich Staatsschutz oder bei personengebundenen Hinweisen. Es ist unstreitig, dass im Polizeibereich die Speicherung von den in Art. 9 DS-GVO genannten besonderen Kategorien von Daten erforderlich ist. Daher muss gewährleistet sein, dass die Speicherung und Nutzung solcher Daten für die tägliche polizeiliche Arbeit zulässig ist. Nach der hier zugrunde gelegten Fassung des Textes des Rates verbleibt den Mitgliedstaaten hier derzeit ein Regelungsspielraum, wie ausgeführt ist auch hier klarzustellen, dass der Regelungsumfang, der dem Mitgliedstaat zur Verfügung steht, dem einer Richtlinie entspricht.

Für den Bereich der Verarbeitung solcher besonderer Kategorien Daten für den öffentlichen Bereich sollte keine Verschärfung der Voraussetzungen vorgenommen werden, wie sie sich im Entwurf des Europäischen Parlamentes finden - dort wird eine solche Verarbeitung nur gestattet, um eine Aufgabe zu erfüllen, an der ein *„hohes öffentliches Interesse"* besteht.

3. Zweckänderung unter dem Regime von DS-RL und DS-GVO

Die Frage, ob ein einmal erhobenes Datum durch die Polizei gespeichert und weiterverarbeitet werden kann, ist für die Polizeiarbeit von besonderer Bedeutung.

a) Ausprägung des Zweckbindungsgrundsatzes bei der polizeilichen Datenverarbeitung

Der Zweckbindungsgrundsatz gehört im deutschen Recht zu den wesentlichen datenschutzrechtlichen Prinzipen. Er ist in allen Polizeigesetzen umgesetzt. Dabei ist anerkannt, dass datenschutzrechtliche Generalnormen zulässig sind. In diesen Fällen ist Zulässigkeitsvoraussetzung für die Datenerhebung und -verarbeitung, dass diese zur

Aufgabenerfüllung erforderlich ist (beispielsweise § 21 BPolG; § 31 BayPAG). Die personenbezogenen Daten können durch die Polizei in den entsprechenden Datenbanken gespeichert und in der Folge für weitere gefahrenabwehrende Maßnahmen der Polizei genutzt werden. Die Daten werden für den gleichen übergeordneten Zweck, nämlich die Gefahrenabwehr, verarbeitet und genutzt. Selbst wenn man davon ausgehen würde, dass die Verwendung von nach den sogenannten Datenerhebungsgeneralklauseln (z.B. § 15 SOG LSA) erhobenen personenbezogenen Daten nicht vom ursprünglichen Erhebungszweck umfasst wäre, so wäre eine (spätere) Nutzung oder Verarbeitung für andere Zwecke im Regelfalle zulässig. Die meisten Polizeigesetze sehen vor, dass bereits gespeicherte Daten genutzt oder verarbeitet werden können, wenn sie auch für die angestrebte neue Nutzung oder Verarbeitung hätten erhoben werden dürfen.

Von diesen Datenerhebungsgeneralklauseln kann die Polizei jedoch nur Gebrauch machen, soweit die Befugnisse zur Datenerhebung, -verarbeitung oder -nutzung nicht speziell geregelt sind. Gerade bei besonders intensiven Eingriffen in das Recht auf informationelle Selbstbestimmung unterliegen die Daten im Regelfall einer strengeren Zweckbindung (mit Ausnahmen z. B. nur bei Gefahr für Leib oder Leben oder der Begehung einer Straftat von erheblicher Bedeutung). Bei eingriffsintensiven Maßnahmen sind die Daten zudem entweder unverzüglich nach Zweckerreichung zu löschen (§ 31a BPolG) oder besonders zu kennzeichnen, so dass diese nur für spezifische Zwecke genutzt werden dürfen; d.h. bei solchen Daten ist eine weitere Nutzung, ein Zweckwechsel, nur bei Vorliegen weiterer Voraussetzungen zulässig (so beispielsweise auch § 38 Abs. 1 PolBW).

Betrachtet man dies systematisch, so ergibt sich bei fast allen deutschen Polizeigesetzen folgendes Bild: Bei weniger eingriffsintensiven Datenverarbeitungen werden diese regelmäßig auf die Aufgabenwahrnehmung als Zweck gestützt. Die entsprechenden Polizeigesetze enthalten insoweit üblicherweise Generalklauseln. Sind die Daten für die Aufgabenerfüllung weiterhin erforderlich, können diese in polizeilichen Datenbanken gespeichert werden. Eine weitere Nutzung ist zulässig, wenn weitere Voraussetzungen vorliegen; beispielsweise verlangt § 29 BPolG, dass bei einem Zweckwechsel innerhalb der allgemeinen Aufgabenerfüllung die Daten auch für den neuen spezifischen Zweck hätten erhoben werden dürfen. Ist eine Datenerhebung wegen ihrer Eingriffsintensität an besondere Voraussetzungen geknüpft, ist der Zweck häufig enger. So werden auf Tatbestandsseite weitere Voraussetzungen verlangt (bestimmte Schwere an Straftaten), zusätzlich sind häufig weitere Verfahrensgarantien aufgenommen (beispielsweise Genehmigung durch Behördenleitung).

Aus Sicht der Arbeitsgruppe muss es auch unter Geltung der DS-GVO möglich sein, Daten zu speichern und für andere spezifische Zwecke innerhalb der übertragenen Aufgabe zu nutzen, wenn dies für die Aufgabenerfüllung erforderlich ist. Unter welchen Voraussetzungen Daten für weitere, innerhalb der Aufgabe liegende spezifische Zwecke genutzt werden können, sollte durch den nationalen Gesetzgeber ausgestaltet werden.

b) Zweckbindung und Zweckänderung in der DS-GVO

Unklar ist, unter welchen Voraussetzungen Daten, die im Rahmen einer unter die DS-GVO fallenden Maßnahme erhoben und für diese gespeichert wurden, für die weitere Aufgabenwahrnehmung noch zur Verfügung stehen. Die DS-GVO verlangt zunächst im auf die Datenverarbeitung der Polizei anwendbaren Art. 6 Abs. 3 Satz 2 DS-GVO, dass der Zweck der Verarbeitung in der Rechtsgrundlage festgelegt ist (1. Alternative) oder für die Aufgabenerfüllung erforderlich ist (2. Alternative). Aus dem Wortlaut wird nicht deutlich, ob die bisher zulässigen datenschutzrechtlichen Generalklauseln weiterhin zulässig sind. Der Wortlaut des Art. 6 Abs. 3 Satz 2, 2. Alternative DS-GVO spricht letztlich eher dagegen, da der Zweck für die Aufgabenerfüllung erforderlich sein soll. Im Umkehrschluss könnte dies indessen bedeuten, dass die Aufgabenerfüllung allein nicht allgemeiner Zweck einer Datenverarbeitung sein kann. Der Zweck nach der DS-GVO wäre dann deutlich enger zu verstehen als nach den Polizeigesetzen. Art. 5 Abs. 1 lit. b DS-GVO spricht von genau festgelegten Zwecken für die Datenverarbeitung, wobei diese Regelung nach Art. 21 (Ratsfassung) wie schon bisher unter der Datenschutz-Richtlinie 95/46 von den Mitgliedstaaten beschränkt bzw. näher ausgestaltet werden kann. Aus polizeilicher Sicht wäre demgegenüber eine Verengung abzulehnen, insbesondere wenn dies dazu führen würde, dass die bisherigen Generalklauseln nicht mehr zulässig wären.

Wesentlich ist in diesem Zusammenhang auch, unter welchen Voraussetzungen Zweckänderungen eines einmal erhobenen Datums zulässig sind. Nach der DS-GVO in der Fassung des Rates und der Kommission können Daten für weitere Zwecke genutzt werden, wenn diese mit dem Zweck der ursprünglichen Erhebung vereinbar sind. In der Fassung der Kommission ergibt sich dies aus dem Umkehrschluss des Art. 6 Abs. 4 DS-GVO und wird ergänzend im Erwägungsgrund 40 klargestellt. In der Fassung des Rates wird dies aufrechterhalten und durch Hinweise ergänzt, welche Punkte für die Beurteilung der Vereinbarkeit der Zwecke besonders zu beachten sind (Art. 6 Abs. 3a DS-GVO).

Die Verwendung für Zwecke, die mit dem ursprünglichen Erhebungszweck nicht vereinbar sind, ist zulässig, wenn dies in einem Gesetz geregelt ist, das auf den Datenverarbeiter

anwendbar ist. Unklar ist in diesem Zusammenhang, ob ein solches Gesetz auch Regelungen zur Frage treffen kann, welche Verarbeitungen mit dem ursprünglichen Verarbeitungszweck vereinbar sind.

Aus Sicht der Arbeitsgruppe ist es wünschenswert, dass die Weiterverwendung zu Zwecken, die mit dem ursprünglichen Erhebungszweck vereinbar sind, erhalten bleibt und die Möglichkeit besteht, die Kompatibilität von Zwecken entsprechend den geltenden Regelungen in den Polizeigesetzen in nationalen Gesetzen näher zu konkretisieren und festzulegen.

c) Zweckbindung und Zweckänderung in der Fassung des Europäischen Parlaments und der Kommission

Wie ausgeführt ist es aus polizeilicher Sicht unerlässlich, dass die Polizei Daten auch aufgrund der bestehenden Generalklauseln erheben kann und dass diese Daten - sofern erforderlich - auch für die weitere polizeiliche Aufgabenwahrnehmung zur Verfügung stehen. Insoweit muss auch ein Zweckwechsel für Zwecke innerhalb der Aufgabenwahrnehmung wie nach dem geltenden und verfassungsrechtlich nicht zu beanstandenen Recht des Bundes und der Länder möglich sein. Bei der Kommissionsfassung wäre eine Weiterverwendung jedenfalls zulässig, wenn diese kompatibel ist. Falls diese nicht kompatibel ist, bedürfte es einer gesetzlichen Grundlage. Dies könnte dann im jeweiligen Polizeigesetz nach Art. 6 Abs. 4 DS-GVO gesetzlich geregelt werden. Aus Sicht der Arbeitsgruppe sollte die nationale Regelung auch Fälle erfassen können, in denen bereits kompatible Zwecke vorliegen.

Es ist allerdings nicht klar, ob dies bei Zugrundlegung der Fassung des Europäischen Parlamentes noch möglich wäre. In dieser sind der in Ratsfassung bestehende Art. 6 Abs. 3a und Art. 6 Abs. 4 gestrichen. **Dies könnte dazu führen, dass eine Weiterverarbeitung zu einem anderen als dem ursprünglichen Erhebungszweck nicht zulässig ist, sofern nicht in jeder Weiterverarbeitung zu einem anderen Zweck eine allgemeine Datenverarbeitung zu sehen ist, die durch Art. 6 Abs. 1 abgedeckt ist. Ein praktisches Verbot der Datenweiterverarbeitung zu anderen Zwecken wäre eine massive Abkehr von den Grundsätzen des Polizeirechts und des Datenschutzrechts von Bund und Ländern und aus Sicht der Arbeitsgruppe inakzeptabel.**

d) Sonderproblem: Zweckänderungen für Verwaltungszwecke

Auch für Zwecke, die nicht direkt Maßnahmen der Aufgabenwahrnehmung, sondern sogenannten Nebenzwecken dienen, muss gewährleistet sein, dass einmal erhobene Daten hierfür genutzt werden können bzw. dass der Gesetzgeber für diese Zwecke festlegen kann,

dass die Datenverarbeitung hierzu zulässig ist. Dies ist insbesondere für die nachfolgenden Bereiche von großer Bedeutung:

(1) Dokumentation und Vorgangsverwaltung

Die Polizei kann zur Vorgangsverwaltung oder zur befristeten Dokumentation ihres Handelns personenbezogene Daten speichern und nutzen, etwa für spätere Auskünfte an Betroffene, Gerichtsverfahren oder parlamentarische Untersuchungsausschüsse. Die Nutzung der bei den Polizeien geführten elektronischen Vorgangsbearbeitungssysteme, Einsatztagebücher oder Journale zu diesen Zwecken muss auch für Datenverarbeitungen, die unter den Anwendungsbereich der DS-GVO fallen, weiterhin möglich sein. Aus Sicht der Arbeitsgruppe kann man durchaus mit guten Argumenten vertreten, dass die Dokumentation und Vorgangsbearbeitung Teil der polizeilichen Aufgabenwahrnehmung ist und somit vom ursprünglichen Erhebungszweck umfasst wird. Geht man davon aus, dass die Dokumentation der polizeilichen Maßnahme ein neuer Verarbeitungszweck ist, muss die Weiterverarbeitung nach Art. 6 Abs. 3a mit dem Zweck, für den die Daten ursprünglich erhoben wurden, kompatibel sein. Legt man die in der Ratsfassung genannten Kriterien zugrunde, könnte von einer Kompatibilität der Zwecke ausgegangen werden, da ein untrennbarer Zusammenhang zwischen dem Ursprungszweck und der Dokumentation oder Vorgangsverwaltung besteht. Selbst wenn man die Kompatibilität verneinen würde, bestände nach Art. 6 Abs. 4 i.V.m Art. 6 Abs. 1e die Möglichkeit eine solche Zweckänderung national zu regeln.

Dass sowohl die Möglichkeit der Dokumentation als auch der elektronischen Vorgangsbearbeitung durch den Mitgliedstaat geregelt werden kann, ist aus Sicht der Arbeitsgruppe unverzichtbar. Das Polizeirecht als staatliches Eingriffsrecht zur Gefahrenabwehr muss überprüfbar sein, hierfür ist eine ordnungsgemäße Dokumentation und Vorgangsbearbeitung unerlässlich. Dies gilt gleichermaßen für die Strafverfolgung. Die Erfüllung der Verpflichtung zur effektiven Strafverfolgung unterliegt der gerichtlichen Kontrolle (§§ 172 ff. StPO) und setzt eine detaillierte und vollständige Dokumentation des Ermittlungsverlaufs voraus.[7] Die Dokumentation erfolgt bei der Polizei sowohl für die Gefahrenabwehr und die Strafverfolgung einheitlich, beispielsweise in Einsatzleitstellensystemen und elektronischen Vorgangsbearbeitungssystemen. Es wird dabei nicht notwendigerweise unterschieden, ob eine Maßnahme der nicht straftatenbezogenen Gefahrenabwehr, der Straftatenverhütung oder der Strafverfolgung dient. Insoweit muss eine einheitliche Ausgestaltung im Anwendungsbereich der DS-GVO

[7] BVerfG, Beschluss vom 6.10.2014 - 2 BvR 1568/12.

und der DS-RL möglich sein, denn nur so kann eine einheitliche Vorgangsverwaltung und Dokumentation innerhalb der polizeilichen Datenverarbeitung erreicht werden.

Aus Sicht der Arbeitsgruppe ist es deshalb unerlässlich, dass die ordnungsgemäße Dokumentation und Vorgangsverwaltung weiterhin einheitlich für den gesamten Bereich der Gefahrenabwehr vorgenommen werden kann und dass dies auf nationaler Ebene ausgestaltet werden kann.

(2) Aus- und Fortbildung

Zwar ist es nicht immer erforderlich, bei der Aus- und Fortbildung mit Echtdaten zu arbeiten, aber es gibt viele Fälle, in denen sich dies nicht vermeiden lässt. Teilweise ist es kaum möglich, beispielsweise bei komplexen polizeilichen Systemen, Test- und Ausbildungsdatenbanken zu erstellen, die die gesamte Fülle an Gestaltungen abbilden, die sich in der Praxis finden. Ähnliches gilt auch für Videoaufzeichnungen; diese können für Ausbildungszwecke sicherlich meistens gepixelt werden, jedoch nicht immer. Bereits heute sehen die Polizeigesetze die Verwendung von Daten für die Ausbildung vor, so beispielsweise § 37 PolBW oder § 29 BPolG. **Auch hier gilt, dass aus polizeilicher Sicht der nationale Gesetzgeber weiterhin einen entsprechenden Handlungsspielraum haben sollte, um die Verwendung polizeilicher Daten zu Aus- und Fortbildungszwecken zu gewährleisten.**

4. Übermittlung von Daten durch öffentliche oder nicht-öffentliche Stellen an die Polizei

a) Sachlicher Anwendungsbereich der Datenschutz-Grundverordnung

Polizeiarbeit ist davon geprägt, dass die Polizei Informationen benötigt. Ohne Informationen und Hinweise von Bürgern ist polizeiliche Arbeit kaum möglich. Die Weitergabe von Informationen, die von öffentlichen oder nicht-öffentlichen Stellen erhoben und verarbeitet wurden, an die Polizei unterfiele mit Inkrafttreten der DS-GVO einheitlich der DS-GVO (Art. 2 Abs. 1 DS-GVO). Die DS-GVO in ihrer Fassung vom 3. Dezember 2014 könnte – wie nachfolgend näher ausgeführt wird – zur Folge haben, dass bestimmte Datenübermittlungen an die Polizei, die zur Wahrung der berechtigten Interessen eines Dritten und für eine effektive Strafverfolgung von Bedeutung sind, künftig nicht mehr zulässig sind. Grund hierfür ist der **fehlende Verweis** in der Zweckänderungsvorschrift des Art. 6 Abs. 4 Satz 1 DS-GVO auf den **Buchstaben f** des Art. 6 Abs. 1 DS-GVO.

b) Datenübermittlungen an die Polizei durch öffentliche Stellen der Polizei auf Ersuchen (Abgrenzung Datenschutz-Grundverordnung – Richtlinie)

Beispiel: Die Polizei ersucht das Jugendamt zur Datenübermittlung in einem Fall, in dem der Verdacht der Kindesmisshandlung begründet sein könnte. Gem. § 68 Abs. 1 Satz 1 SGB X übermittelt das Jugendamt die Daten.

Die Richtlinie gilt gem. Art. 2 Abs. 1 für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den in Art. 1 Abs. 1 der Richtlinie genannten Zwecken (Straftatenverhütung, Strafverfolgung, Strafvollstreckung). Eine „Verarbeitung“ von Daten ist gem. Art. 3 Abs. 3 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie z. B. das Erheben oder Abfragen der Daten. Nach dem Begriffsverständnis des deutschen Datenschutzrechts wird unter Datenerhebung das Beschaffen von personenbezogenen Daten verlangt, wobei das Beschaffen ein aktives Verhalten der erhebenden Stelle zur Erlangung der Informationen voraussetzt (Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, S. 762 f., Rdn. 149). Danach wird man davon ausgehen können, dass eine Datenübermittlung an die Polizei auf deren Ersuchen eine Datenerhebung durch die Polizei darstellt, die unter den Anwendungsbereich der Richtlinie fällt, sofern die Polizei sie zu den in der Richtlinie genannten Zwecken angefordert hat. Für die Datenübermittlung an die Polizei durch öffentliche oder private Stellen auf Ersuchen der Polizei (wie in dem oben genannten Beispielsfall) bedarf es – auch trotz des Ersuchens – einer Übermittlungsregelung, entsprechend des vom Bundesverfassungsgericht postulierten

Doppeltürprinzips. D.h. bei öffentlichen Stellen muss in diesen Fällen eine Rechtsgrundlage im nationalen Recht gemäß Art. 6 Abs. 1 e i.V.m. Art. 6 Abs. 4 DS-GVO bestehen. Im oben genannten Beispielsfall findet sich eine entsprechende Rechtsgrundlage in § 68 SGB X. Ist im jeweiligen Fachgesetz keine Rechtsgrundlage für eine Übermittlung vorhanden, ist eine Datenübermittlung bislang über einen Rückgriff auf die Generalklausel des § 15 BDSG und § 28 Abs. 2 Nr. 2 BDSG zulässig. Geht man für die Zukunft davon aus, dass auch die Übermittlung an die Polizei durch öffentliche und nicht-öffentliche Stellen für deren straftatenbezogene Aufgabenwahrnehmung der DS-GVO unterfällt, so muss in der DS-GVO klargestellt werden, dass eine solche Übermittlung zulässig ist, auch wenn der Übermittlungszweck vom Erhebungszweck abweicht.

Hier wird allerdings erneut deutlich, welche Konsequenzen die rein zweckbezogene Abgrenzung hat. Man könnte ebenso argumentieren, dass die Übermittlung einer Behörde, die gefahrabwehrende Aufgaben hat, wie im genannten Beispiel das Jugendamt zum Schutze des Kindes, hinsichtlich der Übermittlung von straftatenbezogenen Daten vom Anwendungsbereich der DS-RL unterfällt und in diesen Fällen die Übermittlungsvorschrift der Umsetzung der DS-RL dient.

c) Datenübermittlung durch öffentliche Stelle an die Polizei aufgrund gesetzlicher Verpflichtung oder aus eigenem Ermessen

(1) Aufgrund einer gesetzlichen Verpflichtung

Beispiel: Ein Mitarbeiter des Jugendamtes übermittelt personenbezogene Daten eines Kindes und der Eltern an die Polizei, um das betroffene Kind vor drohenden schweren körperlichen Misshandlungen durch die Eltern zu schützen.

i. Geltende Rechtslage

Die Datenübermittlung an die Polizei ist gem. § 8 a Abs. 3 Satz 2 SGB VIII zulässig und geboten, da hier das Kindeswohl akut gefährdet und ein sofortiges Tätigwerden zum Schutz des Kindes erforderlich ist.

ii. Rechtslage nach Inkrafttreten der Datenschutz-Grundverordnung

Geht man von der Unvereinbarkeit des Erhebungs- und des Weiterverarbeitungszwecks aus, ist die Datenübermittlung an die Polizei dennoch zulässig, weil sie gem. Art. 6 Abs. 4 i. V. m. Abs. 1 c der Erfüllung einer gesetzlichen Verpflichtung des Mitarbeiters des Jugendamtes

aus § 8 a Abs. 3 Satz 2 SGB VIII dient und darüber hinaus auch nötig ist, um lebenswichtige Interessen des betroffenen Kindes zu schützen (Art. 6 Abs. 4 i. V. m. Abs. 1d).

(2) Datenübermittlung an die Polizei durch eine öffentliche Stelle nach eigenem Ermessen

Beispiel: Ein Mitarbeiter des Jugendamtes will eine Kindesmisshandlung anzeigen und übermittelt Sozialdaten an die Polizei.

i. Gegenwärtige Rechtslage

Nach § 69 Abs. 1 Nr. 1 SGB X ist eine Übermittlung an die Polizei zulässig, wenn dies zur Erfüllung der eigenen Aufgabe der übermittelnden Stelle erforderlich ist. Die Aufgabe der Jugendhilfe umfasst Leistungen zugunsten des Minderjährigen und seiner Familie und ist u. a. auf den Schutz des Minderjährigen vor Gefahren für sein Wohl ausgerichtet. Die Übermittlungsbefugnis steht allerdings unter dem Vorbehalt des § 64 Abs. 2 SGB VIII. Danach dürfen Daten nur übermittelt werden, soweit dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird. Ob eine Leistung gefährdet ist, muss das Jugendamt beurteilen. Verneint es diese Frage, kann es die Daten übermitteln. Eine gesetzliche Verpflichtung besteht aber nicht.

ii. Rechtslage nach Inkrafttreten der Datenschutz-Grundverordnung

In diesem Fall ist eine zweckändernde Datenübermittlung nach Art. 6 Abs. 4 i. V. m. Abs. 1e DS-GVO zulässig, da die Datenübermittlung zur Erfüllung der eigenen Aufgabe des Jugendamtes erforderlich ist, die im öffentlichen Interesse liegt und die dem für die Verarbeitung Verantwortlichen übertragen wurde.

d) Datenübermittlung durch nicht-öffentliche Stellen an die Polizei

(1) Übermittlung eines Fahrtschreibers zur Strafverfolgung

Beispiel: Ein Transportunternehmer entdeckt eine Delle an der Stoßstange einer seiner Lastkraftwagen. Bei Auswertung des elektronischen Fahrtschreibers bemerkt er, dass der Fahrer mit deutlich überhöhter Geschwindigkeit gefahren ist. Er erfährt, dass ein Kind angefahren wurde und der Fahrer flüchtig ist. Da sich der Unfall an einem Ort ereignete, den der Fahrer zum fraglichen Zeitpunkt mit überhöhter Geschwindigkeit passiert haben könnte, hält der Transportunternehmer eine schuldhafte Beteiligung seines Fahrers an dem Unfall für möglich. Deshalb übersendet er den Fahrtschreiber der Polizei.

i. Gegenwärtige Rechtslage

Die gemäß § 57 a Straßenverkehrszulassungsordnung erhobenen Daten dienen der Kontrolle der Einhaltung der vorgeschriebenen (Höchst-)Lenkzeiten sowie der Ruhezeiten durch den Fahrer. Übermittelt der Transportunternehmer den Fahrtschreiber an die Polizei, um zur Aufklärung einer Straftat (fahrlässige Körperverletzung, Unerlaubtes Entfernen vom Unfallort) beizutragen, liegt eine Übermittlung und mit ihr einhergehend eine Zweckänderung vor.

Dies ist derzeit zulässig, denn die Übermittlung der Daten für einen anderen Zweck ist zulässig, soweit dies zur Wahrung berechtigter Interessen Dritter (§ 28 Abs. 2 Nr. 2 a BDSG) oder zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten (§ 28 Abs. 2 Nr. 2 b BDSG) erforderlich ist und kein Grund für die Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Die Übersendung des Fahrtschreibers an die Polizei ist zur Verfolgung von Straftaten erforderlich. Ferner dient die Datenübermittlung auch den berechtigten Interessen des Kindes, das zur Geltendmachung seiner zivilrechtlichen Ansprüche die Identität des Anspruchsgegners kennen muss. Da keine schutzwürdigen Interessen des betroffenen Fahrers am Ausschluss der Datenübermittlung bestehen, darf der Transportunternehmer den Fahrtschreiber gem. § 28 Abs. 2 Nr. 2 a und b BDSG an die Polizei übermitteln.

ii. Rechtslage nach Inkrafttreten der Datenschutz-Grundverordnung

Nach Art. 6 Abs. 4 Satz 1 DS-GVO ist eine Zweckänderung nur zulässig, wenn mindestens einer der in Art. 6 Abs. 1 Buchstaben a bis e DS-GVO genannten Gründe zutreffen. Allerdings kommt diese Vorschrift nur zur Anwendung, wenn der Zweck der Weiterverarbeitung mit dem Zweck, für den die Daten erhoben wurden, nicht vereinbar ist. Um festzustellen, ob der Weiterverarbeitungs- und der Erhebungszweck vereinbar sind, sieht Art. 6 Abs. 3a DS-GVO in der Ratsfassung einen sog. „Kompatibilitätstest“ vor, bei dem u. a. folgende Kriterien zu berücksichtigen sind:

- eine Verbindung zwischen dem ursprünglichen Erhebungszweck und dem Zweck der weiteren Verarbeitung,
- die Art der personenbezogenen Daten,
- der Kontext, bei dem die Daten erhoben wurden,

- die berechtigten Erwartungen des Betroffenen bezüglich der weiteren Verwendung und

- die Auswirkungen und Folgen der Weiterverarbeitung für den Betroffenen.

Wann im Einzelfall Kompatibilität des ursprünglichen Erhebungszwecks und der Weiterverarbeitungszwecks vorliegt, ist jedoch nicht immer leicht zu beantworten, da die Kriterien des „Kompatibilitätstests“ relativ unbestimmt und auslegungsbedürftig sind. In erster Linie dient ein Fahrtschreiber der Erfassung der Lenk- und Ruhezeiten, damit deren Einhaltung behördlicherseits kontrolliert und gegebenenfalls ein Ordnungswidrigkeitenverfahren eingeleitet werden kann oder Maßnahmen zur Gefahrenabwehr (Verbot der Weiterfahrt bis zur Ableistung einer erforderlicher Ruhezeit) ergriffen werden können. Darüber hinaus kann mit seiner Hilfe eine Geschwindigkeitsüberschreitung nachgewiesen werden, da der Fahrtschreiber auch die gefahrene Geschwindigkeit aufzeichnet. Im Beispielsfall dient die Übersendung des Fahrtschreibers an die Polizei jedoch nicht allein dem Nachweis einer Geschwindigkeitsüberschreitung, sondern der Aufklärung einer Straftat, die mit dem ursprünglichen Erhebungszweck in keiner Verbindung steht. Andererseits ist der Kontext, bei dem die Daten erhoben und weiterverarbeitet werden, ähnlich, denn in beiden Fällen geht es um das Verhalten des Fahrers bei Führung eines Lastkraftwagens. Ob die Erwartungen des Betroffenen, dass der Fahrtschreiber nicht zum Nachweis von während der Fahrt begangenen Straftaten verwendet wird, „berechtigt“ sind, erscheint fraglich. Die Folgen der weiteren Verwendung können jedoch für den Betroffenen gravierend sein. Letztlich dürfte hier eine Unvereinbarkeit der Zwecke vorliegen, da die aufgezeichneten Daten des Fahrtschreibers der Aufklärung eines strafbaren Fehlverhaltens dienen sollen, das nichts mit den ursprünglichen Erfassungszwecken zu tun hat. Geht man davon aus, dass die Zwecke nicht miteinander vereinbar sind, dann ist eine Weiterverarbeitung der Daten gem. Art. 6 Abs. 4 Satz 1 DS-GVO nur zulässig, wenn mindestens einer der in Art. 6 Abs. 1 Buchstaben a bis e DS-GVO genannten Gründe zutrifft.

Hier trifft keiner der genannten Gründe zu. Weder eine Einwilligung (Buchstabe a) noch die Erfüllung eines Vertrages (Buchstabe b). Die Verarbeitung ist auch nicht zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt (Buchstabe c), denn ein Transportunternehmer hat weder den gesetzlichen Auftrag zur Strafverfolgung noch ist er verpflichtet, die Durchsetzung zivilrechtlicher Ansprüche eines Dritten zu ermöglichen. Auch Buchstabe d ist nicht einschlägig, denn die Verarbeitung ist nicht nötig, um lebenswichtige Interessen der betroffenen Person (des Fahrers) zu schützen. Schließlich trifft auch Buchstabe e nicht zu. Danach ist eine Zweckänderung zulässig, wenn

sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt und die dem für die Verarbeitung Verantwortlichen übertragen wurde. Dem Transportunternehmer sind jedoch weder Aufgaben des öffentlichen Interesses übertragen noch übt er hoheitliche Gewalt aus.

Da keiner der in Art. 6 Abs. 1 Buchstaben a bis e DS-GVO genannten Gründe zutrifft, ist die Übersendung des Fahrtschreibers an die Polizei unzulässig (vorausgesetzt, man bejaht die Inkompatibilität des Erhebungs- und Weiterverarbeitungszwecks).

Zulässig wäre die Weiterverarbeitung der Daten durch den Transportunternehmer nur, wenn Art. 6 Abs. 4 Satz 1 DS-GVO auch auf Art. 6 Abs. 1 Buchstabe f DS-GVO verweisen würde. Denn danach ist die Datenverarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Diese Bedingung wäre vorliegend erfüllt, da die Übersendung des Fahrtschreibers auch den berechtigten Interessen eines Dritten (des Kindes) an der Geltendmachung seiner zivilrechtlichen Ansprüche dient und keine überwiegenden Interessen, Grundrechte oder Grundfreiheiten des betroffenen Fahrers entgegenstehen.

(2) Übermittlung durch eine Spielbank

Beispiel: Ein privates Spielbankunternehmen hat den Verdacht, dass der Spieleinsatz eines Spielers Gegenstand einer Straftat nach § 261 StGB (Geldwäsche) ist und meldet die Transaktion mit Angaben zur betroffenen Person dem BKA und dem LKA.

i. Gegenwärtige Rechtslage

Spielbanken sind gem. § 2 Abs. 1 Nr. 11 GWG Verpflichtete des Geldwäschegesetzes und nach § 11 Abs. 1 Satz 1 GwG verpflichtet, dem BKA und der zuständigen Strafverfolgungsbehörde Fälle, in denen der Verdacht besteht, dass Vermögenswerte Gegenstand einer Geldwäsche nach § 261 StGB sind oder im Zusammenhang mit Terrorismusfinanzierung stehen, zu melden.

ii. Rechtslage nach Inkrafttreten der Datenschutz-Grundverordnung

Hier gilt, dass die Datenübermittlung zulässig ist, weil der Erhebungs- und der Weiterverarbeitungszweck miteinander vereinbar sind. Die nach dem Geldwäschegesetz

bestehende Verpflichtung zur Identifizierung eines Vertragspartners dient gerade dazu, dass der Verpflichtete durch die Daten in die Lage versetzt wird, bei verdächtigen Wahrnehmungen eine entsprechende Meldung bei den Strafverfolgungsbehörden zu machen. Selbst wenn aber Inkompatibilität der Zwecke vorläge, wäre die Datenübermittlung nach Art. 6 Abs. 1c DS-GVO zulässig, da die Verarbeitung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist, der der für die Verarbeitung Verantwortliche (das Spielbankunternehmen) unterliegt.

(3) Übermittlung von Daten aus technischen Kontrollen

Beispiel: Bei einer technischen Überprüfung von unerwarteten Netzwerküberlastungen bei einem privaten Unternehmen wird festgestellt, dass kinderpornographisches Material ausgetauscht wird.

i. Gegenwärtige Rechtslage

Nach derzeitigem Recht ist hier eine Übermittlung nach § 28 Abs. 2 Nr. 2 BDSG zulässig.

ii. Rechtslage nach Inkrafttreten der Datenschutz-Grundverordnung

Hier wurden die Daten wurden für eine technische Kontrolle der Netzwerkauslastung erhoben. Es ist zweifelhaft, ob die Übermittlung an die Strafverfolgungsbehörden noch kompatibel ist. Sind die Zwecke jedoch nicht kompatibel, bestünde keine Übermittlungsregelung in der DS-GVO. Keine der Rechtsgrundlagen des Art. 6 a bis e DS-GVO wäre einschlägig. Gleichzeitig ist unklar, ob nach Inkrafttreten der DS-GVO eine Vorschrift wie § 28 Abs. 2 Nr. 2 b BDSG noch bestehen kann.

Aus Sicht der Arbeitsgruppe ist deshalb sicherzustellen, dass eine Übermittlung an die Polizei, selbst wenn dies ein Zweckwechsel ist, auch im Anwendungsbereich der DS-GVO zulässig ist.

(4) Datenübermittlung zur Gefahrenabwehr (Suizidverhinderung)

Beispiel: Ein Psychiater informiert die Polizei über die akute Suizidgefährdung und den Geisteszustand seines an schweren Depressionen leidenden Patienten.

i. Gegenwärtige Rechtslage

Bei Gesundheitsdaten handelt es sich gem. § 3 Abs. 9 BDSG um eine besondere Art von personenbezogenen Daten. Diese dürfen gem. § 4 a Abs. 3 BDSG mit Einwilligung des Betroffenen erhoben werden.

Ein Patient, der sich freiwillig in ärztliche Behandlung begibt, ist damit einverstanden, dass der Arzt Daten über seinen Gesundheitszustand erhebt. Übermittelt der Arzt die im Rahmen der Behandlung erhobenen Daten an die Polizei um einen bevorstehenden Suizid zu verhindern, liegt eine Zweckänderung vor, deren Zulässigkeit sich nach § 28 Abs. 8 BDSG richtet. Danach ist die Übermittlung der Daten für einen anderen Zweck zulässig, soweit dies zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit erforderlich ist. Bei einem drohenden Suizid besteht eine Gefahr für das Leben als Schutzgut der öffentlichen Sicherheit jedenfalls dann, wenn sich der Suizident in einem die freie Willensbestimmung ausschließenden Geisteszustand befindet, wie dies bei einer schwer depressiven Person der Fall ist. Deshalb darf der Arzt die Polizei gem. § 28 Abs. 8 Satz 2 BDSG über die akute Suizidalität seines Patienten und dessen Geisteszustand informieren. Die Verletzung der Schweigepflicht ist hier durch den rechtfertigenden Notstand gem. § 34 StGB gerechtfertigt.

ii. Rechtslage nach Inkrafttreten der Datenschutz-Grundverordnung

Werden Daten über den Gesundheitszustand von einem Arzt weitergegeben, sind diese meistens in einer Datei gespeichert, da der Arzt zur Führung einer Patientenakte verpflichtet ist, so dass der Anwendungsbereich der DS-GVO eröffnet ist.

Bei Gesundheitsdaten handelt es sich um eine besondere Kategorie personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO. Deren Verarbeitung ist grundsätzlich untersagt, es sei denn, es liegt eine Rechtfertigung nach Art. 9 Abs. 2 a bis j DS-GVO vor. Die Datenerhebung im Rahmen der Behandlung ist danach rechtmäßig, da sie mit Einwilligung der Betroffenen erfolgt ist (Art. 9 Abs. 2 a DS-GVO).

Gibt der Arzt Informationen über seinen Patienten zum Zwecke der Gefahrenabwehr an die Polizei, liegt eine Zweckänderung vor. Die Datenerhebung und Dokumentation in der Patientenakte dienen primär dem therapeutischen Interesse des Patienten und der Sicherstellung einer ordnungsgemäßen Behandlung. Die Übermittlung der Daten an die Polizei dient der Abwehr einer Gefahr für die öffentliche Sicherheit, gleichzeitig aber auch dem Schutz des Patienten vor sich selbst.

Ob der Weiterverarbeitungszweck mit dem ursprünglichen Erhebungszweck kompatibel ist, kann hier jedoch dahinstehen, da auch eine nicht kompatible Zweckänderung zulässig ist. Die Datenübermittlung ist hier zur Erfüllung einer gesetzlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt (Art. 6 Abs. 1c DS-GVO). Aufgrund des Behandlungsvertrages ist der Arzt verpflichtet, seinen Patienten vor Schäden zu bewahren und einen auf die zu behandelnde Erkrankung (Depressionen) zurückzuführenden Suizid zu verhindern. Darüber hinaus dürfte die Datenübermittlung auch nötig sein, um lebenswichtige Interessen der betroffenen Person zu schützen (Art. 6 Abs. 1d DS-GVO).

e) Fazit

Unter dem Regime der Datenschutz-Grundverordnung ist eine automatisierte Datenübermittlung oder eine nichtautomatisierte Datenübermittlung von Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen, entgegen der Regelung in § 28 Abs. 2 a und b BDSG durch eine nicht öffentliche Stelle nicht zulässig, soweit die Daten aus eigener Veranlassung zum Zwecke der Strafverfolgung oder zur Wahrung der berechtigten Interessen eines Dritten an die Polizei übermittelt werden. Das Gleiche gilt für Datenübermittlungen zum Zwecke der Gefahrenabwehr, sofern der Übermittelnde die Daten nicht in Erfüllung einer gesetzlichen Verpflichtung übermittelt und die Übermittlung auch nicht nötig ist, um lebenswichtige Interessen der betroffenen Person zu schützen.

5. Rechte der Betroffenen

Ein Kernstück der DS-GVO sind Rechte des Betroffenen. Diese unterteilen sich in ein Informationsrechte(a), ein Auskunftsrecht (b), ein Recht auf Berichtigung und Recht auf Löschung (c), sowie ein Recht auf Datenportabilität nach Art. 18 DS-GVO. Nach Art. 21 DS-GVO haben die Mitgliedstaaten die Möglichkeit, die in der DS-GVO kodifizierten Rechte einzuschränken (d).

a) Informationsrechte des Betroffenen (Art. 14 und 14a)

(1) Voraussetzung und Umfang der Informationsrechte

Nach der DS-GVO in der Ratsfassung vom 3. Dezember 2014 hat der Datenverarbeiter den Betroffenen bei jeder Datenerhebung über festgelegte Punkte zu informieren. Dies gilt sowohl in den Fällen, in denen die Daten beim Betroffenen erhoben wurden (Art. 14 DS-GVO), als auch in Fällen in den die Daten nicht beim Betroffenen erhoben wurden (Art. 14a DS-GVO). Der Umfang der Informationspflichten ist in beiden Fällen im Wesentlichen gleich; so muss über die datenverarbeitende Stelle, den Zweck der Verarbeitung, die Empfänger oder Kategorien von Empfängern, ggf. über die Absicht, die Daten in ein Drittland oder ein

Internationale Organisation zu übermitteln, informiert werden. Weiter ist der Betroffene über die ihm zustehenden Rechte zu informieren. Wurden die Daten nicht beim Betroffenen erhoben, so sind ihm zusätzlich die erhobenen Daten bzw. die Kategorien der Daten und der Ursprung der Daten mittzuteilen.

Dies würde bedeuten, dass die Polizei bei jeder Datenerhebung im Anwendungsbereich der DS-GVO diese umfangreichen Benachrichtigungspflichten hätte, da die in Art. 14 DS-GVO und Art. 14a DS-GVO vorgesehenen Ausnahmen kaum greifen dürften. Diese Informationspflichten träfen zudem die nicht-öffentlichen und öffentlichen Stellen, soweit eine Benachrichtigung des Betroffenen bei einer Übermittlung an Dritte, mithin auch an die Polizei, vorgesehen ist.

(2) In der DS-GVO vorgesehene Ausnahmen für die Datenhebung beim Betroffenen

Zwar sieht auch Art. 14 DS-GVO Ausnahmen vor, ob diese greifen, ist allerdings zweifelhaft. Die Benachrichtigung bei einer Datenerhebung beim Betroffenen entfällt, wenn die zu übermittelnden Informationen bereits bekannt sind (siehe Art. 14 Abs. 5 DS-GVO). Es kann nicht davon ausgegangen werden, dass dem Bürger bei einer polizeilichen Maßnahme die aufgelisteten Informationen bekannt sind, so dass die Informationspflicht bestehen würde. Ob die Ausnahme für die weiteren Informationen im erweiterten Katalog des Art. 14 Abs. 1a DS-GVO greift, ist ebenfalls fraglich. Danach ist nur zu informieren, wenn dies notwendig ist, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten. Diese Formulierung ist wenig aussagekräftig, so dass nicht abgeschätzt werden kann, ob diese bei der polizeilichen Datenverarbeitung einschlägig ist oder nicht.

Es ist deshalb davon auszugehen, dass die Informationspflichten des Art. 14 DS-GVO im Fall der Erhebung beim Betroffenen in der Polizeipraxis zu beachten sind, d.h. die Polizei müsste den Betroffenen bei jeder Erhebung über den Katalog des Art. 14 DS-GVO informieren. Dies ist praxisfern und in der Polizeipraxis kaum umsetzbar. Häufig findet die Datenerhebung „auf der Straße“ und in Situationen statt, die für die Betroffenen schwierig sind. Eine solche Situation mit bürokratischen Informationspflichten zu belasten, ist kontraproduktiv. Sie erschwert die polizeiliche Arbeit und bringt für den Bürger keinen Mehrwert, da die Datenverarbeitung bei polizeilicher Datenerhebung und -verarbeitung stets dezidiert gesetzlich geregelt ist. Aus diesem Grund wurde bisher für den Polizeibereich von so weitreichenden allgemeinen datenschutzrechtlichen Informationspflichten abgesehen (beispielsweise § 37 BPolG, § 23 SOG LSA)

(3) In der DS-GVO vorgesehene Ausnahmen, wenn die Datenhebung nicht beim Betroffenen erfolgt

Hinsichtlich der Informationspflicht bei der Datenerhebung bei Dritten - die in der polizeilichen Praxis auch für die präventive Gefahrenabwehr von großer Bedeutung ist - ist die Regelung etwas anders. Danach entfällt die Informationspflicht, wenn die Erhebung oder Weitergabe durch Rechtsvorschriften der Union oder eines Mitgliedstaates ausdrücklich geregelt ist. Dies entspricht der bisherigen Rechtslage, die auf Art. 11 Abs. 2 der RL 95/46 zurückgeht, für das Bundesdatenschutzgesetz § 19a. Es ist zu begrüßen, dass bei einer gesetzlichen Regelung zur Speicherung und Weitergabe die entsprechende Informationspflicht entfällt. Auch unter dem Regime der DS-GVO muss dies im Polizeibereich vollumfänglich möglich sein.

Aus Sicht der Arbeitsgruppe sollte dies für beide Benachrichtigungspflichten identisch geregelt werden und zwar dahingehend, dass die Regelung des Art. 14a Abs. 4c DS-GVO für beide Benachrichtigungspflichten übernommen wird.

b) Auskunftsrecht des Betroffenen

Ein Auskunftsrecht besteht bereits nach der geltenden Rechtslage, die in den einzelnen Ländern und dem Bund ähnlich ist, zurückgehend auf Art. 11 der RL 95/46. Die in der DS-GVO vorgesehene Regelung geht über die bisher kodifizierten Auskunftsrechte hinaus, so ist nach der DS-GVO die geplante Speicherdauer mitzuteilen, ebenso Informationen über die Herkunft der Daten, die Logik eines etwaigen Profilings und welche Sicherheitsmaßnahmen der Verarbeiter ergriffen hat. Dies bedeutet für die Polizeien einen erheblichen zusätzlichen Verwaltungsaufwand. Am problematischsten ist allerdings die Regelung des Art. 15 DS-GVO, nach der der Datenverarbeiter dem Betroffenen eine Kopie der von ihm verarbeiteten personenbezogenen Daten zu übergeben hat. Dies führt zu unverhältnismäßigen Belastungen, und verlangt von den Polizeien, ihre Systeme, die hierfür nicht ausgelegt sind, auszubauen. Ausdrucke aus polizeilichen Systemen sind wegen der unterschiedlichen Katalogfelder häufig umfangreich, ohne dass sich ein Mehrwert für den Betroffen ergibt. Ein Ausdruck aus einem Vorgangsbearbeitungssystem beispielsweise umfasst alle möglichen Katalogfelder, auch ohne dass diese Daten enthalten. Dadurch sind solche Ausdrucke deutlich unübersichtlicher als die durch die Polizei aufbereitete Form, wie bisher Auskunft erteilt wird. Auch bei der Videoüberwachung wäre der Aufwand enorm. In einer Kopie sind in aller Regel weitere Informationen enthalten, an denen der Betroffene kein berechtigtes Interesse hat, wohl aber die verarbeitende Stelle. Bei einer Videoüberwachung kann z.B. aus den Aufnahmen geschlossen werden, welche Bereiche durch die Kamera nicht einsehbar

sind. Wenn andere Personen auf dem Band wären, müsste diese herausgeschnitten werden, was technisch möglich, aber aufwändig wäre (vgl. Art. 15 Abs. 2a DS-GVO). Aus der „Kopie“ könnten zudem Rückschlüsse über die Arbeitsweise z.B. der Polizei gewonnen werden, etwa bei Überlassung eines Einsatztagebuches.

Aus Sicht der Arbeitsgruppe ist insoweit der Anspruch des Betroffenen auf eine Kopie als wenig sachdienlich zu streichen bzw. es sollte bereits in der DS-GVO eine angemessene Ausnahmeregelung aufgenommen werden.

c) Recht auf Berichtigung und Recht auf Einschränkung der Verarbeitung

Auch soweit ein Recht auf Berichtigung und ein Recht auf Einschränkung der Verarbeitung vorgesehen ist, ist dies für die polizeiliche Aufgabenwahrnehmung nicht sinnvoll und kann zu Einschränkungen bei der polizeilichen Arbeit führen. So ist die Anwendung des derzeit kodifizierten Rechts auf Berichtigung des § 20 BDSG innerhalb der Bundespolizei ausgeschlossen. Eine solche Möglichkeit muss auch weiter bestehen.

d) Ausnahmetatbestände der DS-GVO und die Bedeutung des Art. 21 DS-GVO

Art. 21 DS-GVO erlaubt den Mitgliedstaaten, von den Informations- und Auskunftspflichten abzuweichen, sofern es z.B. für die öffentliche Sicherheit oder die Verhütung, Verhinderung und Verfolgung von Straftaten erforderlich ist. Problematisch an dieser Regelungstechnik ist, dass der nationale Gesetzgeber dann bereits bestehende Betroffenenrechte durch ein Gesetz einschränken muss. Soweit das geltende Recht für die Polizeiarbeit notwendige Beschränkungen nicht bereits enthält, dürfte es schwierig sein, diese im Nachhinein einzuführen. Dies wird durch die Formulierung des Art. 21 Abs. 2 DS-GVO nicht einfacher. Sollte die Öffnungsklausel des Art. 21 DS-GVO eng ausgelegt werden und nur punktuelle Ausnahmen möglich sein mit der Folge, dass umfangreiche Informationspflichten auf die Polizei zukämen, würde dies die Praxis vor erhebliche Probleme in der Umsetzung stellen.

e) Fazit

Aus dem Vorstehenden wird deutlich, dass die Regelungen zu Informations-, Auskunfts- und Widerspruchsrechten für die Polizei wenig praxisnah ist und auch für den betroffenen Bürger letztlich keinen Mehrwert schaffen. Im Regelfall ist dem Bürger bekannt, dass es im gefahrenabwehrenden Bereich zu einer Speicherung der Daten kommt. Es ist in der Praxis nicht zu erkennen, dass ein erhebliches Informationsinteresse bei den betroffenen Bürgern besteht. So sind beispielsweise im Vorgangsbearbeitungssystem der Bundespolizei ca. 3 Mio. Personen gespeichert. Dagegen sind für die gesamte Bundespolizei lediglich 900 Auskunftsersuchen zu verzeichnen. **Es sollten deshalb sinnvolle Ausnahmeregelungen**

entsprechend des bestehenden Rechts geschaffen werden. Aus Sicht der Arbeitsgruppe ist es wesentlich, dass rechtssichere Ausnahmen aufgrund des Art. 21 möglich sind und dass diese so in das nationale Recht eingefügt werden können, dass Auskunfts- und Benachrichtigungspflichten für die gesamte Gefahrenabwehr einheitlich in den Polizeigesetzen geregelt werden können.