Hartmut Aden

Besserer Datenschutz – auch für Polizei und Strafjustiz?*

Parallel zur EU-Datenschutz-Grundverordnung wurde eine EU-Richtlinie für den Datenschutz im Polizei- und Strafjustizbereich ausgehandelt und verabschiedet. Sie war von den Mitgliedstaaten bis zum 6. Mai 2018 umzusetzen. Hartmut Aden analysiert im folgenden Beitrag diese Richtlinie und stellt ausgewählte Aspekte ihrer teilweise defizitären Umsetzung in Deutschland im Kontext des Ausbaus der polizeilichen Informationsverarbeitung in Europa vor.

Die EU-Datenschutz-Grundverordnung (DSGVO) klammert die Datenverarbeitung durch Polizei und Strafjustiz weitgehend aus (Art. 2 Abs. 2 lit. d DSGVO). Diese Felder der EU-Politik waren bis 2009 als „dritte Säule" von der Zusammenarbeit zwischen den Regierungen der Mitgliedstaaten, also intergouvernemental geprägt. Auch unter den Rahmenbedingungen des Vertrages von Lissabon sind die Regierungen der Mitgliedstaaten in diesem Bereich weiterhin faktisch besonders einflussreich (hierzu Albrecht 2015). Sie konnten sich daher für den Polizei- und Strafjustizbereich nicht auf eine ähnlich weitreichende Harmonisierung des Datenschutzrechts verständigen wie für den privaten Sektor und die übrigen staatlichen Behörden, die in den Anwendungsbereich der direkt wirkenden DSGVO fallen. Prägend für die Datenverarbeitung durch Polizei und Strafjustiz ist, dass sie in der Regel auf gesetzlichen Eingriffsbefugnissen und nicht auf einer freiwilligen Einwilligung der Betroffenen beruht.[1]

Datenschutz und Privatsphäre sind seit dem Vertrag von Lissabon (2009) auch in der EU verbindliche Grundrechte, garantiert in Art. 7 und 8 der Grundrechte-Charta. Folglich ist auch der grenzüberschreitende Datenaustausch von Polizei und Strafjustiz an diese Grundrechte gebunden. Datenschutzmaßnahmen haben mit Art. 16 des Vertrages über die Arbeitsweise der EU (AEUV) eine weitere primärrechtliche Grundlage. Parallel zur DSGVO wurde daher eine EU-Richtlinie ausgehandelt und verabschiedet, die nicht unmittelbar gilt, sondern deren Ziele die EU-Staaten in ihre Gesetzgebung übernehmen müssen. Der offizielle Titel lautet: Richtlinie (EU) 2016/680[2] des Europäischen Parlaments und des Rates vom 27. April 2016 *zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstre-*

* Einige Passagen dieses Beitrags basieren auf einer Stellungnahme, die der Verfasser am 27.3.2017 anlässlich einer Anhörung des Innenausschusses des Deutschen Bundestages zur Anpassung des Bundesdatenschutzgesetzes an das neue EU-Datenschutzrecht abgegeben hat.

ckung sowie zum freien Datenverkehr [...]. Wie bei der DSGVO macht bereits der Titel deutlich, dass es nicht nur um Datenschutz geht, sondern auch um „freien Datenverkehr" – was im Anwendungsbereich der Richtlinie vor allem die Erleichterung des grenzüberschreitenden Austauschs von Informationen mit oder ohne Personenbezug zwischen den fachlich zuständigen Behörden meint. Zuvor gab es für den Datenschutz beim Informationsaustausch durch Polizei und Strafjustiz nur den nun aufgehobenen Rahmenbeschluss 2008/977/JI[3] aus der ehemaligen dritten EU-Säule, dessen Inhalte weder besonders ambitioniert waren noch engagiert von den Mitgliedstaaten umgesetzt wurden.

In Deutschland wurde die Richtlinie (EU) 2016/680 als eigener Teil des für die Anpassung an das EU-„Datenschutzpaket" grundlegend überarbeiteten Bundesdatenschutzgesetzes (BDSG) umgesetzt. Gesetzgebungstechnisch ungewöhnlich wurden dabei quasi „zwei Gesetze in einem" geschaffen. Mit Teil 3 des neuen BDSG (§§ 45ff.) beginnt ein völlig eigenständiger Abschnitt mit neuen Begriffsdefinitionen. Diese gesetzgeberische Umsetzung erscheint wenig überzeugend. Denn das Anfang 2012 von der Europäischen Kommission vorgelegte EU-„Datenschutzpaket" verfolgte die Intention, einen Datenschutz „aus einem Guss" zu schaffen. Die Trennung in Richtlinie und Verordnung sollte lediglich den Mitgliedstaaten etwas größere Gestaltungsspielräume für das Datenschutzrecht im Polizei- und Strafverfolgungsbereich überlassen.

1. Datenschutzrichtlinie für Polizei und Strafjustiz im Schatten der DSGVO

Die Datenschutzrichtlinie (EU) 2016/680 für Polizei und Strafjustiz stand in der öffentlichen Wahrnehmung seit der gemeinsamen Einbringung der Entwürfe durch die Europäische Kommission Anfang 2012 im Schatten der DSGVO. Dies ist angesichts der hohen praktischen Relevanz problematisch, die der Datenaustausch zwischen Sicherheitsbehörden seit den 1990er Jahren und verstärkt im Zusammenhang mit der Terrorismusbekämpfung der letzten Jahre erlangt hat. Kernanwendungsbereich der Richtlinie ist der grenzüberschreitende Datenaustausch. Der transnationale Informationsaustausch ist seit langem das zentrale Instrument der internationalen Zusammenarbeit (ausführlich hierzu Aden 2014 und 2016). Die technischen Möglichkeiten, die Rechtsgrundlagen und die Kooperationspraxis zwischen den hier relevanten Behörden der Mitgliedstaaten (Polizei u.a.) haben sich in den letzten Jahren aber erheblich weiterentwickelt.

Die ausgeweitete Praxis ist mit Risiken für die Grundrechte der Bevölkerung verbunden, insbesondere für die Privatsphäre und die informationelle Selbstbestimmung sowie die daran anknüpfenden Grundrechte im Strafverfahren (Unschuldsvermutung, Schutz vor willkürlichen Freiheitsentziehungen usw.). Diese Grundrechtspositionen lassen sich nur durch rigorose Maßnahmen zur Gewährleistung der Qualität der hier verarbeiteten personenbezogenen Daten schützen, die Fehlinformationen, Verwechslungen oder unberechtigte Datenverarbeitung verhindern. Eine solche Qualitätssicherung für die Datenbestände liegt zugleich im Interesse der Sicherheitsbehörden selbst, da Reibungsverluste und fehlinvestierte Arbeitszeit durch veraltete oder unrichtige Daten so vermieden werden können (näher hierzu Aden 2014). Daher ist die

Harmonisierung der Datenschutzstandards durch die Richtlinie (EU) 2016/680 grundsätzlich sowohl für die Betroffenen als auch für die erfassten Behörden ein Schritt in die richtige Richtung.

2. Wachsende Datenmengen bei der europäischen Sicherheitszusammenarbeit – veraltete und zersplitterte Rechtsgrundlagen

Das Datenschutzrecht für die polizeiliche Zusammenarbeit in der Europäischen Union war bisher stark fragmentiert und entsprach weder dem Stand der Zusammenarbeitspraxis noch der technischen Entwicklung (kritische Würdigung bei Boehm 2012: 175ff.; Gutiérrez Zarza 2015; de Hert & Papakonstantinou 2015: 181ff.).

Ein Kernelement der polizeilichen Informationszusammenarbeit in Europa ist der Datenaustausch über zentralisierte Datenbanken, der allerdings von der Richtlinie (EU) 2016/680 gar nicht erfasst wird. Datenbanken wie das *Schengener Informationssystem* und die *Europol*-Datensammlungen enthalten wachsende Mengen personenbezogener Daten, ebenso *Eurodac* und das *Visainformationssystem* als Datenbanken, die für die Migrationssteuerung errichtet wurden, aber in erheblichem Umfang von Sicherheitsbehörden mit genutzt werden. In den nächsten Jahren werden neue Datenbanken im Zusammenhang mit der Außengrenzsicherung der EU (*Entry-Exit-System*) hinzukommen. Diese Datenbanken werden von *eu-LISA*, der 2012 gegründeten *EU-Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht* verwaltet und betrieben. Da die Richtlinie – ebenso wie die DSGVO – nicht für die Datenverarbeitung durch die EU-Organe und -Agenturen gilt, ist die Rechtslage weiterhin zersplittert. Jede Datenbank hat eigene Rechtsgrundlagen und Kontrollstrukturen. Zwar ist bei der Überführung der Rechtsgrundlagen aus der ehemaligen dritten EU-Säule in verbindliche EU-Verordnungen zu beobachten, dass die Datenschutzbestimmungen ausführlicher werden. Die Potentiale für eine Vereinheitlichung auf hohem Niveau wurden aber bisher nicht ausgeschöpft (näher hierzu Aden 2016: 334ff.). Pläne, die „Interoperabilität" dieser Datenbanken zu erhöhen,[4] also die Trennung zwischen den Datenbeständen für Recherchezwecke teilweise aufzuheben, werden eine Neukonzeption des Datenschutzes erfordern (hierzu FRA 2017).

Die Richtlinie (EU) 2016/680 gilt für die behördliche Verarbeitung personenbezogener Daten „*zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit*" (Art. 1 Abs. 1). Damit umfasst sie nach deutschem Recht die Tätigkeit von Polizei, Staatsanwaltschaften, Zoll, Steuerfahndung und Strafvollstreckungsbehörden. Auch die Verfolgung von Ordnungswidrigkeiten wird erfasst (näher hierzu Bäcker 2017: 65f.). Soweit Polizeibehörden auch andere Aufgaben wahrnehmen, fallen diese unter die DSGVO.

Überall wo Polizei und Strafjustiz der Mitgliedstaaten bei der Wahrnehmung der genannten Aufgaben in horizontalen Netzwerken direkt zusammenarbeiten und Informationen austauschen, gilt die Richtlinie (EU) 2016/680. Hierunter fallen auch die Instrumente, die einen Abgleich mit Datenbanken anderer Mitgliedstaaten im Direktzugriff ermöglichen, wie sie 2006 von Deutschland und einigen anderen EU-Staaten im

Vertrag von Prüm vereinbart wurden. Dieses Instrumentarium wurde später weitgehend in den Rahmen der EU überführt (näher hierzu Balzacq & Hadfield 2012). Die beteiligten Länder können so wesentlich einfacher als zuvor herausfinden, ob z.B. eine gefundene DNA-Spur auch in dem anderen Mitgliedstaat bereits in strafrechtlichen Ermittlungsverfahren eine Rolle gespielt hat.

Auch die vielfältigen Formen der Informationszusammenarbeit in Polizei- und Zollkooperationszentren in den Grenzgebieten (näher hierzu Gruszczak 2016) fallen in den Anwendungsbereich der Richtlinie. Da die Bediensteten der beteiligten Mitgliedstaaten hier „unter einem Dach" zusammenarbeiten, ist der Informationsaustausch wesentlich weniger standardisiert als bei Datenbankabfragen, bei denen die Zugriffsberechtigungen technisch festgelegt und begrenzt sind. Ähnlich funktionieren die Zusammenarbeit und der Informationsaustausch über informelle Netzwerke – etwa zwischen Personen, die sich aus früheren gemeinsamen Ermittlungsverfahren, aus Gremien oder gemeinsamen Fortbildungsveranstaltungen kennen. Der rechtliche Rahmen des zulässigen Informationsaustausches ist hier wesentlich gröber abgesteckt als bei den zentralisierten Datenbanken – was die Durchsetzung von Datenschutzstandards erschwert (näher hierzu Aden 2016: 330ff.).

Tätigkeiten, die nicht in den Anwendungsbereich des EU-Rechts fallen, sind vom Geltungsbereich der Richtlinie ausgenommen (Art 2 Abs. 3 lit. b). Damit würde die rein innerstaatliche Datenverarbeitung auf der Basis von Rechtsgrundlagen des mitgliedstaatlichen Rechts nicht unter die Richtlinie fallen. Allerdings kann damit gerechnet werden, dass der Gerichtshof der EU (GHEU/EuGH) diese Regel in konkreten Streitfällen eher eng auslegen und damit – wie in vergleichbaren Fällen auf anderen Rechtsgebieten – den Anwendungsbereich des EU-Rechts und der Richtlinie eher ausweiten wird.

3. Neue Impulse für höhere Datenschutzstandards in der EU

Seit der Etablierung des Grundrechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht im Jahr 1983[5] gelten für Sicherheitsbehörden Mindeststandards für das Datenschutzrecht – auch wenn die Einhaltung in der Praxis mit vielen Defiziten behaftet ist. So bedarf jede Verarbeitung personenbezogener Daten einer normenklaren Rechtsgrundlage. Der Verhältnismäßigkeitsgrundsatz ist gerade im Hinblick auf die Ableitung der informationellen Selbstbestimmung auch aus der Menschenwürde (Art. 1 Abs. 1 GG) besonders zu beachten. Der Zweckbindungsgrundsatz, nach dem Daten nur für die Zwecke verarbeitet werden dürfen, für die sie erhoben wurden, ist einzuhalten. Sollen Daten für einen anderen Zweck verarbeitet werden, so ist auch hierfür eine Rechtsgrundlage erforderlich.

Diese in Deutschland bereits geltenden rechtlichen Rahmenbedingungen werden mit der Richtlinie auch für die Datenverarbeitung durch Polizei und Strafjustiz in der EU zum Standard. So verpflichtet die Richtlinie die Mitgliedstaaten, in den Rechtsgrundlagen für die Datenverarbeitung „*zumindest die Ziele der Verarbeitung [...] und die Zwecke der Verarbeitung*" anzugeben (Art. 8 Abs. 2). Dieser Mindeststandard für gesetzliche Eingriffsbefugnisse zur Verarbeitung personenbezogener Daten ist essentiell für

die Kontrolle der rechtmäßigen Datenverarbeitung durch Datenschutzaufsicht und Gerichte. Personenbezogene Daten, *„aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zu Sexualleben oder sexueller Orientierung*" dürfen nur verarbeitet werden, wenn dies unbedingt erforderlich ist und geeignete „Garantien für die Rechte und Freiheiten der betroffenen Person" vorgesehen sind (Art. 10). Auch der Zweckbindungsgrundsatz wird weiter konkretisiert (Art. 9). Selbst wenn diese Grundsätze bereits seit langem im deutschen Recht gelten, gibt die Richtlinie doch Anlass, die bestehenden gesetzlichen Eingriffsbefugnisse auf ihre Notwendigkeit und die klare Definition der Verarbeitungszwecke hin zu überprüfen.

Für den grenzüberschreitenden Informationsaustausch sind die Vorschriften der Richtlinie zur Berichtigung fehlerhafter Daten von besonderer Bedeutung. Denn gerade hier besteht das Risiko, dass nur eine der beteiligten Behörden fehlerhafte Daten löscht oder berichtigt, diese aber weiterhin bei Behörden anderer Mitgliedstaaten vorhanden sind, an die diese Informationen zuvor übermittelt wurden. Die Richtlinie verpflichtet die Mitgliedstaaten nun ausdrücklich dazu, die Quellen und Empfänger von Informationen über Berichtigungsbedarf zu informieren (Art. 16 Abs. 5 und 6).

Darüber hinaus enthält die Richtlinie einige Elemente, die auch im Vergleich zum bisherigen deutschen Recht Verbesserungen bringen. Hier sei insbesondere die *Data Breach Notication* genannt – die Verpflichtung, die Datenschutzaufsicht und unter Umständen auch die Betroffenen zu informieren, wenn bei der Datenverarbeitung „Verletzungen" bekannt werden, die zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen. Neben Pannen, die innerhalb der Behörde verursacht werden, können auch Angriffe von außen solche „Verletzungen" sein, wenn sie dazu führen, dass Unbefugte Kenntnis von personenbezogenen Daten erlangen. Diese für die Transparenz gegenüber den Betroffenen und daher auch für die informationelle Selbstbestimmung wichtigen Informationspflichten gelten somit nicht nur im Anwendungsbereich der DSGVO (dort Art. 33 und 34), sondern auch für die Informationsverarbeitung durch Polizei und Strafjustiz (Art. 30 und 31 RL (EU) 2016/680). Für die Benachrichtigung der Betroffenen enthält die Richtlinie allerdings die für den Sicherheitsbereich übliche „Hintertür", nach der die Benachrichtigung u.a. aus Sicherheitsgründen unterbleiben kann (Art. 31 Abs. 5 i.V.m. Art. 13 Abs. 3). Die Datenschutzaufsicht wird darauf zu achten haben, dass diese „Hintertür" nicht dazu führt, dass Auskünfte an Betroffenen bei Sicherheitsbehörden weitgehend unterbleiben – so wie es bei vergleichbaren gesetzlichen Auskunftsregelungen in Deutschland zu beklagen war und ist.

4. Weiterhin große Spielräume für Datensammlungen

Die Richtlinie wählt einen vorwiegend prozeduralen Ansatz: Sie legt Verfahren fest, die zu beachten sind, wenn Daten erhoben oder übermittelt werden, wenn sie berich-

tigt oder gelöscht werden müssen oder wenn Datenverarbeitungspannen passiert sind (s.o., Abschnitt 3).

Ihr größtes Defizit besteht indes darin, dass sie keine konkreten inhaltlichen Maßstäbe enthält, die darüber entscheiden, ob Daten für Sicherheitszwecke gesammelt, aufbewahrt und übermittelt werden dürfen. Die Mitgliedstaaten haben hier weiterhin erhebliche Spielräume, etwa bei der Frage, inwieweit Strategien der *Big Data*-Analyse für Strafverfolgungsbehörden zugelassen werden. Erforderlich wären klarere materiell-rechtliche Grenzen für die Datenerhebung und die weitere Verarbeitung. Diese müssen nun von der mitgliedstaatlichen Gesetzgebung etabliert werden. Auch für das deutsche Recht gibt es hier noch erheblichen Entwicklungsbedarf. Immerhin haben die Mitgliedstaaten dabei aber Grundsätze wie die Fairness der Datenverarbeitung, die Zweckbindung und die Pflicht zur Löschung nicht mehr erforderlicher Daten zu beachten (Art. 4 RL (EU) 2016/680). Auf der Basis dieser Maßstäbe werden die Datenschutzaufsicht, die mitgliedstaatlichen Gerichte und der Gerichtshof der EU die Datenverarbeitung der Strafverfolgungsbehörden zukünftig überprüfen können.

5. Probleme der Umsetzung im Bundesdatenschutzgesetz und in weiteren Bundes- und Landesgesetzen

Mit der Umsetzung im neu gefassten Bundesdatenschutzgesetz[6] und im Gesetz über das Bundeskriminalamt[7] hat der Bundesgesetzgeber gegenüber der EU signalisiert, dass er bereit ist, die Richtlinie fristgerecht in das deutsche Recht umzusetzen. Allerdings ist die Umsetzung damit noch lange nicht abgeschlossen. Denn auch die anderen Gesetze über die Tätigkeit der Strafverfolgungs- und Gefahrenabwehrbehörden der Länder und des Bundes müssen entsprechend angepasst werden.

Ob die Umsetzung in einem eigenständigen Teil des novellierten Bundesdatenschutzgesetzes (BDSG) auf die Dauer zielführend ist, kann bezweifelt werden. Das neue BDSG spiegelt eher die Zuständigkeitsverteilung für die beiden EU-Rechtsakte in einer arbeitsteilig organisierten Ministerialverwaltung wider als eine ambitionierte, an der Schaffung systematischer Rechtsgrundlagen orientierte Gesetzgebung. Chancen für die Schaffung eines einheitlichen, benutzerfreundlichen Datenschutzrechts wurden damit vertan. Wesentlich sinnvoller wäre es gewesen, allgemeine Fragen wie Definitionen und Grundsätze in einem gemeinsamen allgemeinen Teil voranzustellen und sodann in einem besonderen Teil zunächst die Anpassung an die DSGVO und in einem weiteren Teil die Umsetzung der Richtlinie vorzunehmen. Trotz des Nebeneinanders unmittelbar geltender Verordnungsinhalte und umsetzungsbedürftiger Richtlinienvorgaben wäre eine Vereinheitlichung der Begrifflichkeiten und allgemeinen Prinzipien im Interesse kohärenter Rechtsanwendung sinnvoll gewesen.

Mangelhaft ist u.a. die Umsetzung der Richtlinienvorgaben zur Zweckbindung. Die Zweckbindung folgt unmittelbar aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und auf den Schutz personenbezogener Daten (Art. 8 EU-Grundrechte-Charta). Sie ist damit ein zentraler Grundsatz für die Datenverarbeitung in Deutschland und in der EU, auch und gerade für den Sicherheitsbereich. Sicherheitsbehörden können für einen bestimmten Zweck erhobene Da-

ten nicht nach Belieben für andere Zwecke verwenden. Zweckänderungen stellen vielmehr erneute Grundrechtseingriffe dar und bedürfen daher einer klaren gesetzlichen Grundlage. Art. 9 der Richtlinie (EU) 2016/680 regelt dies den üblichen Standards entsprechend. Problematisch ist dagegen die Umsetzung der Zweckbindung in § 49 BDSG (neu). Sie dürfte kaum den Anforderungen des grundgesetzlichen Bestimmtheitsgebots genügen. Der pauschale Verweis in § 49 Satz 1 auf die in § 45 genannten „Zwecke" ist viel zu allgemein und unbestimmt. Denn dort sind die nur sehr allgemein genannten Zwecke „*Verhütung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten*" genannt. Die neue Regelung ermöglicht es dem Wortlaut nach, im Rahmen des Verhältnismäßigen vorhandene Datenbestände zwischen diesen verschiedenen Aufgabenbereichen und Zweckbestimmungen hin- und herzuschieben. Eine so allgemein und weit gefasste Zweckänderungs-Generalklausel fiele erheblich hinter den bisherigen Stand der spezialgesetzlichen Zweckänderungsvorschriften in der Strafprozessordnung, den Polizeigesetzen und anderen Fachgesetzen zurück (kritisch zur Entwurfsfassung auch Bäcker 2017: 72). Das Bestimmtheitsgebot erfordert vielmehr spezialgesetzliche Zweckänderungsregelungen. Im Hinblick auf das Wesentlichkeitsprinzip für gravierende Grundrechtseingriffe können diese nur in anderen Parlamentsgesetzen erlassen werden. Die Aufweichung bisheriger Zweckbindungsstandards dürfte auch kaum den Vorgaben in Art. 9 der Richtlinie (EU) 2016/680 entsprechen.

Problematisch ist auch die deutsche Umsetzung der EU-Richtlinienvorgaben zur Verarbeitung besonders sensibler personenbezogener Daten im neuen BDSG, die für die Betroffenen einen schweren Grundrechtseingriff darstellt: Informationen zur rassischen und ethnischen Herkunft, zu religiösen oder weltanschaulichen Überzeugungen, genetische und biometrische Daten sowie Informationen zur Gesundheit oder zum Sexualleben dürfen von Sicherheitsbehörden nur ausnahmsweise und mit besonderer Vorsicht verarbeitet werden. Art. 10 der Richtlinie (EU) 2016/680 erkennt an, dass dieser Ausnahmecharakter auch einer besonderen rechtlichen Absicherung bedarf. Die Regelung in § 48 BDSG (neu) könnte so interpretiert werden, dass eine Verarbeitung solcher Daten bereits dann zulässig sein soll, wenn die dort genannten Voraussetzungen und nur beispielhaft aufgeführten Verfahrensvorkehrungen getroffen werden. Dies würde indes der Schwere des Grundrechtseingriffs durch die Verarbeitung derartiger Daten nicht gerecht. Vielmehr sind im Hinblick auf das grundgesetzliche Bestimmtheitsgebot die Zwecke, für die solche Daten ausnahmsweise erhoben und weiter verarbeitet werden dürfen, in den Fachgesetzen konkret darzulegen. Wegen der Eingriffsintensität erfordert das Wesentlichkeitsprinzip auch hier normenklarere parlamentsgesetzliche Regelungen – die BDSG-Regelung allein kann als Eingriffsbefugnis nicht ausreichen.

Die Auskunftsrechte der betroffenen Personen sind in Art. 14 und 15 der Richtlinie (EU) 2016/680 geregelt und gehen bezüglich des Umfangs des Auskunftsanspruchs weiter als die bisherigen Regelungen im deutschen Recht (hierzu näher Bäcker 2017: 81). Art. 15 ermöglicht zwar Einschränkungen des Auskunftsrechts. Diese sind aber im Lichte der grundrechtlichen Verbürgungen auszugestalten. In § 57 Abs. 7 BDSG (neu) wird eine Konstruktion gewählt, die vorsieht, dass die Bundesdatenschutzbeauftragte in Fällen der Auskunftsverweigerung die mit der Auskunftserteilung verbundene Kon-

trolle bezüglich der Korrektheit der Daten und der Rechtmäßigkeit der Verarbeitung für die Betroffenen wahrnimmt. Diese Konstruktion ist grundsätzlich geeignet, das Spannungsverhältnis zwischen berechtigten Auskunfts- und Kontrollbegehren der Betroffenen und in manchen Fällen berechtigten Geheimhaltungsanliegen der Sicherheitsbehörden aufzulösen. Allerdings enthält § 57 Abs. 7 Satz 3 BDSG (neu) eine Ausnahmeklausel, nach der diese Überprüfung durch die Datenschutzaufsicht im Einzelfall durch die zuständige oberste Bundesbehörde wegen Gefährdung „der Sicherheit des Bundes oder eines Landes“ verweigert werden kann. Diese und weitere Ausnahmeklauseln dürften kaum mit den Bestimmungen der EU-Richtlinie vereinbar sein.[8] Die Bundesbeauftragte verfügt über genügend vertrauenswürdiges und sicherheitsüberprüftes Personal, um diese Aufgabe auch in solchen besonderen Fällen zuverlässig zu erfüllen. Die Einschränkung im BDSG (neu) ist daher weder erforderlich noch mit der Richtlinie vereinbar.

Schwierigkeiten in der praktischen Anwendung können sich auch dort ergeben, wo Vorschriften im Zuge der Richtlinien-Umsetzung auf mehrere Gesetze verteilt wurden. So finden sich die Regelungen zur *Data Breach Notification* in §§ 65, 66 BDSG. Das novellierte BKA-Gesetz enthält zu diesem und weiteren Themen ergänzende Regelungen mit zahlreichen Querverweisen auf das BDSG. Solche Querverweise führen dazu, dass die Vorschriften für interessierte Bürgerinnen und Bürger und für die anwendenden Polizeibediensteten nicht mehr aus sich heraus verständlich sind.

6. Schlussfolgerungen und Ausblick

Führt die Europäisierung des Datenschutzrechts im Ergebnis auch zu einem verbesserten Datenschutz für Polizei und Strafjustiz? Für die EU-Staaten, die bisher über kein ausdifferenziertes Eingriffsrecht auf diesem Gebiet verfügten, dürfte diese Frage mit „ja“ zu beantworten sein.

Darüber hinaus wird es darauf ankommen, wie die Potentiale der Richtlinie und ihrer mitgliedstaatlichen Umsetzung in der Praxis genutzt werden. Eine zentrale Rolle dürfte dabei der Gerichtshof der EU spielen. Er hat in den letzten Jahren signalisiert, dass er den Grundrechten auf Privatsphäre und Datenschutz auch in der Abwägung mit Sicherheitsbelangen einen hohen Stellenwert zumisst – so in seinen Entscheidungen zur Vorratsdatenspeicherung[9] und zur Passagierdatenübermittlung.[10] Daher kann erwartet werden, dass der Gerichtshof auch den Grundrechtsschutz durch die EU-Richtlinie für den Datenschutz im Polizei- und Strafjustizbereich eher ausweitend interpretieren wird. Manche Regelung der halbherzigen Umsetzung in das deutsche Recht dürfte daher nicht lange Bestand haben.

HARTMUT ADEN ist Jurist und Politikwissenschaftler. Er ist Professor für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft an der Hochschule für Wirtschaft und Recht Berlin, dort stellv. Direktor des Forschungsinstituts für Öffentliche und Private Sicherheit (FÖPS) sowie behördlicher Datenschutzbeauftragter der Hochschule. Webseite: www.hwr-berlin.de/prof/hartmut-aden.

Literatur

Aden, Hartmut 2014: Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem, in: Der Moderne Staat, Zeitschrift für Public Policy, Recht und Management (7. Jg., Nr. 1), 55-73.

Aden, Hartmut 2016: The Role of Trust for the Exchange of Police Information in the European Multilevel System, in: Ross, Jacqueline & Delpeuch, Thierry (eds.), Comparing the Democratic Governance of Police Intelligence. New Models of Participation and Expertise in the United States and Europe. Cheltenham, UK: Edward Elgar, 322-344.

Aden, Hartmut 2017: Europäisierung der Polizeiarbeit - ein Sonderfall im europäischen Verwaltungsraum?, in: Kopke, Christoph & Kühnel, Wolfgang (Hg.), Demokratie, Freiheit und Sicherheit. Festschrift zum 65. Geburtstag von Hans Gerd Jaschke, Baden-Baden: Nomos, 241-253.

Albrecht, Jan Philipp 2015: EU police cooperation and information sharing: more influence for the European Parliament?, in: Aden, Hartmut (ed.), Police Cooperation in the European Union under the Treaty of Lisbon – Opportunities and Limitations, Baden-Baden: Nomos, 223-233.

Bäcker, Matthias 2017: Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill, Hermann, Kugelmann, Dieter & Martini, Mario (Hg.), Perspektiven der digitalen Lebenswelt, Baden-Baden: Nomos, 63-88.

Bäcker, Matthias & Hornung, Gerrit 2012: EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa, in: Zeitschrift für Datenschutz, 147-152.

Balzacq, Thierry & Hadfield, Amelia 2012: Differentiation and trust: Prüm and the institutional design of EU internal security, in: Cooperation and Conflict (vol. 47, no. 4), 539-561.

Boehm, Franziska 2012: Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level, Heidelberg: Springer.

FRA (European Union Agency for Fundamental Rights) 2017: Fundamental rights and the interoperatbility of EU information systems: borders and security, Wien: FRA

Gruszczak, Artur 2016: Police and Customs Cooperation Centres and their Role in EU Internal Security, in Bossong, Raphael & Carrapico, Helena (eds.), EU Borders and Shifting Internal Security. Heidelberg: Springer, 157-175.

Gutiérrez Zarza, Ángeles (ed.) 2015: Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe, Heidelberg: Springer.

Hert, Paul de & Papakonstantinou Vagelis 2015: Data protection. The EU institutions' batlle over data processing vs individual rights, in: Trauner, Florian & Ripoll Servent, Ariadna (eds.), Policy Change in the Area of Freedom, Security and Justice. London: Routledge, 178-196.

Stief, Matthias 2017: Die Richtlinie (EU) 2016/680 zum Datenschutz in der Strafjustiz und die Zukunft der datenschutzrechtlichen Einwilligung im Strafverfahren, in: Strafverteidiger (StV) (37. Jg., Nr. 7), 470-477.

Anmerkungen:

1 Zur möglichen Rolle von Einwilligungen in diesem Bereich: Stief 2017.
2 Verabschiedete Fassung: Amtsblatt EU L 119 v. 4.5.2016, 89ff.; Entwurf: KOM 2012(10) endgültig v. 25.1.2012; kritische Würdigung der Entwurfsfassung bei Bäcker & Hornung 2012.
3 Amtsblatt EU L 350 vom 30.12.2008, 60ff.
4 Vgl. hierzu die Vorschläge der Europäischen Kommission, COM(2017) 793 endgültig v. 12.12.2017.
5 BVerfGE 65, 1.
6 BDSG in der Fassung des Datenschutz-Anpassungs- und Umsetzungsgesetzes EU v. 30.6.2017, BGBl. I, 2097.
7 Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes v. 1.6.2017, BGBl. I, 1354ff.
8 S. auch Bäcker 2017, 81f. zu den Ausnahmen zur Auskunftsregelung in der deutschen Umsetzung und ihrer Unvereinbarkeit mit der Richtlinie.
9 U.a. GHEU/EuGH, Rechtssachen C-293/12 und C-594/12, Urteil v. 8.4.2014.
10 U.a. GHEU/EuGH, Gutachten 1/15 v. 26.7.2017.