.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Rieser-Angulo Garcia, Yvonne/Bauer, Elisabeth (2013):

Polizeiliche und justizielle Zusammenarbeit in der EU. Teil II: Polizeilicher Informationsaustausch und Datenschutz

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3), 4-13.

doi: 10.7396/2013_3_A

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Rieser-Angulo Garcia, Yvonne/Bauer, Elisabeth (2013). Polizeiliche und justizielle Zusammenarbeit in der EU. Teil II: Polizeilicher Informationsaustausch und Datenschutz, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3), 4-13, Online: http://dx.doi.org/10.7396/2013_3_A.

Online publiziert: 12/2013

Polizeiliche und justizielle Zusammenarbeit in der EU

Teil II: Polizeilicher Informationsaustausch und Datenschutz

YVONNE RIESER-ANGULO GARCÍA,
Rechtspraktikantin am Bezirksgericht Gmunden, ehemalige stellv. Referatsleiterin im Referat I/7/b „EU-Grundsatzfragen und Koordination" im Bundesministerium für Inneres.

ELISABETH BAUER,
Referentin im Referat I/7/b „EU-Grundsatzfragen und Koordination" im Bundesministerium für Inneres.

Neben der im ersten Teil dieses Beitrages behandelten justiziellen Zusammenarbeit in Strafsachen ist der zweite wesentliche Grundpfeiler der Kooperation zwischen den Strafverfolgungs- und Sicherheitsbehörden in Europa der Austausch von polizeilichen Informationen. Dieser Austausch soll innerhalb der Union gemäß dem Grundsatz der Verfügbarkeit geschehen. Der Verfügbarkeitsgrundsatz beinhaltet das Gebot, dass der Austausch von strafverfolgungsrelevanten Informationen überall in der Union nach denselben Bedingungen zu erfolgen hat. So sollen die Aufklärung von Verbrechen mit grenzüberschreitendem Bezug wesentlich erleichtert und die ermittelnden Behörden rasch unterstützt werden. Damit eng im Zusammenhang stehen naturgemäß heikle und gewichtige Fragen des Schutzes der Daten jener, die vom Austausch dieser Informationen unmittelbar betroffen sind.

I. POLIZEILICHER INFORMATIONSAUSTAUSCH

Grundlage für zahlreiche der heutigen Instrumente zum grenzüberschreitenden Austausch von personenbezogenen Daten und Vorreiter etlicher Informationsmanagementstrategien im Bereich der Strafverfolgung[1] war ein 1985 im deutsch-französisch-luxemburgischen Dreiländereck bei Schengen gefasster Beschluss von Staats- und Regierungschefs fünf europäischer Länder[2]: Am 14. Juni 1985 kamen Deutschland, Frankreich, Belgien, die Niederlande und Luxemburg überein, die Kontrollen an den gemeinsamen Grenzen möglichst bis zum 01.01.1990 abzuschaffen.[3] Der Beschluss von Schengen basierte auf einer der markantesten Wunschvorstellungen zur Einigung Europas: der Abschaffung der Grenzen innerhalb eines gemeinsamen europäischen Rechtsraums und somit der Möglichkeit, alle Binnengrenzen ohne Personenkontrollen überschreiten zu können.

Wegbereiter für Schengen und erster konkreter Vorstoß dahingehend war der Vorschlag der Kommission der damaligen Europäischen Gemeinschaft (EG) zur Schaffung einer Passunion auf der Pariser Gipfelkonferenz 1974.[4] Während dieser erste Versuch scheiterte, konnte man sich

rund zehn Jahre später im Rahmen des „Saarbrückner Abkommens“ von 1984 auf den schrittweisen Abbau beiderseitiger Grenzkontrollen einigen. In weiterer Folge führte dies zum Beschluss von Schengen („Schengen I“) und später zum Abschluss des Schengener Durchführungsübereinkommens (SDÜ oder „Schengen II“)[5] von 1990, an denen sich immer mehr europäische Staaten beteiligen.[6]

Zum Zeitpunkt des Beitritts Österreichs am 28. April 1995[7] waren dem Übereinkommen bereits Italien[8], Spanien[9], Portugal[10] und Griechenland[11] beigetreten. Kurz darauf folgte 1996 der Beitritt von Dänemark[12], Finnland[13] und Schweden[14]. Der Vertrag von Amsterdam hat den Schengen-Acquis 1997 in das Unionsrecht überführt und sohin die Zuständigkeit des EuGH für Auslegungsfragen begründet.[15] Die Staaten, die der Europäischen Union seit Mai 2004 beigetreten sind, müssen den Schengen-Acquis vollständig übernehmen. Dies führt jedoch nicht zu einem sofortigen Entfall der Grenzkontrollen mit ihrem Beitritt.[16] Großbritannien und Irland haben von der Möglichkeit Gebrauch gemacht, den Schengen-Acquis ganz oder teilweise zu übernehmen („opt-in“), obwohl sie selbst nicht Vertragsstaaten des Schengener Übereinkommens sind.

Die Abschaffung der Grenzkontrollen an den Binnengrenzen bedurfte gleichzeitig der Schaffung einer Reihe von Maßnahmen an den Außengrenzen des Schengenraumes. Hinsichtlich der Ausstellung von Visa und der Koordinierung der Asyl- und Einwanderungspolitik wurde eine verstärkte Zusammenarbeit zwischen Polizei-, Justiz- und Zollbehörden notwendig, ebenso zur Bekämpfung der grenzüberschreitenden Kriminalität. Weder der Schengen-Raum noch der EU-Binnenmarkt könnten in ihrer heutigen Form ohne den grenzüberschreitenden Informationsaustausch funktionieren. Das Schengen Informationssystem SIS beispielsweise (neben der Prümer Zusammenarbeit und der Schwedischen Initiative wichtigstes Instrument) enthält Personen- und Sachausschreibungen. Es wird sowohl innerhalb des Schengenraums als auch an den Außengrenzen der EU genutzt und ist ein Großsystem mit mehr als 43 Millionen Ausschreibungen, auf das die Polizeibehörden nach dem Prinzip des „Treffer/kein Treffer“-Systems Zugriff haben. Nach einem Treffer können über die SIRENE-Büros zusätzliche Informationen angefordert werden. Am 9. April 2013 ist das neue SIS-System, „SIS II“, in Betrieb gegangen.

Nach dem Fallen der Binnengrenzen haben zuletzt die Terroranschläge in den USA von 2001 und die Bombenattentate von Madrid und London 2004 bzw 2005 neue Dynamik in die europäische Informationsmanagementpolitik gebracht.[17] Einige der zur Verfügung stehenden Instrumente waren dabei zweifelsohne umstrittener als andere. Während die Akzeptanz des Austausches von Daten rechtskräftig Verurteilter wenige Probleme bereitet, wird es beim Austausch von Spuren gesuchter Täter schon deutlich schwieriger. Am heikelsten sind natürlich Vorhaben zur Speicherung und Weitergabe von Informationen Unbescholtener.

Salopp formuliert, braucht man in den internationalen Gremien wohl kaum Argumentationskünste, um die europäischen Partner davon zu überzeugen, dass ein in Schweden gesuchter, rechtskräftig verurteilter Mörder auch in Italien ausgeforscht werden können soll, sollte er sich dorthin absetzen. Dass die Festnahme eines noch nicht rechtskräftig Verurteilten, jedoch dringend Tatverdächtigen auch noch gewünscht ist, selbst wenn dies die Weitergabe seiner am Tatort hinterlassenen Fingerabdrücke (als Teil seiner personen-

bezogenen Daten) bedarf, klingt für die meisten ebenfalls noch nachvollziehbar. Besonders diffizil, sei es unter den Mitgliedstaaten selbst, sei es gegenüber dem Europäischen Parlament und schließlich der Öffentlichkeit, werden die Verhandlungen jedoch, wenn Daten Unbescholtener zur Bekämpfung von Terrorismus und schwerer organisierter Kriminalität gespeichert und ausgetauscht werden sollen.

VORRATSDATENSPEICHERUNG

Anfang 2006 wurde die Richtlinie über die Vorratsdatenspeicherung[18] verabschiedet, die von Anbeginn für viele Kontroversen gesorgt hat. Sie soll es den nationalen Behörden ermöglichen, schwere Kriminalität durch die Speicherung von Telekommunikationsverkehrs- und Standortdaten zu bekämpfen. Die Bestimmungen der Vorratsdatenspeicherungsrichtlinie wurden in Österreich im Rahmen der sechsten Novelle des Telekommunikationsgesetzes (TKG) 2003[19] umgesetzt und sind am 01.04.2012 in Kraft getreten.[20] Entsprechend dazu wurden die notwendigen Novellierungen der Strafprozessordnung (StPO) und des Sicherheitspolizeigesetzes (SPG)[21] durchgeführt. Das TKG legt nunmehr die Verpflichtung der Anbieter öffentlicher Kommunikationsdienste zur Speicherung bestimmter, in § 102a TGK taxativ aufgezählter Daten (=Vorratsdaten) für die Dauer von sechs Monaten[22] fest. In Ergänzung dazu finden sich im SPG[23] und der StPO[24] die Voraussetzungen, unter denen ein Zugriff auf diese Vorratsdaten durch die Sicherheits- bzw Strafverfolgungsbehörden erfolgen darf. Die Speicherdauer von sechs Monaten steht im Gegensatz zur bisherigen Rechtslage, wonach seitens der Betreiber öffentlicher Kommunikationsdienste ohne Ausnahme eine unverzügliche Löschung aller nicht (mehr) für Betriebs- oder Verrechnungszwecke benötigten Daten zu erfolgen hatte. Auf Grund der gesetzlich verankerten Möglichkeit der Kunden, innerhalb von drei Monaten Einspruch gegen die Verrechnung zu erheben, war jedoch auch schon vor Umsetzung der Vorratsdatenspeicherungsrichtlinie ein Großteil der von den Strafverfolgungsbehörden benötigten Daten für drei Monate gespeichert, allerdings bisher nur als Betriebsdaten und nicht wie nunmehr (nach Betriebs- und Verrechnungszwecken) als Vorratsdaten.[25]

SCHWEDISCHE INITIATIVE

Gegen Ende des Jahres 2006[26] wurde die Schwedische Initiative[27] zur Vereinfachung des grenzüberschreitenden Austauschs von Informationen und Erkenntnissen für die Zwecke strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren vom Rat angenommen. Hinsichtlich der Eingriffsintensität ist die Schwedische Initiative im Vergleich zur Vorratsdatenspeicherung moderater.[28] Sie geht auf eine Initiative des Königreichs Schweden zurück[29] und umfasst im Kern Regeln, nach denen die Strafverfolgungsbehörden der Mitgliedstaaten wirksam und rasch bestehende Informationen und Erkenntnisse zur Durchführung strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren austauschen können.[30] Mit ihr sollen das bisherige Fehlen eines gemeinsamen Rechtsrahmens auf diesem Gebiet beseitigt[31] und gleichzeitig ein angemessenes Gleichgewicht zwischen einer effizienten Zusammenarbeit der Strafverfolgungsbehörden und den Grundsätzen des Datenschutzes, der Grundfreiheiten, der Menschenrechte und der individuellen Freiheit angestrebt werden.[32] Der Rahmenbeschluss erstreckt sich grundsätzlich auf alle Arten von Informationen, die bei Strafverfolgungsbehörden vorhanden sind.[33] Er verpflichtet die Mitgliedstaaten aber nicht, Informationen und Erkennt-

nisse mit dem Ziel zu sammeln und zu speichern, sie den Strafverfolgungsbehörden anderer Mitgliedstaaten bereitzustellen.[34] Die Mitgliedstaaten werden weder verpflichtet, Informationen und Erkenntnisse bereitzustellen, die als Beweismittel vor einer Justizbehörde verwendet werden sollen, noch verleiht er das Recht, solche Informationen vor Gericht zu verwenden. Sollte die Verwendung von durch die Schwedische Intiative gewonnenen Informationen vor einer Justizbehörde durch einen Mitgliedstaaten beabsichtet werden, muss jener Mitgliedstaat, der die Information bereitgestellt hat, um Einwilligung[35] ersucht werden.[36] Der Rahmenbeschluss legt Fristen für die Zurverfügungstellung von Informationen und Erkenntnissen fest. Demnach muss im Regelfall innerhalb von höchstens acht Stunden auf dringende Ersuchen[37] geantwortet werden.[38] In allen anderen Fällen ist seitens der Mitgliedstaaten sicherzustellen, dass die Beantwortung innerhalb von einer Woche[39] bzw 14 Tagen[40] erfolgt. Ziel war es, den ehemals in der Praxis vorgekommenen extrem langen Wartezeiten bis zur Übermittlung der Informationen entgegen zu wirken.[41] Eines der Grundprinzipien der Schwedischen Initiative ist das Prinzip des „gleichberechtigten Zugangs", wonach die Bedingungen für die Bereitstellung von Informationen für ersuchende Mitgliedstaaten nicht strenger sein dürfen als die auf nationaler Ebene geltenden.[42] Neben den Mitgliedstaaten der Europäischen Union beteiligen sich auch Island, Norwegen[43] und die Schweiz[44] an der Schwedischen Initiative. Eine Begrenzung findet der durch die Schwedische Initative errungene Fortschritt darin, dass es nicht um eine gegenseitige Verfügbarkeit von Daten geht, sondern um einen gleichberechtigten Zugang zu Informationen nach dem geltenden Recht des jeweiligen Mitgliedstaats, was in der Praxis zu Problemen führen kann. Als größte Hürde haben sich die Verzögerungen bei der Umsetzung ins nationale Recht seitens vieler Mitgliedstaaten gezeigt.[45] Im ursprünglichen Text war eine Umsetzung bis zum 19. Dezember 2006 vorgesehen[46], eine Berichtigung des Rahmenbeschlusses im Jahr 2007[47] erstreckt die Frist zur Umsetzung auf den 19. Dezember 2008.[48] Mit wenigen Ausnahmen[49] haben die meisten Mitgliedstaaten den Rahmenbeschluss mittlerweile in nationales Recht umgesetzt.[50] Für einige[51], darunter Österreich, war eine Umsetzung nicht erforderlich, da das innerstaatliche Recht, nach eigenen Angaben, bereits in Einklang mit der Initiative stand. In Österreich sind für den Anwendungsbereich der Schwedischen Initiative das Polizeikooperationsgesetz (PolKG)[52], das EU-Polizeikooperationsgesetz (EU-PolKG)[53] und das Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG)[54] relevant.

Die Europäische Kommission hat in ihrer aktuellen Mitteilung zum Informationsaustausch[55] festgestellt, dass die Schwedische Initiative, ungeachtet der mittlerweile hohen Umsetzungsquote und trotz ihrer Vorteile, in der Praxis noch immer keine breite Anwendung findet. Es habe sich gezeigt, so die Kommission, dass in Fällen, in denen zusätzliche Informationen als Beweismittel vor Gericht benötigt werden, in der Regel ein Antrag auf justizielle Zusammenarbeit erforderlich ist. In den Fällen, in denen gerichtliche Beweismittel nicht (oder noch nicht) benötigt werden, sollte aus Sicht der Kommission die systematische Verwendung der Schwedischen Initiative als Rechtsgrundlage gefördert werden, um ihre Vorteile (genaue Fristen, Prinzip des „gleichberechtigten Zugangs") in vollem Umfang nutzen zu können und um dazu beizutragen, dass die Mitgliedstaaten beim Informationsaustausch einheitliche bewährte Verfahren anwenden.[56]

PRÜMER BESCHLUSS

Am 23. Juni 2008 erfolgte die Annahme des Beschlusses von Prüm[57], mit dem der Austausch von DNA-Profilen, Fingerabdrücken und Daten aus Fahrzeugregistern zur Bekämpfung des Terrorismus und anderer Formen der Kriminalität beschleunigt wurde. Der Prümer Beschluss erging auf Initiative von Deutschland, Spanien, Frankreich, Luxemburg, der Niederlande, Österreich, Slowenien, der Slowakei, Italien, Finnland, Portugal, Rumänien und Schweden[58] und hatte die Überführung des zentralen Inhalts des Prümer Vertrags[59] in den Rechtsrahmen der Europäischen Union zum Ziel.[60] Gleichzeitig nahm der Rat den Beschluss 2008/616/JI[61] zur Durchführung des Prümer Beschlusses (2008/615/JI) an. Im November 2009 haben sich Island und Norwegen beiden Beschlüssen angeschlossen.[62] Mit dem Beschluss von Prüm wurde ein System für den automatisierten Austausch von DNA-Daten, Fingerabdrücken und KfZ-Zulassungsdaten geschaffen. Beim Abgleich biometrischer Daten (DNA, Fingerabdrücke) wird ein „Treffer/kein-Treffer"-System angewandt: Ein automatisierter Abgleich anonymer Profile führt zu einem „Treffer", wenn die Daten des ersuchenden Mitgliedstaats mit den Daten eines anderen Mitgliedstaats übereinstimmen. Zusätzliche personen- oder fallbezogene Daten werden nur auf ein gesondertes Folgeersuchen hin übermittelt. Österreich hat im Rahmen der Prümer Zusammenarbeit gemeinsam mit Deutschland bei Verhandlung und Umsetzung eine Vorreiterrolle eingenommen.

FALLBEISPIELE[63]

Anhand der folgenden Beispiele[64] soll illustriert werden, wie die europäischen Instrumente in der Praxis genutzt werden.

Fall 1: In Deutschland wurde ein Mann erstochen in seiner Wohnung aufgefunden. Die Ermittler entdeckten einen Fingerabdruck am Türrahmen und führten eine Prüm-Abfrage durch. Es kam zu einem automatisierten Treffer in Bulgarien, woraufhin die deutsche Polizei ihre bulgarischen Kollegen um Übermittlung von Zusatzinformationen ersuchte. Binnen drei Stunden sendete die bulgarische Polizei die ihr zum vermeintlichen Täter zur Verfügung stehenden Dokumentationen. Unverzüglich gaben die deutschen Behörden die Informationen in das Schengen Informationssystem ein. Am nächsten Tag konnte die betreffende Person in Österreich festgenommen werden.

Fall 2: Bei einem Diebstahl von Ausrüstungsgegenständen aus einem Polizeiauto in Wien hinterließ der unbekannte Täter einen Fingerabdruck. Die österreichische Polizei konnte diesen mit anderen Spuren in der Prüm-Datenbank abgleichen. Dank eines Treffers in Deutschland konnte ein polnischer Serieneinbrecher identifiziert werden. Österreich stellte sogleich einen Europäischen Haftbefehl aus. Ein Treffer bei einer SIS-Ausschreibung führte zur Festnahme in Polen.

Fall 3: Einem – in seiner Heimat bereits bekannten – italienischen Betrüger gelang es, einen schwedischen Geschäftsführer dazu zu bringen, 65.000 Euro auf ein italienisches Bankkonto einzuzahlen. Die italienische Polizei erhielt Kenntnis davon und nahm über den SIRENE-Kanal Kontakt zur nationalen Europol-Kontaktstelle in Schweden auf. Die schwedischen Behörden wurden ersucht, mit dem Geschäftsführer Kontakt aufzunehmen und zu prüfen, ob die Zahlung bereits getätigt worden war. Italien sagte zu, das Geld einzufrieren, wenn dem so sei. Schweden wurde tätig und reagierte gemäß der Schwedischen Initiative binnen weniger als 24 Stunden. Dank des raschen Handelns wurde die

schwedische Polizei über den Betrug informiert und die italienischen Behörden erhielten alle erforderlichen Informationen, um vor Ort eingreifen zu können. Der schwedische Unternehmer wird sein Geld aller Voraussicht nach in Kürze zurückerhalten.

Fall 4: Ein Belgier wurde mit einer schweren Schussverletzung in die Notaufnahme eines Pariser Krankenhauses eingeliefert. Seine Erklärungen, wie es zur Verletzung kam, waren unschlüssig, was zur Befragung seines Begleiters – und in weiterer Folge zur Aufnahme von Ermittlungen – führte. Die französische Polizei vermutete eine mögliche Straftat. Ein internationaler Datenabgleich ergab, dass der Verletzte in Belgien u.a. bereits wegen Totschlags verurteilt worden war. Im Rahmen der Schwedischen Initiative übermittelten die französischen Behörden unverzüglich Informationen zum Betroffenen an die belgische Polizei, die so rasch eine Verbindung zu einem zwei Tage zuvor in Belgien stattgefundenen Überfall herstellen konnte. Bei dem Überfall wurde ein Angestellter eines Juwelierladens von vier bewaffneten Männern entführt. Bei Eintreffen der Polizei gelang den Männern zwar die Flucht, allerdings wurde einer von Ihnen beim Schusswechsel mit der Polizei getroffen. Diese Informationen veranlassten die französischen Behörden, den Mann unter Beobachtung zu stellen. Noch am selben Tag stellte Belgien einen Europäischen Haftbefehl aus und schickte diesen über den SIRENE-Kanal an Frankreich, wo sodann die Festnahme erfolgte.

Fall 5: In ganz Slowenien wurden mithilfe gefälschter Bankomatkarten große Geldsummen abgehoben. Die Ermittlungen brachten die slowenischen Behörden auf die Spur zweier bulgarischer Betrüger. Das Europol-Informationssystem führte zu einem Treffer, wonach einer der beiden Verdächtigen bereits ähnliche Straftaten in Frankreich und Italien verübt hatte. Slowenien bat um Zusatzinformationen, Frankreich antwortete über den sicheren Kanal SIENA. Dank der raschen Rückmeldung der französischen Behörden konnte es zur Festnahme und in weiterer Folge zur Anklage in Slowenien kommen. Mithilfe der Europol-Arbeitsdatei zu Analysezwecken konnten weitere Verbindungen der Angeklagten zu Straftaten in Bulgarien, Frankreich, Irland und Norwegen aufgedeckt werden.

II. DATENSCHUTZ IN DER EU

In Art 16 Abs 1 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) ist der Grundsatz verankert, dass jeder Mensch das Recht auf Schutz seiner personenbezogenen Daten hat. Mit dem Inkrafttreten des Vertrages von Lissabon im Dezember 2009 wurde in Art 16 Abs 2 AEUV eine neue Rechtsgrundlage für den Erlass von Sekundärrecht geschaffen, die auch für die polizeiliche und justizielle Zusammenarbeit gilt.[65] Weitere Bestimmungen zum Grundrecht auf Datenschutz befinden sich in Art 8 Abs 1 und 2 der Charta der Grundrechte der EU (GRCh) und in Art 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK).

Mit der vermehrten Kooperation zwischen den Strafverfolgungs- und Sicherheitsbehörden in Europa und der steigenden Anzahl der Instrumente, der sich diese bedienen können, gehen die Ausweitung datenschutzrechtlicher Regelungen und die Zunahme der Bedeutung derselben einher. Beispielsweise zeichnet sich der zuletzt behandelte Prümer Beschluss in seiner Charakteristik durch ausführliche Datenschutzbestimmungen aus: Im Kapitel „Allgemeine Bestimmungen zum Datenschutz“[66] werden in Art 24 bis 32 unter

anderem Begriffsbestimmungen, das Datenschutzniveau, Zweckbindungen, Behördenzuständigkeit, Speicherungsdauer, technische und organisatorische Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit, Dokumentation und Protokollierung sowie Rechte der Betroffenen auf Auskunft und Schadenersatz[67] geregelt.

Ferner stellen einige Instrumente der EU datenschutzrechtliche Herausforderungen dar, wie zum Beispiel die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.[68] Nach wie vor ist nicht restlos geklärt, ob die Vorratsdatenspeicherungs-Richtlinie im Einklang mit grundrechtlichen Anforderungen steht.[69]

Vor dem Hintergrund eines sich rasant entwickelnden technischen Fortschrittes und damit verbundenen, teils unbekannten Sicherheitsrisiken hat die EU-Kommission am 25. Jänner 2012 ein neues Datenschutzpaket vorgelegt. Der neue Rechtsrahmen besteht aus einer Datenschutz-Grundverordnung[70] und einer Richtlinie für den Bereich der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten.[71] Diese beiden Rechtsakte sollen die folgenden, derzeit noch bestehenden EU-Datenschutzregelungen ersetzen: Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[72] soll durch die Datenschutz-Grundverordnung und der 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[73], soll durch die Richtlinie für den Bereich der justiziellen und polizeilichen Zusammenarbeit aufgehoben werden.

Der sehr umfassende Vorschlag für eine Datenschutz-Grundverordnug soll erstmals ein einheitlicher und in jedem Mitgliedstaat unmittelbar anwendbarer Rechtsrahmen im Bereich des Datenschutzes sein, mit dem Ziel der Erreichung einer weitgehenden Harmonisierung im betreffenden Bereich.

Ziel des Vorschlages für eine Richtlinie für den polizeilichen und justiziellen Bereich ist es, „ein hohes, einheitliches Datenschutzniveau in diesem Bereich zu garantieren und damit das gegenseitige Vertrauen zwischen den Polizei- und Justizbehörden verschiedener Mitgliedstaaten zu stärken und den freien Datenverkehr und die Zusammenarbeit zwischen Polizei- und Justizbehörden zu erleichtern“.[74]

Während der derzeit in Kraft stehende Rahmenbeschluss 2008/977/JI nur für den grenzüberschreitenden Austausch personenbezogener Daten innerhalb der EU und nicht für Datenverarbeitungen innerhalb der Mitgliedstaaten gilt, soll sich der Anwendungsbereich des Richtlinien-Entwurfes sowohl auf inländische als auch auf grenzüberschreitende Datenübermittlungen im Anwendungsbereich des Unionsrechts erstrecken.[75] Die Europäische Kommission führt in der Mitteilung zum Stockholmer Programm und im Aktionsplan zur Umsetzung des Stockholmer Programms[76] an, dass der Rahmenbeschluss zu viele Ausnahmen vom Zweckbindungsprinzip vorsehe.[77] Die Richtlinie soll neben der Ausdehnung des Anwendungsbereichs noch weitere Neuerungen für die polizeiliche Zusammenarbeit bringen, wie zum Beispiel neue Begriffsbestimmungen („genetische Daten“[78] und „Kind“[79]), die Einführung einer Pflicht zur Unterscheidung

verschiedener Kategorien von betroffenen Personen[80], wonach bei Verarbeitung der Daten klare Hinweise auf die Eigenschaft einer Person („Verdächtiger", „Opfer", „Beschuldigter", Verurteilter" etc) schließen lassen müssen, die Kategorisierung genetischer Daten als „sensible" Daten[81] und die Einführung eines grundsätzlichen Verarbeitungsverbotes (anders als Art 6 des Rahmenbeschlusses 2008/977/JI, wonach nur ein angemessener Schutz gefordert wurde) dergleichen, sowie die Möglichkeit der Ausnahme von diesem Verbot unter näher definierten Voraussetzungen[82] (zB wenn angemessene Garantien vorgesehen sind, Wahrung lebenswichtiger Interessen etc). Ferner sieht der Vorschlag detailliertere Regelungen der Betroffenenrechte[83], Dokumentationspflichten des Auftraggebers[84], die Pflicht von Auftraggebern zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde[85] und die verpflichtende Einsetzung eines Datenschutzbeauftragten[86] vor. Die beiden Rechtsakte befinden sich derzeit in Verhandlung.

Die EU nimmt im Hinblick auf die datenschutzrechtliche Entwicklung eine Doppelrolle ein: Einerseits gilt es als ihre Aufgabe, die Gesellschaft so sicher wie möglich zu erhalten, und gleichzeitig muss sie die Grundrechte der Menschen achten und schützen. Dies stellt die EU vor viele, alte und neue Herausforderungen, die auch in Zukunft nach derzeitiger Prognose nicht weniger werden. Vertrauensbildende Maßnahmen, welche den Bürgern vor Augen führen, dass der Datenschutz als Grundrecht durch die EU wirksam gewährleistet wird, sind die Voraussetzung, um die Bevölkerung zu überzeugen, dass bestimmte, angemessene Einschränkungen notwendig sind, um Sicherheit langfristig gewährleisten zu können.

[1] *Europäische Kommission (2010a) 2.*
[2] *Hetzer (2011) 651, RZ 50.*
[3] *ABl L 239 vom 22.09.2000, 13 ff.*
[4] *Hetzer (2011) 651, RZ 50.*
[5] *ABl L 239 vom 22.09.2000, 19 ff.*
[6] *Hetzer (2011) 652.*
[7] *ABl L 239 vom 22.09.2000, 90–96.*
[8] *ABl L 239 vom 22.09.2000, 63–68.*
[9] *ABl L 239 vom 22.09.2000, 69–75.*
[10] *ABl L 239 vom 22.09.2000, 76–82.*
[11] *ABl L 239 vom 22.09.2000, 83–89.*
[12] *ABl L 239 vom 22.09.2000, 97–105.*
[13] *ABl L 239 vom 22.09.2000, 106–114.*
[14] *ABl L 239 vom 22.09.2000, 115–126.*
[15] *Hetzer (2011) 652, RZ 51.*
[16] *Hetzer (2011) 652, RZ 50.*
[17] *Europäische Kommission (2010a) 2.*
[18] *Richtlinie 2002/58/EG idF 2006/24/EG ABl L 105 vom 13.04.2006.*
[19] *Änderung des Telekommunikationsgesetzes 2003 – TKG 2003, BGBl I 2011/27.*
[20] *§ 137 Abs 4 TKG „(4) §§ 94 Abs 1 und 102a Abs 1 in der Fassung des Bundesgesetzes BGBl I Nr 27/2011 treten am 1. April 2012 in Kraft".*
[21] *Änderung der Strafprozessordnung 1975 und des Sicherheitspolizeigesetzes, BGBl I 2011/33.*
[22] *§ 102a Abs 1 TKG.*
[23] *Vgl § 53 Abs 3a, 3b und 3c SPG.*
[24] *Vgl § 76a StPO.*
[25] *Vgl ausführlich zur Vorratsdatenspeicherungsrichtlinie und der österreichischen Umsetzung Pühringer (2012/2013).*
[26] *Am 18.12.2006.*
[27] *Rahmenbeschluss 2006/960/JI des Rates, ABl L 386 vom 29.12.2006, 89, Berichtigung durch ABl L 75 vom 15.03.2007, 26 (2006/960/JI).*

[28] *Zöller (2011) 65.*
[29] *Rahmenbeschluss 2006/960/JI des Rates, ABl L 386 vom 29.12.2006, 89.*
[30] *Art 1 Abs 1 Rahmenbeschluss 2006/960/JI.*
[31] *Erwägungsgrund 8 Rahmenbeschluss 2006/960/JI.*
[32] *Erwägungsgrund 11 Rahmenbeschluss 2006/960/JI.*
[33] *Art 2 lit d Rahmenbeschluss 2006/960/JI.*
[34] *Art 1 Abs 3 Rahmenbeschluss 2006/960/JI.*
[35] *Falls nach dem nationalen Recht des übermittelnden Mitgliedstaats erforderlich, unter Rückgriff auf die zwischen den Mitgliedstaaten geltenden Rechtsinstrumente für die justizielle Zusammenarbeit, vgl Art 1 Abs 4 Rahmenbeschluss 2006/960/JI.*
[36] *Art 1 Abs 4 Rahmenbeschluss 2006/960/JI.*
[37] *Ersuchen über Straftaten nach Art 2 Abs 2 des Rahmenbeschlusses 2002/584/JI.*
[38] *Art 4 Abs 1, sollte die Beantwortung binnen acht Stunden nicht möglich sein, siehe Art 4 Abs 2 Rahmenbeschluss 2006/960/JI.*
[39] *Art 4 Abs 3 Rahmenbeschluss 2006/960/JI bezüglich nicht dringende Ersuchen nach Art 2 Abs 2 des Rahmenbeschlusses 2002/584/JI.*
[40] *Art 4 Abs 4 Rahmenbeschluss 2006/960/JI betreffend alle weiteren Fälle.*
[41] *Zöller (2011) 65.*
[42] *Art 3 Abs 3 Rahmenbeschluss 2006/960/JI.*
[43] *Erwägungsgrund 13 Rahmenbeschluss 2006/960/JI, für Island und Norwegen stellt die Schwedische Initiative eine Weiterentwicklung des Schengenbesitzstandes dar.*
[44] *Erwägungsgrund 14 Rahmenbeschluss 2006/960/JI, für die Schweiz stellt die Schwedische Initiative eine Weiterentwicklung des Schengenbesitzstandes dar.*
[45] *Zöller (2011) 65.*
[46] *Ex Art 11 Abs 1 Rahmenbeschluss 2006/960/JI idF ABl L 386 vom 29.12.2006, 89.*
[47] *C1 Berichtigung Rahmenbeschluss 2006/960/JI, ABl L 75 vom 15.03.2007, 26.*
[48] *Art 11 Abs 1 Neu Rahmenbeschluss 2006/960/JI idF C1 Berichtigung Rahmenbeschluss 2006/960/JI, ABl L 75 vom 15.03.2007.*
[49] *Belgien, Griechenland, Italien und Luxemburg müssen noch Durchführungsvorschriften annehmen.*
[50] *Bulgarien, Tschechische Republik, Dänemark, Deutschland, Estland, Spanien, Frankreich, Zypern, Ungarn, Litauen, Lettland, Niederlande, Polen, Portugal, Rumänien, Slowenien, Slowakei, Finnland, Schweden.*
[51] *Irland, Malta, Österreich, Vereinigtes Königreich.*
[52] *Bundesgesetz über die internationale polizeiliche Kooperation, BGBl I Nr 104/1997.*
[53] *Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol), BGBl I Nr 132/2009.*
[54] *Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union, BGBl I Nr 36/2004.*
[55] *Europäische Kommission (2010a).*
[56] *Europäische Kommission (2010a) 10.*
[57] *Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität („Prümer Beschluss"), ABl L 210 vom 06.08.2008, 1.*
[58] *Beschluss 2008/615/JI ABl L 210 vom 06.08.2008, 1.*
[59] *Geschlossen am 27. Mai 2005 in Prüm (Deutschland) zwischen Belgien, Deutschland, Spanien, Frankreich, Luxemburg, den Niederlanden und Österreich zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration. Finnland, Slowenien, Ungarn, Estland, Rumänien, die Slowakei und Bulgarien sind dem Prümer Vertrag beigetreten.*
[60] *Erwägungsgrund 1 Beschluss 2008/615/JI.*
[61] *ABl L 210 vom 06.08.2008, 12.*
[62] *Beschluss des Rates vom 21. September 2009 über die Unterzeichnung im Namen der Europäischen Union und die vorläufige Anwendung einiger Bestimmungen des Übereinkommens zwischen der Europäischen Union sowie Island und Norwegen über die Anwendung einiger Bestimmungen des Beschlusses 2008/615/JI des Rates zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, und des Beschlusses 2008/616/JI des Rates zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, und seines Anhangs, ABl L 353 vom 31.12.2009, 1–8.*
[63] *Bauer/Rieser-Angulo Garcia (2013) 46.*
[64] *Vgl Mitteilung der Kommission: Europäische Kommission (2012a).*
[65] *Vgl Geiger/Khan/Kotzur (2010) 213.*
[66] *Beschluss 2008/615/JI, Kapitel 6, „Allgemeine Bestimmungen zum Datenschutz".*
[67] *Vgl Art 24 bis 32 Beschluss 2008/615/JI.*
[68] *Amtsblatt Nr L 105 vom 13.04.2006, 54–63.*
[69] *Vgl zB Tretter (2010) 165.*
[70] *Europäische Kommission (2012b).*
[71] *Europäische Kommission (2012c).*
[72] *ABl L 281 vom 23.11.1995, 31–50.*
[73] *ABl L 350 vom 30.12.2008, 60–71.*
[74] *Europäische Kommission (2012a) 5.*

[75] *Vgl Art 2 des RL-Entwurfes.*
[76] *Europäische Kommission (2009); Europäische Kommission (2010b).*
[77] *Vgl Souhrada-Kirchmayer (2011) 33.*
[78] *Europäische Kommission (2012a) 10, Art 3, Z 10.*
[79] *Europäische Kommission (2012a) 10, Art 3, Z 13.*
[80] *Europäische Kommission (2012a) 10, Art 5.*
[81] *Europäische Kommission (2012a) 10, Art 8, Abs 1.*
[82] *Europäische Kommission (2012a) 10, Art 8, Abs 2.*
[83] *Europäische Kommission (2012a) 10, Art 10, 11, 12, 15, 16.*
[84] *Europäische Kommission (2012a) 10, Art 24.*
[85] *Europäische Kommission (2012a) 10, Art 28.*
[86] *Europäische Kommission (2012a) 10, Art 30 bis Art 32.*

Quellenangaben

Bauer/Rieser-Angulo Garcia, Den Tätern auf der Spur, Öffentliche Sicherheit, 2013/5–6, 46.
Europäische Kommission (2005). Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit, KOM(2005) 490 endgültig.
Europäische Kommission (2009). Mitteilung der Kommission an das Europäische Parlament und den Rat, Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger, KOM (2009) 262 endgültig vom 10.06.2010.
Europäische Kommission (2010a). Mitteilung der Kommission an das Europäische Parlament und den Rat, Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht, KOM(2010) 385 endgültig.
Europäische Kommission (2010b). Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Ein Raum der Freiheit, der Sicherheit und des Rechts für die Bürger Europas Aktionsplan zur Umsetzung des Stockholmer Programms, KOM (2010) 171 endgültig vom 20.04.2010.
Europäische Kommission (2012a). Mitteilung der Kommission an das Europäische Parlament und den Rat, Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch, KOM(2012) 735 endgültig.
Europäische Kommission (2012b). Vorschlag für eine VO des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(2012) 11 endgültig vom 25.01.2012.
Europäische Kommission (2012c).Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endgültig vom 25.01.2012.
Geiger/Khan/Kotzur, EUV, AEUV, Kommentar (2010).
Hetzer, Zusammenarbeit von Polizei und Zoll, in Sieber/Brüner et al, Europäisches Strafrecht (2011).
Pühringer, Vorratsdatenspeicherung; Zugriffsmöglichkeiten durch Sicherheits- und Strafverfolgungsbehörden, JAP 2012/2013/10.
Souhrada-Kirchmayer, Das Gesamtkonzept für den Datenschutz in der Europäischen Union, Jahrbuch Datenschutzrecht (2011) 33.
Tretter, Der Digital bewegte Mensch, Europäische Präsidentenkonferenz 2010, AnwBl 2010, 165.
Zöller, Der Austausch von Strafverfolgungsdaten zwischen den Mitgliedstaaten der Europäischen Union, ZIS 2011/2.

Weiterführende Literatur und Links

Bauer/Rieser-Angulo Garcia, Polizeiliche und justizielle Zusammenarbeit in der EU, Teil I: Europäisches Strafrecht und die justizielle Zusammenarbeit in Strafsachen in der EU, SIAK-Journal 2013/2, 4.
Borchhardt, Die rechtlichen Grundlagen der Europäischen Union (2010).
Callies/Ruffert, EUV AEUV Kommentar (2011).