

Vorblatt

1. Problem:

Die Entwicklungen der letzten Jahre in den Bereichen des internationalen Terrorismus und der grenzüberschreitenden Kriminalität haben die Notwendigkeit einer verstärkten internationalen Zusammenarbeit von Polizei und Justiz verdeutlicht. Die USA, deren Kongress 2007 die Ausführungsgesetzgebung zum sog. „09/11 Commission Act“ annahm, sind ein wichtiger Partner Österreichs in der grenzüberschreitenden Bekämpfung von schweren Straftaten. Das mit den USA ausgehandelte Abkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerer Straftaten, das auf dem Vorbild des in der EU entwickelten Prümmer Regelwerks beruht, entspricht diesem Ziel.

2. Ziel:

Die Vertragsparteien bezwecken mit diesem Abkommen, die grenzüberschreitende polizeiliche Zusammenarbeit, insbesondere auf dem Gebiet des Informationsaustausches zum Zwecke der Verhinderung und Bekämpfung von schweren Straftaten, zu vertiefen. Dies liegt im Zeitalter des visafreien Reiseverkehrs auch im Interesse eines erhöhten Schutzes der österreichischen StaatsbürgerInnen vor internationaler organisierter Kriminalität und Terrorismus.

3. Inhalt, Problemlösung:

Intensivierung des Informationsaustausches durch die Ermöglichung eines automatisierten Abrufs von daktyloskopischen Daten sowie von DNA-Profilen im Einzelfall, und zwar im Rahmen eines sog. Treffer-/Nicht-Trefferprinzips („hit/no hit-Verfahrens“) und Festlegung (datenschutz-) rechtlicher Rahmenbedingungen für die Ermöglichung eines proaktiven Austausches von personenbezogenen und anderen Daten zur Verhinderung schwerer Straftaten mit einer transnationalen Dimension und terroristischer Straftaten sowie die Festlegung (datenschutz-)rechtlicher Rahmenbedingungen für die genannten. Ein automatisierter wechselseitiger Austausch von DNA-Profilen kann allerdings erst nach Änderung der bezüglichen innerstaatlichen Rechtslage in den USA erfolgen.

4. Alternativen:

Der Austausch daktyloskopischer Daten und DNA-Profile mittels elektronischer Datenübermittlung auf Anfrage ohne wechselseitigen Direktzugriff auf die jeweiligen nationalen daktyloskopischen bzw. DNA-Dateien wäre weniger effizient bzw. würde den Verzicht auf Beschleunigungseffekte bei der polizeilichen Zusammenarbeit bedingen.

5. Auswirkungen des Regelungsvorhabens:

5.1 Finanzielle Auswirkungen:

Das Abkommen wird voraussichtlich keine erheblichen finanziellen Auswirkungen haben; sofern es dennoch zu solchen kommen sollte, werden sie aus den dem zuständigen Ressort zur Verfügung gestellten Mitteln bedeckt.

5.2 Wirtschaftspolitische Auswirkungen:

5.2.1. Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Keine

5.2.2. Auswirkungen auf die Verwaltungskosten für Bürger/innen und Unternehmen

Keine

5.3 Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit:

Keine

5.4 Auswirkungen in konsumentenschutzpolitischer sowie sozialer Hinsicht:

Keine

5.5 Geschlechtsspezifische Auswirkungen:

Keine

6. Verhältnis zu Rechtsvorschriften der Europäischen Union:

Gemäß Erklärung 36 zum Vertrag von Lissabon (BGBl. III Nr. 132/2009) dürfen Mitgliedstaaten der Europäischen Union Übereinkünfte mit Drittstaaten oder internationalen Organisationen im Bereich der polizeilichen Zusammenarbeit aushandeln und schließen, sofern diese Übereinkünfte mit dem

Unionsrecht im Einklang stehen. Das gegenständliche Abkommen steht nicht in Widerspruch zu Rechtsvorschriften der Europäischen Union.

7. Besonderheiten des Normerzeugungsverfahrens:

Keine.

Erläuterungen

Allgemeiner Teil

Das 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 hat gesetzändernden bzw. gesetzesergänzenden Inhalt und bedarf daher der Genehmigung durch den Nationalrat gemäß Art. 50 Abs. 1 Z 1 B-VG. Es hat nicht politischen Charakter. Es ist nicht erforderlich, eine allfällige unmittelbare Anwendung des Abkommens im innerstaatlichen Rechtsbereich durch einen Beschluss gemäß Art. 50 Abs. 2 Z 3 B-VG, dass dieser Staatsvertrag durch Erlassung von Gesetzen zu erfüllen ist, auszuschließen. Da durch das Abkommen keine Angelegenheiten des selbständigen Wirkungsbereichs der Länder geregelt werden, bedarf es keiner Zustimmung des Bundesrates gemäß Art. 50 Abs. 2 Z 2 B-VG.

Die Entwicklungen der letzten Jahre in den Bereichen des internationalen Terrorismus und der grenzüberschreitenden Kriminalität haben die Notwendigkeit einer verstärkten internationalen Zusammenarbeit von Polizei und Justiz verdeutlicht. Diesem Ziel dient in den USA der vom US-Kongress im Jahre 2007 angenommene sog. „09/11 Commission Act“. Die USA sind ein wichtiger Partner Österreichs in der grenzüberschreitenden Bekämpfung von schweren Straftaten. Die Zusammenarbeit mit den USA ist im Zeitalter des visafreien Reiseverkehrs daher auch im Interesse des Schutzes österreichischer StaatsbürgerInnen.

Die USA traten im Jahr 2008 mit dem Vorschlag des Abschlusses bilateraler Abkommen im vorstehenden Sinne an Österreich und an andere europäische Staaten heran. Auch in der Erwägung, dass eine solche verstärkte Zusammenarbeit den Schutz der österreichischen BürgerInnen vor internationaler organisierter Kriminalität erhöhen würde, hat die Bundesregierung am 9. März 2010 (siehe Pkt. 18 des Beschl. Prot. Nr. 52) beschlossen, Verhandlungen über ein Abkommen mit den USA zur Zusammenarbeit bei der Verhinderung und Bekämpfung schwerer Straftaten („Agreement on Enhancing Cooperation in Preventing and Combating Serious Crime“, PCSC-Abkommen) aufzunehmen.

Das Verhandlungsmandat der österreichischen Bundesregierung hat hierbei den Abschluss des Abkommens an die Sicherstellung eines aus österreichischer Sicht angemessenen Datenschutzniveaus geknüpft.

Mit Beschluss der Bundesregierung vom 19. Oktober 2010 (sh. Pkt. 18 des Beschl. Prot. Nr. 76) wurde das ausgehandelte Abkommen genehmigt und am 15. November 2010 in Wien unterzeichnet.

Das Abkommen ermöglicht den österreichischen Sicherheitsbehörden eine noch effizientere Zusammenarbeit mit den US-Behörden bei der Bekämpfung schwerer Straftaten einschließlich des Terrorismus.

Der Anwendungsbereich des Abkommens ist auf terroristische und schwerwiegende Straftaten eingeschränkt, die in Artikel 1 des Abkommens definiert werden (Strafdrohung von mehr als einem Jahr Freiheitsstrafe). Hinsichtlich automatisierter Abfragen von daktyloskopischen Daten bzw. DNA-Profilen gemäß Artikel 4 bzw. Artikel 7 beruht der Informationsaustausch auf dem Prinzip der Einzelabfragen und zwar sowie nach dem sog. Treffer-/Nicht-Trefferprinzip (hit-/no hit-Verfahren). Das Treffer-/Nicht-Trefferprinzip sieht vor, dass beim automatisierten Abruf von daktyloskopischen Daten bzw. DNA-Profilen gemäß Artikel 4 bzw. Artikel 7 zunächst nur die Tatsache eines Treffers durch Übermittlung der passenden daktyloskopischen Daten und DNA-Profilen sowie der dazugehörigen Kennungen, mitgeteilt wird. Die Übermittlung weiterer personenbezogener und sonstiger Daten erfolgt gemäß Artikel 5 bzw. 8 in einem zweiten Schritt nach Maßgabe des innerstaatlichen Rechts. Weiters statuieren die Vertragsparteien in Artikel 10 die Möglichkeit, sich unter genau normierten Bedingungen wechselseitig über schwere Straftaten mit einer transnationalen Dimension und terroristische Straftaten auch ohne vorhergehendes Ersuchen zu informieren, sofern die Interessen einer der beiden Vertragsparteien berührt sind.

Neben allgemeinen Datenschutzgrundsätzen (siehe Artikel 11) werden im Abkommen spezifische Übermittlungs- bzw. Verwendungsbeschränkungen (Artikel 12 und 13) sowie Vorgaben zur Gewährleistung der Datenrichtigkeit (Artikel 14), Dokumentation (Artikel 15) und Datensicherheit

(Artikel 16) gemacht. Artikel 17 und 19 beziehen sich auf die datenschutzrechtlichen Optionen der Betroffenen. Artikel 18 sieht zudem die Möglichkeit der Vertragsparteien vor, im Interesse einzelner Betroffener eine Überprüfung von Datenverwendungen durch die Datenschutz- oder sonstige Kontrollbehörden der jeweils anderen Vertragspartei anzuregen.

Mit Artikel 25 wurde eine Suspendierungsklausel in den Abkommenstext aufgenommen, die es erlaubt, die Anwendung von Teilen des Abkommens insgesamt oder von Teilen desselben (zB die Übermittlung von daktyloskopischen Daten via Online-Zugriff) auszusetzen, wenn Verstöße gegen Vertragsbestimmungen feststellbar sind oder wenn sich die Rechtslage in einem der beiden Vertragsparteien so ändert, dass dadurch u.a. der Schutz von übermittelten Daten nicht mehr gewährleistet werden kann.

Das Abkommen steht nicht in Widerspruch zu Rechtsvorschriften der Europäischen Union. Gemäß Erklärung 36 zum Vertrag von Lissabon (BGBl. III Nr. 132/2009) dürfen Mitgliedstaaten der Europäischen Union, Übereinkünfte mit Drittstaaten oder internationalen Organisationen im Bereich der polizeilichen Zusammenarbeit aushandeln und schließen, sofern diese Übereinkünfte mit dem Unionsrecht im Einklang stehen. In Hinblick auf die Schaffung gemeinsamer Datenschutzstandards sind Verhandlungen zwischen der EU und den USA im Gange. Die allfällige Berücksichtigung deren Ergebnis im bilateralen Verhältnis hängt von der Bereitschaft beider Parteien zu Verhandlungen über eine Abkommensänderung gemäß Artikel 26 ab. Unter diesen Rahmenbedingungen soll das Abkommen den österreichischen Sicherheitsbehörden eine noch effizientere Zusammenarbeit mit den US-Behörden bei der Bekämpfung schwerer Straftaten einschließlich des Terrorismus ermöglichen.

Die Kompetenz des Bundes zur Gesetzgebung stützt sich hinsichtlich der sicherheitspolizeilichen Aspekte der Gefahrenabwehr auf Artikel 10 Absatz 1 Ziffer 7 B-VG (Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit) und hinsichtlich der Strafverfolgungsaspekte auf Artikel 10 Absatz 1 Ziffer 6 B-VG (Strafrechtswesen).

Die Regelungen ergänzen die Bestimmungen des Bundesgesetzes über die internationale polizeiliche Kooperation (PolizeiKooperationsgesetz – PolKG; BGBl. I Nr. 104/1997) sowie die mit den USA bestehenden bilateralen Rechtshilferegulungen auf dem Felde der Strafverfolgung.

Besonderer Teil

Zur Präambel

Die Präambel des vorliegenden Abkommens betont in der einleitenden Bestimmung den Wunsch, durch partnerschaftliche Zusammenarbeit schwere Straftaten, insbesondere Terrorismus, zu bekämpfen und dass dabei der Austausch von Informationen ein wesentlicher Faktor ist. Als Vorbild des Abkommens dienen sowohl der Prümer Vertrag (BGBl. III Nr. 159/2006) als auch der Beschluss des Rates 2008/615/JI vom 23. Juni 2008, ABl. Nr. L 210, 1 (Prümer Beschluss), mit dem Teile des Prümer Vertrags in das EU-Recht überführt wurden.

Die im Vertrag geregelte Zusammenarbeit, insbesondere in Form des Informationsaustausches, hat ,unter Achtung der Grundrechte und Grundfreiheiten, insbesondere des Schutzes der Privatsphäre und des Datenschutzes, zu erfolgen. Ausdrücklich Bezug genommen wird in der Präambel auch auf die von der EU-US hochrangigen Kontaktgruppe zum Datenschutz im Bereich der Strafverfolgung ausgearbeiteten allgemeinen Datenschutzprinzipien.

Zu Artikel 1 - Begriffsbestimmungen:

Zu Ziffer 1

Diese Definition entspricht Artikel 2 Buchstabe c des Beschlusses des Rates der Europäischen Union 2008/616/JI vom 23. Juni 2008, ABl. L 210, 12, zur Durchführung des Beschlusses 2008/615/JI vom 23. Juni 2008 (Prümer Durchführungsbeschluss). Sie entspricht auch der in § 21 Absatz 2 des Bundesgesetzes über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union (BGBl. I Nr. 132/2009 idF BGBl. I Nr. 2010/105) enthaltenen Definition, mit dem der Prümer Beschluss und der Prümer Durchführungsbeschluss in der österreichischen Rechtsordnung umgesetzt wurden.

Zu Ziffer 2

Hier werden die sog. Fundstellendatensätze für die Zusammenarbeit bei automatisiertem Abruf von daktyloskopischen Daten gemäß Artikel 3 und DNA-Profilen gemäß Artikel 7 definiert. Diese Fundstellendatensätze umfassen die aus erkennungsdienstlichen Maßnahmen gewonnenen daktyloskopischen Daten oder DNA-Profildaten sowie eine diesen Daten jeweils zugeordnete Kennung. Die Kennung ist notwendig, um die besagten daktyloskopischen und DNA-Daten den damit korrespondierenden direkt personenbezogenen Daten (v.a. Namensdaten) und sonstigen Informationen

zuordnen zu können. Das in der Definition der Z 2 des Artikel 1 enthaltene Verbot, diesen Fundstellendatensätze weitere den Betroffenen unmittelbar identifizierende Daten anzuschließen (zB Geschlecht, Geburtsdatum, Hinweise auf die Tat) entspricht wiederum den Bestimmungen der Artikel 2 Absatz 2 Satz 2 und Artikel 8 Absatz 2 Z 2 des Prümer Vertrags.

Datensätze und die personenbezogenen Daten und sonstigen Informationen sind in getrennten Dateien zu speichern, um

- a) den gegenseitigen automatisierten Abruf oder Abgleich im Hit/No Hit-Verfahren (Treffer-/Nichttrefferverfahren) zu ermöglichen; und
- b) dem Gebot der Verhältnismäßigkeit des Verfahrens (§ 1 Absatz 2 Datenschutzgesetz 2000, § 29 Sicherheitspolizeigesetz) Rechnung zu tragen.

Die Vorgabe, dass Fundstellendatensätze, die keiner Person zugeordnet werden können (offene Spuren) als solche zu kennzeichnen sind, wurde gleichfalls aus dem Artikel 2 Absatz 2 Satz 3 bzw. Artikel 8 Absatz 2 Satz 3 des Prümer Vertrags übernommen, hat aber im Rahmen dieses Abkommens keine Bedeutung, da keine spezielle Form der Zusammenarbeit in Bezug auf offene Spuren vereinbart wurde. Bei den Verhandlungen wurde übersehen, diese Bestimmung zu streichen. Dies hat aber keine praktischen Auswirkungen auf die Zusammenarbeit.

Die österreichische DNA-Datei wird vom Bundesministerium für Inneres (Bundeskriminalamt) auf Grundlage des § 75 Sicherheitspolizeigesetz (BGBl. 1991/566 idgF) geführt. In dieser Datei sind die Fundstellen-Datensätze von den personenbezogenen Daten und sonstigen Informationen getrennt, wie dies vom Vertrag gefordert ist.

Das Abkommen verwendet den englischsprachigen Begriff der DNA (deoxyribonucleic acid) und nicht den deutschsprachigen Begriff der DNS (Desoxyribonucleinsäure). Es folgt damit dem international üblichen Gebrauch, der sich auch in der nationalen Gesetzgebung in Österreich widerspiegelt. Das Sicherheitspolizeigesetz verwendet gleichfalls DNA. Weiters wird der Begriff des DNA-Profiles verwendet, der ausschließlich den nicht codierenden Teil der DNA umfasst.

Zu Ziffer 3

Da im Rahmen des Abkommens nur personenbezogene Daten und sonstige Informationen natürlicher Personen ausgetauscht werden sollen, ist die Definition des Abkommens im Gegensatz zu § 4 Ziffer 1 des Datenschutzgesetzes 2000 (BGBl. I 1999/165 idF BGBl. I Nr. 133/2009) nur auf natürliche Personen beschränkt. Im Übrigen entspricht die Definition des Abkommens jener des Datenschutzgesetzes.

Zu Ziffer 4

Diese Bestimmung entspricht Artikel 33 Absatz 1 Ziffer 1 des Prümer Vertrags. Wobei bei den Verhandlungen zum Prümer Vertrag, um Auslegungsschwierigkeiten zu vermeiden, die sich aus Unterschieden zwischen den einzelstaatlichen rechtssprachlichen Traditionen ergeben könnten, für die Umschreibung der diversen Arten der Handhabung von personenbezogenen Daten auf die in Art. 2 Buchstabe b der EG-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 (ABl. EG Nr. L 281 vom 23.11.1995 S. 31) enthaltene Definition der „Verarbeitung personenbezogener Daten“ zurückgegriffen wurde.

Zu Ziffer 5

„Sperren“ verfolgt dezidiert das Ziel, die künftige Verarbeitung gespeicherter personenbezogener Daten, deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, auf eng begrenzte Zwecke im Interesse des Betroffenen zu beschränken. Da es keine global anerkannte Definition von „terroristischer Straftaten“ gibt, werden diese für Zwecke dieses Abkommens als strafbares Verhalten im Sinne jener internationaler Abkommen verstanden, die für beide Vertragsparteien verbindlich sind. Dies sind insbesondere die sechzehn Terrorismuskonventionen der Vereinten Nationen.

Zu Ziffer 7

Die in dieser Bestimmung vorgenommene Definition schwerer Straftaten ist enger gefasst, als die in der EU übliche Definition derartiger Delikte (vgl. dazu Artikel 2 Absatz 1 des Rahmenbeschlusses 2002/584/JI vom 13. Juni 2002, ABl. L 190 vom 18.7.2002, S. 1, über den Europäische Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten). Abgestellt wird nämlich auf eine Strafdrohung von mehr als einem Jahr Freiheitsstrafe. Insofern ist der Anwendungsbereich des vorliegenden Abkommens mit dem USA eingeschränkter als derjenige, der auf Basis des „Prümer Beschlusses“ im Verhältnis der Mitgliedstaaten der EU untereinander gilt.

Zu Artikel 2 - Zweck und Anwendungsbereich dieses Abkommens:

In Absatz 1 wird der Zweck des Abkommens im Wesentlichen so umschrieben, wie er sich bereits im Titel des Abkommens widerspiegelt.

In Absatz 2 wird der Anwendungsbereich des Abkommens in Bezug auf den automatisierten Abruf von daktyloskopischen Daten und DNA-Profilen präziser als nach dem Prümer Vertrag oder dem Prümer Beschluss geregelt:

1. ist der Abruf nur zur Verhinderung, Aufdeckung und Ermittlung schwerer Straftaten zulässig (siehe Erläuterungen zu Artikel 1 Ziffer 7) und
2. müssen besondere und rechtsgültige Umstände in Bezug auf eine bestimmte Person gegeben sind, die den automatisierten Abruf der Daten rechtfertigen.

Mit dieser Bestimmung soll der willkürliche Abruf von Daten von Personen im Zuge von Routinekontrollen ausgeschlossen werden. Erst bei Vorliegen der in Absatz 2 angeführten qualifizierten Kriterien ist ein derartiger Abruf zulässig.

Zu Artikel 3 - Daktyloskopische Daten:

Auf der Grundlage dieses Vertrags arbeiten die Vertragsparteien im Bereich des automatisierten Austauschs daktyloskopischer Daten zusammen. Der Begriff „daktyloskopische Daten“ umfasst Fingerabdrücke sowie Abdrücke von Hand- oder Fußflächen, also aller jener Körperteile, die Papillarlinien aufweisen. Diese Papillarlinien sind bei jedem Menschen verschieden und ermöglichen die eindeutige Identifizierung dieses Menschen.

Die Zusammenarbeit im Bereich der daktyloskopischen Daten beschränkt sich auf die zum Zwecke der Verhinderung und Verfolgung von Straftaten eingerichtete Dateien, die im Anhang des Abkommens angeführt sind. Für Österreich bedeutet dies, dass ein Zugriff nur auf jene Daten eingeräumt werden darf, die auf der Grundlage des § 75 Sicherheitspolizeigesetz beim Bundeskriminalamt eingerichteten Automatische Fingerabdruck-Informationssystem (AFIS), dort für Zwecke des SPG und/oder der StPO verarbeitet werden. Auf anderer Rechtsgrundlage für administrative Zwecke erhobene Daten (zB für Asyl-, fremdenpolizeiliche oder Passausstellungszwecke) sind von der Einbeziehung in die Zusammenarbeit ausgeschlossen.

Damit eine Zusammenarbeit zwischen den Vertragsparteien möglich wird, verpflichten sich diese, die in ihren nationalen polizeilichen Datenbanken vorhandenen daktyloskopischen Daten im Wege von Fundstellendatensätzen der anderen Vertragspartei zugänglich zu machen. Zum Begriff der Fundstellendatensätze siehe die Erläuterungen zu Artikel 1 Ziffer 2 oben.

Zu Artikel 4 - Automatisierter Abruf daktyloskopischer Daten:

Die Zusammenarbeit im Rahmen des Vertrags erfolgt hinsichtlich der daktyloskopischen Daten in Form des automatisierten Abrufs durch die in Artikel 6 bezeichneten Kontaktstellen. Der automatisierte Abruf ist der Vergleich zwischen einem daktyloskopischen Datum, das bei einer (uzw. der jeweils abrufenden) Vertragspartei vorliegt, mit den daktyloskopischen Daten in der Datei der anderen (der empfangenden) Vertragspartei. Dabei wird das daktyloskopische Datum von der abrufenden Vertragspartei über eine sichere Leitung an die daktyloskopischen Dateien der empfangenden Partei übermittelt und dort mit den vorhandenen Fundstellendatensätzen (siehe Begriffsbestimmung Artikel 1 Ziffer 2) verglichen. Anders als bei DNA-Profilen ist es auf Grund des unterschiedlichen technischen Verfahrens nicht möglich, bereits beim ersten Vergleich eine eindeutige Zuordnung des übermittelten daktyloskopischen Datums mit dem entsprechenden Fundstellendatensatz bei der empfangenden Vertragspartei vorzunehmen. Zur endgültigen Zuordnung muss daher eine in den Durchführungsbestimmungen festzulegende Anzahl annähernd übereinstimmender Fundstellendatensätze von der empfangenden Partei an die abrufende Partei rückübermittelt werden. Vergleich und Übermittlung der annähernd übereinstimmenden Fundstellendatensätze erfolgt automatisiert. Dies bedeutet, dass dieser Vergleich durch ein technisches Verfahren ohne Einbeziehung eines Beamten der empfangenden Vertragspartei abläuft. Bei der abrufenden Vertragspartei erfolgt dann durch einen Experten die eindeutige Zuordnung („Verifikation“) des daktyloskopischen Datums zu einem der automatisiert übermittelten Fundstellendatensätze.

Das Verfahren gemäß Artikel 4 erfolgt in folgenden Schritten:

1. Die abrufende Vertragspartei übermittelt das daktyloskopische Datum.
2. Das übermittelte daktyloskopische Datum wird mit den in den Fundstellendatensätzen vorhandenen daktyloskopischen Daten der empfangenden Vertragspartei automatisiert verglichen.
3. Von der empfangenden Vertragspartei wird automatisiert eine festgelegte Anzahl ähnlicher Fundstellendatensätze der abrufenden Vertragspartei zur Verifikation übermittelt.

4. Durch einen Experten der abrufenden Vertragspartei erfolgt die eindeutige Zuordnung des daktyloskopischen Datums zu einem der übermittelten Fundstellendatensätze oder die endgültige Feststellung, dass kein Treffer erzielt wurde.
5. Das weitere Verfahren bei Vorliegen eines Treffers erfolgt im Wege der Amts- oder Rechtshilfe gemäß Artikel 5.

Auf Seiten der empfangenden Vertragspartei verläuft das Verfahren durchgängig automatisiert. Die Einzelheiten des technischen Verfahrens werden gemäß Artikel 6 Ziffer 2 in einer Durchführungsvereinbarung geregelt. Der gemäß Artikel 7 vorgesehene automatisierte Abruf von DNA-Profilen entspricht in seinem technischen Verfahren etwa dem automatisierten Abruf von daktyloskopischen Daten.

Der automatisierte Abruf darf nur im Einzelfall erfolgen. Das heißt, die abrufende Vertragspartei darf jeweils nur ein daktyloskopisches Datum mit den Fundstellendatensätzen der empfangenden Vertragspartei vergleichen. Der Vergleich darf nur zur Verhinderung und Verfolgung von schweren Straftaten (siehe Definition in Artikel 1 Ziffer 2), nach Maßgabe der in Artikel 2 Absatz 2 beschriebenen Umstände und des Rechts der abrufenden Vertragspartei erfolgen. Jede Vertragspartei kann daher unter denselben Bedingungen auf die daktyloskopische Dateien der anderen Vertragspartei zugreifen, wie sie für den Zugriff auf die eigenen daktyloskopischen Dateien gelten. Die Prüfung der Zulässigkeit erfolgt nur nach Maßgabe der Bestimmungen dieses Vertrags und dem jeweilig geltenden innerstaatlichen Recht.

Nach § 65 Sicherheitspolizeigesetz sind die Sicherheitsbehörden ermächtigt, eine Person, die im Verdacht steht, eine mit Strafe bedrohte Handlung begangen zu haben, erkennungsdienstlich zu behandeln, wenn diese im Rahmen einer kriminellen Organisation tätig wurde oder dies sonst auf Grund von Umständen in der Person des Betroffenen oder nach der Art der begangenen mit Strafe bedrohten Handlung zur Vorbeugung gefährlicher Angriffe des Betroffenen erforderlich erscheint. Gemäß § 118 Absatz 1 StPO kann eine Identitätsfeststellung vorgenommen werden, wenn auf Grund bestimmter Tatsachen angenommen werden kann, dass eine Person an einer Straftat beteiligt ist, über die Umstände der Begehung Auskunft geben kann oder Spuren hinterlassen hat, die der Aufklärung dienen könnten. Soweit dies zur Identitätsfeststellung erforderlich ist, ist die Kriminalpolizei dazu ermächtigt, u.a. die Papillarlinienabdrücke der betroffenen Personen abzunehmen.

Aus dem Gesagten folgt, dass die Schwelle für die Gewinnung von daktyloskopischen Daten insofern deutlich niedriger liegt als jene für die Übermittlung solcher Daten zwecks automatisiertem Abgleich in die USA.

Zur Verarbeitung der gemäß Artikel 4 übermittelten Daten werden in Art. 13 Absatz 4 besondere datenschutzrechtliche Bestimmungen vereinbart. Weiters ist gemäß Artikel 15 Absatz 2 Buchstabe b jeder automatisierte Abruf sowohl von der abrufenden als auch der empfangenden Vertragspartei zu protokollieren (doppelte Protokollierung).

Zu Artikel 5 - Übermittlung weiterer personenbezogener und sonstiger Daten:

Der automatisierte Abruf von daktyloskopischen Daten erfolgt im Hit/No Hit-Verfahren (Treffer-/Nichttrefferverfahren). Zunächst wird daher festgestellt, ob in einer der Dateien der anderen Vertragspartei ein übereinstimmender Fundstellendatensatz vorhanden ist. Wird ein Treffer erzielt, richtet die anfragende Partei ein Ersuchen um Übermittlung der weiteren personenbezogenen Daten und sonstigen Informationen an die andere Vertragspartei.

Die Anfrage wird nach dem nationalen Recht der anfragenden Vertragspartei in Form eines Amts- oder Rechtshilfeverfahrens gestellt. Österreich kann diese Anfrage im Rahmen der polizeilichen Amtshilfe nach § 6 ff Polizeikooperationsgesetz iVm den Artikel 4 und 5 des vorliegenden Abkommens stellen bzw. gemäß §§ 3 und 5 Polizeikooperationsgesetz (BGBl. I 1977/104 idgF) iVm mit den Artikel 4 und 5 des vorliegenden Abkommens eingehende Anfragen auf dieser Rechtsgrundlage beantworten.

Zu Artikel 6 - Nationale Kontaktstellen und Durchführungsvereinbarungen:

Der automatisierte Abruf von daktyloskopischen Daten gemäß Artikel 4 und die Übermittlung weiterer personenbezogener Daten gemäß Artikel 5 erfolgt ausschließlich über die nationalen Kontaktstellen. Diese werden von den Vertragsparteien benannt. Für Österreich wird die Generaldirektion für die öffentliche Sicherheit, Bundeskriminalamt, als nationale Kontaktstelle benannt. Der Vertrag trifft keine Aussagen über die Befugnisse der nationalen Kontaktstellen, sondern überlässt dies dem nationalen Recht. Dieser Datenaustausch soll nach Möglichkeit im Wege des Amtshilfeverfahrens erfolgen. Über die österreichischen Möglichkeiten zur Nutzung des Amtshilfeweges siehe die Erläuterungen zu Artikel 5. Nur wenn es notwendig wird, solche Daten für ein Strafverfahren zu authentifizieren, hat der Datenaustausch im Wege eines Rechtshilfeverfahrens zu erfolgen. Der Rechtshilfeverkehr in Strafsachen zwischen Österreich und den USA findet die Grundlage des Vertrags zwischen der Regierung der

Republik Österreich und der Regierung der Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen vom 23. Februar 1995, BGBl. III Nr. 107/1998, in der Fassung des Protokolls vom 20. Juli 2005 im Sinne des Artikels 3 Absatz 2 des am 25. Juni 2003 unterzeichneten Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe, BGBl. III Nr. 7/2910, statt.

In Absatz 2 sieht Artikel 6 hinsichtlich des automatisierten Abrufs von daktyloskopischen Daten zwingend den Abschluss von Durchführungsvereinbarungen vor.

Zu Artikel 7 - Automatisierter Abruf von DNA-Profilen:

In Artikel 7 wird Zusammenarbeit im Bereich des automatisierten Abrufs von DNA-Profilen festgelegt. Die Begriffsbestimmung von DNA-Profilen erfolgt in Artikel 1 Ziffer 1. Der automatisierte Abruf ist der Vergleich zwischen einem DNA-Profil, das bei der einen (uzw. der jeweils abrufenden) Vertragspartei vorliegt, mit den DNA-Profilen in der Datei der anderen (der empfangenden) Vertragspartei. Dabei wird das DNA-Profil von der abrufenden Vertragspartei über eine sichere Leitung an die DNA-Analyse-Datei der empfangenden Partei übermittelt und dort automatisiert mit den vorhandenen Fundstellendatensätzen (siehe Begriffsbestimmung in Artikel 1 Ziffer 2) verglichen. Die Trennung von DNA-Profilen und der damit verbundenen Kennung von den sonstigen, den Betroffenen unmittelbar identifizierenden, Daten hat gemäß Artikel 1 Ziffer 2 zu erfolgen. Automatisiert heißt, dass dieser Vergleich durch ein technisches Verfahren ohne Einbeziehung eines Beamten der empfangenden Vertragspartei erfolgt. Die Einzelheiten dieses technischen Verfahrens werden gemäß Artikel 9 in einer Durchführungsvereinbarung geregelt. Ein analoges Verfahren ist gemäß Artikel 4 für den automatisierten Abruf von daktyloskopischen Daten vorgesehen.

Anders als bei daktyloskopischen Daten ist bei der Zusammenarbeit gemäß Artikel 7 auf die Zulässigkeit dieser Zusammenarbeit nach dem innerstaatlichen Recht beider Vertragsparteien und die ausdrückliche Gegenseitigkeit dieser Zusammenarbeit abgestellt. Dazu findet sich auch in Artikel 27 Absatz 2 eine eigene Bestimmung über das Inkrafttreten der Artikel 7 – 9.

Der automatisierte Abruf darf nur im Einzelfall erfolgen. Das heißt, die abrufende Vertragspartei darf jeweils nur ein DNA-Profil mit den Fundstellendatensätzen der empfangenden Vertragspartei vergleichen. Der Vergleich darf nur zur Verfolgung von schweren Straftaten (Begriffsbestimmung siehe Artikel 1 Ziffer 7), nach Maßgabe der in Artikel 2 Absatz 2 beschriebenen Umstände und des Rechts der abrufenden Vertragspartei erfolgen. Die Zwecke der Zusammenarbeit nach Artikel 7 sind enger gefasst, als jene nach Artikel 4. DNA-Profile dürfen nur zur Aufklärung von schweren Straftaten, aber nicht zur Verhinderung dieser automatisiert abgerufen werden.

Gemäß § 67 Absatz 1 Sicherheitspolizeigesetz darf die DNA einer Person im Rahmen deren erkennungsdienstlicher Behandlung ermittelt werden, wenn der Betroffene im Verdacht steht, einen gefährlichen Angriff gemäß § 16 Sicherheitspolizeigesetz begangen zu haben und wenn in Hinblick auf diese Tat oder die Persönlichkeit des Betroffenen erwartet werden kann, dieser werde bei Begehung weiterer gefährlicher Angriffe Spuren hinterlassen, die seine Wiedererkennung auf Grund der ermittelten genetischen Informationen ermöglichen würde. Unter denselben Bedingungen dürfen DNA-Profile und die vorhandenen personenbezogenen Daten und sonstigen Informationen gespeichert und abgerufen werden. Wie bereits im Rahmen des automatisierten Abrufs von daktyloskopischen Daten ist somit aus der Perspektive der österreichischen Behörden auch bei DNA-Profilen auf das Auseinanderfallen der Bedingungen für die Ermittlung von DNA-Profilen und jenen für deren Übermittlung in die USA zu unterscheiden. Konkret bedeutet dies, dass für die Übermittlung in die USA eine höhere Schwelle gilt als beispielsweise für den innerstaatlichen Abgleich von DNA-Profilen aus Tatortspuren gegen die österreichische DNA-Analysedatei.

Nicht nur der Vergleich des übermittelten DNA-Profiles erfolgt automatisiert, sondern auch die Mitteilung eines Treffers. Treffer ist die Übereinstimmung des von der abrufenden Vertragspartei übermittelten DNA-Profiles mit einem DNA-Profil in der DNA-Analyse-Datei der empfangenden Vertragspartei. Mit der automatisierten Mitteilung des Treffers wird auch die Kennung des passenden DNA-Profiles mitgeteilt. Durch die Übermittlung der Kennung wird die nachfolgende Anfrage gemäß Artikel 8 zur Übermittlung weiterer personenbezogener Daten und sonstiger Informationen erleichtert. Wird kein Treffer erzielt, wird dies gleichfalls automatisiert mitgeteilt.

Das Verfahren gemäß Artikel 7 erfolgt in folgenden Schritten:

1. Die abrufende Vertragspartei übermittelt das DNA-Profil.
2. Das übermittelte DNA-Profil wird mit den in den Fundstellendatensätzen vorhandenen DNA-Profilen der empfangenden Vertragspartei automatisiert verglichen.

3. Die Tatsache eines Treffers wird gemeinsam mit der Kennung automatisiert der abrufenden Vertragspartei mitgeteilt.
4. Gleichfalls automatisiert erfolgt die Mitteilung, dass kein Treffer vorliegt.
5. Das weitere Verfahren bei Vorliegen eines Treffers erfolgt im Wege der Amts- oder Rechtshilfe gemäß Artikel 8.

Auf Seiten der empfangenden Vertragspartei verläuft das Verfahren durchgängig automatisiert. Außer der Kennung und dem Vorliegen oder Nichtvorliegen eines Treffers werden keine Daten von der empfangenden Partei an die abrufende Partei übermittelt. Zur Verarbeitung der gemäß Artikel 7 übermittelten Daten werden in Art. 13 Absatz 4 besondere datenschutzrechtliche Bestimmungen vereinbart. Weiters ist gemäß Artikel 15 Absatz 2 Buchstabe b jeder automatisierte Abruf sowohl von der abrufenden als auch der empfangenden Vertragspartei zu protokollieren (doppelte Protokollierung).

Zu Artikel 8 - Übermittlung weiterer personenbezogener und sonstiger Daten:

Der automatisierte Abruf und der automatisierte Abgleich von DNA-Profilen erfolgt im Hit/No Hit-Verfahren (Treffer-/Nichttrefferverfahren). Zunächst wird daher festgestellt, ob in den DNA-Analyse-Dateien der anderen Vertragspartei ein übereinstimmender Fundstellendatensatz vorhanden ist. Wird ein Treffer erzielt, richtet die anfragende Partei ein Ersuchen um Übermittlung der weiteren personenbezogenen Daten und sonstigen Informationen an die andere Vertragspartei.

Die Anfrage wird nach dem nationalen Recht der anfragenden Vertragspartei in Form eines Amts- oder Rechtshilfeverfahrens gestellt. Österreich kann diese Anfrage im Rahmen der polizeilichen Amtshilfe nach § 6 ff Polizeikooperationsgesetz iVm den Artikel 7 und 8 des vorliegenden Abkommens stellen bzw. gemäß §§ 3 und 5 Polizeikooperationsgesetz iVm mit den Artikel 7 und 8 des vorliegenden Abkommens eingehende Anfragen auf dieser Rechtsgrundlage beantworten.

Zu Artikel 9 - Nationale Kontaktstelle und Durchführungsvereinbarungen:

Der automatisierte Abruf von DNA-Profilen gemäß Artikel 7 und die Übermittlung weiterer personenbezogener Daten gemäß Artikel 8 erfolgt ausschließlich über die nationalen Kontaktstellen. Diese werden von den Vertragsparteien benannt. Für Österreich wird die Generaldirektion für die öffentliche Sicherheit, Bundeskriminalamt, als nationale Kontaktstelle benannt. Der Vertrag trifft keine Aussagen über die Befugnisse der nationalen Kontaktstellen, sondern überlässt dies dem nationalen Recht. Nach dem Abkommen soll dieser Datenaustausch nach Möglichkeit im Wege des Amtshilfeverfahrens erfolgen. Über die österreichischen Möglichkeiten zur Nutzung des Amtshilfeweges siehe die Erläuterungen zu Artikel 8. Nur wenn es notwendig wird, solche Daten für ein Strafverfahren zu authentifizieren hat der Datenaustausch im Wege eines Rechtshilfeverfahrens zu erfolgen. Der Rechtshilfeverkehr in Strafsachen zwischen Österreich und den USA findet auf Grundlage des Vertrags zwischen der Regierung der Republik Österreich und der Regierung der Vereinigten Staaten von Amerika über die Rechtshilfe in Strafsachen vom 23. Februar 1994, BGBl. III Nr. 107/1998, in der Fassung des Protokolls vom 20. Juli 2005 im Sinne des Artikels 3 Absatz 2 des am 25. Juni 2003 unterzeichneten Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe, BGBl. III Nr. 7/2010, statt.

In Absatz 2 sieht Artikel 9 hinsichtlich des automatisierten Abrufs von DNA-Profilen zwingend den Abschluss von Durchführungsvereinbarungen vor.

Zu Artikel 10 - Übermittlung personenbezogener und anderer Daten zur Verhinderung schwerer Straftaten mit einer transnationalen Dimension und terroristischer Straftaten:

Diese Bestimmung weist einen im Vergleich zum Vorbild des Artikel 16 Prümer Vertrag deutlich erweiterten Anwendungsbereich auf. Zu „terroristischen Straftaten“ kommen damit verbundene Straftaten, Straftaten, die einen Bezug zu einer terroristischen Gruppe oder Vereinigung haben und nach dem Recht der anfragenden Vertragspartei gerichtlich strafbar sind, die Absolvierung einer Ausbildung zur Begehung solcher Kriminalität sowie schwere Straftaten mit einer transnationalen Dimension hinzu., Auch der Kreis der zur Übermittlung zugelassenen Datenarten wurde im Vergleich zu Artikel 16 Absatz 2 Prümer Vertrag insbesondere durch die Einbeziehung erkennungsdienstlicher Daten ausgeweitet. Diese Erweiterung erscheint vor dem Hintergrund der Einbeziehung der vorgenannten Tatbestände zweckmäßig und vertretbar.

Beide Vertragsparteien gingen in den Verhandlungen davon aus, dass unter Straftaten grenzüberschreitender Natur solche i.S. Artikel 3 Absatz 2 des Übereinkommens der Vereinten Nationen gegen die grenzüberschreitende organisierte Kriminalität zu verstehen sind. Demnach ist eine Straftat grenzüberschreitender Natur (transnational) wenn sie

- a) in mehr als einem Staat begangen wird;

- b) in einem Staat begangen wird, jedoch ein maßgeblicher Teil ihrer Vorbereitung, Planung, Leitung oder Kontrolle in einem anderen Staat stattfindet;
- c) in einem Staat begangen wird, jedoch eine organisierte kriminelle Gruppe an ihr mitwirkt, die in mehr als einem Staat kriminellen Tätigkeiten nachgeht, oder
- d) die in einem Staat begangen wird, jedoch erhebliche Auswirkungen in einem anderen Staat hat.

Die Zusammenarbeit nach Artikel 10 erfolgt nur im Einzelfall und wenn durch die genannten Straftaten die Interessen einer der Vertragsparteien betroffen werden. Weiters müssen bestimmte Tatsachen die Annahme rechtfertigen, dass der oder die Betroffene diese Handlungen begehen werden oder begangen haben.

Die Übermittlung erfolgt nach Maßgabe des innerstaatlichen Rechts der übermittelnden Partei im Wege von nationalen Kontaktstellen. Die österreichische Rechtsgrundlage für die Übermittlung derartiger Informationen und Daten ist die Leistung der internationalen polizeilichen Amtshilfe gemäß § 3 Polizeikooperationsgesetz. Durch den Abschluss dieses Vertrags wird die vom Polizeikooperationsgesetz geforderte völkerrechtliche Verpflichtung geschaffen und die Gegenseitigkeit sichergestellt. Die Bestimmungen des § 8 Polizeikooperationsgesetz (Datenschutz) sind bei der Prüfung der Zulässigkeit der Übermittlung personenbezogener Daten heranzuziehen.

Absatz 3 entspricht grundsätzlich Art. 16 Absatz 4 Prümmer Vertrag. Der Verweis auf Verpflichtungen der Vertragsparteien, die sich aus dem Völkerrecht ergeben, wurde auf österreichischen Wunsch aufgenommen. Damit hat Österreich die Möglichkeit, Bedingungen für die Nutzung der übermittelten Daten in US-Gerichtsverfahren zu stellen.

Mit der Bestimmung in Absatz 4 soll vermieden werden, dass die Vertragsparteien auf der Grundlage von Absatz 3 jede Übermittlungen gemäß Artikel 10 unter Bedingungen stellen. Absatz 5 sieht die Übermittlung sonstiger nicht personenbezogener Informationen vor. Dafür gelten die gleichen Bedingungen, wie für die Übermittlung personenbezogener Daten.

Die Übermittlung von Informationen zur Verhinderung terroristischer Straftaten erfolgt ausschließlich über nationale Kontaktstellen, wobei jede Vertragspartei mehrere Kontaktstellen benennen kann. Für Österreich werden

- a) für schwere Straftaten mit transnationaler Dimension die Generaldirektion für die öffentliche Sicherheit, Bundeskriminalamt und
- b) für terroristische Straftaten die Generaldirektion für die öffentliche Sicherheit, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung

als nationale Kontaktstellen benannt. Der Vertrag trifft keine Aussagen über die Befugnisse der nationalen Kontaktstellen, sondern überlässt dies dem nationalen Recht.

Zu Artikel 11 - Allgemeine Prinzipien des Datenschutzes:

In Absatz 1 anerkennen beide Vertragsparteien die Bedeutung des Datenschutzes bei der Umsetzung und Anwendung des Abkommens. Diese Vereinbarung schließt an die, in dieselbe Richtung weisenden Erwägungsgründe in der Präambel an und wird in den folgenden Bestimmungen der Artikel 11 bis 20 konkretisiert. In Absatz 2 werden die dem Abkommen zu Grunde liegenden allgemeinen Datenschutzprinzipien angeführt und deren Einhaltung für beide Vertragsparteien verpflichtend gemacht. Die angeführten Prinzipien entsprechen bis auf jenen der Zweckbindung jenen, die dem österreichischen Datenschutzgesetz 2000 zu Grunde liegen.

Das Datenschutzregime des Abkommens richtet sich nach Absatz 3 des Artikels 11 ausschließlich an die Vertragsparteien. Damit wird klargestellt, dass Privatpersonen direkt aus dem Abkommen keine Rechte ableiten können. Diese Bestimmung ist Ausfluss des Konzepts des indirekten Schutzes der Interessen von betroffenen Personen, welches das Abkommen kennzeichnet.

In Absatz 4 wird auf jene nationalen Stellen verwiesen, die nach dem jeweiligen innerstaatlichen Recht für die rechtliche Kontrolle des Datenschutzes zuständig sind. Während dies auf österreichischer Seite, die unabhängige Datenschutzkommission ist, nehmen auf US-Seite sogenannte Chief Privacy Officer diese Aufgabe wahr. Diese sind grundsätzlich Beamte des jeweiligen Ministeriums (Justiz oder Heimatschutz), genießen aber in Bezug auf ihre Tätigkeit eine Sonderstellung, da sie direkt gegenüber dem Kongress berichtspflichtig sind.

Zu Artikel 12 - Zusätzlicher Schutz bei der Übermittlung von personenbezogenen Daten besonderer Kategorien:

Artikel 12 sieht den zusätzlichen Schutz besonderer Kategorien von Daten vor. Die in Absatz 1 angeführten besonderen Kategorien von Daten entsprechen den in § 4 Z 2 DSG 2000 angeführten sog.

„sensiblen Daten“. Diese Daten dürfen nach dem Abkommen nur zur Verfügung gestellt werden, wenn sie für die Zwecke des Abkommens besonders relevant sind. Die Übermittlung derartiger Daten auf der Grundlage dieses Abkommens ist nur gemäß Artikel 10 denkbar, da bei der Zusammenarbeit nach den Artikeln 4 und 7 nur die Übermittlung von daktyloskopischen Daten und DNA-Profilen sowie den dazugehörigen Kennungen vorgesehen ist. Nach Absatz 2 sind für die Verwendung derartiger Daten darüber hinaus besondere Schutzvorkehrungen vorzusehen.

Zu Artikel 13 - Verwendungsbeschränkungen zum Schutz personenbezogener und sonstiger Daten:

In Absatz 1 wird der in Artikel 11 Absatz 2 Buchstabe b vereinbarte Grundsatz der Zweckbindung der übermittelten Daten konkretisiert. Diese Bestimmung entspricht vom Regelungsansatz her Artikel 35 Absatz 1 Prümer Vertrag. Nach Artikel 10 Absatz 3 können im Einzelfall noch weitere Auflagen zur Verwendung von übermittelten Daten vorgesehen werden.

Nach Absatz 2 ist die Weitergabe von im Rahmen des Abkommens übermittelten Daten an Drittstaaten, internationale Organe (zB Interpol oder die Vereinten Nationen) oder Private nur mit ausdrücklicher und dokumentierter Zustimmung der übermittelnden Vertragspartei sowie unter Einhaltung geeigneter Schutzvorkehrungen zulässig. Das Abkommen legt keine weitere Grundsätze für die Weiterleitung dieser Daten an die genannten Stellen vor, sondern überlässt dies der Prüfung durch die übermittelnde Vertragspartei. Österreich wird zur Beurteilung der Zulässigkeit von Anfragen der USA zur Weiterleitung solcher Daten auf die Bestimmungen der Artikel 13 und 14 des Rahmenschlusses 2008/977/JI vom 27. November 2008, zurückgreifen.

Die Absätze 3 und 4 sind als eine Konkretisierung des allgemeinen Grundsatzes der Zweckbindung mit Blick für die spezifischen Fälle des automatisierten Abrufes aus Dateien nach den Art. 4 und 7 des Übereinkommens zu verstehen und entsprechen im Wesentlichen Artikel 35 Absatz 2 Prümer Vertrag.

Zu Artikel 14 - Berichtigung, Sperrung und Löschung von Daten:

Gemäß Artikel 11 Absatz 1 Buchstabe c verpflichten sich die Vertragsparteien ua. die Richtigkeit, Aktualität, Angemessenheit und Relevanz sicherzustellen. Dazu korrespondierend legt Artikel 14 Absatz 1 die Verpflichtung der empfangenden Vertragspartei fest, über Verlangen der übermittelnden Vertragspartei, übermittelte Daten auf Grund bestimmter, von der übermittelnden Vertragspartei festgestellter Gründe, zu sperren oder zu löschen. Der Begriff des „Sperrens“ wird in Artikel 1 Ziffer 5 definiert. Diese Bestimmung ist wesentlicher Teil des besonderen Datenschutzregimes, das im Rahmen des Abkommens vereinbart wurde und das bereits bei den Erläuterungen zu Artikel 11 Absatz 3 Erwähnung fand.

Nach Absatz 2 wird die empfangende Vertragspartei verpflichtet, bei übermittelten Daten, deren Unrichtigkeit sie festgestellt hat, von sich aus umgehend die notwendigen Maßnahmen zu ergreifen, um die Verwendung dieser unrichtigen Daten auszuschließen. Dazu werden beispielhaft die Maßnahmen der Ergänzung, Löschung, Berichtigung und als ergänzende Maßnahme, die Kennzeichnung genannt.

Gemäß Absatz 3 besteht für die empfangende Vertragspartei auch die Verpflichtung, auf die zweifelsfreie Richtigkeit und Verlässlichkeit der an sie übermittelten Daten zu achten und gegebenenfalls die übermittelnde Vertragspartei über unrichtige, unzuverlässige oder zweifelhafte Daten zu informieren.

Absatz 4 legt ausdrücklich die Verpflichtung beider Vertragsparteien fest, bei einer geplanten Löschung die Interessen des Betroffenen zu berücksichtigen. Hier ist im Interesse des Betroffenen vom Instrument der Sperrung Gebrauch zu machen. Nach Aufhebung der Sperrung können die Daten nach Maßgabe des Abkommens weiter verwendet werden.

Zu Artikel 15 - Dokumentation:

Den Dokumentationspflichten nach dieser Bestimmung kommt eine zentrale Bedeutung zu. Ihre strikte Einhaltung ist die Voraussetzung für die wirksame nachprüfende Kontrolle der Rechtmäßigkeit von Datenübermittlungen. Die Bestimmungen entsprechen im Wesentlichen Artikel 39 Prümer Vertrag. Bemerkenswert ist, dass eine generelle „Vollprotokollierung“ angeordnet wird, dh. jede Übermittlung und jeder Empfang personenbezogener Daten sind in Bezug auf Anlass, Inhalt, Datum etc. festzuhalten (vgl. Absatz 1 und Absatz 2 Buchstabe b). Darüber hinaus hat bei den automationsunterstützten Abrufverfahren nach Artikel 4 und 7 die jeweils anfragende Stelle nicht nur jene Person zu protokollieren die einen automatisierten Abruf durchführt, sondern auch jene, die die Anfrage veranlasst hat. Auf diese Weise soll die Rückverfolgbarkeit von automatisierten Abrufen nicht nur bis zu einem bestimmten Terminal in einer Zentralstelle ermöglicht werden, sondern bis hin zu jener Person, die die Information letztlich in einem bestimmten Fall angefordert bzw. verwendet hat.

Sowohl im Falle der konventionellen Datenübermittlung als auch im Fall des automatisierten Abrufes sind die Protokolldaten zwei Jahre aufzubewahren und danach unverzüglich zu löschen, sofern keine rechtliche Verpflichtung nach dem innerstaatlichen Recht dagegen steht.

Zu Artikel 16 - Datensicherheit:

Die Besonderheit der automationsunterstützten Abrufverfahren (vgl. dazu Artikel 4 und 7 des Abkommens) erfordert besondere technische Vorkehrungen zur Gewährleistung von Datenschutz und Datensicherheit. Um das vorliegende Abkommen nicht mit technischen Details zu überfrachten, deren konkrete Ausgestaltung zudem vom jeweiligen „Stand der Technik“ abhängt, verweist Artikel 16 auf die zu den Artikeln 4 und 7 auszuarbeitenden Durchführungsvereinbarungen, die zudem in Artikel 6 Absatz 2 bzw. 9 Absatz 2 Erwähnung finden.

Zu Artikel 17- Transparenz, Bereitstellen von Information an die Betroffenen:

In Absatz 1 wird ausdrücklich darauf verwiesen, dass durch das im Abkommen vereinbarte spezifische Datenschutzregime (siehe dazu die Anmerkungen zu Artikel 11 Absatz 3 und Artikel 14 Absatz 1) bestehenden Pflichten der Vertragsparteien zur Gewährleistung des Datenschutzes nach rein innerstaatlichem Recht nicht beeinträchtigt werden.

In Absatz 2 sind Gründe angeführt, nach denen Auskünfte über Datenverarbeitung unter dem Abkommen in Übereinstimmung mit dem nationalen Recht der betroffenen Vertragspartei verweigert werden können. Die in dieser Bestimmung aufgeführten Gründe für Auskunftsverweigerungen sind den in § 26 Absatz 2 des Datenschutzgesetzes genannten Gründen vergleichbar.

Zu Artikel 18 - Überprüfung:

In Artikel 18 wird das Recht der Vertragsparteien statuiert, sich wechselseitig auch dann zu konsultieren, wenn Interessen Einzelner an der Überprüfung der Rechtmäßigkeit einer sie betreffenden Datenverwendung durch eine Datenschutzbehörde der jeweils anderen Vertragspartei angesprochen sind. Konkret bedeutet dies, dass sich ein Betroffener zwar nach Maßgabe des für ihn geltenden nationalen Rechts nur an jene nationalen Stellen seines Staates, die gemäß Artikel 11 Absatz 4 für die Umsetzung der Datenschutzbestimmungen zuständig sind wenden kann. Diese Stelle wiederum kann dann bei Bedarf unter Berufung auf Artikel 18 die gemäß Artikel 11 Absatz 4 zuständige Behörde der anderen Vertragspartei mit dem Ersuchen um Überprüfung der Rechtmäßigkeit der Verarbeitung der übermittelten Daten herantreten. Die Behörde der anderen Vertragspartei an die diese Anfrage ergangen ist, hat Anfragen der anderen Vertragspartei zügig zu erledigen (vgl. Art. 18 letzter Satz). Diese Form der Zusammenarbeit zwischen den Vertragsparteien zum Zwecke des Datenschutzes besteht neben der in Artikel 14 vereinbarten amtswegigen Zusammenarbeit zur Berichtigung, Sperrung und Löschung von Daten und lässt diese unberührt.

Zu Artikel 19 – Antrag von Personen auf Zugang zu und Berichtigung, Sperrung und Löschung von Daten:

Diese Bestimmung korrespondiert mit der Zusammenarbeit zwischen den Vertragsparteien nach Artikel 18 und hält fest, dass sich Betroffene nach ihrem jeweiligen nationalen Recht, an die für sie zuständige Datenschutzbehörde oder eine andere zuständige Behörde wenden können. Welche Behörden dies sind, geben die Vertragsparteien einander gemäß Artikel 11 Absatz 4 bekannt. Die für Österreich zuständige Datenschutzbehörde ist die Datenschutzkommission. Die direkte Zusammenarbeit zwischen den Datenschutzbehörden bzw. -stellen zu Zwecken des Datenschutzes ist in Artikel 18 geregelt.

Zu Artikel 20 - Unterrichtung:

Im Lichte der sehr unterschiedlichen nationalen Datenschutzsysteme vereinbaren die Vertragsparteien, sich über diese zu informieren und vor allem Änderungen dieser nationalen Bestimmungen der anderen Vertragspartei bekannt zu geben.

Die Bestimmung des Absatzes 2 bezieht sich primär auf die Wahrnehmung von polizeilichen und Strafverfolgungsinteressen. Hinsichtlich der Überprüfung einer Datenverwendung im Interesse einzelner Betroffener wird im Übrigen auf Artikel 18 letzter Satz verwiesen.

Zu Artikel 21 - Verhältnis zu anderen Verträgen:

Dieser Artikel legt fest, dass dieses Abkommen den Informationsaustausch im Bereich der Strafverfolgung zwischen Österreich und den USA auf der Grundlage von Bestimmungen eines anderen Vertrags, von sonstigen Absprachen oder des innerstaatlichen Rechts, nicht beschränkt oder beeinträchtigt.

Zu Artikel 22 - Konsultationen:

Das Abkommen sieht regelmäßige Konsultationen sowohl über dessen Umsetzung als auch über Entwicklungen auf EU-US Ebene hinsichtlich des Schutzes personenbezogener Daten im Bereich der Strafverfolgung vor. Letzteres ist insbesondere im Hinblick auf den möglichen Abschluss eines EU-US Datenschutzabkommens von Bedeutung. Des Weiteren werden Konsultationen als Mittel zur Streitbeilegung festgelegt.

Zu Artikel 23 - Kosten:

Jede Vertragspartei hat die Kosten, die ihr bei der Umsetzung des Abkommens entstehen, selbst zu tragen, es sei denn, die Vertragsparteien vereinbaren fallbezogen etwas anderes.

Zu Artikel 24 - Kündigung des Abkommens:

Die Kündigungsklausel ermöglicht eine – im Vergleich zu anderen Abkommen – kurzfristige Kündigung des Abkommens (drei Monate nach schriftlicher Mitteilung der Kündigung). Gleichzeitig wird festgelegt, dass das Abkommen auf vor der Kündigung übermittelte Daten weiterhin Anwendung findet.

Zu Artikel 25 - Aussetzung:

Dieser Artikel enthält eine Suspendierungsklausel, die es erlaubt, die Anwendung von Teilen des Abkommens (zB Datenübermittlung mittels automatisiertem Abgleich von daktyloskopischen Daten) auszusetzen, wenn Verstöße gegen Vertragsbestimmungen feststellbar sind oder wenn sich die Rechtslage in einer der beiden Vertragsparteien so ändert, dass dadurch ua. der Schutz von übermittelten Daten nicht mehr gewährleistet werden kann.

Zu Artikel 26 - Änderungen:

Jede der Vertragsparteien kann Konsultationen über Änderungen des Abkommens verlangen. Eine Änderung unterliegt jedoch der Schriftform und den sonst üblichen Vertragsabschlussverfahren.

Zu Artikel 27 - Inkrafttreten:

Das Abkommen tritt nach dem üblichen diplomatischen Notenwechsel in Kraft, durch den die Erfüllung der jeweiligen innerstaatlichen Voraussetzungen für das Inkrafttreten mitgeteilt wurde. Das Inkrafttreten der Artikel 7 bis 9 (DNA-Austausch und Übermittlung weiterer personenbezogener Daten) wird jedoch zusätzlich vom Abschluss der in Artikel 9 vorgesehenen Durchführungsvereinbarungen und der Bestätigung der Gegenseitigkeit hinsichtlich der Durchführung dieser Artikel (das ist gegeben, wenn das Recht beider Vertragsparteien den DNA-Austausch erlaubt) abhängig gemacht.

Zum Anhang:

Zu dem von österreichischer Seite benannten automatisierten daktyloskopischen Identifizierungssystem siehe die Anmerkungen zu Artikel 3.