Datenschutzrecht und E-Government

Jahrbuch 2012

herausgegeben

von

ao. Univ.-Prof. Dr. Dietmar Jahnel

Universität Salzburg
Fachbereich Öffentliches Recht

nw neuer wissenschaftlicher Verlag

RECHT

Wien · Graz 2012

Bei der Implementierung von eArchivanwendungen sollte technisch unbedingt eingeschränkt werden, dass Daten nicht in einer Art und Weise abrufbar gehalten werden, die über das erforderliche Ausmaß hinausgehen und dies dann uU weder arbeitsverfassungsrechtlich noch datenschutzrechtlich rechtfertigbar wäre. Um solche Problematiken zu minimieren, wird eine Vorgangsweise ähnlich der unter Punkt VI. geschilderten Prozesse empfohlen.

Gerhard KUNNERT*

„Tausche Visafreiheit gegen Datenschutz" – Die neue Polizeikooperation auf Basis des US-österreichischen „Prüm-like"-Abkommens

Inhaltsübersicht

* Der Autor hat als Experte des Bundeskanzleramt-Verfassungsdienstes an den formellen Vertragsverhandlungen über den „Prümer Vertrag" bzw (teilweise) an jenen über das bilaterale „Prüm-like"-Abkommen zwischen Österreich und den USA mitgewirkt. Die dem Beitrag zu entnehmenden Wertungen spiegeln ausschließlich die persönliche Meinung des Autors wider.

I. Einleitung

Im Mai 2005 unterzeichneten sieben von damals bereits 27 EU-Mitgliedstaaten den „Vertrag von Prüm" (auch: „Prümer Vertrag")[1]. Mit diesem multilateralen Abkommen sollte ein neues Kapitel in der grenzüberschreitenden Polizeizusammenarbeit aufgeschlagen werden. Bis dahin stützte sich die EU-weite polizeiliche Kooperation im Wesentlichen auf das sog „Schengener Durchführungsübereinkommen"[2] aus 1990 (kurz: „SDÜ") sowie auf dieses ergänzende „herkömmliche" bilaterale Abkommen. Das ursprünglich außerhalb des EU-Rechtsrahmens geschlossene multilaterale SDÜ war infolge des Vertrages von Amsterdam (1997)[3] zwar zum Bestandteil des EU-Acquis geworden. Aus Sicht der Sicherheitsbehörden gelang es aber in den Folgejahren nicht, dieses Übereinkommen „im gewünschten Maße den steigenden Notwendigkeiten zum Ausbau der polizeilichen Zusammenarbeit bei der Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration anzupassen".[4] Einschlägige Initiativen zur Weiterentwicklung der polizeilichen Zusammenarbeit waren va von Deutschland ausgegangen. Sie scheiterten infolge des damals für die sog „3. Säule" der EU[5] geltenden Einstimmigkeitsprinzips im Rat jedoch oftmals am Widerstand einzelner Mitgliedstaaten.[6] Vor diesem Hintergrund initiierte Deutschland im Februar 2003 ein Treffen der Innen- und Justizminister Deutschlands und der Benelux-Staaten in Luxemburg, wo diese beschlossen, Verhandlungen über einen multilateralen Vertrag zur Verstärkung der polizeilichen Zusammenarbeit aufzunehmen.[7] Analog dem SDÜ sollte es sich dabei zunächst um ein bewusst außerhalb des EU-Rahmens angesiedeltes Instrument handeln, dessen

1 Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration; Quellen: (dt): öBGBl III 2006/159; (engl): Anl zu Ratsdok 10900/05 v 7.5.2005: Note from Council Secretariat to delegations. Subject: Prüm Convention. Dazu insgesamt *Mutschler*, Der Prümer Vertrag (2010).

2 Übereinkommen zur Durchführung des Übereinkommens von Schengen v 14. 6. 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (Quelle: ABl 2000 L 239, 19) . Näheres dazu bei *O'Keeffe*, The Schengen Convention: A Suitable Model for European Integration? in YEL 1991, 185 ff; *Taschner*, Schengen. Die Übereinkommen zum Abbau der Personenkontrollen an den Binnengrenzen von EU-Staaten[1] (1997) Rn 40 ff.

3 Vertrag von Amsterdam zur Änderung des Vertrags über die Europäische Union, der Verträge zur Gründung der Europäischen Gemeinschaften sowie einiger damit zusammenhängender Rechtsakte v 2.10.1997 ABl C 340, 1.

4 Vgl idS Vorblatt („Problem:") RV 1155 BlgNR 22. GP, 1.

5 Dh die polizeiliche und justizielle Zusammenarbeit in Strafsachen (PJZS); vgl Art 29 ff EUV idF vor dem Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft v 13.12.2007 ABl C 306, 1 (kurz: VvL).

6 Vgl idS wieder Vorblatt („Problem:") RV 1155 BlgNR 22. GP, 1.

7 Vgl Erl „Allgemeiner Teil" RV 1155 BlgNR 22. GP, 3.

Inhalte jedoch später wiederum in das EU-Recht integriert werden sollten.[8]

Tatsächlich gelang es der vorstehend genannten Pioniergruppe um Deutschland, ab November 2003 ergänzt um Österreich,[9] mit der Ausverhandlung des Prümer Vertrages direkte Vorarbeiten für die EU zu leisten. Schon im Juni 2008 konnte nämlich auf Initiative der Erstunterzeichner[10] des Prümer Vertrages und einiger weiterer EU-Mitgliedstaaten[11] vom Rat für Justiz und Inneres ein Ratsbeschluss[12] zwecks „Überführung"[13] des (wesentlichen) Inhalts des Prümer Vertrags in den Rechtsrahmen der EU angenommen werden (kurz: „Prümer Beschluss"). Dass das „Vorpreschen" der besagten „Pionierstaaten" unter völliger Außerachtlassung des in den Verträgen vorgesehenen Mechanismus der sog „verstärkten Zusammenarbeit"[14] und insofern in Verletzung des unionsrechtlichen „Loyalitätsgebots"[15] erfolgt war,[16] steht auf einem anderen Blatt.

Das quasi „revolutionäre" an diesem Instrument war darin zu sehen, dass hier erstmals ein **direkter grenzüberschreitender Zugriff** auf nationale **Polizeidatenbanken** vorgesehen worden war. Konkret beziehen sich diese **wechselseitigen „Online-Zugriffe"[17] auf** sog DNA-Analyse-Dateien[18], automatisierte daktyloskopische Identifizierungssysteme (vereinfachend auch: Fingerabdruckdaten-

8 Vgl ebenda.

9 Vgl ebenda.

10 Vgl wieder FN 1.

11 Nämlich der Republik Bulgarien, der Republik Slowenien, der Slowakischen Republik, der Italienischen Republik, der Republik Finnland, der Portugiesischen Republik, Rumäniens und des Königreichs Schweden (vgl 2. Einleitungssatz des Beschlusses 2008/615/JI des Rates v 23.6.2008 ABl L 210, 1, zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität).

12 Beschluss 2008/615/JI (FN 11).

13 Vgl 1. Erwägungsgrund des Beschlusses 2008/615/JI (FN 11).

14 Vgl Art 40, 40a, 40b u 43 ff EUV idF vor dem Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft v 13.12.2007 ABl C 306, 1 (kurz: VvL) bzw Art 20 EUV idF VvL sowie Art 11 EGV (nunmehr: Art 326 ff AEUV).

15 Vgl Art 10 EGV idF vor VvL (nunmehr: Art 4 Abs 3 EUV).

16 Kritisch dazu etwa *Balzacq*, The Treaty of Prüm and the Principle of Loyality (Art 10 TEC), CEPS Briefing Paper No IP/C/LIBE/OF/2005-168 (January 2006); Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB) v 4.4.2007 ABl C 169, 2 (4), zur Initiative des Königreichs Belgien [...] zum Erlass eines Beschlusses des Rates zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität; *Morini*, La Convenzione di Prüm sulla cooperazione transfrontaliera specialmente in materia di lotta al terrorismo, al crimine transnazionale e all'immigrazione illegale, Studi sull'integrazione europea 3 (2008) 1, 181 (196); *Papayannis*, Die Polizeiliche Zusammenarbeit und der Vertrag von Prüm, ZEuS 11 (2008) 239 ff (242 f); aA *Niemeier/Zerbst*, Der Vertrag von Prüm - vertiefte grenzüberschreitende Zusammenarbeit zur Kriminalitätsbekämpfung in der EU, ERA-Forum 8 (2007) 4, 535 (542 f).

17 Im Prümer Vertrag selbst ist vom „automatisierten Abruf" (Art 3, 9, 12 iVm Art 33 Abs 1 Z 2 bzw vom „automatisierten Abgleich" (Art 4) von Daten die Rede.

18 DNA steht für „desoxyribonucleic acid" (dt: Desoxyribonucleinsäure [DNS]). Die Zitierung in diesem Beitrag folgt der Praxis des österreichischen Gesetzgebers, der die engl Abkürzung verwendet (vgl idS bspw Art 1 § 4 Z 23 GentechnikG öBGBl 1994/510 idF öBGBl I 2005/127; § 67 SPG; § 117 Z 5 StPO).

banken bzw automatisierte Fingerabdruck-Identifizierungssysteme [kurz: AFIS][19]) sowie Kfz-Zulassungsevidenzen (auch: „Fahrzeugregister"). Hinzu kommen eine Reihe von konventionellen, jedoch aus Datenschutzperspektive nicht weniger relevanten Kooperationsformen wie der anlasslose Austausch von Informationen über „Gefährder" bzw potentielle Terroristen.

Der Prümer Vertrag inspirierte in der Folge auch die **US-Regierung** in Washington bei ihrem Kampf gegen den „internationalen Terrorismus" und die „schwere grenzüberschreitende Kriminalität". In enger inhaltlicher Anlehnung an den Prümer Vertrag haben die USA inzwischen zahlreiche bilateralen Polizeikooperationsabkommen geschlossen. Diese werden kurz als **„PCSC[20] agreement"** oder **„Prüm-like agreement"** bezeichnet. Für die EU-Mitglieder unter den europäischen „Prüm-like"-Vertragspartnern der USA ergab sich eine spezifische Problematik aus dem Umstand, dass Letztere eine vollumfängliche Übernahme der datenschutzrechtlichen Gewährleistungen des Prümer Vertrags ausdrücklich ablehnten.

Bevor exemplarisch näher auf das bilaterale US-österreichische Prüm-like-Abkommen und die damit verbundenen Probleme eingegangen wird (dazu ab Abschn IV.B nach FN 137), erscheint es angezeigt, einen Überblick über die zentralen datenschutzrelevanten Inhalte des als Vorbild dienenden Prümer Vertrages zu geben.

II. Exkurs: Zentrale Inhalte des Prümer Vertrages mit Datenschutzrelevanz

A. „Vernetzung" der DNA-Analysedateien

Als ein erstes wesentliches Feld der Kooperation im Rahmen des Prümer Vertrages ist jenes des **automatisierten Abgleichs** von sog **DNA-Profilen** (auch: „DNA-Identifizierungsmustern"[21]) zu nennen. Solche Profile werden aus biologischen Spuren, die von Tatorten stammen („offene Spuren")[22], oder aus Körperzellen Tatverdächtiger gewonnen („DNA-Personenprofile")[23].[24] Ein DNA-Profil kann als Buchstaben- bzw Zahlencode umschrieben werden, der eine Reihe von Identifikationsmerkmalen des sog „nichtcodierenden" Teils einer aus Körperzellen gewonnenen und analysierten menschlichen DNA-Probe abbildet.[25] Mit „nichtcodierend" sind wiederum jene Chromosomenbereiche gemeint, die keine „genetische" Information iS von Hinweisen auf funktionale Eigenschaften eines Organismus enthalten („Erbinformationen" ieS).[26] Die besagten Buchstaben- bzw Zahlencodes zweier DNA-Profile, etwa einer offene Spur und eines Personenprofils, können automatisiert miteinander verglichen werden. Je nach Ausmaß der Übereinstimmung liegt eine höhere oder geringere Wahrscheinlichkeit der Personenidentität vor. Auf diese Weise können Verdächtige mit Tatorten oder mit Opfern in Verbindung gebracht oder – umgekehrt – als Verdächtige ausgeschlossen werden.

Um nun einen grenzüberschreitenden automatisierten Abgleich von DNA-Profilen zu ermöglichen, muss sichergestellt werden, dass die beteiligten Staaten 1. überhaupt eine systematische Auswertung etwa von Tatortspuren sowie deren Speicherung in sog DNA-Analysedateien vornehmen und dass 2. zumindest einer zentralen Stelle in jedem Vertragsstaat der automatisierte Abruf von (bzw der „Online-Zugriff" auf) DNA-Profilen in anderen Vertragsstaaten eröffnet wird. Eben dazu verpflichten sich die Parteien des Prümer Vertrages ausdrücklich.[27] Vor allem aus Verhältnismäßigkeitsgründen ist allerdings vorgesehen, dass die solcherart bewirkte wechselseitige „Vernetzung" **nicht automatisch** zur Zugänglichkeit **direkt personenbezogener Daten** in Form von Namens- bzw Falldaten führt. Vielmehr werden einem im Online-Wege anfragenden Beamten einer Vertragspartei im Übereinstimmungsfall („Treffer-Fall") zunächst nur sog **„Fundstellendatensätze"** übermittelt.[28] Dabei handelt es sich um eine Kombination aus jeweils einem DNA-Profil und einer diesem zugeordneten „Kennung".[29] Bei Letzterer handelt es sich um eine Referenznummer, die – je nach Fall – auf einen Datensatz mit Identitätsdaten des/der Betroffenen oder auf einen bestimmten (ungeklärten) Fall („offene Spur") verweist.[30] Die Kennung selbst wiederum darf keine, eine Person direkt identifizierende Informationen (Name, Geschlecht, Geburtsdatum, Tatverdacht etc) enthalten.[31]

Insgesamt kann man daher auf der ersten Stufe von einem **Hit-/No Hit-Verfahren** (Treffer-/Nichttrefferverfahren) sprechen.[32] Erst unter Vorlage eines solcherart ermittelten Fundstellendatensatzes kann ein Beamter weitere darauf

19 Engl: „Automated Fingerprint Identification Systems".

20 Abkürzung für „Preventing and Combating Serious Crime".

21 Dieser Begriff wird in Deutschland überwiegend verwendet (vgl idS die Fußnote zu Art 2 Abs 2 Satz 2 Prümer Vertrag bzw § 81g Abs 1 dStPO).

22 Vgl idS die Legaldefinitionen in Abschn 2.8 der Durchführungsvereinbarung zum Prümer Vertrag (zitiert nach „Draft ATIA REV 11 FINAL [DE] v 26.11.2006" = Blg zum Vortrag an den Ministerrat v 30.11.2006, GZ BMaA-AT.4.36.31/0056-IV.7/2006 [s Pkt 62 des Beschlussprotokolls Nr 148 zur Sitzung des Ministerrates am 5.12.2006]; im Folgenden nur: „Durchführungsvereinbarung").

23 Vgl idS ebenda, Abschn 2.9, bzw in Art 2 lit f Beschluss 2008/616/JI des Rates v 23.6.2008 ABl L 210, 12 (13), zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität.

24 Vgl dazu einführend *Interpol*, Interpol Handbook on DNA Data Exchange and Practice[2] (2009) 23 f.

25 Vgl Pkt 2.4 der Durchführungsvereinbarung (FN 22) bzw Art 2 lit c Beschluss 2008/616/JI (FN 23). S weiters einführend zum Verfahren zu Gewinnung eines DNA-Profils *Interpol*, Handbook (FN 24) 29 ff (34).

26 Vgl Pkt 2.5 der Durchführungsvereinbarung (FN 22) bzw Art 2 lit d Beschluss 2008/616/JI (FN 23).

27 Vgl Art 2 („Einrichtung von nationalen DNA-Analyse-Dateien") Prümer Vertrag.

28 Vgl idS Art 3 Abs 2 Prümer Vertrag iVm Annex A.3 Pkt 1.1.1-1.1.2 der Durchführungsvereinbarung (FN 22) bzw Art 8 Abs 2 Beschluss 2008/616/JI (FN 23); s weiters Erl „Zu Artikel 3 (Automatisierter Abruf von DNA-Profilen)" RV 1155 BlgNR 22. GP, 9.

29 Vgl idS Art 2 Abs 2 Satz 2 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]) bzw die Legaldefinitionen in Abschn 2.6 der Durchführungsvereinbarung (FN 22) bzw in Art 2 lit e Beschluss 2008/616/JI (FN 23).

30 Implizit aus Art 2 Abs 2 Satz 2 u 3 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).

31 Vgl Art 2 Abs 2 Satz 3 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).

32 Vgl idS Erl „Zu Artikel 2 (Einrichtung von nationalen DNA-Analyse-Dateien)" RV 1155 BlgNR 22. GP, 7.

Bezug habende direkt personenbezogene Daten im Wege der örtlich in Betracht kommenden nationalen Kontaktstellen erhalten.[33]

Auf den automatisierten Vergleich im vorstehend skizzierten Sinne darf nur zur **Verfolgung von Straftaten** und „nach Maßgabe des Rechts der abrufenden Vertragspartei" zurückgegriffen werden.[34] Letzteres gilt aber nur insofern, als eine Vertragspartei nicht von der Möglichkeit Gebrauch gemacht hat, mittels einseitiger Erklärung eine spezifische materielle Schwelle einzuziehen.[35] Letztere Option haben Österreich[36], Slowenien[37] oder die Niederlande[38] in Anspruch genommen.

Über das soeben skizzierte Verfahren hinaus ist auch ein grenzüberschreitender automatisierter **Massenabgleich** von offenen DNA-Spuren vorgesehen. Ein solcher muss allerdings zuvor zwischen den Vertragsparteien für den Einzelfall vereinbart werden.[39]

B. Gewinnung molekulargenetischen Materials und Übermittlung von DNA-Profilen

Es kann vorkommen, dass Behörden im Zuge eines laufenden Ermittlungs- oder Strafverfahrens auf eine in einem anderen Vertragsstaat aufhältige verdächtige Person stoßen, deren DNA-Profil zwecks Abgleichs mit offenen Tatortspuren benötigt würde. Für einen solchen Fall sieht der Prümer Vertrag nach dem Vorbild des bilateralen österreichisch-deutschen Polizei- und Justizkooperationsvertrages aus 2003[40] die Rechtshilfeleistung durch Gewinnung von molekulargenetischem Material nebst Übermittlung von daraus erstellten DNA-Profilen vor.

Voraussetzung für die Gewährung von Rechtshilfe im vorstehenden Sinne ist allerdings, das Vorliegen folgender kumulativ verknüpfter Bedingungen: Die ersuchende Vertragspartei muss 1. mitteilen, zu welchem Zweck das DNA-Profil benötigt wird (zulässiger Zweck ist nur die Verfolgung einer Straftat), 2. eine nach ihrem innerstaatlichen Recht erforderliche Untersuchungsanordnung oder

33 Vgl Art 5 iVm Art 3 Abs 2 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]); s weiters Erl „Zu Artikel 3 (Automatisierter Abruf von DNA-Profilen)" RV 1155 BlgNR 22. GP, 9.

34 Vgl Art 3 Abs 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).

35 Vgl Art 2 Abs 3 Prümer Vertrag iVm den einschlägigen Erklärungen der Vertragsparteien hiezu.

36 Österreich hat die Zulässigkeit des Zugriffes durch andere Vertragsparteien auf die Zwecke der Verfolgung solcher Straftaten eingeschränkt, die die Voraussetzung für die Erlassung eines sog Europäischen Haftbefehls erfüllen (vgl die österr Erklärung zu Art 2 Abs 3 anlässlich der Hinterlegung der Ratifikationsurkunde, abgedruckt in der Anl zu öBGBl III 2006/159).

37 Vgl die slowenische Erklärung zu Art 2, abgedruckt in öBGBl 2007/81 Seite 2.

38 Vgl die niederländische Erklärung zu Art 2 Abs 3, abgedruckt in öBGBl 2008/63 Seite 4 f.

39 Vgl Art 4 Abs 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]); s weiters Erl „Zu Artikel 3 (Automatisierter Abruf von DNA-Profilen)" RV 1155 BlgNR 22. GP, 9.

40 Vgl Art 7 Abs 3 („Ersuchen um körperliche Untersuchung") Vertrag zwischen der Republik Österreich und der Bundesrepublik Deutschland über die grenzüberschreitende Zusammenarbeit zur polizeilichen Gefahrenabwehr und in strafrechtlichen Angelegenheiten v 10.11.2003 (Text: Anl zu öBGBl III 2005/210; in Kraft seit 1.12.2005; vgl öBGBl III 2005/210 Seite 1).

-erklärung vorlegen, aus welcher hervorgeht, dass an der bestimmten Person eine DNA-Analyse vorgenommen werden könnte, wenn sich diese auf ihrem eigenen Hoheitsgebiet befände, und es müssen 3. auch nach dem Recht der ersuchten Vertragspartei die gesetzlichen Voraussetzungen für die Gewinnung und Untersuchung des molekulargenetischen Materials und der Übermittlung des dabei gewonnenen DNA-Profils vorliegen.[41]

C. „Vernetzung" daktyloskopischer Identifizierungssysteme

Dem **Hit-/No Hit-Verfahren** beim automatisierten Abruf von DNA-Profilen vergleichbar ist jenes, das beim ebenfalls automatisierten grenzüberschreitenden Abgleich von daktyloskopischen Daten zur Anwendung gelangt. Zu letzterer Datenkategorie zählen Fingerabdrücke,[42] aber auch Hand-[43] und (potentiell) Fußflächenabdrücke[44].

Der **wesentliche Unterschied** im Vergleich zu DNA-Profilen liegt bei daktyloskopischen Daten darin, dass sie sich nicht als einfache Kombination von alphanumerischen Daten und Buchstaben darstellen lassen. Vielmehr werden hier die bei jedem Menschen einzigartigen Linienmuster (Papillarlinien bzw deren Endungen, Kontenpunkte oder Verzweigungen [sog „Minutien"]) der Fingerkuppen bzw seine Handabdrücke (Handinnenflächen) gescannt. Anschließend wird mittels einer speziellen Software aus den so gewonnenen digitalen Bildern eine Art digitale Schablone (engl: „template") erstellt. Und diese wird dann für automatisierte Vergleiche herangezogen.[45]

„Eindeutige" Treffer können dabei am ehesten beim Vergleich von identifizierten daktyloskopischen Daten miteinander (va „Zehnfingerabdruck" [engl: „ten-pint"] gegen „Zehnfingerabdruck"; [engl: „criminal print-to-print search"]) erzielt werden. Offene Spuren zeichnen sich dagegen idR dadurch aus, dass nur Fragmente von Finger- oder Handabdrücken vorhanden sind. Deren automatisierter Abgleich gegen identifizierte daktyloskopischen Daten (engl: „latent-to-print search") führt deshalb idR zu einer **Mehrzahl** von lediglich **„potentiellen" Treffern.** Letztere können in Form einer Liste angezeigt werden. Je nach Einstellung des Systems (Stichwort: „Fehlertoleranz") kann die Zahl der möglichen Treffer höher oder niedriger liegen. „Mögliche" Treffer müssen von Fingerabdruckexperten auf Seite der anfragenden[46] Partei **„manuell"** auf ihre tatsächli-

41 Vgl Art 7 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]) iVm Erl „Zu Artikel 7 (Gewinnung molekulargenetischen Materials und Übermittlung von DNA-Profilen)" RV 1155 BlgNR 22. GP, 10 f.

42 Vgl idS die Legaldefinitionen in Abschn 2.10 der Durchführungsvereinbarung (FN 22).

43 Zusätzlich zu Fingerabdrücken werden in den Systemen Handflächenabdrücke verarbeitet; vgl idS die Legaldefinitionen in Abschn 2.10 der Durchführungsvereinbarung (FN 22).

44 Vgl Erl „Zu Artikel 8 (Daktyloskopische Daten)" RV 1155 BlgNR 22. GP, 11.

45 Näheres mwN bei *O'Gorman,* Fingerprint Verification, in *Jain et al* (eds), Biometrics. Personal Identification in Networked Society (1999) 43 ff; *Behrens/Heumann*, Fingerbilderkennung, in *Behrens/Roth* (Hrsg), Biometrische Identifikation (2001) 81 ff (91 ff).

46 Vgl Art 9 Abs 2 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]); weiters Erl „Zu Artikel 9 (Automatisierter Abruf von daktyloskopischen Daten)" RV 1155 BlgNR 22. GP, 11 f.

che Übereinstimmung bzw Nichtübereinstimmung mit der Spur überprüft werden (**„Verifikation"**).[47] Dies geschieht dadurch, dass die im daktyloskopischen Identifizierungssystem ebenfalls gespeicherten, bei der Erstellung der „Templates" angefallenen, digitalen Fingerabdruckbilder miteinander durch den abrufenden Experten verglichen werden. Diese Bilder werden im Trefferfall gemeinsam mit der jeweiligen „Treffermeldung" und einer Kennung an die abrufende Stelle übermittelt.[48]

Auch im Falle eines „eindeutigen" Treffers beim Abgleich eines vollständigen Satzes von Fingerabdrücken gegen einen Satz identifizierter Fingerabdrücke bedarf es im Übrigen zur Qualitätssicherung der „manuellen" Nachprüfung des automatisiert erzielten Treffers. Insgesamt stellt sich der „automatisierte" Abgleich von daktyloskopischen Daten insofern im Grunde nur als **„halbautomatischer" Vorgang** dar.

Ein weiterer Unterschied zur Kooperation auf dem Felde der DNA-Analysedateien besteht darin, dass die nationalen automatisierten daktyloskopischen Identifizierungssysteme nicht nur für Strafverfolgungszwecke sondern **auch** im Interesse der **Verhinderung** von **Straftaten** geöffnet werden.[49] Da **dezidiert** auf die Fundstellendatensätze der **„zum Zweck** der Verhinderung und Verfolgung von Straftaten" **eingerichteten** Identifizierungssysteme abgestellt wird,[50] **scheiden anderen Zwecken dienende** Systeme wie etwa „fremdenpolizeiliche" oder „asylrechtliche" **aus.**[51] Diese Differenzierung gebietet sich im Übrigen schon aus Verhältnismäßigkeitsgründen.

D. Automatisierter Abruf von Fahrzeugregisterdaten

Im Unterschied zu den bisher behandelten beiden automatisierten Verfahren (Abgleich von DNA-Profilen und daktyloskopischen Daten) handelt es sich bei dieser Zusammenarbeitsform nicht um ein bloßes Hit-/No Hit-Verfahren. Vielmehr räumen sich die Vertragsparteien wechselseitig sog **„Lesezugriffe"** auf ihre Kfz-Zulassungsregister (Fahrzeugregister) ein.[52] Dies bedeutet, dass Eigentümer- beziehungsweise Halterdaten in Bezug auf ein Kfz sowie die (technischen und weiteren) Fahrzeugdaten direkt eingesehen werden können. Hier kommt also ein einstufiges Verfahren zum Tragen. Um missbräuchliche Abfragen zu unterbinden, beschränkt der Prümer Vertrag die Nutzung freilich auf **Einzelfälle**[53] und verlangt die Eingabe eines **vollständigen** Kfz-Kennzeichens **oder** einer **vollständigen** Fahrzeugidentifizierungsnummer („Fahrgestellnummer")[54].

Zulässige **Zwecke** für die Inanspruchnahme der besagten Lesezugriffe sind 1. die **Verhinderung** und **Verfolgung** von **Straftaten**, 2. die Verfolgung solcher Verstöße, die bei der abrufenden Vertragspartei in die Zuständigkeit der Gerichte

47 Vgl Erl „Zu Artikel 9 (Automatisierter Abruf von daktyloskopischen Daten)" RV 1155 BlgNR 22. GP, 11 f.
48 Vgl Annex B.1 Abschn 1 iVm Abschn 3.1.4 der Durchführungsvereinbarung (FN 22).
49 Vgl Art 9 Abs 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).
50 Vgl ebenda, Art 9 Abs 1 Satz 1.
51 Vgl insofern zutreffend die Erl „Zu Artikel 8 (Daktyloskopische Daten)" RV 1155 BlgNR 22. GP, 11.
52 Vgl idS Erl „Zu Artikel 12 (Automatisierter Abruf von Daten aus den Fahrzeugregistern)" RV 1155 BlgNR 22. GP, 13.
53 Vgl Art 12 Abs 1 UAbs 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).
54 Vgl ebenda, Art 12 Abs 1 UAbs 2.

oder Staatsanwaltschaften fallen oder 3. die **Abwehr** von **Gefahren** für die öffentliche Sicherheit.[55] Der zweite Fall ist ein – bedingt gelungener – Formulierungskompromiss, der Bagatelldelikte (bspw Tempoüberschreitung ohne gleichzeitige Gefährdung anderer Verkehrsteilnehmer; Parkvergehen) aus dem Anwendungsbereich ausschließen soll.[56] Ebendiese, auf österreichischen Wunsch zurückgehende, Zweckbeschränkung war vor dem Hintergrund der seinerzeit gegenüber der Öffentlichkeit kommunizierten „Antiterrorzielrichtung" des Prümer Vertrages zu sehen. Infolge einer im Oktober 2011 erlassenen EU-Richtlinie[57] wurde mittlerweile die Zusammenarbeit auch auf geringfügige Verkehrsdelikte ausgeweitet.[58]

E. Übermittlung von Daten über „Gefährder" im Vorfeld „internationaler" Großveranstaltungen

Als ein weiterer Bereich der Zusammenarbeit wurde im Prümer Vertrag der Austausch personenbezogener Daten im Rahmen von Großveranstaltungen (Sportveranstaltungen, politische „Gipfeltreffen" uä) mit grenzüberschreitendem Bezug vereinbart. Zum **Zweck** der **Verhinderung** von **Straftaten** und der **Abwehr** einer **Gefahr** für die **öffentliche Sicherheit** und **Ordnung** übermitteln die Vertragsparteien einander sowohl auf Ersuchen als auch aus eigener Initiative Daten von sog „Gefährdern".[59] Voraussetzung für die Übermittlung ist, dass entweder rechtskräftige Verurteilungen oder andere Tatsachen die Annahme rechtfertigen, dass die betroffenen Personen bei der Veranstaltung Straftaten begehen werden oder von ihnen eine Gefahr für die öffentliche Ordnung und Sicherheit ausgeht.[60]

Die sich hier va stellende Problematik der **Prognosequalität** wird insofern gemildert, als ausdrücklich angeordnet ist, dass die besagten Daten nur für das genau umschriebene Ereignis, für das sie mitgeteilt wurden, verarbeitet werden dürfen[61] und unverzüglich zu löschen sind, sobald die verfolgten Zwecke erreicht worden sind oder nicht mehr erreicht werden können, spätestens aber nach einem Jahr[62].

F. Übermittlung von Informationen zur Verhinderung terroristischer Straftaten

Schließlich sieht der Prümer Vertrag die anlasslose Übermittlung personenbezogener Daten und Informationen zur **Verhinderung terroristischer Straftaten** vor. Sie soll im Einzelfall und unter der Voraussetzung erfolgen, dass die Übermittlung erforderlich ist, weil **bestimmte Tatsachen die Annahme rechtferti-**

55 Vgl wieder Art 12 Abs 1 UAbs 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).
56 Vgl idS Erl „Zu Artikel 12 (Automatisierter Abruf von Daten aus den Fahrzeugregistern)" RV 1155 BlgNR 22. GP, 13.
57 RL 2011/82/EU des Europäischen Parlaments und des Rates v 25.10.2011 ABl L 288, 1, zur Erleichterung des grenzüberschreitenden Austauschs von Informationen über die Straßenverkehrssicherheit gefährdende Verkehrsdelikte.
58 Vgl Art 2 RL 2011/82/EU (FN 57).
59 Vgl Art 14 Abs 1 Satz 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).
60 Vgl ebenda.
61 Vgl ebenda, Art 14 Abs 2 Satz 1.
62 Vgl ebenda, Art 14 Abs 2 Satz 2.

gen, dass der/die Betroffene „terroristische Straftaten" begehen werde.[63] Als Letztere werden die im Rahmenbeschluss „Terrorismus"[64] vom Juni 2002 genannten Straftaten definiert. Die zu übermittelnden Datenkategorien sind abschließend festgelegt und umfassen Namen, Vornamen, Geburtsdatum und Geburtsort sowie die Darstellung der Tatsachen, aus denen sich die Annahme ergibt, dass diese Person terroristische Straftaten begehen werde.[65] Mit Blick auf die potentielle Sensibilität der bezüglichen Informationen, ist es der übermittelnden Behörde explizit eröffnet, „nach Maßgabe des innerstaatlichen Rechts **Bedingungen für die Verwendung** dieser Daten und Informationen durch die empfangende Behörde fest(zu)legen", an welche die empfangende Behörde gebunden ist.[66]

G. Datenschutzregelungen

Ein Mehr an Möglichkeiten für die polizeiliche informationelle Zusammenarbeit korrespondiert typischerweise mit erhöhten Risiken für die Datenschutzgrundrechte Betroffener. Charakteristisch für den Regelungsansatz des Prümer Vertrages ist, dass diesem Umstand durch ausführliche Datenschutzbestimmungen Rechnung getragen wird. Damit sind nicht nur die in einem eigenen Datenschutzkapitel[67] zusammengefassten Regelungen, sondern auch an anderen Stellen normierte Zweckbeschränkungen[68] für Datenverwendungen angesprochen.

Zur Struktur des besagten Datenschutzkapitels sei angemerkt, dieses neben einer Liste mit Legaldefinitionen[69] allgemeine Vorgaben für das „Datenschutzniveau"[70] sowie Regelungen über die Zweckbindung[71], Behördenzuständigkeiten[72], Datenqualität[73], Datensicherheit[74], Dokumentation bzw Protokollierung[75], Individualrechtsschutz[76] sowie wechselseitige Auskunftspflichten bzw -rechte der Vertragsparteien[77] im Verhältnis untereinander beinhaltet.

Das allgemeine Schutzniveau wurde durch die Anknüpfung an die sog Datenschutzkonvention des Europarates aus 1981[78], das Zusatzprotokoll hiezu aus

63 Vgl Art 16 Abs 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).
64 Vgl Art 1-3 Rahmenbeschluss 2002/475/JI des Rates der Europäischen Union v 13.6. 2002 ABl L 164, 3, zur Terrorismusbekämpfung.
65 Vgl Art 16 Abs 2 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).
66 Vgl ebenda, Art 16 Abs 4.
67 Kapitel 7 („Allgemeine Bestimmungen zum Datenschutz").
68 Vgl bspw wieder Art 1 Abs 1 Satz 1, Art 1 Abs 2 Satz 1, Art 9 Abs 1 Satz 1 Prümer Vertrag (bzw Beschluss 2008/615/JI [FN 11]).
69 Vgl Art 33 Abs 1 Prümer Vertrag bzw Art 24 Abs 1 Beschluss 2008/615/JI (FN 11).
70 Vgl Art 34 Abs 1 Prümer Vertrag bzw Art 25 Abs 1 Beschluss 2008/615/JI.
71 Vgl Art 35 Prümer Vertrag bzw Art 26 Beschluss 2008/615/JI.
72 Vgl Art 36 Prümer Vertrag bzw Art 27 Beschluss 2008/615/JI.
73 Vgl Art 37 Prümer Vertrag bzw Art 28 Beschluss 2008/615/JI.
74 Vgl Art 38 Prümer Vertrag bzw Art 29 Beschluss 2008/615/JI.
75 Vgl Art 39 Prümer Vertrag bzw Art 30 Beschluss 2008/615/JI.
76 Vgl Art 40 Prümer Vertrag bzw Art 31 Beschluss 2008/615/JI.
77 Vgl Art 41 Prümer Vertrag bzw Art 32 Beschluss 2008/615/JI.
78 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten v 28.1.1981 (kurz: „Datenschutzkonvention"); Text: öBGBl 1988/317; allg in Kraft seit 1.10.1985; f Österreich seit 1.7.1988 (vgl öBGBl 1988/317, 2441).

2001[79] sowie eine die Nutzung personenbezogener Daten im Polizeibereich betreffende Empfehlung des Ministerkomitees des Europarates aus 1987[80] festgelegt.[81] Österreichischerseits wurde besonderer Wert auf eine Pflicht zur umfassenden Dokumentation der Datenverwendungen gelegt, insbesondere auf dem Feld der Kooperation mittels automatisierter Abrufmöglichkeiten.[82] Nur so erscheint gewährleistet, dass auch nachträglich die Verantwortlichkeit für Abrufe bis herunter zum einzelnen Beamten festgestellt und rechtlich evaluiert werden kann. Ebenfalls maßgeblich auf die österreichische Verhandlungsdelegation geht die Aufnahme konkreter Vorgaben für den Individualrechtsschutz zurück.[83] Dieser entspricht im Wesentlichen dem institutionellen Rechtsschutzkonzept der EG-Datenschutzrichtlinie aus 1995[84]. Konkret bedeutet dies die Verpflichtung der Vertragsparteien, sowohl einen gerichtlichen Rechtsschutz gegen Datenschutzverletzungen im Allgemeinen vorzusehen, als auch einen zusätzlichen Zugang der Betroffenen zu einer spezialisierten unabhängigen Datenschutzkontrollbehörde zu gewährleisten.

III. Verstärkung des US-amerikanischen „Hungers" auf Daten von USA-Reisenden

Dass die US-Sicherheitsbehörden sich durch eine hohe Affinität zu technologischen Hilfsmitteln und die Tendenz zu deren ungezügelten Einsatz auszeichnen, kann als allgemein bekannt gelten. Insofern konnte es im Lichte der zahlreichen in Reaktion auf die Anschläge vom 11. September 2011 ergriffenen US-Maßnahmen auf dem Feld der Informationssammlung nicht übermäßig überraschen, dass die „europäische" Polizeikooperation auf Grundlage des Prümer Vertrages alsbald auch das Interesse der US-Administration wecken würde. Deren gesteigerte Aufmerksamkeit galt va dem automatisierten Abruf von **Fingerabdruckdaten** und dem anlasslosen Austausch von Informationen über **„Terrorverdächtige"**.

Da sich das außenpolitische Denken führender US-Politiker erfahrungsgemäß durch einen gewissen Hang zum Unilateralismus auszeichnet, war es aus Sicht der USA nur folgerichtig, sich ihrer nationalen Gesetzgebung zu bedienen, um **„Anreize"** zu setzten, die die europäischen und andere Staaten de facto **zu** einer **verstärkten informatorischen Zusammenarbeit „zwingen"** würden.

79 Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr v 23.5.2001 (Text: öBGBl III 2008/91; für Österreich in Kraft seit 1.8.2008; vgl öBGBl III 2008/91, Seite 1).
80 Empfehlung Nr R (87) 15 des Ministerkomitees an die Mitgliedstaaten über die Nutzung personenbezogener Daten im Polizeibereich v 17.9.1987 (Text: [engl]: http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf).
81 Vgl Art 34 Abs 1 Prümer Vertrag bzw Art 25 Abs 1 Beschluss 2008/615/JI (FN 11).
82 Vgl Art 39 ff Prümer Vertrag bzw Art 30 Beschluss 2008/615/JI (FN 11).
83 Vgl Art 40 Prümer Vertrag bzw Art 31 Beschluss 2008/615/JI (FN 11).
84 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v 24.10.1995 ABl L 281, 31, zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Die formale innerstaatliche Grundlage für das nachfolgend skizzierte Vorgehen der USA bildete der sog „9/11 Commission Act" (auch: „9/11 Act")[85] aus dem Jahre 2007. Mit diesem Gesetz wurden zahlreiche Empfehlungen der sog „9/11 Commission"[86] legistisch umgesetzt. Letztere war 2002 auf Initiative des US-Kongresses zur Aufklärung der Terroranschläge des 11. September 2001 auf das World Trade Center in New York eingesetzt worden und hatte ihren Abschlussbericht („9/11 Commission Report")[87] im Juli 2004 vorgelegt.

Der zitierte 9/11 Commission Act modifizierte nun den sog „Immigration and Nationality Act"[88] (kurz: INA) dahingehend, dass zusätzliche Anforderungen für die Teilnahme am seit 1986[89] bestehenden Programm für die visafreie Einreise in die USA (sog **„Visa waiver"-Programm** [im Folgenden kurz: VWP][90]) statuiert wurden.[91] Generell wurde die US-Regierung dazu verpflichtet, das Visa waiver-Programm zu modernisieren und zu stärken, uzw durch die gleichzeitige **Erhöhung der Sicherheitsanforderungen** für die Teilnahme an diesem Programm sowie dessen Ausweitung auf Angehörige solcher Staaten, die mit den USA **aktiv** bei der Hinderung von Terroristen an der Entfaltung von Reisetätigkeiten **kooperieren**, insbesondere durch den **Austausch** von **Informationen** aus den Feldern **„Strafverfolgung"** und **„Terrorbekämpfung"**.[92]

85 Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law [PL] No 110-53; 121 Stat 266).

86 Offizielle Bezeichnung: „National Commission on Terrorist Attacks upon the United States" (s dazu http://www.9-11commission.gov/about/bios.htm).

87 The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks upon the United States (Quelle: http://govinfo.library.unt.edu/911/report/index.htm); dazu kritisch: *Ridgeway*, The 5 Unanswered Questions about 9/11: What the 9/11 Commission Report Failed to Tell Us (2005).

88 Immigration and Nationality Act of 1952 (INA) (ch 477, 66 Stat 163) (= 8 USC §§ 1101 et seq).

89 1986 wurde das „visa waiver program" als Pilot-Programm etabliert (vgl The Immigration Reform and Control Act of 1986 [PL 99-603]); im Jahr 2000 wurde es zur Dauereinrichtung (vgl Visa Waiver Permanent Program Act [PL 106-396, Oct 30, 2000]).

90 Dieses ist in sec 217 des Immigration and Nationality Act of 1952 (FN 88) (= 8 USC §§ 1187 et seq) geregelt. Derzeit nehmen 36 Staaten am Programm teil (s dazu die Liste bei http://travel.state.gov/visa/temp/without/without_1990.html#countries). Zu Ursprüngen und historischer Entwicklung des Programms s *United States Government Accountability Office* (GOA), Border Security. Implications of Eliminating the Visa Waiver Program, Report to the Chairman, Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives (Washington, DC November 2002) 1 ff; *dass*, Border Security. Stronger Actions Needed to Assess and Mitigate Risks of the Visa Waiver Program, Report to the Chairman, Committee on the Judiciary, House of Representatives (Washington, DC July 2006) 1 ff; *dass*, Visa Waiver Program. Additional Actions Needed to Mitigate Risks and Strengthen Overstay Enforcement. Statement of Rebecca Gambler, Acting Director Homeland Security and Justice and Michael J. Courts, Acting Director International Affairs and Trade, Testimony Before the Subcommittee on Immigration, Refugees, and Border Security, Committee on the Judiciary, U.S. Senate (Washington, DC March 27, 2012) 1 ff.

91 Vgl sec 711 („modernization of the visa waiver program") of 9/11 Act (FN 85) .

92 Vgl sec 711(b)(1)-(2) of 9/11 Act (FN 85).

Neben einer bedingungslosen Rücknahmepflicht für Staatsangehörige, ehemalige Staatsangehörige oder sonstige Bürger im Falle einer Ausweisung durch die US-Behörden[93] wurden konkret insbesondere der **Abschluss bilateraler Abkommen** zwischen den USA und den am besagten VWP teilnehmenden Staaten betreffend die Information der US-Behörden über verlorene und gestohlene Reisepässe[94] („reporting lost and stolen passports") sowie über Bürger bzw Staatsangehörige, die im Fall ihrer Einreise ein **Risiko** für „Sicherheit und Wohlfahrt" der USA darstellen könnten, vorgesehen („passenger information exchange")[95]. Davon abgesehen wurde den zuständigen US-Behörden auferlegt, im Rahmen des ihnen eingeräumten Ermessens bei der **Beurteilung** der **„VWP-Kompatibilität"**[96] einzelner Staaten neben bereits bestehenden Kriterien wie bspw der Erfüllung von technischen Anforderungen an die Dokumentensicherheit (Stichwort: „maschinenlesbare Pässe")[97] besonderes Augenmerk auf die Zusammenarbeit solcher Staaten mit den USA in Bezug auf **Initiativen zur Terrorbekämpfung** sowie va beim **nachrichtendienstlichen Informationsaustausch** betreffend **terroristische Bedrohungen**[98] zu legen.

Eine zentrale Rolle bei der Beurteilung der Erfüllung der genannten Anforderungen durch „VWP-Kandidaten" bzw „-Staaten" wurde durch den 9/11 Act dem „Direktor Nationale Nachrichtendienste" („Director of National Intelligence")[99] [100] zugedacht. Dessen Prüffokus liegt wiederum auf dem „Anti-Terror-Engagement" sowie insbesondere dem Ausmaß der Lieferung von nützlichen Information zur Unterdrückung terroristischer Reiseaktivitäten oder Aktionen bzw deren Finanzierung.[101]

Einzelnen Reisenden unter dem VWP wurde zudem auferlegt, sich noch vor Reiseantritt via Internetportal bei den US-Grenzschutzbehörden anzumelden (elektronisches Reisegenehmigungssystem [ESTA[102]]) und dabei umfangreiche Identitäts-, Adress- und biographische Daten offenzulegen.[103] Die Aufgabe der Entwicklung bzw Errichtung dieses Systems wurde dem US-Heimatschutzminister („Secretary of Homeland Security") in Abstimmung mit dem US-Außenminis-

93 Vgl sec 711(d)(1)(B)(i)(II) of 9/11 Act (FN 85) bzw sec 217(c)(2)(E) of INA (FN 88) (= 8 USC § 1187[c][2][E]).

94 Vgl sec 711(d)(1)(B)(i)(I) of 9/11 Act bzw sec 217(c)(2)(D) of INA (= 8 USC § 1187[c][2][D]).

95 Vgl sec 711(d)(1)(B)(i)(II) of 9/11 Act bzw sec 217(c)(2)(F) of INA (= 8 USC § 1187[c][2][F]).

96 Vgl dazu sec 217(c) („designation of program countries") of INA (= 8 USC § 1187[c]).

97 Vgl sec 217(c)(2)(B) of INA (= 8 USC § 1187[c][2][B]).

98 Vgl sec 711(c) of 9/11 Act (FN 85) bzw Sec 217(c)(9) of INA (FN 88) (= 8 USC § 1187[c][9]).

99 Dieser fungiert als „Direktor" der in der „Intelligence Community" zusammengefassten einzelnen US-amerikanischen Nachrichtendienste (Central Intelligence Agency [CIA], Defense Intelligence Agency [DIA] usw). S dazu http://www.dni.gov/.

100 Vgl sec 711(d)(1)(B)(iii) of 9/11 Act (FN 85) bzw Sec 217(c)(11)(A) of INA (FN 88) (= 8 USC § 1187[c][11][A]).

101 Vgl Sec 217(c)(11)(C) of INA (FN 88) (= 8 USC § 1187[c][11][C]).

102 ESTA steht für „Electronic System for Travel Authorization" (s https://esta.cbp.dhs.gov/esta/) und ist im INA (FN 88) verankert (s sec 217[h][3][B] (= 8 USC § 1187[h][3][B]).

103 Vgl sec 711(d)(1)(A)(i) of 9/11 Act (FN 85) bzw Sec 217(a)(11) of INA (FN 88) (= 8 USC § 1187[a][11]). S dazu auch *Springer*, USA-Reisende müssen zuerst ins Netz, Der Standard, 14.11.2008, 6.

ter („Secretary of State") zugewiesen.[104]

Weiters zu erwähnen ist im gegebenen Zusammenhang eine spezifische – wiederum den US-Heimatschutzminister in Abstimmung mit dem US-Außenminister treffende – **Berichtspflicht gegenüber dem US-Kongress**: Im 2-Jahres-Rhythmus (bis zum Jahr 2002: mindestens alle 5 Jahre)[105] hat Ersterer die fortgesetzten Anstrengungen der am VWP teilnehmenden Staaten im Hinblick auf die US-Strafverfolgungs- bzw Sicherheitsinteressen zu evaluieren und darüber schriftlich Bericht an einschlägige Ausschüsse von US-Repräsentantenhaus und US-Senat zu legen.[106] Diese grundsätzlich bereits vor dem 9/11 Act bestehenden Berichtspflichten schlugen naturgemäß auch auf die oben skizzierten verschärften Anforderungen für die Teilnahme am VWP durch. Die Entscheidung über die Aufnahme eines Staates in das VWP obliegt im Übrigen grundsätzlich dem US-Justizminister[107] in Abstimmung mit dem US-Außenminister,[108] die Suspendierung der Anwendung des VWP dagegen dem US-Heimatschutzminister in Abstimmung mit dem US-Außenminister[109].

Im Rahmen des bereits oben erwähnten, durch den 9/11 Act **verpflichtend zu institutionalisierenden** sog **„passenger information exchange"** legte das US-Heimatschutzministerium iVm anderen Behörden nun – je nach Zählweise – **drei** bzw **vier Typen** von **Abkommen** fest, durch deren (kumulativen) Abschluss VWP-Partnerstaaten ihre diesbezüglichen Pflichten erfüllen können/müssen: 1. „Homeland Security Presidential Directive 6 (HSPD-6)"-Abkommen, 2. „Preventing and Combating Serious Crime" (PCSC)-Abkommen, 3. Abkommen betreffend verlorene und gestohlene Pässe bzw 4. Abkommen über den Austausch von ([Flug-]Passagierdaten).[110]

Bei ersterer Kategorie geht es speziell um den Informationsaustausch über bekannte Terroristen oder Terrorverdächtige. Vereinfacht gesagt gewähren die Vertragsparteien hier einander Online-Zugriffe auf ihre jeweiligen nationalen „Watch-Listen".[111] Auf Seite der USA wurde auf Grundlage der zitierten Präsidentenrichtlinie eine spezielle Datenbank, die sog „Terrorist Screening Database" (TSDB) eingerichtet, welche vom sog „Terrorist Screening Center" (TSC), einer

104 Vgl sec 711(d)(1)(A)(i) of 9/11 Act (FN 85) bzw Sec 217(h)(3)(A) of INA (FN 88) (= 8 USC § 1187[h][3][A]).

105 Vgl sec 217(c)(5)(A)(i) of INA (FN 88) idF vor der Änderung durch sec 307(a)(2) of Enhanced Border Security and Visa Entry Reform Act of 2002 (PL 107-173).

106 Vgl sec 217(c)(5)(A)(i) of INA (FN 88) (= 8 USC § 1187[c][5][A][i]).

107 Eigentlich „Generalbundesanwalt der Vereinigten Staaten" („United States Attorney General").

108 Vgl sec 217(c)(1) bzw 217(c)(5)(A)(i) of INA (FN 88) (= 8 USC § 1187[c][1] bzw § 1187[c][5][i]).

109 Vgl sec 217(c)(5)(A)(i)(II) iVm 217(d) of INA (FN 88) (= 8 USC § 1187[c][5][A][i][II] iVm § 1187[d]).

110 Nach einer Lesart werden hier die Fälle 1 bis 3 aufgeführt (vgl idS *United States Government Accountability Office* (GOA), Visa Waiver Program, 2012 [FN 90] 6), nach anderen Quellen die Fälle 1, 2 und 4 unter „Information Sharing Agreements" subsumiert und der Fall 3 als davon abgesondertes Erfordernis genannt (vgl *Department of Homeland Security – Visa Waiver Program Office*, Summary of Findings on the compliance of Austria with the information-sharing requirements and other provisions of the 9/11 Act [December 30, 2008, 1 f]).

111 Vgl idS *United States Government Accountability Office* (GOA), Visa Waiver Program, 2012 (FN 90) 6.

Abteilung des „Federal Bureau of Investigation" (FBI) geführt wird.[112]

Die zweite Kategorie von Abkommen ist – wie bereits an früherer Stelle erwähnt (s oben nach FN 19) – vom Muster[113] des Prümer Vertrages inspiriert. Zur dritten Kategorie von Abkommen ist präzisierend anzumerken, dass die Zugänglichmachung der geforderten Daten auch ohne formelles Abkommen, etwa über die Beteiligung an der bezüglichen Interpol-Datenbank („Stolen and Lost Travel Documents")[114] gewährleistet werden kann.[115] Die Thematik der (Flug-)Passagierdaten-Übermittlung schließlich ist im Verhältnis zwischen EU und USA mittels eines einschlägigen Abkommens („EU-USA-PNR-Abkommen")[116] geregelt.

Die vorstehend erwähnte **Rechtslage** bildete quasi den **argumentatorischen Hebel**, insbesondere gegenüber den EU-Staaten, um diplomatischen Druck in Richtung der Aufnahme **bilateraler** Verhandlungen über den Abschluss ua der besagten „Prüm-like"-Abkommen aufzubauen. Nachdem es den USA alsbald gelungen war, mit etlichen EU-Staaten, darunter auch Deutschland[117], Einvernehmen über solche Abkommen herzustellen, stieg auch auf das „befreundete" Österreich der (politische) Druck, in entsprechende Gespräche einzutreten.[118]

112 S dazu http://www.fbi.gov/about-us/nsb/tsc/tsc.

113 Vgl idS etwa Erwägungsgrund 5 des US-österreichischen „Prüm-like"-Abkommens (Quelle: Blg 1 [engl] u 2 [dt] RV 1388 BlgNR 24. GP in dem ausdrücklich auf Prümer Vertrag und Prümer Beschluss Bezug genommen wird.

114 Vgl Databases. Interpol Fact Sheet COM/FS/2011-01/GI-04, 2 (s https://www.interpol.int/Public/ICPO/FactSheets/GI04.pdf).

115 Vgl sec 217(c)(2)(D) of INA (FN 88) (= 8 USC § 1187[c][2][D]).

116 Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union v 17.11.2011 über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security (Text: Ratsdok 17434/11 v 8.12.2011: Legislative Acts and other Documents. Subject: Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 2); s weiters *Europäische Kommission,* Pressemitteilung: „Neues PNR-Abkommen EU-USA stärkt Datenschutz sowie Verbrechens- und Terrorismusbekämpfung", Reference: IP/11/1368 Date: 17/11/2011.

117 Abkommen zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika vom 1.10.2008 über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität (Text: dBGBl 2009 II 1010, 1011); s dazu kritisch aus integrationspolitischer bzw -theoretischer Sicht *Bellanova,* Prüm: A Model 'Prêt-à-Exporter'? The 2008 German–US Agreement on Data Exchange, CEPS Research Paper No 13/March 2009.

118 Noch bevor Österreich in formelle Verhandlungen mit den USA eingetreten war, hatten neben Deutschland bspw Portugal, Tschechien, Ungarn, Litauen, Griechenland und die Slowakei bereits einschlägige Abkommen unterzeichnet. Spanien und das Vereinigte Königreich hatten keine „Prüm- like"-Abkommen ieS, aber solche zu ähnlichen Inhalten geschlossen.

IV. Das bilaterale österreichisch-amerikanische „Prüm-like"-Abkommen

A. Disparitäten in punkto Daten- und Menschenrechtsschutz

Die Vertreter der europäischen Sicherheitsbehörden begriffen das US-amerikanische „Angebot" primär als Chance für eine technisch verbesserte transatlantische Zusammenarbeit in der Verbrechens- bzw Terrorbekämpfung. Bei Verfassungsjuristen, Datenschutzexperten und einer kritischen Öffentlichkeit stießen die Vorschläge der USA dagegen primär auf Skepsis. Dies va deshalb, da sich der „Prüm-like"-Ansatz in eine Serie von US-Initiativen seit dem 11. September 2001 einreihte, die auf eine **breitflächige informationstechnische Überwachung** nicht nur der eigenen Bevölkerung, sondern etwa auch des gesamten Einreiseverkehrs in Richtung der USA (Stichworte: „Vorabübermittlung von Fluggastdatensätzen"[119], „ESTA"[120], usw), und - mehr noch - sogar des innereuropäischen elektronischen grenzüberschreitenden Zahlungsverkehrs (Stichwort: „SWIFT"[121] bzw „TFTP"[122]) abzielten. So interessiert sich die US-Administration

119 S dazu PL No 107–71 (= 49 USC § 44909c [3]) iVm 19 C.F.R. § 122.49(b) iVm Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union v 17.11.2011 (FN 116); kritisch dazu *Committee on Civil Liberties, Justice and Home Affairs*, Draft Recommendation on the draft Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (2011/0382 [NLE]) (1.2.2012). Rapporteur: Sophia in 't Veld (= PE Dok 480.773v01-00); Stellungnahme des Europäischen Datenschutzbeauftragten v 9.12.2011 ABL C 35, 16, zu dem Vorschlag für einen Beschluss des Rates über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security; weiters *Hornung/ Boehm*, Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security (Manuskript Passau/Luxembourg, 14.3.2012); weiters Spiegel Online, 19.4.2012 (s http://www.spiegel.de/reise/aktuell/fluggastdaten-eu-und-usa-schliessen-abkommen-a-828496.html, abgerufen am 28.7.2012).

120 Vgl wieder FN 102.

121 Abkürzung für „Society for Worldwide Interbank Financial Telecommunication". Es handelt sich um eine 1973 gegründete, in Belgien ansässige internationale Genossenschaft der Geldinstitute, die ein Telekommunikationsnetz (das sog SWIFT-Netz) für den standardisierten Nachrichtenaustausch zwischen den Mitgliedern betreibt (s dazu http://www.swift.com/home/index.page?lang=en).

122 Abkürzung für „Terrorist Finance Tracking Program" (s http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx). Unter diesem vom US-Finanzministerium („US Treasury Department" - UST) im Gefolge der Anschläge vom 11. September 2011 initiierten Programm verschafften sich die USA Zugriff auf bestimmte vertrauliche Überweisungsdaten aus dem automatisierten internationalen Interbanken-Zahlungsverkehr, der über SWIFT (FN 121) abgewickelt wurde/wird. Näheres zur seinerzeitigen Praxis insbes aus datenschutzrechtlicher Sicht: *Artikel 29-Datenschutzgruppe*, Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) (=WP 128) (angenommen am 22.11.2006).

an personenbezogenen Daten insbesondere aus Europa zeigte, so wenig konnte sie gleichzeitig mit **europäischen Datenschutzstandards** anfangen.

Letztere Tatsache hat(t)e nicht zuletzt damit zu tun, dass die US-**Verfassung** eine dem **Grundrecht auf Datenschutz** vergleichbare Gewährleistung **nicht beinhaltet**, was bedeutet, dass es dem einfachen Gesetzgeber bspw erlaubt ist, die Privatsphäre als solche bzw zum Schutz dieser einfachgesetzlich eingeräumte (Datenschutz)Rechte (auf Auskunft etc) jederzeit weitgehenden Einschränkungen zu unterwerfen, wovon der US-Gesetzgeber auch umfassend Gebrauch gemacht hat. Davon abgesehen unterscheidet sich der US-amerikanische Zugang zur Thematik des Privatsphären-Schutzes auch auf einfachrechtlicher Ebene grundlegend von jenem in Europa. Während der europäische Datenschutz stark auf formalisierte Rechtsmittelverfahren und eine institutionell gesicherte Unabhängigkeit[123] der Datenschutzaufsicht setzt, legt der US-amerikanische Ansatz das (argumentatorische) Schwergewicht auf die faktische Effizienz[124].

Zwar existiert in der Form des sog „Privacy Act of 1974"[125] ein Datenschutzgesetz. Allerdings reicht dessen Schutzwirkung wesentlich weniger weit als jene der europäischen Datenschutzrichtlinie bzw der aus Art 8 Abs 2 EMRK bzw Art 7, 8 GRC ableitbaren Gewährleistungen. Der Privacy Act 1974 zielt nur auf das Verhältnis zwischen (US-)Bürger(n) und Staat ab. Datenverwendungen **durch Private liegen nicht** in seinem **Fokus.**[126] Dies hat insbesondere Konsequenzen für Fälle der unrechtmäßigen Weitergabe von Daten durch staatliche Stellen an

Nachdem diese Praxis 2006 öffentlich geworden war (vgl bspw *Lichtblau/Risen*, Bank Data Is Sifted by U.S. in Secret to Block Terror, The New York Times [June 23, 2006]) und SWIFT in Reaktion darauf seine in den USA lozierte „Spiegeldatenbank" nach Europa verlegt hatte, sahen sich die USA genötigt, mit der EU ein Abkommen zu schließen, um den Datenzugriff solcherart auf eine formalrechtliche Grundlage zu stellen und fortsetzen zu können. Vgl dazu das Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika v 13.7.2010 ABl L 195, 5, über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus sowie den bezüglichen Beschluss des Rates v 13. Juli 2010 ABl L 195, 3 (kurz auch: EU-US TFTP-Abkommen). Kritisch dazu Stellungnahme des Europäischen Datenschutzbeauftragten v 22.6.2010 ABl C 355, 10, zum Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP II).

123 Vgl dazu nur EuGH U (Große Kammer) 9.3.2010, Rs C-518/07 - Europäische Kommission / Bundesrepublik Deutschland - Slg 2010, I-01885.

124 Vgl idS den Überblick bei *Kropf*, Networked and Layered: Understanding the US Framework for Protecting Personally Identifiable Information, World Data Protection Report Vol 7 (2007) No 6, 3 ff.

125 PL No 93-579, 110 Stat 3048 (= 5 USC § 552a); s dazu auch den kommentierten Gesetzestext des U.S. Department of Justice (http://www.justice.gov/opcl/1974privacyact.pdf).

126 Vgl idS insbesondere 5 USC § 552a(g)(1) bzw 5 USC § 552a(q). Zur fehlenden bzw eingeschränkten Reichweite der US-Datenschutzgesetzgebung gegenüber privaten Datenverwendungen s überblicksmäßig bspw *J. S. Stratford /J. Stratford*, Data Protecton and Privacy in the United States and Europe, IASSIST Quarterly - Fall 1998, 17 (18 ff).

Private. Während Art 8 Abs 2 EMRK (bzw § 1 Abs 1 DSG 2000) zufolge der stRsp insbesondere einen **Schutz vor** unrechtmäßiger bzw unverhältnismäßiger Datenerhebung bieten (**„Ermittlungsschutz"**),[127] ist dem Privacy Act bzw dem US-Recht überhaupt eine solche Gewährleistung unbekannt. Erst, wenn Daten sich bereits in der staatlichen Verfügungsgewalt befinden, greifen allenfalls Ansprüche auf Auskunft und Richtigstellung ein. Letztere unterliegen freilich zahlreichen Einschränkungen im Interesse der öffentlichen bzw nationalen Sicherheit und der Strafverfolgung.[128] Im Übrigen kommt den Betroffenen kein dem europäischen Datenschutzrecht vergleichbarer, gerichtlich durchsetzbarer Anspruch auf **Löschung** zu. Rechtsschutz bzw Kontrolle durch **unabhängige datenschutzspezifische** Einrichtungen, wie nach der EG-Datenschutzrichtlinie[129] oder der GRC[130] zwingend vorgesehen, sucht man in den USA bis dato ebenfalls vergeblich.[131] Als „Datenschutzkontrollstellen" stehen in den USA dort typischerweise keine unabhängigen Behörden, sondern nur sog verwaltungsinterne „(Chief) Privacy Officers"[132] zur Verfügung, welche grundsätzlich Beamte des jeweiligen Ministeriums sind, allerdings in Bezug auf ihre Tätigkeit eine gewisse Sonderstellung genießen.[133] Am ehesten sind sie dem europäischen Ombudsmann-Modell (mit erweiterten Befugnissen) vergleichbar.

Zu all den vorgenannten Aspekten gesellt sich der Umstand, dass sich der persönliche **Anwendungsbereich** des besagten Privacy Act auf US-Bürger und in den USA daueraufenthaltsberechtigte Drittstaatsangehörige beschränkt.[134] Der auch auf Nicht-US-Bürger anwendbare sog „Freedom of Information Act" aus 1966 (FOIA)[135] wiederum gewährt ausschließlich ein (nicht datenschutzspezifisches) allgemeines Auskunftsrecht gegenüber der Verwaltung.

Last but not least liegen die USA heute auch aus **rechtsstaatlicher** Sicht deutlich unter dem „EMRK-Standard". Dies liegt nicht nur am Festhalten zahlreicher Bundesstaaten an der Todesstrafe, sondern va auch an der aufrechten Weigerung, Terrorverdächtigen einen uneingeschränkten Zugang zu **fairen Verfahren** vor **ordentlichen Strafgerichten** zu gewähren. An die Praxis der menschenrechtswidrigen Anhaltung und Folterung „Terrorverdächtiger" in „Geheimgefängnissen", einige davon auch in EU-Staaten eingerichtet, sei in diesem

127 Vgl idS (Zu Art 8 MRK) s zB EKMR E 4. 12. 1962 – X – BeschwNr 1307/61, CD 9, 53; U EGMR 6. 9.1978 – Klass ua/Deutschland – Serie A Bd 28 Rn 41 = EuGRZ 1979, 278; U 28. 1. 2003 – Peck/ Vereinigtes Königreich – BeschwNr 44647/98 Rn 59 ff = ÖJZ 2004/20 (MRK).

128 Vgl 5 USC § 552a(j)-(k).

129 Vgl Art 28 RL 95/46/EG (FN 84).

130 Vgl Art 8 Abs 3 Charta der Grundrechte der Europäischen Union, ABl 2010 C 83, 389.

131 Vgl kritisch zur europäischen Betonung der „unabhängigen" Datenschutzaufsicht *Kropf*, Independence Day: How to Move the Global Privacy Dialogue Forward, Privacy & Security Law Report Vol 8 (2008) No 2, 1 ff (3).

132 Vgl etwa für das Department of Homeland Security sec 222 of the Homeland Security Act of 2002 (= 6 USC § 142).

133 Vgl dazu bspw *Kropf*, (FN 124) 3 (4); s auch Erl „Zu Artikel 11 – Allgemeine Prinzipien des Datenschutzes" RV 1388 BlgNR 24. GP, 9.

134 Vgl 5 USC § 552a(a)(2).

135 PL No 104-231, 110 Stat 3048 (=5 USC § 552); Text: (US Justizministerium): http://www.justice.gov/oip/amended-foia-redlined.pdf.

Kontext erinnert.[136] Angesichts der potentiellen „Fernwirkung" einer informationellen Polizeizusammenarbeit mit den USA im Einzelfall für Betroffene, hat der österreichische Datenschutzrat bereits im Jahr 2008 zu Recht darauf hingewiesen, „dass der durch das Abkommen ermöglichte unmittelbare Datenverkehr mit den USA [...] nicht ausschließt, dass die Daten letztlich in Verfahren, die nicht den Fair-trial-Grundsätzen (des Art 6 EMRK) genügen oder in denen die Todesstrafe verhängt wird, verwendet werden". Auch eine Verwendung im Zusammenhang mit Ermittlungsmethoden, die nach Art 3 EMRK als Folter zu qualifizieren wären, könne nicht ausgeschlossen werden.[137]

B. Zum Verhandlungsverlauf

Nachdem die Thematik des Abschlusses eines „PCSC-Abkommens" bereits anlässlich bilateraler US-österreichischer Besuchskontakte auf politischer Ebene angeschnitten worden war,[138] wurde Österreich im Februar 2008 durch die US-Behörden offiziell über die neuen Anforderungen an die informationelle Zusammenarbeit für Teilnehmer am „Visa waiver"-Programm (VWP) in Kenntnis gesetzt. Im Dezember 2008 folgte dann seitens des US-Heimatschutzministeriums die Mitteilung des Evaluierungsergebnisses betreffend die Erfüllung der Anforderungen des Visa waiver-Programms durch Österreich. Darin wurde festgestellt, dass Österreich insbesondere mit Blick auf das bereits bestehende EU-US-PNR-Abkommen[139], die EU-rechtliche Selbstverpflichtung[140] zur Kooperation mit der Interpol-Datenbank über gestohlene und verlorene Reisedokumente oder seine Rücknahmepraxis betreffend eigene Staatsangehörige den inhaltlich korrespondierenden Anforderungen aus dem VWP im Grunde bereits ausreichend Rechnung trage.[141] Zur vollumfänglichen Erfüllung der oben dargestellten (nach FN 109) VWP-Anforderungen bedürfe es allerdings noch des Abschlusses eines PCSC-Abkommens sowie eines HSPD-6-Abkommens.[142] Angepeilt hatten die USA die Finalisierung des Abschlusses ursprünglich bis Ende 2009.[143]

136 Vgl idS *Parliamentary Assembly / Assemblée parlementaire - Committee on Legal Affairs and Human Rights*, Secret detentions and illegal transfers of detainees involving Council of Europe member states: second report Explanatory memorandum. Rapporteur: Mr Dick Marty, Switzerland, ALDE (7 June 2007).

137 Vgl Stellungnahme des Datenschutzrates v 28.11.2008, GZ BKA-817.345/0002-DSR/2008, betr Datenaustausch mit den USA a) EU-US Visa Waiver Programme b) Bilaterales EU-US Prüm-Abkommen, 2.

138 So etwa anlässlich eines Zusammentreffens des damaligen österr Innenministers mit dem US-Heimatschutzminister in den USA im Oktober 2007.

139 Vgl dazu wieder FN 116.

140 Vgl Art 2 Nr 2 und 3 iVm Art 3 Abs 1 Gemeinsamer Standpunkt 2005/69/JI des Rates v 24.1.2005 ABl L 27, 61, zum Austausch bestimmter Daten mit Interpol.

141 Vgl *Department of Homeland Security – Visa Waiver Program Office*, Summary of Findings on the compliance of Austria with the information-sharing requirements and other provisions of the 9/11 Act (December 30, 2008) 1 f.

142 Vgl ebenda, 1.

143 So Presseberichte (vgl *Wetz*, USA wollen Österreichs Polizeidaten, Die Presse, 26.3.2009, 1).

Der Öffentlichkeit gegenüber war man lange bemüht, die Verknüpfung von Visafreiheit mit dem Abschluss der besagten Abkommen möglichst „in den Hintergrund" zu rücken.[144]

Auf einen von den USA Anfang März 2009 vorgelegten Übereinkommensentwurf[145] reagierte Österreich vor dem im Vorabschnitt skizzierten rechtlichen und politischen Hintergrund sowie angesichts einer ablehnenden Stellungnahme des Datenschutzrates vom November 2008[146] zurückhaltend und beschränkte sich zunächst auf die Sammlung von Informationen über die auf US-Seite intendierte praktische Nutzung der in Aussicht genommenen Kooperationsformen. Hinzu kam, dass schon damals auf EU-Ebene Bemühungen im Gange waren, die latenten Datenschutzprobleme im transatlantischen Kontext im Wege eines **Datenschutz-Rahmenabkommens** zwischen **USA** und **EU** über den Datenaustausch für Strafverfolgungszwecke zu lösen. Die **US-Strategie**, den angestrebten Informationszugang möglichst über bilaterale Verträge zu sichern und dabei möglichst keine Verpflichtungen zur Änderung ihrer eigenen Datenschutzrechtslage einzugehen, stand dem Verhandlungsziel der EU (Erhöhung des US-Schutzniveaus) insgesamt freilich diametral entgegen. Aus der traditionell datenschutzkritischen bzw grundrechtsambitionierten österreichischer Perspektive war schon damals absehbar, dass die USA **nach** erfolgtem **Abschluss** einschlägiger bilateraler Abkommen mit **sämtlichen** EU-Staaten kaum mehr zu substantiellen Zugeständnissen im Rahmen eines EU-US-Datenschutzabkommens motiviert sein würden.

Auf Drängen der US-Administration entschloss sich die österreichische Bundesregierung schließlich nach exploratorischen Gesprächen, ua in Washington, trotz Vorbehalten im März 2010 zur Aufnahme förmlicher Vertragsverhandlungen.[147] Um den Grundrechtsbedenken des Bundeskanzleramtes Rechnung zu tragen, hielt das bezügliche Verhandlungsmandat ausdrücklich fest, dass ein Abschluss eines derartigen Abkommens **nur möglich** sei, wenn darin ein **aus europäischer** und insbesondere **österreichischer Sicht befriedigendes** und **angemessenes Datenschutzniveau verankert** wird, wobei insbesondere auf die Verhältnismäßigkeit der Datenübermittlungen und auf geeignete Rechtsschutzmechanismen für die Durchsetzung der Rechte der/des Betroffenen abzustellen sein werde. Im Übrigen würden die Verhandlungen mit den USA über ein solches Abkommen [...] im vollen Einklang mit Österreichs internationalen Verpflichtungen geführt werden.[148] Damit folgte das Verhandlungsmandat im Wesentlichen den Forderungen des Datenschutzrates vom November 2008.[149]

144 Vgl *Wetz*, US-Informationen mit Widersprüchen, Die Presse, 20.4.2009, 11; *ders*, Visafreiheit für US-Reisen auf Prüfstand, Die Presse, 1.6.2010, 1.

145 „Agreement on Enhancing Cooperation in Preventing and Combating Serious Crime" (Abkommen zwischen der Regierung der Republik Österreich und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerer Straftaten).

146 Vgl Stellungnahme des Datenschutzrates v 28.11.2008 (FN 137).

147 Vgl Pkt 18 des Beschlussprotokolls Nr 52 zur Sitzung des Ministerrates am 9.3.2010 iVm dem bezüglichen Vortag an den Ministerrat v 2.3.2010, GZ BMeiA-AT.4.36.33/0001-IV.4a/2010, betr Abkommen zwischen der Republik Österreich und den Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Straftaten; Verhandlungen.

148 Vgl wieder Vortag an den Ministerrat v 2.3.2010, GZ BMeiA-AT.4.36.33/0001-IV.4a/2010 (FN 147) sowie Erl („Allgemeiner Teil") RV 1388 BlgNR 24. GP, 2.

Trotz redlicher Bemühungen der österreichischen Verhandlungsdelegation in den ab Juni 2010[150] intensiv geführten Gesprächen wurden die vorgenannten **Ziele letztlich nicht erreicht**. Wie sich herausstellte, war die US-Seite zwar willens, ihren Entwurf in einigen „technischen" Punkten an das Vorbild des Prümer Vertrages bzw Beschlusses anzunähern. Im aus österreichischer Sicht zentralen Punkt des Individualrechtsschutzes durch unabhängige Kontrollinstanzen waren die USA jedoch zu keinerlei Zugeständnissen bereit. Anzumerken ist zudem, dass sich wesentliche Auffassungsunterschiede zwischen US- und österreichischen Stellen in Bezug auf die Auslegung des Zweckbindungsgrundsatzes zeigten.

Dass das Verhandlungsergebnis dennoch im Oktober 2010 von der Bundesregierung genehmigt[151] und am 15. November 2010 unterzeichnet[152] wurde, war primär dem „nachdrücklichen" US-Interesse[153] bzw innen- und außenpolitischen Erwägungen auf Regierungsebene geschuldet. Die USA hatten auf einen Abschluss bis spätestens zum 31. Dezember 2010 gedrängt.[154] Auch scheint die Möglichkeit der visafreien Einreisemöglichkeit für österreichische Bürger in die USA durch die österreichische Regierung eine Gewichtung erfahren zu haben, die durchaus hinterfragungswürdig erscheint (dazu noch unten vor FN 202).

Nach einem kleinen innenpolitischen „Nachspiel" – dh „Vertagung" im Innenausschuss des Nationalrates am 24. November 2011 infolge oppositioneller Proteste[155] und (zusätzlicher) Befassung des Datenschutzrates am 20. Jänner 2012[156] samt Interventionen der US-Botschaft in Wien[157] – konnte das parlamentarische Ratifikationsverfahren mittlerweile im März 2012 abgeschlossen werden.[158]

149 Vgl wieder Stellungnahme des Datenschutzrates v 28.11.2008 (FN 137) 2.

150 Vgl *Möseneder*, Verhandlungen mit den USA über Datenweitergabe starten, Der Standard, 1.6.2010, 10.

151 Vgl Pkt 18 des Beschlussprotokolls Nr 76 zur Sitzung des Ministerrates am 19.10.2010

152 Vgl Erl („Allgemeiner Teil") RV 1388 BlgNR 24. GP, 2.

153 Vgl *Wetz*, USA wollen Österreichs Polizeidaten, Die Presse, 26.3.2009, 1; *ders*, USA drohten Österreich mit Visapflicht, Die Presse, 29.9.2010, 1; *ders*, Visafreiheit für US-Reisen auf Prüfstand, Die Presse, 1.6.2010, 1; „Österreich gewährt USA Zugriff auf Polizeicomputer", Der Standard, 1.10.2010; *Hecking*, Supermacht kontra Bergvolk, Financial Times Deutschland (Onlineausgabe), 4.10.2010; *Wetz*, Polizeidaten: Wien gibt US-Druck nach, Die Presse (Onlineausgabe), 23.11.2011; *ders*, Weitergabe von Polizeidaten: Wien geriet in Zwickmühle zwischen EU und USA, Die Presse, 30.12.2011, 11.

154 Vgl wieder *Wetz* (FN 153), Die Presse, 29.9.2010, 1; *ders*, Polizeidaten: Wien gibt US-Druck nach, Die Presse (Onlineausgabe), 23.11.2011.

155 Vgl „Innenausschuss diskutiert aktuelle sicherheitspolitische Fragen. Beratungen über Datenaustausch-Abkommen mit den USA vertagt", Parlamentskorrespondenz Nr 1130 v 24.11.2011; „Abkommen mit USA: Datenschutzrat prüft erneut", Die Presse (Onlineausgabe), 24.11.2011; „Daten an USA: Beschluss verschoben", Die Presse (Onlineausgabe), 24.11.2011.

156 Vgl ebenda. S zum Vorwurf der Opposition, der Datenschutzrat habe sich nicht mit der Endfassung des Abkommens auseinandergesetzt: „Datenschutzrat hat zu Abkommen Österreich-USA bereits vor drei Jahren Stellung genommen" (OTS0355 II 24. Nov 2011).

157 Vgl *Brickner*, US-Botschafter plädiert für Fingerprint-Vertrag mit Österreich, Der Standard, 2.2.2012.

158 Beschluss im Nationalrat am 29.2.2012, Beschluss im Bundesrat am 15.3.2012.

C. Das Verhandlungsergebnis und seine Bewertung aus Datenschutzsicht

Das bilaterale US-österreichische Prüm-like-Abkommen übernimmt **nicht sämtliche** informationelle Kooperationsformen des Prümer Vertrages bzw Prümer Beschlusses. Nicht Gegenstand des Abkommens sind insbesondere der Zugriff auf Fahrzeugregister oder der Massenabgleich von DNA-Profilen aus offenen Spuren. Auch eine Rechtshilfe in Form der Gewinnung bzw Untersuchung von menschlicher DNA ist nicht vorgesehen.

Hinsichtlich seiner **Zwecksetzung** weicht das „Prüm-like"-Abkommen von Prümer Vertrag bzw Beschluss durch eine eingezogene materielle Schwelle ab, nach welcher sich die Zusammenarbeit auf die **„Verhinderung** und **Bekämpfung schwerer Straftaten"**[159] bzw **„terroristischer" Straftaten**[160] konzentriert. Bei genauerer Betrachtung zeigt sich allerdings, dass diese Schwelle insofern ziemlich niedrig liegt, als unter den Begriff der „schweren Straftaten" schon jedes strafbare Verhalten, das mit einer Freiheitsstrafe von mehr als einem Jahr oder einer schwereren Strafe bedroht ist, fällt.[161] Zutreffender wäre es, hier von einer **mittleren Kriminalität** zu sprechen. Der Titel des Abkommens ist insofern irreführend.

Positiv zu bemerken ist angesichts des relativ unberechenbaren Anti-Terror-Kampfes der USA allerdings, dass man sich auf österreichischen Vorschlag hin auf eine vergleichsweise enge **Definition** der „terroristischen Straftat" verständigen konnte. Als solche gilt nach dem Abkommen nur ein solches ein strafbares Verhalten iS eines „internationalen Übereinkommens zur Bekämpfung des Terrorismus, das für **beide** Vertragsparteien **in Kraft ist**". Für den **anlasslosen** Austausch von Informationen wird im Übrigen auf den Zweck der Verhinderung schwerer Straftaten „mit einer transnationalen Dimension" (oder terroristischer Straftaten) abgestellt.[162] Soweit der vorgenannte Zweck verfolgt wird, können aber **auch geringfügigere Delikte** Gegenstand eines Datenaustausches werden. Dies va, wenn der Betroffene an einer organisierten kriminellen Gruppe oder Vereinigung beteiligt ist.[163] Zu bedenken ist, dass hier ggf die Gefahr besteht, dass Personen, lediglich auf Grund ihrer Sympathie-Bekundungen in Richtung einer radikalen Gruppierung zum Ziel von Übermittlungen werden könnten. Auch sei daran erinnert, dass in Österreich in einem rezenten Fall 13 Tierschützer (zu Unrecht) als „kriminelle Organisation" iSd § 278a StGB behandelt wurden.[164] Harmlose Studenten wurden zudem anlässlich einer Ordnungsstörung („irrtümlich") unter der Rubrik „Extremismus" gespeichert.[165] Gleich erging es einem Auskunftswerber gegenüber dem Innenministerium.[166]

159 Vgl Art 2 Abs 1 leg cit.
160 Vgl Art 10 Abs 1 leg cit.
161 Vgl Art 1 Z 7 leg cit.
162 Vgl Art 10 Abs 1 leg cit.
163 Vgl Art 10 Abs 1 lit c leg cit. S idS auch die Erl „Zu Artikel 10" RV 1388 BlgNR 24. GP, 8.
164 Vgl „Tierschützer: ‚Mafiaparagraf'-Freispruch rechtskräftig", Die Presse (Onlineausgabe), 29.6.2012.
165 Vgl dazu „Ex-ÖH-Chefin auf Extremismusliste: Rechtswidrig?", Die Presse (Onlineausgabe), 29.09.2011.
166 Vgl dazu die Blg zu *Datenschutzrat* - Votum Separatum Dr. Hans G. Zeger v 20.10.2012 betreffend des Vertrags „Abkommen zwischen der Regierung der Republik Österreich und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerer Straftaten" (bilaterales Ö-US „Prüm-like"-Abkommen).

Um der Gefahr willkürlicher Abfragen mittels „routinemäßig" anlässlich der US-Einreisekontrollen (bspw im Rahmen von „US-VISIT"[167]) erhobener daktyloskopischer Daten zu unterbinden bzw einzudämmen, hat Österreich in den Verhandlungen darauf gedrängt, die Zulässigkeit der **automatisierten Abfrage** mittels solcher Daten **auf konkrete Verdachtsfälle zu begrenzen**. Dies ist der Hintergrund der Kompromissformulierung des nunmehrigen Art 2 Abs 2 des Abkommens, wonach solche Online-Abfragen insbesondere nur dann gestattet sind, wenn **besondere** und **rechtsgültige Umstände** in Bezug auf eine **bestimmte** Person **Anlass** zur Nachforschung geben, ob diese Person eine solche schwere Straftat begehen wird oder begangen hat. Eine allgemeine Terrorwarnung am Flughafen wäre bspw kein solcher Anlass. Von dieser Facette einmal abgesehen, bietet die zitierte Bestimmung freilich **keinen wirklich justiziablen Maßstab** im Hinblick auf eine allfällige Überprüfung der Rechtmäßigkeit einer Abfrage im hier interessierenden Sinn.

Im Lichte der bereits angesprochenen (Abschn IV.A nach FN 135) spezifischen rechtsstaatlichen Defizite der USA lag es darüber hinaus im Interesse Österreichs, sich durch **„Fluchtklauseln"** Möglichkeiten zu schaffen, die Zusammenarbeit bei Bedarf einzuschränken. Eine solche Klausel findet sich quasi versteckt in den Legaldefinitionen des Abkommens. Nach Art 1 Z 7 iVm Art 6 und 9 leg cit können die Vertragsparteien nämlich im Interesse der Sicherstellung der Einhaltung ihres innerstaatlichen Rechts **„besondere"** schwere **Straftaten festlegen**, für die eine Vertragspartei nicht verpflichtet ist, anlässlich einer „Nachfrage" infolge eines im automatisierten Verfahren erzielten **Treffers** personenbezogene Daten zu übermitteln.

Das damit angesprochene **Hit-/No Hit-Verfahren** im Falle des automatisierten Abgleichs von DNA- und daktyloskopischen Daten mildert insofern auf den ersten Blick die datenschutzrechtliche Problematik. Tatsächlich bestimmt § 8 Abs 2 Z 2 Polizeikooperationsgesetz (PolKG)[168], dass die **Übermittlung personenbezogener Daten** im Rahmen der Amtshilfe insbesondere dann **zu unterbleiben hat**, wenn Grund zur Annahme besteht, dass **„überwiegende schutzwürdige Interessen** des Betroffenen oder Dritter **verletzt werden**, insbesondere jene Rechte, die im internationalen Pakt über bürgerliche und politische Rechte[169] gewährt werden". Auf den zweiten Blick muss allerdings angemerkt werden, dass dem einzelnen Beamten derzeit **keinerlei konkrete Anhaltspunkte** zur Verfügung stehen, **in welchen Fällen** er infolge einer Nachfrage der US-Seite tatsächlich gehalten ist, **keine direkt personenbezogenen** Daten **oder** lediglich **Identi-**

167 US VISIT steht für: „United States Visitor and Immigrant Status Indicator Technology pogram"; im Rahmen dieses Verfahrens werden Einreisende entweder anlässlich eines Visumantrages (bspw in einem Konsulat) oder direkt bei der Grenzkontrolle „biometrisch" behandelt, dh ihre Fingerabdrücke werden gescannt und es wird zusätzlich ein digitales Porträtfoto angefertigt. Die so gewonnenen Fingerabdruckdaten werden mit daktyloskopischen Datenbanken, in denen gesuchte bzw für die Einreise gesperrte Personen dokumentiert sind („watch-list"), abgeglichen und zudem langfristig gespeichert (s dazu http://www.dhs.gov/files/programs/gc_1214422497220.shtm).
168 ÖBGBl I 1997/104 idF BGBl I 2012/50.
169 Quelle: öBGBl 1978/591.

tätsdaten ohne bezügliche „Falldaten" preiszugeben. Dazu bedürfte es zumindest eines entsprechenden behördeninternen Erlasses. Auch ein solcher böte aber keine dauerhafte solide Grundlage, da er jederzeit inhaltlich geändert oder aufgehoben werden könnte. Am ehesten gangbar erschiene es, bestimmte Deliktsgruppen bzw Sachverhalte global zu regeln.

Die **Brisanz** der vorstehend angesprochenen Fragestellung wird erst klar, wenn man sich bewusst macht, wie **groß** gerade auch das **Ermessen** der österreichischen Behörden in punkto Gewinnung und Verspeicherung von DNA-Profilen bzw Fingerabdruckdaten ist. Für eine erkennungsdienstliche Behandlung (Abnahme von Fingerabdrücken, Gewinnung von DNA usw) reicht es aus, dass die betreffende Person im **Verdacht** steht, (irgend)eine **mit Strafe bedrohte Handlung begangen zu haben**, wenn sie im Rahmen einer kriminellen Verbindung tätig wurde oder dies „wegen der Art oder Ausführung der Tat oder der Persönlichkeit des Betroffenen zur Vorbeugung gefährlicher Angriffe erforderlich scheint".[170] Sinngemäßes gilt für die Vornahme einer DNA-Analyse des erhobenen biologischen Materials. Es muss nur der Verdacht gegeben sein, eine Person habe einen **„gefährlichen Angriff"** begangen, verbunden mit der (naturgemäß wieder subjektiven) Einstufung als potentieller künftiger Wiederholungstäter.[171] Als gefährlicher Angriff im vorstehenden Sinn ist – vereinfacht gesagt – jede die Bedrohung eines Rechtsgutes durch eine vorsätzlich begangene gerichtlich strafbaren Handlung (Bsp: Ladendiebstahl) oder eine zeitnah zur Begehung gesetzte Vorbereitungshandlung zu verstehen.[172] Auch für die Gewinnung von menschlicher DNA für Strafverfolgungszwecke reicht es aus, dass dies wesentlich für die Aufklärung einer (nicht qualifizierten) Straftat ist.[173] Auch für die Erstellung eines DNA-Profils aus solcherart gewonnenem Material reicht als Zweck die „Aufklärung einer Straftat".[174]

Zum vorstehend dargelegten Fehlen einer signifikanten materiellen Hürde für die Gewinnung und Speicherung erkennungsdienstlicher Daten nach der innerstaatlichen Rechtslage in Österreich kommt erschwerend der Umstand hinzu, dass sich auch die bezüglichen **Höchstspeicherfristen** je nach Fall als extrem lang darstellen können. Im Fall einer rechtskräftigen Verurteilung, aufrechter Verdachtsmomente in den Augen der Sicherheitsbehörden (ohne Anklage bzw trotz Freispruchs) oder bei einer Diversion bleiben Profile bis zur Vollendung des 80. Lebensjahres des Betroffenen gespeichert.[175]

Dass das Abkommen selbst trotz seiner thematischen Spezifik überhaupt keine ausdrücklichen Höchstspeicherfristen vorgibt, sondern nur den allgemeinen Grundsatz der begrenzten Speicherdauer wiedergibt, erleichtert die Situation nicht.[176]

170 Vgl § 65 Abs 1 Sicherheitspolizeigesetz (SPG) öBGBl 1991/566 idF BGBl I 2012/13.
171 Vgl § 67 Abs 1 SPG.
172 Vgl § 16 Abs 2 u 3 SPG.
173 Vgl § 123 Abs 1 Z 1 StPO.
174 Vgl § 124 Abs 1 StPO.
175 Vgl § 73 Abs 1 Z 1 iVm § 65 iVm § 67 SPG bzw § 75 Abs 4 StPO.
176 Vgl Art 11 Abs 2 lit c leg cit; zum inhaltlich korrespondierenden Art 11 Abs 2 lit b des US-dt „Prüm-like"-Abkommens s kritisch die Stellungnahme des Rechtsausschusses des dt Bundesrates (BR-Drs 637/1/09, 6.7.2009, 3) bzw Pkt 5 der Stellungnahme des BR v 15.5.2009 (BR-Drs 331/09 [Beschluss], 15.5.2009, 3).

Aus all dem Gesagten folgt, dass es anlässlich einer Überprüfung einer aus Österreich stammenden Person an der US-Grenze anhand ihrer Fingerabdruckdaten mittels Onlineabfrage in der österreichischen automatisierten Fingerabdruckdatenbank schon deshalb zu einem Treffer kommen kann, weil diese in ihrer Jugend Ziel einer erkennungsdienstliche Behandlung aus geringfügigem Anlass war (bspw angeblicher Widerstand gegen die Staatsgewalt bei einer Studentendemonstration).[177] Es erscheint nun im Lichte der anhaltenden „Übersensibilisierung" der US-Sicherheitsbehörden nicht unplausibel, dass Letztere schon aus der **alleinigen Tatsache** einer **Speicherung** der Person in einer österreichischen Polizeidatei negative Rückschlüsse ziehen und bspw eine Einreisesperre verhängen. Davon abgesehen ist auf darauf zu verweisen, dass die automatisierten Abgleichverfahren nur wahrscheinliche Übereinstimmungen liefern, welche einer Verifikation bedürfen.[178]

Die **Konsequenz** aus den obigen Überlegungen müsste darin bestehen, das gesamte innerstaatliche Regime betreffend den Umgang mit erkennungsdienstlichen Daten, insbesondere mit Blick auf die Speicherdauer grundlegend zu hinterfragen. Zudem müsste im Falle von US-Treffern auf österreichische Daten gewissermaßen eine systematische Filterung der allenfalls von US-Seite nachgefragten „Falldaten" Platz greifen. Bis dato zeichnen sich freilich keinerlei Aktivitäten des österreichischen Gesetzgebers respektive der Regierung in diese Richtung ab.

Erhebliche Probleme aus dem US-österreichischen „Prüm-like"-Abkommen selbst ergeben sich weiters aus dem Kreis der darin explizit angesprochenen übermittelbaren Datenkategorien. So scheint Art 12 leg cit auf den ersten Blick den Schutz sog sensibler Daten im Auge zu haben. „In Anerkennung der besonderen Schutzbedürftigkeit" dieser Kategorien „treffen die Vertragsparteien geeignete Schutzvorkehrungen, insbesondere geeignete Sicherheitsmaßnahmen, um solche Daten zu schützen", heißt es in Art 12 Abs 2 leg cit. Dass in Art 12 Abs 1 leg cit „politische Anschauungen, religiöse oder sonstige Überzeugungen oder die **Mitgliedschaft in Gewerkschaften"** dezidiert als mögliche Gegenstände eines Datenaustausches genannt werden, der dann in Betracht kommt, wenn solche Daten „für die Zwecke dieses Abkommens besonders relevant sind", sorgte angesichts der Unbestimmtheit dieser Vorgabe freilich zu Recht für massive Kritik.[179]

177 Vgl dazu das Bsp einer Demonstration in Graz im April 2010 („Polizei Graz sammelt Fingerabdrücke von Demonstranten", Der Standard, 1.6.2010.
178 Insofern zutreffend *Datenschutzrat* - Votum Separatum Dr. Hans G. Zeger v 20.10.2012 (FN 166) 2.
179 Der dt Bundestag hat zur inhaltlich korrespondierenden Bestimmung des Art 12 des US-dt „Prüm-like"-Abkommens in einer Entschließung festgehalten, dass er „ebenso wie der Bundesrat nicht zu erkennen vermag, dass die Mitgliedschaft in einer Gewerkschaft in Deutschland je die notwendige besondere Relevanz für die Bekämpfung und Verhinderung schwerwiegender Kriminalität haben kann. Der Deutsche Bundestag bekräftigt den besonderen verfassungsrechtlichen Schutz der Gewerkschaften, die ein Grundpfeiler unseres pluralen demokratischen Gemeinwesens sind." (BT-Drs 16/13659, 1.7.2009, 5). Der dt Bundesrat hat in einer Entschließung ausdrücklich Nachverhandlungen in diesem Punkt gefordert (BR-Drs 637/09 [Beschluss], 10.7.2009, 1 f). S auch die Stellungnahme des Rechtsausschusses des dt Bundesrates (BR-Drs 637/1/09, 6.7.2009, 4). S auch den Kommentar von *Rief*, Transparenz für die Bürger, Die Presse (Onlineausgabe), 23.11.2011.

Unter dem Gesichtspunkt des **Zweckbindungsgrundsatzes** positiv zu werten ist zwar, dass den Vertragsparteien eine Weitergabe der Daten, die nach diesem Abkommen bereitgestellt wurden, an Drittstaaten, internationale Organe oder Private ohne die vorige, in geeigneter Weise dokumentierte, Zustimmung der bereitstellenden Vertragspartei und ohne geeignete Schutzvorkehrungen untersagt ist.[180] Gleichzeitig ist zu bemängeln, dass die **Zulässigkeit** einer **Weiterverwendung** von Daten durch die empfangende Vertragspartei für **alle möglichen Zwecke** durch (bloße) Zustimmung der übermittelnden Vertragspartei bewerkstelligt werden kann.[181] Welche innerstaatliche Instanz unter welchen Bedingungen eine solche Zustimmung erteilen kann, bleibt allein den innerstaatlichen Rechtsordnungen überlassen.[182]

Erwähnenswert in diesem Kontext ist weiters die nach Art 25 leg cit vorgesehene Möglichkeit der **zeitweisen einseitigen Aussetzung** der Anwendung des Abkommens oder von Teilen desselben unter Verweis auf die Nichteinhaltung von Pflichten aus dem Abkommen durch die jeweils andere Partei. Einem solchen Fall gleichzuhalten ist jener, dass „Entwicklungen im innerstaatlichen Recht einer der Vertragsparteien den Zweck und den Anwendungsbereich dieses Abkommens, insbesondere in Bezug auf den **Schutz personenbezogener Daten, untergraben**". Kritisch könnte man hier aus europäischer Sicht fragen, ob gegenüber den USA jemals ein Zeitpunkt gegeben sein wird, in dem eine Berufung auf diesen zweiten Fall nicht (mehr) plausibel wäre.

Wenig praktischer Relevanz kommt der im Kontext des anlasslosen Informationsaustausches (Art 10) der jeweils übermittelnden Vertragspartei eingeräumten **Option** zu, „im Einklang mit ihren Verpflichtungen, die sich aus dem Völkerrecht und ihrem innerstaatlichen Recht ergeben, **Bedingungen für die Verwendung** dieser Daten durch die empfangende Vertragspartei **fest[zu]legen**".[183] Der vorzitierte Verweis auf „völkerrechtliche" Verpflichtungen wurde auf Wunsch Österreichs eingefügt und stellt einen impliziten Reflex auf menschenrechtliche Standards dar, an die Österreich sich gebunden sieht. Ansonsten entspricht der Text dem ursprünglichen US-Vorschlag. Die besagte Möglichkeit, (restriktive) Bedingungen aufzuerlegen wird aber gleich wieder eingeschränkt. Einmal werden solche Bedingungen überhaupt nur wirksam, wenn die empfangende Vertragspartei die Daten „annimmt".[184] Unklar ist hier, ob es überhaupt denkbar ist, dass eine Vertragspartei Informationen ablehnen kann, ohne nicht zuvor schon Kenntnis von deren Inhalt erlangt zu haben. Weiters hält Art 10 Abs 4 fest, dass „**allgemeine Einschränkungen** in Bezug auf die **rechtlichen Standards** der **empfangenden Vertragspartei** für die Verarbeitung personenbezogener Daten" ausdrücklich **nicht** als Bedingung im vorstehenden Sinne auferlegt werden können. Es ist nicht ersichtlich, welcher Spielraum hier in der Praxis noch bleiben soll. Denn gerade im Fall der USA wäre es im Lichte der dortigen Rechtslage sinnvoll, bspw Übermittlungsverbote an weitere Behörden uä aufzuerlegen.

180 Vgl Art 13 Abs 2 leg cit.
181 Vgl Art 13 Abs 1 lit d leg cit.
182 Vgl kritisch zur inhaltlich korrespondierenden Regelungen des Art 13 des US-dt „Prüm-like"-Abkommens den Rechtsausschuss des dt Bundesrates (BR-Drs 637/1/09, 6.7.2009, 3).
183 Vgl Art 10 Abs 3 leg cit.
184 Vgl Art 10 Abs 3 letzter Satz leg cit.

Die **Datenschutzvorschriften ieS** lehnen sich teilweise eng an jene des Prümer Vertrages an (Bsp „Datensicherheit"[185] und „Dokumentation"[186]), teils übernehmen sie diese auch nur summarisch bzw stark verkürzt. Die vom Datenschutzrat im Jahre 2008 als „wesentlich" erachtete „vollständige Wiedergabe der Datenschutzbestimmungen des Prümer Beschlusses in einem bilateralen Abkommen mit den USA"[187] wurde insofern verfehlt.

Die **Dokumentationsregeln** konnte Österreich erst in den Verhandlungen stark an den „europäischen" Prüm-Standard annähern. Dies gilt va im Hinblick auf den automatisierten Abruf und die dabei zu gewährleistende Nachvollziehbarkeit bis hin zur Person des einzelnen abrufenden Beamten.[188]

Davon und von einer Präzisierung der Regeln für die Sperrung von Daten im Interesse Betroffener[189] abgesehen wurden Österreich – gemessen am Ausgangstext bzw bereits geschlossenen anderen „Prüm-like"-Abkommen, wie etwa jenem mit Deutschland – lediglich kosmetische Ergänzungen zugestanden. Dazu gehört Art 18 („Überprüfung") leg cit, der ausdrücklich festhält, dass das allgemein in Art 20 Abs 2 verankerte **Auskunftsrecht** der **Vertragsparteien im Verhältnis zueinander** auch die Befugnis einschließt, „von der Datenschutzbehörde oder einer anderen zuständigen Behörde der anderen Vertragspartei **zu verlangen**, dass diese **überprüft**, ob die personenbezogenen Daten eines bestimmten Betroffenen, die auf Grund dieses Abkommens übermittelt wurden, **in Übereinstimmung mit diesem Abkommen verarbeitet** wurden". Die Besonderheit dieser Anordnung liegt lediglich darin, dass sich die Vertragsparteien insofern das Recht einräumen, **direkt** mit bestimmten ihrer (nachgeordneten) Behörden zu kommunizieren. Dass „Interventionen" zwischen Staaten je nach Fall auch im Interesse einzelner ihrer Bürger stattfinden, ist per se keine Novität, sondern an sich selbstverständlich. Je nachdem, wo sich der Betroffene aufhält, kann dies als Ausfluss der traditionellen konsularischen Schutzfunktion oder als sonstige Serviceleistung interpretiert werden.

Liest man nun Art 18 leg cit in der Zusammenschau mit Art 19[190] – ebenfalls einer in anderen vergleichbaren Abkommen nicht enthaltene Bestimmung – könnte auf den ersten Blick der Eindruck entstehen, **Betroffenen** käme ein **Rechtsanspruch auf** eine **Intervention** im vorstehenden Sinne, uzw durch die eigene Datenschutzbehörde bzw eine sonst zuständige Behörde, zu. Zufolge Art 19 kann nämlich „jede Person, die Informationen über die Nutzung ihrer personenbezogener Daten gemäß diesem Abkommen verlangt oder das ihr gemäß dem innerstaatlichen Gesetzen zustehende Recht auf Berichtigung, Sperrung oder Löschung solcher Daten ausüben will, einen Antrag an ihre Datenschutzbehörde oder eine andere zuständige Behörde gemäß Art 11 Abs 4 richten, die in Übereinstimmung mit ihrem innerstaatlichen Recht gemäß Art 14 Abs 1 oder Art 18 vorzugehen hat."

Tatsächlich aber ist zu betonen, dass Art 11 („Allgemeine Prinzipien des Datenschutzes") leg cit bestimmt, dass „dieses Abkommen die **Rechte** und Pflichten

185 Vgl Art 16 leg cit.
186 Vgl Art 15 leg cit.
187 Vgl Stellungnahme des Datenschutzrates v 28.11.2008 (FN 137) 2.
188 Vgl Art 15 Abs 2 leg cit.
189 Vgl Art 14 Abs 4 leg cit.
190 Diese Bestimmung ist überschrieben mit „Antrag von Personen auf Zugang zu und Berichtigung, Sperrung und Löschung von Daten".

der **Vertragsparteien** in Bezug auf den Gebrauch personenbezogener Daten einschließlich der Berichtigung, Sperrung und Löschung gemäß Artikel 14 regelt", **Privatpersonen** jedoch **keine Rechte aus** diesem **Abkommen erwachsen.**[191] Daraus ergibt sich, dass sich unmittelbar aus dem Abkommen selbst bspw für österreichische Staatsbürger **kein subjektiv-öffentliches Recht auf** eine **Intervention** – durch die Datenschutzkommission – bei US-amerikanischen (Datenschutz)Behörden ergibt. Ein solcher Anspruch müsste erst im innerstaatlichen österreichischen Recht – etwa analog dem deutschen Recht[192] – geschaffen werden. Würde man dies ins Auge fassen, stellte sich einmal die Problematik der „Einklagbarkeit" bzw faktischen Durchsetzbarkeit eines solchen „Anspruchs auf Intervention". Davon abgesehen wäre auch damit **weder ein direkter Zugang** eines österreichischen Betroffenen **zu** einer verbindlichen **Entscheidung** einer **unabhängigen Kontrollstelle** iSd Art 28 Datenschutzrichtlinie noch eine effektive Durchsetzung von Berichtigungs-, Sperrungs- oder Löschungsansprüchen gewährleistet.[193] Ebenfalls keine Regelungen trifft das Abkommen übrigens über **Schadenersatzansprüche** Betroffener.

Vor allem mit Blick auf den insofern **fehlenden Individualrechtsschutz** gegenüber allfälligen Abkommens-widrigen Datenverwendungen durch US-Behörden ist es daher weder gelungen, ein im Vergleich zu anderen „Prüm-like"-Abkommen signifikant günstigeres Ergebnis zu erzielen,[194] noch ein insgesamt **adäquates Datenschutzniveau**, wie es die einschlägigen europäischen Rechtsvorschriften als Zulässigkeitsvoraussetzung für Übermittlungen in Drittstaaten, verlangen,[195] zu etablieren.[196] Österreich hat daher mit dem Abschluss des hier diskutierten Abkommens nicht nur gegen seine internationalen Verpflichtungen

191 Vgl idS auch Erl „Zu Artikel 11 – Allgemeine Prinzipien des Datenschutzes" RV 1388 BlgNR 24. GP, 9.

192 Vgl Art 1 § 5 Abs 1 und 5 („Rechte des Betroffenen auf Geltendmachung von Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsansprüchen gegenüber den Vereinigten Staaten von Amerika durch das Bundeskriminalamt") Gesetz zur Umsetzung des Abkommens zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika vom 1.10.2008 über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität, dBGBl 2009 I 2998.

193 Insofern zutreffend die kritische Einschätzung der zitierten dt Regelungen (FN 192) durch den Rechtsausschuss des dt Bundesrates (BR-Drs 637/1/09, 6.7.2009, 3, 4).

194 AA aber der Datenschutzrat in seiner Stellungnahme v 20.1.2012, GZ BKA-817.394/0001-DSR/2012, betr Abkommen zwischen der Regierung der Republik Österreich und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerer Straftaten (PCSC), 3.

195 Vgl Art 25 Abs 1 RL 95/46/EG (FN 84) bzw Art 25 Abs 1 Rahmenbeschluss 2008/977/JI des Rates v 27.11.2008 ABl L 350, 60, über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

196 So zutreffend auch *Datenschutzrat* - Votum Separatum Dr. Hans G. Zeger v 20.10.2012 (FN 166), 1 (3). S weiters zu den inhaltlich korrespondierenden Regeln des US-dt „Prüm-like"-Abkommen (Art 11-17) (FN 117) die Einschätzung des Rechtsausschusses des dt Bundesrates (BR-Drs 637/1/09, 6.7.2009, 3), welcher zur Auffassung gelangte, dass das fragliche Abkommen selbst **keinen angemessenen Datenschutz gewährleistet** bzw den Betroffenen **praktisch keine Datenschutzrechte eingeräumt werden.** Folgerichtig hat der BR in einer Entschließung ausdrücklich Nachverhandlungen in diesem Punkt gefordert (BR-Drs 637/09 [Beschluss], 10.7.2009, 2).

auf dem Gebiete des Datenschutzes verstoßen, sondern auch die **gesamteuropäische Verhandlungsposition** gegenüber den USA mit Blick auf das zu verhandelnde Rahmenabkommen **geschwächt**[197]. Die EU-Kommission hätte sich ein Vorgehen der EU-Mitgliedstaaten unter ihrer Koordination gewünscht.[198]

Vor obigem Hintergrund umso weniger nachvollziehbar ist aus europäischer Sicht die von den US-Vertretern in Österreich im Nachhang zu den Verhandlungen offensiv vorgetragene, gewagte These eines nicht nur gleichwertigen, sondern sogar **„überlegenen" US-Datenschutzsystems.**[199]

Abgelehnt haben die USA im Übrigen auch das österreichische Ansinnen, im „Prüm-like"-Abkommen vorzusehen, dass die dortigen Datenschutzbestimmungen im Falle der Vereinbarung höherwertiger Regelung im Rahmen der EU-US-Verhandlungen über ein Rahmenabkommen zum Datenschutz automatisch durch Letztere ersetzt werden. Dazu sei ergänzend angemerkt, dass sich trotz jahrelanger Verhandlungen der Europäischen Kommission mit den USA nach wie vor kein Entgegenkommen Letzterer in den Punkten Aufsichtsbehörden, Individualrechte / Rechtsbehelfe und Speicherdauer abzeichnet.[200] Die Forderung des Datenschutzrates, das besagte Rahmenabkommen müsse „jedenfalls die der Datenschutz-Konvention des Europarates samt Zusatzprotokoll entsprechenden Mindeststandards normieren", dürfte daher auf absehbare Zeit ein frommer Wunsch bleiben.[201]

V. Resümee

Wiewohl die österreichische Verhandlungsdelegation der US-Seite gewisse Präzisierungen abringen und etwa im „technischen Datenschutz" (dh bspw bei den Protokollierungsvorgaben) eine gewisse Annäherung an den Standard des Prümer Vertrags bzw Prümer Beschlusses erreichen konnte, blieb insbesondere die zentrale Frage des **Individualrechtsschutzes ungelöst.** Im Ergebnis hat sich Österreich damit nicht nur in Widerspruch zu seinen **europarechtlichen Verpflichtungen** zur Gewährleistung eines angemessenen Datenschutzes gegenüber Drittstaaten anlässlich der Datenübermittlung gesetzt, sondern auch die **EU-Gesamtposition** in den transatlantischen Datenschutzverhandlungen weiter **geschwächt.**

Die Erfahrungen der bilateralen US-österreichischen Verhandlungen haben insgesamt gezeigt, dass es sowohl angesichts des Machtgefälles, als auch infolge

197 IdS auch *Datenschutzrat* - Votum Separatum Dr. Hans G. Zeger v 20.10.2012 (FN 166) 4.

198 Vgl dazu *Wetz,* Weitergabe von Polizeidaten: Wien geriet in Zwickmühle zwischen EU und USA, Die Presse, 30.12.2011, 11, der einen Bericht des österr Justizministeriums an das österr Außenministerium v 23.12.2008 zitiert, wonach ein leitender Beamter der EU-Kommission (Bereich „Polizeikooperation und Informationszugang") die bilateralen Gespräche Österreichs mit den USA als „nicht besonders loyal" eingestuft habe.

199 Vgl dazu das Interview mit US-Botschafter Eacho: „US-Botschafter: ‚Unser Datenschutz ist überlegen'", Die Presse (Onlineausgabe), 28.11.2011.

200 So wieder der jüngste Sachstandsbericht der Europäischen Kommission im Rahmen der Ratsarbeitsgruppe „transatlantische Beziehungen" (COTRA) v 17.4.2012.

201 Vgl Stellungnahme des Datenschutzrates v 20.1.2012, GZ BKA-817.394/0001-DSR/2012, 4 (FN 194).

der fehlenden Grundrechtssensibilität und Flexibilität der USA auf einem Feld wie dem vorliegenden ohne eine mit den EU-Partnern koordinierte Vorgangsweise de facto aussichtslos ist, befriedigende Verhandlungsergebnisse zu erzielen.

Spielräume im innerstaatlichen Recht zur „Abmilderung" möglicher negativer Folgen für einzelne Betroffene wären vorhanden, wurden aber bis dato nicht genutzt.

Neben Eigeninteressen der österreichischen Sicherheitsbürokratie spielte bei der Vorgangsweise der österreichischen Administration das selbst gesetzte **Ziel**, nicht aus dem **„Visa waiver"-Programm** ausscheiden zu müssen, eine zentrale Rolle. Dazu sei angemerkt, dass sich für den einzelnen Staatsbürger der **„Komfortgewinn"** aus der visumfreien Einreisemöglichkeit **„in engen Grenzen"** hält. Denn die Visafreiheit bewahrt den Einreisewilligen nicht vor zahlreichen administrativen „Schikanen" bzw grundrechtlich problematischen „Informationseingriffen". So muss er sich vorab via Internetportal anmelden (ESTA), die Übermittlung umfassender Buchungsdaten durch das gewählte Flugunternehmen an die US-Behörden noch vor Abflug dulden (PNR) und schließlich an der Grenze die Erfassung und Speicherung biometrischer Daten (US-VISIT) hinnehmen. Zusätzlich muss er seit 8. September 2010 mit Gebühren die Einreisebürokratie mitfinanzieren.[202]

202 Dzt sind 14 $ im Rahmen des ESTA zu bezahlen; vgl Section 9(e) of the United States Capitol Police Administrative Technical Corrections Act of 2009 (PL No 111-145 [2010]) (auch: „Travel Promotion Act of 2009"), mit dem Sec 217(h)(3)(B) (= 8 USC § 1187[h][3][B]) des Immigration and Nationality Act of 1952 (ch 477, 66 Stat 163) (= 8 USC §§ 1101 et seq) geändert wurde.