ERKLÄRUNG

Die Europäische Union hat verschiedene Initiativen zur Verbesserung der Effizienz der Strafverfolgung und des Kampfes gegen den Terrorismus in der Europäischen Union eingeleitet. In diesem Zusammenhang ist der Austausch von Informationen zur Strafverfolgung in Übereinstimmung mit dem Verfügbarkeitsgrundsatz („principle of availability“) eine Schlüsselfrage.

Angesichts dieser Entwicklungen rief die Europäische Datenschutzkonferenz die Mitgliedstaaten der Europäischen Union sowie die Kommission, den Rat und das Europäische Parlament dazu auf, tragfähige und harmonisierte Maßnahmen zur Sicherung des Datenschutzes einzuführen.[1]

Die verschiedenen Ausprägungen, in denen dieses Prinzip der „Verfügbarkeit“ explizit oder implizit zur Entwicklung von Strategien und Rechtsakten zur Verbesserung der Effizienz bei der Strafverfolgung genutzt wird, macht auch die Einführung eines umfassenden Rahmens zur Beurteilung der Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags zur Verfügung gestellt, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effizienz von Strafverfolgung nutzt. Ein solcher Rahmen soll somit dazu beitragen, eine ausgewogene Beurteilung der Wechselwirkung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten vorzunehmen.

Die Konferenz hat den folgenden Gemeinsamen Standpunkt über die Anwendung des Verfügbarkeitsgrundsatzes bei der Strafverfolgung angenommen. Dieser Gemeinsame Standpunkt enthält eine Checkliste für die Beurteilung eines jeden Vorschlags, dessen Grundlage die Verfügbarkeit von personenbezogenen Daten ist.

Dieses Dokument und die Checkliste sind insbesondere an alle EU-Institutionen und die nationalen Parlamente adressiert, als ein konstruktiver Beitrag zur Achtung und Stärkung der bürgerlichen Freiheiten der in der EU lebenden Bürger bei der Ausweitung der Möglichkeiten zur Nutzung von Informationen durch Strafverfolgungsbehörden.

---

[1] Erklärung von Krakau, 25./26. April 2005,
Erklärung von Budapest, 24./25. April 2006.

Gemeinsamer Standpunkt der Europäischen Datenschutzkonferenz über die Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung

Angenommen am 11. Mai 2007

Erläuternde Zusammenfassung

Im Zusammenhang mit dem Kampf gegen Terrorismus und zur Verbesserung der inneren Sicherheit hat die Europäische Union verschiedene Initiativen zur Verbesserung der Effizienz der Strafverfolgung in der Europäischen Union eingeleitet und dabei das Verfügbarkeitsprinzip als ein Leitprinzip für den Austausch von Informationen zur Strafverfolgung bei der Zusammenarbeit in der dritten Säule angewandt.

Die verschiedenen Ausprägungen, in denen dieses Verfügbarkeitsprinzip explizit oder implizit zur Verbesserung der Effizienz der Strafverfolgung angewandt wird, macht auch die Einführung eines umfassenden Rahmens zur Beurteilung der datenschutzrechtlichen Aspekte im Zusammenhang mit der Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags zur Verfügung gestellt, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effektivität von Strafverfolgung nutzt. Ein solcher Rahmen soll somit dazu beitragen, eine ausgewogene Beurteilung der Wechselwirkung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten vorzunehmen, wie er in der Charta der Grundrechte der Europäischen Union verankert ist.

Die Europäische Datenschutzkonferenz, die Notwendigkeit der Schaffung eines solchen Rahmens betonend, hat einige Bedingungen und Leitlinien für die Beurteilung der Anwendung des Verfügbarkeitsprinzips im folgenden Gemeinsamen Standpunkt und der Checkliste entwickelt. Diese Checkliste kann zur Beurteilung eines jeden Vorschlags genutzt werden, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung nutzt. Die Europäische Datenschutzkonferenz fordert die Kommission, den Rat und das Europäische Parlament dringend dazu auf, diese Checkliste bei der Entwicklung, Beurteilung und Annahme eines jeden Vorschlags zu nutzen, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung oder der Zusammenarbeit zwischen Strafverfolgungsbehörden nutzt.

Gemeinsamer Standpunkt zur Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung

1. Einführung

Im Zusammenhang mit der Bekämpfung von Terrorismus und der Verbesserung der internationalen Sicherheit, leitete die Europäische Union verschiedene Initiativen ein, um die Effektivität der Strafverfolgung in der Europäischen Union zu verbessern. Artikel 29 EUV zielt darauf ab, den Bürgern ein hohes Maß an Sicherheit in einem Raum der Freiheit, der Sicherheit und des Rechts zu verschaffen. Dieser Raum der Freiheit, der Sicherheit und des Rechts entwickelt sich schrittweise und führt zur Abschaffung der Grenzen zwischen den Mitgliedstaaten bezüglich der Informationen zur Strafverfolgung. Jedoch sind die Durchsetzungsbefugnisse der Mitgliedstaaten noch immer an diese nationalen Grenzen gebunden.

In diesem Zusammenhang ist der Austausch von Strafverfolgungs-Informationen unter Anwendung des Verfügbarkeitsprinzips zu einer Schlüsselfrage bei der Zusammenarbeit innerhalb der dritten Säule geworden:
- als wichtiges Instrument bei der Verwirklichung eines freien Flusses von Strafverfolgungs-Informationen, der nicht durch Binnengrenzen behindert wird,
- durch Gewährleistung von Sicherheit für den Bürger im Wege der Vereinfachung des Kampfes gegen grenzüberschreitende Straftaten,
- durch Achtung des Schutzes der Grundrechte und -freiheiten des Bürgers, insbesondere des Rechts auf Privatsphäre und Datenschutz.

Diese drei Ziele müssen in ausgewogener Weise erreicht werden. Dies liegt mit Blick auf den besonderen Charakter der Strafverfolgung und in Anbetracht der Tendenz zur zunehmenden Nutzung personenbezogener Daten für proaktive Nachforschungen der Polizei nicht auf der Hand. Ein Leitsatz bei der Strafverfolgung scheint zu sein: wenn Daten gebraucht werden, sollten sie genutzt werden. Oder noch deutlicher: wenn Daten verfügbar sind, können sie genutzt werden.

Dieses Thema demonstriert deutlich die enge Wechselbeziehung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten, wie es in der Charta der Grundrechte der Europäischen Union verankert ist.

Ein wichtiger Bestandteil in dieser Wechselbeziehung ist gegenseitiges Vertrauen. Gegenseitiges Vertrauen (und gegenseitige Anerkennung) ist eine entscheidende Bedingung für den Austausch von Strafverfolgungs-Informationen. Regierungen und Regierungsbehörden sind zum wirksamen Austausch mit (Behörden in) anderen Mitgliedstaaten nur bereit, wenn sichergestellt ist, dass diese anderen Mitgliedstaaten die Informationen im Einklang mit angemessenen rechtlichen Bestimmungen nutzen, aus Gründen des Datenschutzes und der Sicherheit.

Bereits verabschiedete EU-Rechtsakte und neuere Initiativen beschränken sich nicht darauf, den Austausch solcher personenbezogener Daten zwischen Strafverfolgungsbehörden zu fördern, die bereits von den Behörden verarbeitet werden. Einige konzentrieren sich auch auf die Nutzung solcher personenbezogener Daten zum Zwecke der Strafverfolgung, die von privaten und öffentlichen Stellen oder in europäischen Datenbanken verarbeitet werden. Wenn es Hinweise darauf gibt, dass diese für die Zwecke der Strafverfolgung benötigt werden, werden sie (so vorgeschlagen) den Strafverfolgungsbehörden zugänglich gemacht.

Die verschiedenen Ausprägungen, in denen dieses Verfügbarkeitsprinzip bei der Entwicklung von Strategien und Rechtsinstrumenten zur Verbesserung der Effektivität der Strafverfolgung implizit oder explizit angewandt wird, macht die Schaffung eines umfassenden Rahmens für die Beurteilung datenschutzrechtlicher Aspekte in Bezug auf die Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags gegeben, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effektivität der Strafverfolgung nutzt.

Die Europäische Datenschutzkonferenz, die Notwendigkeit der Schaffung eines solchen Rahmens betonend, hat einige Bedingungen und Leitlinien für die Beurteilung der Nutzung des Verfügbarkeitsprinzips entwickelt. Die Europäische Datenschutzkonferenz fordert die Kommission, den Rat und das Europäische Parlament dringend dazu auf, diese bei der Entwicklung, Beurteilung und Annahme jeglichen Vorschlags anzuwenden, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung oder der Zusammenarbeit zwischen Strafverfolgungsbehörden nutzt.

2. Anwendungsbereich des Verfügbarkeitsprinzips

Die Strategie der Europäischen Union, wie sie im Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht beschrieben wird[2] zielt darauf, dass mit Wirkung vom 1. Januar 2008 der Austausch von Strafverfolgungs-Informationen durch den Verfügbarkeitsgrundsatz bestimmt wird.

In Verfolgung dieser Strategie legte die Kommission am 12. Oktober 2005 ihren Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit vor.[3] Dieser Vorschlag statuiert eine Verpflichtung der Mitgliedstaaten, Zugang zu bestimmten Daten zu ermöglichen, die für ihre Behörden verfügbar sind oder diese zu beschaffen (vgl. Erwägung 6).

Der Verfügbarkeitsgrundsatz, wie er im Haager Programm und dem vorgeschlagenen Rahmenbeschluss zur Anwendung kommt, bedeutet, dass in der gesamten Europäischen Union in einem Mitgliedstaat ein Polizist, der Informationen zur Erfüllung seiner Pflichten benötigt, in der Lage sein sollte, diese von einem anderen Mitgliedstaat zu

[2] Amtsblatt Nr. C 53 vom 3.3.2005, S. 1.
[3] KOM (2005) 490.

erhalten und dass die Strafverfolgungsbehörde in dem anderen Staat, die über diese Information verfügt, sie zum genannten Zweck zugänglich machen wird. Der vorgeschlagene Rahmenbeschluss begrenzt den Verfügbarkeitsgrundsatz, indem er feststellt, dass er keine Verpflichtung auferlegt, Informationen zum alleinigen Zweck der Zurverfügungstellung zu sammeln oder zu speichern (Artikel 2 (1)).

Die Weitergabe verfügbarer Informationen wie personenbezogener Daten ist bereits in bestehender EU-Gesetzgebung sowie in multilateralen Übereinkommen vorgesehen. Neuere Vorschläge zur Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden enthalten das Verfügbarkeitsprinzip ebenfalls als Leitsatz. Jedoch wird in all diesen Rechtsinstrumenten und Vorschlägen die Verfügbarkeit personenbezogener Daten in unterschiedlicher Art und Weise ausgelegt, was zu unterschiedlichen Konsequenzen führt. Diese Unterschiede machen die weitere Untersuchung des Anwendungsbereichs dieses Prinzips erforderlich.

Eines der ersten Beispiele für den Austausch personenbezogener Daten als besonderem Bestandteil effektiver Zusammenarbeit zwischen europäischen Strafverfolgungsbehörden ist vielleicht das Übereinkommen vom 19. Juni 1990 zur Durchführung des Schengener Übereinkommens vom 14. Juni 1985.[4] Die Verarbeitung personenbezogener Daten besonderer Personenkategorien und deren Zurverfügungstellung – unter Nutzung eines zentralen Informationssystems – für verschiedene Behörden in den Staaten, die das Schengener Übereinkommen umgesetzt haben, wird als notwendige, ausgleichende Maßnahme zur Schaffung eines hohen Sicherheitsstandards in einem Raum des freien Personenverkehrs angesehen.

Ein weiterer Schritt zur Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden fand durch das Europol-Übereinkommen[5] und die Eurojust-Entscheidung[6] statt. Zwei Europäische Ämter wurden geschaffen, deren besondere Aufgabe es unter anderem war, den Austausch von Strafverfolgungs-Informationen zu erleichtern.

Diese Formen der Zusammenarbeit können charakterisiert werden als Zusammenarbeit durch Äußerung der Absicht zur Zusammenarbeit ohne besondere Verpflichtung dazu.

Neuere Beispiele der Zurverfügungstellung personenbezogener Daten für Strafverfolgungsbehörden sind der Rahmenbeschluss über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union[7] und der Vertrag von Prüm vom 27. Mai 2005. Diese beiden Rechtsinstrumente führen einen neuen Aspekt in die Zusammenarbeit bei der Strafverfolgung ein: Mitgliedstaaten sind grundsätzlich verpflichtet, personenbezogene Daten zur Verfügung zu stellen. Die Benutzung von Formulierungen wie: „sollen auf Ersuchen“ (Rahmenbeschluss) und „gestatten Zugriff …

4 Amtsblatt Nr. L 239 vom 22.9.2000, S. 19.
5 Amtsblatt Nr. C 316 vom 27.11.1995, S. 1.
6 Amtsblatt Nr. L 63 vom 6.3.2002, S. 1.
7 Amtsblatt Nr.. L 386 vom 29.12.2006, S. 89.

und das Recht zum Abruf“ (z.B. Artikel 3 (1) Vertrag von Prüm) zeigen deutlich den verpflichtenden Charakter der Zurverfügungstellung von Daten.

Der Vertrag von Prüm führt darüber hinaus eine Verpflichtung zur Erstellung bestimmter Dateien ein, um die Verhütung und Verfolgung von Straftaten zu erleichtern. Die Vertragsparteien müssen zum Beispiel die Verfügbarkeit von Fundstellendatensätzen von Fingerabdrücken garantieren (Artikel 8).

Der bestehende, mehr oder minder freiwillige Austausch von Informationen wird auf diesen Gebieten nicht nur durch eine Verpflichtung zur Zurverfügungstellung von Informationen ersetzt, sondern auch durch die Verpflichtung, für bestimmte Kategorien personenbezogener Daten eine Infrastruktur zu schaffen, die anderen Strafverfolgungsbehörden den Zugriff darauf ermöglicht.

Eine solche Verpflichtung zur Zurverfügungstellung von Informationen beschränkt sich nicht notwendig auf Strafverfolgungsbehörden. Zum Beispiel wird in Erwägung 19 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze gewonnen oder verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG ausdrücklich erwähnt, dass *„es notwendig ist, dass vorhandene Daten zugänglich gemacht werden*“. Auf europäischer Ebene wird abgesichert, dass bestimmte Kategorien von Daten, die durch private Stellen verarbeitet werden, für die Strafverfolgung zugänglich gemacht werden sollen.

Das Verfügbarkeitsprinzip ist ebenfalls ein wichtiges Thema der Mitteilung der Kommission an den Rat und das Europäische Parlament vom 24. November 2005 über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen[8]. Die Weitergabe verfügbarer Informationen durch die Verbindung von Datenbanken ist ein Schlüsselelement bei den Zukunftsplanungen in der Europäischen Union.
Andere Initiativen wie die neue Rechtsgrundlage des Schengener Informationssystems der zweiten Generation und die Schaffung des Visa-Informationssystems beinhalten ebenfalls Aspekte des Verfügbarkeitsprinzips. Personenbezogene Daten, die für einen bestimmten Zweck verarbeitet wurden, werden für andere Zwecke wie etwa Strafverfolgung zugänglich gemacht.

Im Hinblick auf diese Bandbreite der Erscheinungsformen des Verfügbarkeitsprinzips als Schlüsselelement bei der Verbesserung der Strafverfolgung und der Auswirkung auf das Grundrecht auf den Schutz personenbezogener Daten, betont die Europäische Datenschutzkonferenz die Notwendigkeit, die Nutzung des Verfügbarkeitsprinzips in umfassender Weise in den Kontext zu setzen. Jegliche Harmonisierung der Verarbeitung personenbezogener Daten durch die Einführung von Verpflichtungen zur Vorratsspeicherung personenbezogener Daten oder von Verpflichtungen zur Erstellung spezifischer Datenbestände und die Absicht oder die Verpflichtung, diese personenbezogenen Daten für Strafverfolgungsbehörden oder für mit der Strafverfolgung

[8] KOM (2005) 597.

in Zusammenhang stehende europäische oder internationale Einrichtungen verfügbar zu machen, sollte als Umsetzung des Verfügbarkeitsprinzips angesehen werden.

Unter Zugrundelegung dieses Anwendungsbereiches hat die Europäische Datenschutzkonferenz seine Auswirkungen im Hinblick auf anwendbare Datenschutzbestimmungen untersucht.

3. Anwendbares Recht

Zusätzlich zum Recht auf die Achtung des Privat- und Familienlebens, das durch Artikel 8 der EMRK garantiert und durch Artikel 7 der Charta der Grundrechte der Europäischen Union nochmals bestätigt wird, ist das neue Grundrecht auf Datenschutz in Artikel 8 der Charta verankert.

Die EMRK erlaubt den Eingriff in den Schutzbereich des Rechts auf Privatleben, wenn er zur Wahrung der im zweiten Absatz des Artikel 8 bezeichneten Interessen notwendig und durch diese Interessen gerechtfertigt ist; ein solcher Eingriff muss dem Verhältnismäßigkeitsgrundsatz entsprechen. Artikel 8 der Charta der Grundrechte weitet dies aus, indem er festlegt, dass personenbezogene Daten nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen legitimen Grundlage verarbeitet werden müssen. Diese legitime Grundlage muss ebenfalls dem Verhältnismäßigkeitsgrundsatz entsprechen.

Das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 (Konvention 108) enthält spezifischere Grundsätze für den Datenschutz, die auch innerhalb der dritten Säule anwendbar sind. Es gibt auch eine Empfehlung (Nr. R(87) 15) mit spezifischen Datenschutzvorschriften für die Verwendung personenbezogener Daten bei der Polizei, die 1987 vom Ministerkomitee der Mitgliedstaaten zur Regelung der Verwendung personenbezogener Daten bei der Polizei verabschiedet wurde.[9]

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[10] sieht eine harmonisierte Datenschutzordnung in der Europäischen Union vor. Obwohl Maßnahmen, die in Titel V und VI des Vertrages über die Europäische Union bezeichnet sind, außerhalb des Anwendungsbereichs dieser Richtlinie liegen, wenden Mitgliedstaaten die allgemeinen Datenschutz-Grundsätze auf Maßnahmen der Strafverfolgung an.

Die Verordnung 45/2001 des Europäischen Parlaments und des Rates vom 18. September 2000[11] sieht Regeln für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und

[9] Empfehlung Nr. R (87) 15 vom 17. September 1987.
[10] Amtsblatt Nr. L 281 vom 23.11.1995, S. 31.
[11] Amtsblatt Nr. L 8 vom 12.1.2001, S. 1.

zum freien Datenverkehr vor. Die Grundsätze dieser Verordnung werden zur Definition der Datenschutz-Ordnung genutzt, die auf die Verarbeitung personenbezogener Daten in Europäischen Datenbanken wie dem Visa-Informationssystem und dem Schengener Informationssystem der zweiten Generation anwendbar ist.

Das Europol-Übereinkommen und die Eurojust-Entscheidung enthalten für diese Organisationen spezifische Datenschutzregelungen, die auf den allgemeinen Datenschutz-Prinzipien beruhen, wie sie in der Konvention 108 und der Empfehlung Nr. R(87) 15 definiert werden, die oben genannt wurden.

Für Datenverarbeitung durch private und öffentliche Stellen sowie durch die Europäischen Institutionen und in Europäischen Datenbanken enthält das anwendbare EU-Recht einen Grundsatz über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten: Daten sollten für ausdrückliche und legitime Ziele gesammelt werden und nicht in einer Art und Weise weiterverarbeitet werden, die mit diesen Zielen unvereinbar ist. Eine Ausnahme oder Beschränkung ist nur dann erlaubt, wenn diese gesetzlich vorgesehen ist und eine notwendige Maßnahme zum Schutz der nationalen und öffentlichen Sicherheit oder zur Verhütung, Aufklärung, Entdeckung und Verfolgung von Straftaten darstellt. Die in diesen Rechtsinstrumenten genutzte Definition der Datenverarbeitung umfasst die Bekanntgabe durch Weitergabe, Verbreitung oder sonstige Zurverfügungstellung.

In den Situationen, in denen das Verfügbarkeitsprinzip angewendet wird, um ursprünglich zu anderen Zwecken als der Strafverfolgung verarbeitete Daten für die Strafverfolgung zu nutzen, muss die Ausnahme vom Grundsatz der Zweckbestimmung alle Bedingungen für das Eingreifen dieser Ausnahme erfüllen.

4. Umsetzung des Verfügbarkeitsprinzips

Die Effektivität der Strafverfolgung wird von der Informationslage der Strafverfolgungsbehörden abhängen, von der Möglichkeit, innerhalb der Grenzen des Rechts Informationen zu sammeln, von der Qualität und dem Nutzen dieser Daten und der Fähigkeit zur Weitergabe dieser Daten an andere Strafverfolgungsbehörden. Die verschiedenen Arten der Zusammenarbeit bei der Strafverfolgung in der Europäischen Union, wie sie in Kapitel 2 beschrieben wurden, umfassen all diese Gesichtspunkte.

Bezüglich aller Initiativen zum Austausch personenbezogener Daten zwischen Strafverfolgungsbehörden in der Europäischen Union und dem Austausch mit Drittstaaten und -stellen, hat die Europäischen Datenschutzkonferenz bereits erklärt, dass „*In Anbetracht der Verpflichtung der Union zur Achtung der Menschenrechte und der Grundfreiheiten, Initiativen zur Verbesserung der Strafverfolgung in der EU, wie der Verfügbarkeitsgrundsatz, nur auf Grundlage eines angemessenen Systems von Vorkehrungen zum Datenschutz eingeführt werden sollten, das einen hohen und gleichwertigen Standard beim Datenschutz gewährleistet.*“[12]

[12] Erklärung von Krakau, 25./26. April 2005.

Diesbezüglich begrüßt die Europäische Datenschutzkonferenz den Entwurf eines Rahmenbeschlusses des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.[13] Ein harmonisierter und hoher Standard des Datenschutzes im Bereich der Strafverfolgung, wie er von einem Rahmenbeschluss des Rates gewährleistet werden sollte, wird nun als unabdingbare Voraussetzung für die Strafverfolgung in der Europäischen Union bezeichnet.

Es sollte jedoch betont werden, dass ein solcher harmonisierter Datenschutz-Rahmen an sich noch kein umfassendes Instrument zur Beurteilung der Umsetzung des Verfügbarkeitsprinzips in all seinen in Kapitel 2 beschriebenen Erscheinungsformen darstellt. Dieser Rahmen ist nur dann anwendbar, wenn personenbezogene Daten bereits von Strafverfolgungsbehörden verarbeitet werden. Darüber hinaus wird der Entwurf des Rahmenbeschlusses im Rat weiter diskutiert.

Da die Bandbreite der Nutzung des Verfügbarkeitsprinzips zur Anwendung verschiedener Rechtsinstrumente führt, sollte ein umfassender Rahmen zur Beurteilung der Nutzung dieses Prinzips sämtliche Gesichtspunkte der Nutzung des Verfügbarkeitsprinzips abdecken. Ein solcher Rahmen sollte in einem gesonderten Instrument bestehen, das nachträglich auch auf bestehendes Recht angewendet wird.

5. Ein umfassender Rahmen zur Beurteilung der Nutzung des Verfügbarkeitsprinzips.

Strafverfolgung ist von Informationen abhängig. Grundsätzlich werden zweierlei Informationsquellen genutzt: Informationen, die bereits von Strafverfolgungsbehörden verarbeitet werden und Informationen, die von anderen verarbeitet werden. Diese Unterscheidung ist in gewisser Weise künstlich, weil Daten, die von Strafverfolgungsbehörden verarbeitet werden, von privaten oder öffentlichen Stellen erlangt worden sein können.

Wenn personenbezogene Daten durch private oder öffentliche Stellen verarbeitet werden, sind die in der Richtlinie 95/46/EG definierten Datenschutzgrundsätze maßgeblich. Wenn diese Daten entweder von Europäischen Organen oder in Europäischen Datenbanken verarbeitet werden, sind die Grundsätze der Verordnung 45/2001 und/oder die für diese Dateien einschlägigen spezifischen Regeln anwendbar.

Wie bereits dargelegt, stellt die Nutzung dieser Daten zum Zwecke der Strafverfolgung in der Regel eine Ausnahme vom Grundsatz der Zweckbindung dar, die nur erlaubt ist, wenn dies gesetzlich vorgesehen ist und es um eine notwendige Maßnahme zum Schutz der nationalen und öffentlichen Sicherheit oder zur Verhütung, Aufklärung, Entdeckung und Verfolgung von Straftaten geht.

[13] KOM (2005) 475.

In dem Falle, dass die Daten bereits von Strafverfolgungsbehörden verarbeitet werden, wird der (Entwurf des) Rahmenbeschluss des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen für den notwendigen rechtlichen Datenschutz-Rahmen bei der Verarbeitung und dem Austausch von Informationen zwischen Strafverfolgungsbehörden sorgen. Es könnten jedoch neue Initiativen für die Verarbeitung dieser Daten vorgelegt werden, die auf dem Verfügbarkeitsprinzip basieren.

Zur Beurteilung, ob eine Ausnahme notwendig ist und den formellen Bedingungen entspricht, oder bei der Beurteilung neuer Initiativen zur Bereitstellung von Daten zur Strafverfolgung, wird es notwendig sein, die verschiedenen Bedingungen in den Blick zu nehmen, die die einschlägigen Datenschutzvorschriften enthalten.

Die erste Bedingung bezieht sich auf die Anforderung, dass jede Maßnahme gesetzlich vorgesehen sein soll. Dieses Gesetz muss strengen Anforderungen entsprechen, so muss es klar, einfach und präzise sein: es soll transparent und für jedermann leicht verständlich sein. Nach der Rechtsprechung des Gerichtshofes erfordert der Grundsatz der Rechtssicherheit, dass Gesetze klar und präzise sein müssen und ihre Anwendung für den Einzelnen vorhersehbar. Darüber hinaus müssen die Gesetze immer Begründung und Zweck sowie die Bedingungen für die Verarbeitung festlegen und ein angemessenes und effektives Kontrollsystem festsetzen.

Die zweite Bedingung, die erfüllt werden muss, ist, dass jede Maßnahme erforderlich und verhältnismäßig sein muss. Insbesondere die Beurteilung dieses Aspekts erfordert einen umfassenden Ansatz. Ein solcher Ansatz sollte die folgenden Beurteilungs-Schritte enthalten:

A. Evaluation bereits bestehender rechtlicher Maßnahmen, die die Verarbeitung inklusive des Austauschs von Daten erlauben.
Sind diese Maßnahmen nicht ausreichend oder sind ihre Umsetzung und die Folgemaßnahmen nicht effektiv? Wenn eine rechtliche Maßnahme tatsächlich genutzt wird, anscheinend aber keinen ausreichenden und effektiven Beitrag zur Verbrechensbekämpfung leistet, kann dies ein Anzeichen dafür sein, dass eine andere Maßnahme benötigt wird. Wenn jedoch die Evaluation ergibt, dass bereits bestehende Möglichkeiten nicht ausreichend genutzt werden, kann dies erhebliche Zweifel darüber wecken, ob die vorgeschlagene neue Maßnahme gerechtfertigt ist.

Für den Fall, dass diese Beurteilung anzeigt, dass die rechtliche Maßnahme gerechtfertigt sein könnte, sollten die folgenden Bedingungen erfüllt werden:

B. Verhältnismäßigkeit
Effektive Durchsetzung, aber mit minimalen Eingriffen in die Privatsphäre. Dies bedeutet einen Verhältnismäßigkeitstest mit den folgenden Bestandteilen:

* Die Maßnahme muss geeignet sein, was bedeutet, dass ihr Beitrag zur Strafverfolgung klar aufgezeigt werden muss.
* Eine weniger eingreifende Maßnahme kann nicht zum gleichen Ergebnis führen.
* Ein Gleichgewicht muss bestehen: wo ein Eingriff in den Datenschutz gerechtfertigt sein kann, um Terrorismus und andere schwere Straftaten zu bekämpfen (wie in Artikel 2 (2) der Rahmentscheidung zur Einführung des Europäischen Haftbefehls genannt), bedeutet dies nicht, dass die Daten auch zum Kampf gegen geringfügige Vergehen zur Verfügung stehen.
* Das Rechtsinstrument sollte Gegenstand einer verbindlichen Evaluation sein.

Die dritte Bedingung bezieht sich auf die Kategorien der zu verarbeitenden Daten und auf weitere besondere Bedingungen.
Verschiedene Arten von Daten sind betroffen: von Daten zur Identifikation (genutzt sowohl zur Identifikation des Betroffenen als auch zu dessen Kontaktierung) sowie allgemein und spezifisch kennzeichnenden Daten (z.B. Intelligenz) bis zu Arten, die aufgrund ihrer Biometrie dechiffriert werden (z.B. Fingerabdrücke und digitale Darstellung der DNA) und empfindlichen Daten (wie in Artikel 8 der Richtlinie 95/46 genannt). Gleichermaßen sind verschiedene Arten von Personen betroffen: Verdächtige, Nicht-Verdächtige, Zeugen, verurteilte oder freigesprochene Personen. Die folgenden Punkte sollten berücksichtigt werden:

A. Gesetzgebung muss zwischen diesen Daten unterscheiden und zusätzliche Schutzvorkehrungen für die Verarbeitung solcher Daten gewährleisten, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, insbesondere für empfindliche Daten; durch die Einführung einer gleitenden Skala von Sicherungsmaßnahmen, bei der die Eigenschaften der Daten bestimmte Sonderbedingungen und Begrenzungen ihrer Nutzung festlegen. Sie sollte Maßstäbe für eine klare Unterscheidung personenbezogener Daten enthalten, indem sie zwischen Kategorien personenbezogener Daten und deren Verfügbarkeit für besondere Arten von Verbrechen unterscheidet. Zum Beispiel sollten Personen, die von einer Anklage freigesprochen wurden oder gegen die keine Beschuldigungen erhoben werden, klar von verurteilten Personen unterschieden werden. Daten über Nicht-Verdächtige und Zeugen sollten klar von Daten über Verdächtige unterschieden werden.
Eine solche Unterscheidung könnte mit der Unterscheidung zwischen verschiedenen Kategorien von Personen verbunden sein, wie sie sich in Artikel 4 (3) des Kommissionsvorschlags für den Entwurf eines Rahmenbeschlusses des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen findet.

B. Spezifische Maßnahmen zur Beurteilung der Qualität von Daten müssen eingeführt werden, um den höchstmöglichen Qualitätsstandard der Daten zu garantieren, bevor diese verfügbar gemacht werden. Im Hinblick auf die Auswirkungen der Nutzung von Daten auf die Strafverfolgung sollten

ausreichende technische und organisatorische Maßnahmen zur Hand sein, um die Qualität der Daten zu garantieren. Für den Fall, dass solche Garantien nicht gewährleistet werden können, muss dies vermerkt werden und die Nutzung solcher Daten muss auf spezifische Strafverfolgungsmaßnahmen mit zusätzlichen Sicherheitsvorkehrungen beschränkt bleiben. Eine Verpflichtung, den Empfänger personenbezogener Daten über jede Änderung bei diesen Daten zu informieren, muss verbindlich sein.

C. Die Nutzung biometrischer Daten bei der Strafverfolgung erfordert zusätzliche Sicherheitsvorkehrungen. Insbesondere die Identifikation anhand der Nutzung solcher Daten, die manchmal unter Verwendung von Vorrichtungen zur Verarbeitung riesiger Mengen von Daten geschieht, wie beim neuen Schengener Informationssystem, muss begleitet sein von Verfahren, die dem Individuum die Möglichkeit bieten, das Ergebnis des Abgleichs überprüfen zu lassen.

D. Besondere Operationen bei der Verarbeitung, die besondere Gefahren darstellen können (z.B. Ausforschungsaufträge, themenbezogene Datensuche, spezielle Überwachungstechniken) erfordern zusätzliche Sicherheitsvorkehrungen für die Nutzung dieser Daten und die Überwachung der Nutzung solcher Operationen.

E. Es wird wichtig sein, mit technischen und organisatorischen Maßnahmen und Verfahren abzusichern, dass die Empfänger personenbezogener Daten mit den nötigen Informationen versorgt werden, um die Daten für die Zwecke nutzen zu können, für die sie ausgetauscht wurden und um diese auf aktuellem Stand zu halten.

F. Wenn eine Initiative oder ein Vorschlag die Wahl zwischen der Verarbeitung personenbezogener Daten auf zentralisierter oder dezentralisierter Ebene trifft, kann diese Wahl nicht nur aufgrund praktischer Erwägungen getroffen werden. Eine solche Wahl muss auch die Notwendigkeit berücksichtigen, den höchstmöglichen Stand der Datenqualität und des Datenschutz-Niveaus zu garantieren. Wenn eine dezentralisierte Verarbeitung die besten Sicherheitsvorkehrungen gewährleistet, sollte eine zentralisierte Verarbeitung keine Option sein.

Die vierte Bedingung bezieht sich auf den Zugang zu diesen Daten.

Routinemäßiger Zugang zu personenbezogenen Daten muss verboten sein. Zugang sollte auf bestimmte Fälle oder eine bestimmte Strafverfolgungsmaßnahme begrenzt sein und die Kontrolle der Nutzung dieses Zugangs muss ausreichend sichergestellt sein. Empfänger-Behörden müssen klar identifiziert sein. Wenn direkter Zugang zu Daten vorgeschlagen wird, sind die Nutzung eines Index oder von hit/no hit-Systemen und eine ausreichende Zugangskontrolle erforderlich.

Die fünfte Bedingung bezieht sich auf Kontrolle und Aufsicht.

Über die gewöhnlichen Zuständigkeiten von Strafverfolgungsbehörden, Organen der Rechtspflege und Datenschutzkontrollinstanzen für die Kontrolle von und die Aufsicht über solche Datenverarbeitungsvorgänge, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, hinaus sollten zusätzliche maßgeschneiderte Kontroll- und Aufsichtsmaßnahmen für alle operationellen Tätigkeiten inklusive der Nutzung und des Missbrauchs personenbezogener Daten eingeführt werden. Besondere Vorschriften werden benötigt, die den Schwierigkeiten vorbeugen, die sich aus dem Austausch von Daten zwischen Mitgliedstaaten ergeben. Da diese Daten in verschiedenen Zuständigkeitsbereichen zugänglich sind, muss sichergestellt werden, dass Kontrolle und Aufsicht in allen betroffenen Zuständigkeitsbereichen wirksam sind.

6. Schlussfolgerung

Die Europäische Datenschutzkonferenz erkennt an, dass Informationen und personenbezogene Daten für eine effektive Strafverfolgung entscheidend sind. Sie wiederholt jedoch, dass jegliche Maßnahme unter Nutzung des Verfügbarkeitsprinzips verhältnismäßig sein und die Grundrechte des Einzelnen achten sollte. Dieser Gemeinsame Standpunkt und die Checkliste richten sich insbesondere an die EU-Organe, als ein konstruktiver Beitrag zu gegenwärtigen Initiativen. Sie stellen die Bedingungen dar, die erfüllt werden müssen, um einen hohen Datenschutz-Standard auf dem Gebiet der Strafverfolgung aufrecht zu erhalten. Die Europäische Datenschutzkonferenz ist natürlich bereit, weiter dazu beizutragen, dass der Vorgang der Verbesserung der Strafverfolgung sich im Einklang mit der Achtung von Grundrechten befindet.

Checkliste zur Beurteilung jeglicher Maßnahme zur Umsetzung des Verfügbarkeitsprinzips bei der Strafverfolgung

I. Recht und Evaluation

Jede Maßnahme muss gesetzlich vorgesehen sein. Das Gesetz muss strengen Anforderungen entsprechen. So muss es klar sein und Verlässlichkeit und Vorhersehbarkeit schaffen.

Darüber hinaus muss Gesetzgebung immer:

* Begründung und
* Zweck festlegen, sowie
* die Bedingungen für die Verarbeitung.
* Ein angemessenes und effektives System zur unabhängigen Kontrolle einsetzen.

II. Bedarf und Verhältnismäßigkeit

Die Maßnahme sollte eine notwendige Sicherheitsvorkehrung darstellen.

A. Evaluation bereits bestehender rechtlicher Maßnahmen, die die Verarbeitung inklusive des Austauschs von Daten erlauben.

* Sind diese Maßnahmen nicht ausreichend?

  Wenn eine rechtliche Maßnahme tatsächlich genutzt wird, anscheinend aber keinen ausreichenden und effektiven Beitrag im Kampf gegen Straftaten leistet, kann dies ein Anzeichen dafür sein, dass eine andere Maßnahme benötigt wird.

* Sind ihre Umsetzung und die Folgemaßnahmen nicht effektiv?

  Wenn die Evaluation zeigt, dass bereits bestehende Möglichkeiten nicht ausreichend genutzt werden, kann dies erhebliche Zweifel darüber wecken, ob die vorgeschlagene neue Maßnahme eine gerechtfertigte Ausnahme vom Grundsatz der Zweckbegrenzung ist.

* Für den Fall, dass diese Beurteilung anzeigt, dass die rechtliche Maßnahme gerechtfertigt sein könnte, sollten die folgenden Bedingungen erfüllt sein:

B. Verhältnismäßigkeit

* Die Maßnahme sollte darauf zugeschnitten sein, folgendes zu erreichen:
  - Effektive Durchsetzung,
  - Minimale Eingriffe in die Privatsphäre.
* Dies bedeutet einen Verhältnismäßigkeitstest mit den folgenden Bestandteilen:
  - Die Maßnahme muss geeignet sein, was bedeutet, dass ihr Beitrag zur Strafverfolgung klar aufgezeigt werden muss.
  - Sie darf nicht gegen das Erforderlichkeitsgebot verstoßen, was bedeutet, dass eine weniger eingreifende Maßnahme nicht zum gleichen Ergebnis führen kann.
  - Ein Gleichgewicht muss bestehen: wo ein Eingriff in den Datenschutz gerechtfertigt sein kann, um Terrorismus und andere schwere Straftaten zu bekämpfen (wie in Artikel 2 (2) des Rahmenbeschlusses zur Einführung des Europäischen Haftbefehls genannt), bedeutet dies nicht, dass die Daten auch zum Kampf gegen geringfügige Vergehen zur Verfügung stehen.
* Das Rechtsinstrument sollte Gegenstand einer verbindlichen Evaluation sein.

III. Besondere Bedingungen

Verschiedene Arten von Daten sind betroffen: von Daten zur Identifizierung (genutzt zur Identifizierung des Betroffenen und dessen Kontaktierung) sowie allgemein und spezifisch kennzeichnenden Daten (z.B. Intelligenz) bis zu Arten, die aufgrund ihrer Biometrie dechiffriert werden (z.B. Fingerabdrücke und digitale Darstellung der DNA) und empfindlichen Daten (wie in Artikel 8 der Richtlinie 95/46 genannt). Gleichermaßen sind verschiedene Arten von Personen betroffen: Verdächtige, Nicht-Verdächtige, Zeugen, verurteilte oder freigesprochene Personen. Die folgenden Punkte sollten berücksichtigt werden:

A. Gesetzgebung muss:

* Zwischen diesen Daten unterscheiden,
* Besondere zusätzliche Schutzvorkehrungen für die Verarbeitung solcher Daten gewährleisten, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, insbesondere für die Nutzung empfindlicher Daten durch die Einführung einer gleitenden Skala von Sicherungsmaßnahmen, bei der die Eigenschaften der Daten bestimmte Sonderbedingungen und Begrenzungen ihrer Nutzung festlegen.
* Maßstäbe für eine klare Unterscheidung personenbezogener Daten enthalten, indem sie zwischen Kategorien personenbezogener Daten und deren Verfügbarkeit für spezifische Arten von Verbrechen unterscheidet. (Zum Beispiel sollten Personen, die von einem Vorwurf freigesprochen wurden oder gegen die keine Vorwürfe erhoben werden, deutlich von verurteilten Personen unterschieden werden. Daten über Nicht-Verdächtige und Zeugen sollten deutlich von Daten über Verdächtige unterschieden werden.)

B. Spezifische Maßnahmen zur Beurteilung der Qualität von Daten müssen eingeführt werden, um den höchstmöglichen Qualitätsstandard der Daten zu garantieren, bevor diese verfügbar gemacht werden. Im Hinblick auf die Auswirkungen der Nutzung von Daten auf die Strafverfolgung sollten ausreichende technische und organisatorische Maßnahmen zur Hand sein, um die Qualität der Daten zu garantieren. Für den Fall, dass solche Garantien nicht gewährleistet werden können, muss dies vermerkt werden und die Nutzung solcher Daten muss auf spezifische Strafverfolgungsmaßnahmen mit zusätzlichen Sicherheitsvorkehrungen beschränkt bleiben. Eine Verpflichtung, den Empfänger personenbezogener Daten über jede Änderung bei diesen Daten zu informieren, muss verbindlich sein.

C. Die Nutzung biometrischer Daten bei der Strafverfolgung verlangt zusätzliche Sicherheitsvorkehrungen. Insbesondere die Identifizierung anhand der Nutzung solcher Daten, die manchmal unter Verwendung von Vorrichtungen zur Verarbeitung umfangreicher Mengen von Daten geschieht, wie beim neuen Schengen-Informationssystem, muss begleitet sein von Verfahren, die dem Individuum die Möglichkeit bieten, das Ergebnis des Abgleichs überprüfen zu lassen.

D. Besondere Verfahren bei der Verarbeitung, die besondere Gefahren darstellen können (z.B. Ausforschungsaufträge, themenbezogene Datensuche, spezielle Überwachungstechniken) erfordern zusätzliche Sicherheitsvorkehrungen für die Nutzung dieser Daten und die Überwachung der Nutzung solcher Operationen.

E. Es wird wichtig sein, mit technischen und organisatorischen Maßnahmen und Verfahren abzusichern, dass die Empfänger personenbezogener Daten mit den nötigen Informationen versorgt werden, um die Daten für die Zwecke nutzen zu können, für die sie ausgetauscht wurden und um diese auf aktuellem Stand zu halten.

F. Wenn eine Initiative oder ein Vorschlag die Wahl zwischen der Verarbeitung personenbezogener Daten auf zentralisierter oder dezentralisierter Ebene trifft, kann diese Wahl nicht nur aufgrund praktischer Erwägungen getroffen werden. Eine solche Wahl muss auch die Notwendigkeit berücksichtigen, den höchstmöglichen Standard der Datenqualität und des Datenschutz-Niveaus zu garantieren. Wenn eine dezentralisierte Verarbeitung die besten Sicherheitsvorkehrungen gewährleistet, sollte eine zentralisierte Verarbeitung keine Option sein.

IV. Zugang der Strafverfolgungsbehörden zu personenbezogenen Daten

* Routinemäßiger Zugang zu personenbezogenen Daten muss verboten sein.
* Zugang sollte auf bestimmte Fälle oder eine bestimmte Strafverfolgungs-Aufgabe begrenzt sein.
* Kontrolle der Nutzung dieses Zugangs muss ausreichend sichergestellt sein.
* Wenn direkter Zugang zu Daten vorgeschlagen wird, ist die Nutzung eines Index oder von hit/no hit - Systemen und eine ausreichende Zugangskontrolle erforderlich.
* Die Empfänger-Behörden müssen klar identifiziert sein.

V. Kontrolle und Aufsicht

* Über die gewöhnlichen Zuständigkeiten von Strafverfolgungsbehörden, Organen der Rechtspflege und Datenschutzkontrollinstanzen für die Kontrolle von und die Aufsicht über solche Datenverarbeitungs-Vorgänge, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, hinaus sollten zusätzliche maßgeschneiderte Kontroll- und Aufsichtsmaßnahmen für alle operationellen Vorgänge inklusive der Nutzung und des Missbrauchs personenbezogener Daten eingeführt werden.
* Besondere Vorschriften werden benötigt, die den Schwierigkeiten vorbeugen, die sich aus dem Austausch von Daten zwischen Mitgliedstaaten ergeben. Da diese Daten in verschiedenen Zuständigkeitsbereichen zugänglich sind, muss sichergestellt werden, dass Kontrolle und Aufsicht in allen betroffenen Zuständigkeitsbereichen wirksam sind.